1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
36019669	Armando Cotarelo Valledor	Vilagarcía de Arousa	2022/2023

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	2022/2023	6	105	126

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

Profesorado responsable

Profesorado asignado ao módulo	SILVIA FRAMIÑÁN FONDEVILA
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 ou 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 tipificalas e avalialas, 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 comunicacións Panorámica da seguridade informática	6	5
2	Criptografía	Técnicas de cifraxe, signaturas e certificados dixitais	23	18
3	Test de intrusión	Simulación de ataques	8	7
4	Ameazas, ataques e forense dixital	Identificación de tipos de ataques e as correspondentes salvaguardas	9	7
5	Tornalumes	Configuración de tornalumes	28	21
6	Servidores proxy	Configuración de servidores proxy	15	12
7	Xestión de intrusións e de eventos de seguridade	Configuración de sistemas de deteción de intrusións, sistemas de prevención de intrusión e sistemas de xestión de eventos de seguridade	12	9
8	Acceso remoto	Configuración de acceso remoto con SSH, RDP e VPN	15	11
9	Implantación de solucións de alta disponibilidade	Configuración balanceo de carga, redundancia e virtualización para asegurar a máxima operatividade de sistemas e servizos mediante unha alta tolerancia a fallos	5	5
10	Normativa legal en materia de seguridade informática	Lexislación vixente sobre seguridade informática	5	5

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Introdución a seguridade informática	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
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 Describíronse 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.
CA1.5 Adoptáronse políticas de contrasinais.
CA1.6 Valoráronse as vantaxes do uso de sistemas biométricos.
CA2.3 Identificouse a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.

4.1.e) Contidos

Contidos
Elementos vulnerables no sistema informático: hardware, software e datos. Pautas e prácticas seguras. Tipos de ameazas: físicas e lóxicas. Seguridade física e ambiental: Localización e protección física dos equipamentos e dos servidores. Sistemas de alimentación ininterrompida. Ataques e contramedidas en sistemas informáticos. Copias de seguridade e imaxes de respaldo. 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	Criptografía	23

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
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

4.2.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.
CA2.2 Verificouse a orixe e a autenticidade das aplicacións instaladas nun equipamento, así como o estado de actualización do sistema operativo.
CA2.6 Utilizáronse técnicas de cifraxe, 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.
CA3.3 Identificáronse os protocolos seguros de comunicación e os seus ámbitos de uso.

4.2.e) Contidos

Contidos
Fiabilidade, confidencialidade, integridade e dispoñibilidade. Seguridade lóxica: Criptografía. Listas de control de acceso. Establecemento de políticas de contrasinais. Sistemas biométricos de identificación. Políticas de almacenamento. Medios de almacenamento. Cifraxe simétrico Cifraxe asimétrico Funcións hash criptográficas Códigos de autentificación de mensaxes Firma dixital 0Técnicas de cifraxe 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 Seguridade nos protocolos para comunicacións sen fíos.

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Test de intrusión	8

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
CA1.3 Clasificáronse os tipos principais de vulnerabilidade dun sistema informático, segundo a súa tipoloxía e a súa orixe.
CA2.8 Recoñeceuse a necesidade de inventariar e controlar os servizos de rede que se executan nun sistema.

4.3.e) Contidos

Contidos
Análise das principais vulnerabilidades dun sistema informático. Riscos potenciais dos servizos de rede. Software para detección de vulnerabilidades. Realización de auditorías de seguridade.

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Ameazas, ataques e forense dixital	9

4.4.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

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

Criterios de avaliación
CA1.4 Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas.
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.
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
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. Anatomía de ataques e análise de software malicioso. Ferramentas preventivas e paliativas: instalación e configuración.

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Tornalumes	28

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
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

4.5.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.
CA3.2 Clasificáronse as zonas de risco dun sistema, segundo criterios de seguridade perimetral.
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.

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. 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.

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

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Servidores proxy	15

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
RA5 - Implanta servidores proxy, aplicando criterios de configuración que garantan o funcionamento seguro do servizo.	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.
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.
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.

4.6.e) Contidos

Contidos
Ferramentas preventivas e paliativas: instalación e configuración. 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.

Contidos
Probas de funcionamento.

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Xestión de intrusións e de eventos de seguridade	12

4.7.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

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

Criterios de avaliación
CA2.9 Describíronse os tipos e as características dos sistemas de detección de intrusións.
0CA2.10 Describironse 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

4.7.e) Contidos

Contidos
Monitorización do tráfico en redes: captura e análise; aplicacións.
Intentos de penetración: tipoloxía.
Sistemas de detección de intrusións.
Sistemas de prevención de intrusións
Sistemas de xestión de eventos de seguridade
Ferramentas preventivas e paliativas: instalación e configuración.

4.8.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
8	Acceso remoto	15

4.8.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

4.8.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.
CA3.1 Describíronse escenarios típicos de sistemas con conexión a redes públicas en que cumpra fortificar a rede interna.
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.

4.8.e) Contidos

Contidos
0Técnicas de cifraxe da información: clave pública e clave privada; certificados dixitais; sinaturas. Seguridade nos protocolos para comunicacións sen fíos. Riscos potenciais dos servizos de rede. Software para detección de vulnerabilidades. Ferramentas preventivas e paliativas: instalación e configuración. 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.

4.9.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
9	Implantación de solucións de alta disponibilidade	5

4.9.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

4.9.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.

4.9.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.

4.10.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
10	Normativa legal en materia de seguridade informática	5

4.10.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

4.10.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.

4.10.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

* Mínimos exixibles:
Os criterios de avaliación mínimos exixibles do módulo son os establecidos para cada unha das unidades didácticas nas que se organiza o módulo.

* Avaliación
Os instrumentos de avaliación que se utilizarán son:

- Probas de avaliación: poderase facer unha proba por cada UD ou bloque de UDs. Unha proba de avaliación poderá estar desglosada nas seguintes dúas partes:
  > Proba obxectiva teórica: que consistirá en preguntas de resposta curta, cuestionarios, etc, relacionados cos criterios de avaliación máis teóricos da UD ou bloque.
  > Proba obxectiva práctica: que consistirá na realización de casos prácticos en ordenador e entrega de proxectos relacionados cos criterios de avaliación máis prácticos da UD ou bloque. En cada trimestre deberase entregar un ou máis proxectos nos que se reflectirán todas as destrezas e contidos vistos ao longo do trimestre. Cada proxecto deberá elaborarse seguindo as instrucións indicadas con anterioridade á súa elaboración. O proxecto para ser avaliado deberá entregarse en tempo, xa que haberá unha data de entrega fixa. Proxectos entregados fóra de prazo serán avaliados cun 0. En cada proxecto valorarase entre outros:
    * Contido
    * Deseño
    * Documentación entregada: claridade, redacción, deseño, etc.

Cada unha das partes que compoñen cada proba de avaliación terá unha ponderación respecto a todas as partes de todas as probas de avaliación realizadas ao longo do curso.

- Entrega de exercicio ou traballos, realizados individualmente ou en grupo, segundo se indique. A entrega deberase realizar en tempo en forma, e obrigatoriamente deberase subir a través da aula virtual. Se non se cumpren estes criterios a nota desta entrega será de 0 puntos.
Cada entrega terá unha ponderación respecto a todas as entregas realizadas ao longo do curso.

A nota de cada avaliación obterase logo de aplicar a ponderación correspondente a cada instrumento que será a seguinte:
- Probas de avaliación: 90% aplicada á suma ponderada de cada unha das probas de avaliación realizadas ao longo da avaliación.
- Entrega de tarefas: 10% aplicada á suma ponderada de cada unha das tarefas entregadas ao longo da avaliación.

No caso do cálculo da nota da avaliación soamente se terán en conta as probas de avaliación e entrega de tarefas realizados nesa avaliación.
Para poder ter superada a avaliación, todas e cada unha das partes que compoñen as probas de avaliación deberán ter unha nota mínima de 5 sobre 10, independentemente de que o cálculo en conxunto das probas de avaliación, entrega de tarefas e participación en clase sexa igual ou superior a 5.

O cálculo da nota final do módulo será a media aritmética das notas acadadas en cada unha das avaliacións.

Para poder ter superado o módulo, é dicir, obter unha nota mínima de 5, todas e cada unha das partes que compoñen as probas de avaliación deberán ter unha nota mínima de 5, independentemente de que o cálculo en conxunto das probas de avaliación, e entrega de tarefas sexa igual ou superior a 5. Adicionalmente, cada un dos proxectos entregados ten que ter unha nota mínima de 5.

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

Por cada avaliación parcial, hai un exame de recuperación que consta dunha proba de conceptos e/ou procedementos (7 puntos).

A nota de recuperación calcularase sumando a nota do exame de recuperación
* Ata 1 punto: actitude.
* Ata 2 puntos: traballo de clase (avaliación continua).
Requisitos para recuperar cada avaliación parcial:
* Exame de recuperación: 3,5 puntos.
* Realizar polo menos o 80% das actividades.
Para aprobar a avaliación continua é condición necesaria, pero non suficiente, non exceder o número máximo permitido de faltas de asistencia (10%).
Se se perde o dereito de avaliación continua, para aprobar o módulo hai que recuperar as dúas avaliacións parciais.

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

O exame extraordinario para o alumnado con perda de avaliación continua realizarase no último trimestre antes da avaliación do ciclo e constará de tres partes, cada unha das cales abrangará os contidos impartidos no correspondente trimestre. Cada parte estará formada por dúas probas: unha conceptual e outra procedimiental. Para aprobar haberá que obter unha puntuación maior ou igual ca 5 puntos en cada proba.

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

A avaliación da propia práctica docente constitúe unha das estratexias de formación mais poderosas para mellorar a calidade do proceso ensinanza aprendizaxe.
Para valorala correctamente é necesario ser crítico e reflexivo, valorando o que se fai, identificado os problemas e buscar as solucións.
Avaliarase a práctica docente en relación á consecución dos obxectivos educativos do currículo.
Analizaranse os resultados do proceso ensinanza-aprendizaxe, facendo unha autoavaliación crítica e reflexiva da programación e de cada unidade didáctica para mellorar a práctica docente.
As melloras que se decidan tomar incluiranse para o curso seguinte na programación.

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

Realizarase unha enquisa na que porá en coñecemento do profesorado coñecementos, inquietudes, nivel de estudos dos alumnos para que así o profesor teña unha posición inicial da que partir á hora que dar por sentados coñecementos ou posibles agrupamentos para os traballos que se propoñan.

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

Atención personalizada aos alumnos/as con un ritmo de aprendizaxe máis lento, axudándolles na resolución de problemas, dándolles máis tempo para a realización dos exercicios, prácticas, traballos, y propoñéndolles actividades de reforzo que lles permitan a comprensión dos contidos traballados na clase.
Proporcionar actividades complementarias e de ampliación os alumnos/as mais avantaxados para ampliar coñecementos sobre os contidos tratados e outros relacionados.
Por outra parte, todos aqueles alumnos/as con un ritmo de aprendizaxe mais rápido poderán implicarse na axuda os seus compañeiros de clase

como monitores en aquelas actividades nas que sexan mais destros.
Preténdese así traballar as habilidades sociais dos alumnos e alumnas, reforzando a cohesión do grupo e fomentando a aprendizaxe colaborativa.

9. Aspectos transversais

9.a) Programación da educación en valores

Asemade dos contidos anteriormente detallados, na dinámica diaria do proceso de ensinanza¿aprendizaxe, traballaranse os seguintes temas transversais:

¿ Educación moral e cívica, os alumnos van mostrar aspectos da vida diario sobre a necesidade de respectar as normas básicas e adoptar actitudes positiva e de apoio para a convivencia en sociedade, que será aplicado con actividades en grupo mentres que o traballo será asociado a esa clase efectuados en sociedades, particularmente en tendas de informática.
¿ Educación para a Paz: debe en todo momento, comunicando a través de non violencia, linguaxe e atención incidir na prevención de conflitos na clase e para a súa resolución pacífica.
¿ Educación para a Igualdade de Oportunidades para ambos os sexos: Ten que para mostrar a igualdade ao facer a agrupación de estudantes e os alumnos a desenvolver cada unha das actividades propostas, aumentando tamén utilizar unha linguaxe co-educativa na clase.
¿ Educación en saúde: atención especial á hixiene e postural, ergonomía para evitar dores de costas, así como estándares de seguridade deben ser atendidos e os elementos de protección debe ser usado en diferentes operacións de montaxe de equipos.
¿ Educación Ambiental: promover a utilización e xeración de documentación en dixital para evitar, na medida do posible o desperdicio de papel. Ademáis, ao longo da operación de montaxe e mantemento de ordenadores, deben dirixirse a eliminación selectiva de residuos xerados.
¿ Educación do Consumidor: que os estudantes van tentar reflexionar sobre o hábitos de consumo, promovendo a reutilización de compoñentes hardware.

Tratar o tema do software libre. Avantaxes, motivacións económicas, morais, e aspectos sociais do movemento.
Falar do fenómeno da piratería informática, das redes sociais, da seguridade e as repercusións que ten para a industria.

9.b) Actividades complementarias e extraescolares

Teñen un papel moi importante na formación integral do alumnado, abordando temas de interese, e ofrecendo a posibilidade de poñer o alumnado en contacto con unha realidade descoñecida ou só coñecida a nivel teórico.
Os seus obxectivos son:
* Poñer en contacto o alumnado coas actividades obxecto de estudio.
* Que o alumno coñeza sobre a realidade aspectos só estudados a nivel teórico.

Suxírese a visita a unha empresa ou organismo, na que o alumno tomará conciencia sobre os procesos que se abordan nela, documentos xerados, o traballo do departamento de informática e das xestións que este realiza para o funcionamento da mesma.
Tamén serán propostas unha visita o CESGA (Centro de Supercomputación de Galicia) en Santiago e unha visita a algún certame informático onde coñecer as novidades no campo da informática. Ademais de apreciar as magnitudes dun sistema informático punteiro de ámbito nacional.
No caso de se celebrar as XORNADAS SOBRE SEGURIDADE INFORMÁTICA planificarase unha visita a Facultade de Informática na Coruña para asistir a elas.

10.Outros apartados

10.1) Metodoloxía

Por mor da COVID19 e co fin de manter a distancia de seguridad na aula, impartirase ensino semi-presencial. O alumnado distribuirase en dúas quendas que asistirán a clase en días alternos. A explicación dos conceptos e das actividades farase de forma presencial para as dúas quendas. O alumnado realizará as actividades na súa casa cando non lle toque asistir a clase a súa quenda.