1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
36015159	Chan do Monte	Marín	2021/2022

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	2021/2022	6	105	126

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

Profesorado responsable

Profesorado asignado ao módulo	ROSENDO DAVID GORES FANDIÑO
Outro profesorado	

Estado: Pendente de supervisión inspector

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

O ámbito produtivo do Instituto son empresas PEME que se adican á consultoría e a distintos servizos informáticos e/ou a programación nos diferentes ámbitos da informática (web, programación a medida, etc.).
Neste módulo de Seguridade Informática e Alta Disponibilidade tratarase de orientar aos alumnos/as para axudar a mellorar a seguridad e a posta en funcionamento de sistemas de alta dispoñibilidadea estas empresas.

No currículo especifícase, nas orientacións pedagóxicas do módulo, as funcións que obterán os alumnos/as ao aprobar este módulo.
Tamén no currículo, nas competencias competencias profesionais, persoais e sociais especifícanse varias habilidades e capacidades que terán os alumnos/as.
En concreto destacar as seguintes:
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 deseguridade, 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 (programandoe verificando ou seu cumprimento), en función das cargas de traballo e o plan demantemento.

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 á seguridade informática.		6	7
2	Seguridade física.		8	8
3	Criptografía.		25	15
4	Seguridade Lóxica. Servidor.		15	5
5	Seguridade Lóxica. Seguridade Perimetral.		10	5
6	Implantación de firewalls.		15	15
7	Implantación de proxys.		10	10
8	Sistemas de alta dispoñibilidade. Clusters.		12	10
9	Virtualización.		10	10
10	Analisis forense.		10	7
11	Lexislación.		5	8

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Introdución á 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
RA7 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia.	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.
CA1.5 Adoptáronse políticas de contrasinais.
CA1.6 Valoráronse as vantaxes do uso de sistemas biométricos.
CA7.2 Determinouse a necesidade de controlar o acceso á información persoal almacenada.
CA7.7 Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable.

4.1.e) Contidos

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

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Seguridade física.	8

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
CA1.5 Adoptáronse políticas de contrasinais.
CA1.6 Valoráronse as vantaxes do uso de sistemas biométricos.
CA1.8 Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.

4.2.e) Contidos

Contidos
Tipos de ameazas: físicas e lóxicas. 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	Criptografía.	25

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
CA1.7 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.

4.3.e) Contidos

Contidos
Pautas e prácticas seguras. Seguridade lóxica: Criptografía. Listas de control de acceso. Establecemento de políticas de contrasinais. Sistemas biométricos de identificación. Políticas de almacenamento. Medios de almacenamento. 0Técnicas de cifraxe da información: clave pública e clave privada; certificados dixitais; sinaturas. Seguridade na conexión con redes públicas.

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Seguridade Lóxica. Servidor.	15

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
CA1.3 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.
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.
CA2.2 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.
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.
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.

4.4.e) Contidos

Contidos
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. Ataques e contramedidas en sistemas informáticos. Clasificación dos ataques. Anatomía de ataques e análise de software malicioso. Realización de auditorías de seguridade. Ferramentas preventivas e paliativas: instalación e configuración. Copias de seguridade e imaxes de respaldo.

Contidos
Recuperación de datos. Actualización de sistemas e aplicacións.

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Seguridade Lóxica. Seguridade Perimetral.	10

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
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade.	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.
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.
CA3.1 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.
CA3.3 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.

4.5.e) Contidos

Contidos
Análise das principais vulnerabilidades dun sistema informático.
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.
Ferramentas preventivas e paliativas: instalación e configuración.

Contidos
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.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Implantación de firewalls.	15

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

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

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

Criterios de avaliación
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.

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

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Implantación de proxys.	10

4.7.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

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

Criterios de avaliación
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.

4.7.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.

4.8.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
8	Sistemas de alta dispoñibilidade. Clusters.	12

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.	NO

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.
CA6.4 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. 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.

4.9.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
9	Virtualización.	10

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.	NO

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

Criterios de avaliación
CA6.3 Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.

4.9.e) Contidos

Contidos
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	Analisis forense.	10

4.10.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
RA7 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia.	NO

4.10.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.
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.
CA7.7 Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable.

4.10.e) Contidos

Contidos
Análise forense en sistemas informáticos: obxectivo. Recollida e análise de incidencias. Ferramentas empregadas na análise forense. Lexislación sobre protección de datos e sobre os servizos da sociedade da información e o correo electrónico.

4.11.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
11	Lexislación.	5

4.11.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

4.11.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.

4.11.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

A avaliación do alumnado será continua, e haberase de ter en conta o grao de consecución dos obxectivos específicos deste módulo.
Durante o desenvolvemento das clases, procederase á observación sistemática e pautada do proceso de aprendizaxe de cada alumno co fin de avaliar o progreso do mesmo en relación ao grao de consecución dos obxectivos xerais descritos no currículo do ciclo formativo.
Para acadar unha cualificación o máis obxectiva posible, empregaranse os seguintes instrumentos de avaliación:
* A participación activa na clase propoñendo solucións aos diferentes casos prácticos que se expoñan.
* A realización, presentación (dentro do prazo previsto) e exposición (no seu caso), das tarefas encomendadas debidamente documentadas.
Farase unha recollida puntual de exercicios e realizaranse probas puntuais para obter información sobre capacidades ou destrezas concretas como se describe nas unidades didácticas correspondentes.
* O traballo dentro da aula. Tamén se comprobará o traballo en equipo, se resultou óptimo ou deficiente e comprobando se o alumno tivo un talante aberto ás solucións aportadas polos demais por ser máis eficaces. Asemade, valorarase a capacidade para aceptar as críticas ao seu traballo e o tesón á hora de defender as súas solucións. Tratando de evitar a ensinanza mecánica e memorística, fomentarase a participación do alumno no proceso de aprendizaxe. Valorarase a capacidade para resolver problemas sobre o ordenador, a facilidade de acceso ós manuais técnicos, bibliografía e utilidades de software dispoñible, así como o interese, esforzo persoal e responsabilidade de cada quen. Este curso 2020-21 e máis complexo este traballo en grupo e terá que fomentarse o traballo en grupo pero non presencial, senon por medio de videoconferencias ou utilización de entornos colaborativos online.
* Probas individuais sobre os coñecementos teórico-prácticos, que permitirán determinar se un alumno alcanzou os obxectivos específicos propostos no deseño curricular do módulo e desenvolvidas nesta programación, e tamén permitirán comprobar que o alumno/a fixo o traballo da clase e non o plagiou dotro compañeiro ou de Internet. Estas probas individuáis poderanse facer dunha ou varias unidades didácticas e terán un peso na nota obtida polo alumno na avaliación dun 90% e serán como se explica a continuación:
->Probas escritas onde se preguntará aos alumnos/as conceptos teóricos relacionados cos traballos feitos na aula. Poderán ser tipo test, de resposta curta ou longa sobre un tema.
->Probas prácticas onde os alumnos deberán realizar configuracións (de servizos, equipos ou redes) que xa prácticaron na aula.
Con estas probas preténdese facer un seguimento individualizado da asimilación de tódolos conceptos impartidos segundo os criterios de avaliación establecidos en cada unidade didáctica ata o momento impartida e o grao de consecución dos obxectivos do módulo.
En cada proba indicarase ao alumno/a que partes corresponden a un CA considerado MÍNIMO EXIXIBLE e será OBRIGATORIO facer ben esa parte da proba para superala.
* Recolleranse as tarefas que se desenvolven na clase para valorar o grao de consecución dos obxectivos de cada un dos alumnos.

Antes de cada avaliación pódese realizar unha proba global que permita valorar o grao de integración de coñecementos que acadou cada un dos alumnos.
Nas probas valorarase principalmente a sinxeleza, claridade e comprensión dos procedementos asociados.
A cualificación da avaliación será a media ponderada (indicarase o tanto por cento de cada unha das probas para a nota total) das notas obtidas nas probas, valorándose ademais tódolos aspectos arriba indicados de acordo cos seguintes porcentaxes:
* Un 90% da nota será a nota media (ponderada) obtida nas probas.
* Un 10% estará constituído pola valoración realizada en canto aos aspectos indicados de traballo na aula e participación nos traballos e prácticas propostas sexan en grupo ou individuais.

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

* Recuperación ó longo do curso:
As actividades desenvolveranse para cada unidade didáctica co alumno ou alumna que non supere a proba da unidade didactica, buscando sempre que o alumno ou alumna recupere canto antes a unidade de traballo. Para isto, desenvolveránse exercicios e explicacións personalizadas,

así como avaliacións iniciais máis afinadas que permitan detectalas posibles causas da non superación da unidade de traballo e así axustalos procesos de ensino-aprendizaxe.
Ben ao remate de cada trimestre ou ben antes do inicio do período de formación en centros de traballo(FCT), farase unha proba ou probas de recuperación de natureza práctica e escrita dos contidos das unidades didácticas desenvolvidas no periodo da avalizacion (1er o 2º tirmestre)
O alumno deberá superar cunha cualificación superior a 5 en tódalas probas de recuperación realizadas. Neste caso, a nota final será a media das notas correspondentes a cada proba. Si a proba é de recuperación.
* Recuperación dun módulo pendente:
Para o alumnado que non acceda a la FCT por no ter superado o módulo na convocatoria ordinaria, haberá un período destinado a súa recuperación que coindidirá co periódo destinado a FCT e estará comprendido dende a data de avaliación ordinaria previa a FCT(no mes de marzo) ata ó 15 de xuño (aprox) no último trimestre do curso(abril xuño).
O profesor proporá un calendario de actividades de recuperación e horarios de titorías.
No procedementos de avaliación e cualificación do alumnado con o módulos pendentes, distinguense os seguintes casos:
caso1) Alumnado có módulo pendente que asiste habitualmente a clase e realiza as actividades de recuperación. Neste caso o profesor pode facer un seguimento do seu traballo e da sua evolución e será avaliado cos mesmos criterios de avaliación empregados durante o curso.
caso2) Alumnado có módulo pendente que non asiste habitualmente a clase e non realiza tódalas actividades de recuperación propostas. Neste caso deberá superar a mesma proba ou probas que o alumnado que perdeu o dereito a avaliación continua para superar o módulo.

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

Os instrumentos de avaliación neste caso que se empregarán son os seguintes:
* Proba escrita: constará de cuestións, problemas e outras tarefas a desenvolver de forma escrita, da mesma natureza e complexidade, cas desenvolvidas ó longo do curso académico polo alumnado avaliado de forma continua baseadas nos contidos desenvolvidos nas diferentes unidades didácticas do módulo.
* Proba práctica: constará de tarefas e preguntas da mesma natureza e da mesma complexidade cas desenvolvidas ó longo do curso académico polo alumnado de forma continua baseadas nos contidos desenvolvidos nas diferentes unidades didácticas do módulo.
Para superar o módulo profesional compre acadar unha puntuación de, a lo menos, 5 puntos en cada proba. A cualificación final da proba será a media ponderada das puntuacións obtidas en cada proba escrita e práctica, valorándose a proba escrita nun 40% e a proba práctica nun 60%.
Poderanse realizar as probas en días distintos se houbese algún problema por realizalas nun mesmo día. As probas poderán durar ata 5 horas cada unha de elas. Se lle comunicarán o interesado ou interesada as datas e horas das probas coa debida antelación.
O profesor tamén avaliará se a alumna ou alumno reúne os requisitos de madurez, autonomía ou identidade persoal e profesional, dentro das devanditas probas.

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

O finalizar cada unidade didáctica, o profesor realizará unha reflexión do proceso de ensino-aprendizaxe de dita unidade coa finalidade de recoller, revisar e analizar o desenrolo de dito proceso, os logros e debilidades dos resultados obtidos a través das distintas fontes e instrumentos de avaliación (observacións, cuestionario, probas de rendemento, etc..) utilizados en cada unidade didáctica.
Segundo estes resultados, revisarase a programación didáctica e faranse as correccións necesarias, se é o caso, nas actividades de ensino e aprendizaxe, nos materiais, nos recursos necesarios para a súa realización e nos instrumentos de avaliación para así mellorar o proceso de ensino de cada alumno, os rendementos destes, o funcionamento do grupo de clase e a propia práctica docente do profesor.

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

O comezo do curso realizarase a avaliación inicial para avaliar os coñecementos e destrezas dos alumnos, a fin de adecuar estratéxicamente o proceso de ensino-aprendizaxe, introducir adaptacións na programación do módulo, una vez coñecida a realidade dos alumnos e adoptar outro tipo de medidas para unha mellor atención á diversidade.
O instrumento de avaliación inicial estará baseado na experiencia profesional do profesor e terá carácter principalmente de observación das actividades propostas, comportamentos e actitudes durante as primeiras semanas do inicio curso, que permiten obter unha fonte de datos, para o seu posterior análise e toma de decisións respecto á diversidade que puidera aparecer. Como documentos complementarios utilizáranse as actas de avaliación e informes individuais dispoñibles do curso anterior.
A finais do primeiro mes reuniranse os profesores do equipo docente do curso coa finalidade de describir a situación inicial, deducir as necesidades que aparecen, realizar propostas e tomar decisións conxuntas en torno a un alumno o a un grupo.

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

As medidas de reforzo educativo constitúen un continuo de atención á diversidade. Para elo, planificaranse actividades extra para aqueles alumnos aos que lles custe especialmente a consecución dalgún dos obxectivos do módulo.
Favorecerase a colaboración entre compañeiros para axudar a comprender distintos puntos de vista e reforzar o explicado na aula.

9. Aspectos transversais

9.a) Programación da educación en valores

Esta programación ten presente que os obxectivos esenciais da educación actual non se limitan á formación profesional ou cultural do seu alumnado, se non que hai que incluír, ádemas, a formación cívico-ética dos alumnos e as alumnas en todos aqueles valores ós que aspira a sociedade.
Entre os temas transversais para o desenrolo da Educación en Valores encóntranse, entre outros:
* Coñecemento e respecto pola normativa TIC legal vixente; en especial a Lei de Protección de Datos de Carácter Personal(LOPD)
* Aprendizaxe permanente ó longo da vida.
* Explicar ó alumnado a importancia que ten o movemento de ¿Software Libre¿ no desenvolvemento da súa carreira profesional, o contorno productivo de Galicia e as súas implicacións sociais.
* Na educación Moral e Cívica: Promover a actitude receptiva, colaboradora e tolerante nas relaciones entre os alumnos e nas actividades en grupo e rexeitar calquer tipo de discriminación baseada en diferenza de sexos, raza, clase, social, ideoloxías , etc.
* Na Educación para a Paz: Fomentar o respecto polas opinións e crenzas doutras persoas.
* Na Educación para a Saúde: Potenciar hábitos de hixiene e coidado corporal e recoñecer e seguir as normas de seguridade das diferentes aulas para evitar accidentes.
* Na Educación para a Igualdade: Rexeitar calquera prantexamento e/ou actitude sexista, promovendo o desenrolo persoal, equilibrado e cooperativo de todos os alumnos.
* Na Educación Ambiental: Concienciar dos problemas medioambientais producidos polo material informático en desuso e promover hábitos de reutilización e reciclaxe nos materiais empregados.

9.b) Actividades complementarias e extraescolares

Prevese que na Facultade de Informática de A Coruña realizaranse unhas xornadas de seguridade da información que son de moita utilidade e importancia para calquera profesional que se adique a este ámbito da tecnoloxía.

Intentarase asistir as citadas xornadas co grupo de alumnos deste módulo.
A xira UpToSecure, organizada pola empresa Informática64, e que no mes de xaneiro fai unhas charlas en Vigo, tamén son interesantes polos temas tratados e tanto de seguridade coma de últimas tecnoloxías que hai no ámbito informático.
Procurarase asistir a calquera outra actividade que durante o curso se nos informase que se vaia a realizar e estivese relacionada coa seguridade informática.

10.Outros apartados

10.1) Docencia a distancia.

Podería ocurrir que este curso tivésemos que facer algunha clase en modo semipresencial ou a distancia por causa da pandemia provocada polo Covid19.
Os contidos e prácticas deste módulo está na aula virtual, o que permitiría a continuación das clases prácticas como se fose na aula e as clases teóricas teríamos que utilizar algunha ferramenta de video conferencia, coma Falamos ou Webex Meeting.

10.2) Acceso á programación

A programación debe ser un documento público e accesible por calquera persoa que requira consuntala. Esta programacíon estará accesible cunha copia que se gardará no sistema para poder consultala.