ANEXO XIII
MODELO DE PROGRAMACIÓN DE MÓDULOS PROFESIONAIS

1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
15021482	San Clemente	Santiago de Compostela	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 de adultos

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	4	105	126

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

Profesorado responsable

Profesorado asignado ao módulo	ENRIQUE AGRASAR MARTÍNEZ (Subst.)
Outro profesorado	ENRIQUE AGRASAR MARTÍNEZ

Estado: Pendente de supervisión departamento

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

O desenvolvemento curricular deste módulo profesional fíxose tomando como referencia o Centro educativo IES San Clemente que cumpre as condicións establecidas pola L.O.E. e os Reais Decretos que a desenvolven en canto a espazos, instalacións, alumado, etc.
Se o contextualizamos para o entorno da cidade de Santiago de Compostela, no entorno do centro encóntranse varias empresas de servizos informáticos que acollen á gran maioría dos alumnos do ciclo para a Formación en Centros de Traballo e onde é previsible que poidan desenrolar a súa carreira profesional estes alumnos.

- Este módulo profesional contén a formación necesaria para seleccionar e utilizar técnicas e ferramentas específicas de seguridade informática no ámbito da administración de sistemas. Ademais, ha servir para coñecer arquitecturas de alta dispoñibilidade e utilizar ferramentas de virtualización na implantación de servizos de alta dispoñibilidade.
- As funcións da administración segura de sistemas abranguen aspectos como:
  * Coñecemento e correcta manipulación de todos os elementos que forman o compoñente físico e lóxico dos equipamentos.
  * Adopción de prácticas seguras consonte os plans de seguridade física e lóxica do sistema.
  * Coñecemento e uso de técnicas seguras de acceso remoto a un sistema, tanto en modo usuario como en modo administrativo.
  * Selección e aplicación de técnicas e ferramentas de seguridade activa que actúen como medidas preventivas ou paliativas ante ataques a ao sistema.
  * Instalación e configuración de ferramentas de protección perimetral, tornalumes e servidores proxy.
  * Instalación e configuración de servizos de alta dispoñibilidade que garantan a continuidade de servizos e a dispoñibilidade de datos.
  * Coñecemento e aplicación da lexislación no ámbito do tratamento dixital da información.
- As actividades profesionais asociadas a estas funcións aplícanse en:
  * Mantemento de equipamentos (hardware e software).
  * Administración de sistemas en pequenas e medianas empresas.
  * Persoal técnico de administración de sistemas en centros de procesamento de datos.
  * Persoal técnico de apoio en empresas especializadas en seguridade informática.
- A formación do módulo contribúe a alcanzar os seguintes obxectivos xerais:
  * Seleccionar sistemas de protección e recuperación, analizando as súas características funcionais, para pór en marcha solucións de alta dispoñibilidade.
  * Identificar condicións de equipamentos e instalacións, interpretando plans de seguridade e especificacións de fábrica, para supervisar a seguridade física.
  * Aplicar técnicas de protección contra ameazas externas, así como tipificalas e avalialas, para asegurar o sistema.
  * Aplicar técnicas de protección contra perdas de información, analizando plans de seguridade e necesidades de uso para asegurar os datos.
  * Establecer a planificación de tarefas, analizando actividades e cargas de traballo do sistema, para xestionar o mantemento.
  * 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.
- A formación do módulo contribúe a alcanzar as seguintes competencias profesionais, persoais e sociais:

* Mellorar o rendemento do sistema configurando os dispositivos de hardware consonte os requisitos de funcionamento.
* Avaliar o rendemento dos dispositivos de hardware identificando posibilidades de mellora segundo as necesidades de funcionamento.
* Pór en práctica solucións de alta dispoñibilidade, analizando as opcións do mercado, para protexer e recuperar o sistema ante situacións imprevistas.
* Supervisar a seguridade física segundo especificacións de fábrica e o plan de seguridade, para evitar interrupcións na prestación de servizos do sistema.
* Asegurar o sistema e os datos segundo as necesidades de uso e as condicións de seguridade establecidas, para previr fallos e ataques externos.
* Diagnosticar as disfuncións do sistema e adoptar as medidas correctivas para restablecer a súa funcionalidade.
* Xestionar e/ou realizar o mantemento dos recursos da súa área (programando e verificando ou seu cumprimento), en función das cargas de traballo e o plan de mantemento.
* 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.
* Xestionar a propia carreira profesional, analizando as oportunidades de emprego, de autoemprego e de aprendizaxe.
* Participar de xeito activo na vida económica, social e cultural, con actitude crítica e responsable.

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	Adopción de pautas de seguridade informática.	Nesta unidade de traballo o alumnado deberá adquirir os conceptos básicos sobre seguridade informática.	13	10
2	Implantación de mecanismos de seguridade activa. Creación de escenarios de ciberseguridade.	Analizarase os tipos de ataque que pode sufrir un sistema informático, así como as vulnerabilidades das que se pode aproveitar para realizalos. Aa unidade segue estudando as posibles ferramentas utilizadas para previr e paliar as posibles incidencias que se produzan. O punto 3 da unidade xustifica a existencia dos manuais de seguridade e plans de continxencia, tamén se especifican os puntos máis importantes que deben conter. Por último, trátase a seguridade nas redes corporativas, analizando as vulnerabilidades máis comúns, así como as ferramentas de protección existentes para facer que a rede sexa máis segura. Traballarase na creación de escenarios de ciberseguridade para poñer en práctica mecanismos de seguridade activa.	20	16
3	Implantación de técnicas de acceso remoto.	Nesta unidade o alumnado estudiará as principais técnicas de acceso remoto, así como as medidas de seguridade básicas que se establecen para que dito acceso sexa seguro para a rede corporativa.	20	16
4	Instalación e configuración de tornalumes.	Aprenderase os conceptos básicos relativos ao funcionamento, instalación e configuración dos tornalumes.	20	16
5	Instalación e configuración dun servidor proxy.	Con esta unidade preténdese que o alumnado aprenda as nocións básicas de instalación e configuración dun servidor proxy.	20	16
6	Implantación de soluciones de alta disponibilidad.	Nesta unidade de traballo o alumnado comprenderá o funcionamento das solucións de alta dispoñibilidade, así como a configuración dalgunha delas.	20	16
7	Lexislación e normas sobre seguridade.	Preténdese que o alumnado se familiarice con leis que rexen o tratamento dos datos.	13	10

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Adopción de pautas de seguridade informática.	13

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.	SI

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.
CA1.4 Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas.
CA1.5 Adoptáronse políticas de contrasinais.
CA1.6 Valoráronse as vantaxes do uso de sistemas biométricos.
CA1.7 Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información.
CA1.8 Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.
CA1.9 Identificáronse as fases da análise forense ante ataques a un sistema.
0CA1.10 Empregáronse sistema de control de versións para o correcto emprego dos artefactos xerados nunha contorna de ciberseguridade e, nun contexto máis amplo, de toda a actividade da operación dun sistema informático.

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.
Tipos de ameazas: físicas e lóxicas.
Seguridade física e ambiental: Localización e protección física dos equipamentos e dos servidores. Sistemas de alimentación ininterrompida.
Seguridade lóxica: Criptografía. Listas de control de acceso. Establecemento de políticas de contrasinais. Sistemas biométricos de identificación. Políticas de almacenamento. Medios de almacenamento.
Análise forense en sistemas informáticos: obxectivo. Recollida e análise de incidencias.
Ferramentas empregadas na análise forense.
Creación de escenarios de ciberseguridade empregando ferramentas como docker, vagrant, compose

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Implantación de mecanismos de seguridade activa. Creación de escenarios de ciberseguridade.	20

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.	SI

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

Criterios de avaliación
0CA1.10 Empregáronse sistema de control de versións para o correcto emprego dos artefactos xerados nunha contorna de ciberseguridade e, nun contexto máis amplo, de toda a actividade da operación dun sistema informático.
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.
CA2.6 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.
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.

4.2.e) Contidos

Contidos
Ataques e contramedidas en sistemas informáticos.
0Técnicas de cifraxe da información: clave pública e clave privada; certificados dixitais; sinaturas.
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.

Contidos
Sistemas de detección de intrusións.
Creación de escenarios de ciberseguridade empregando ferramentas como docker, vagrant, compose
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.
Recuperación de datos.
Actualización de sistemas e aplicacións.
Seguridade na conexión con redes públicas.

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Implantación de técnicas de acceso remoto.	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
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade.	SI

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

Criterios de avaliación
0CA1.10 Empregáronse sistema de control de versións para o correcto emprego dos artefactos xerados nunha contorna de ciberseguridade e, nun contexto máis amplo, de toda a actividade da operación dun sistema informático.

Criterios de avaliación
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.

4.3.e) Contidos

Contidos
Creación de escenarios de ciberseguridade empregando ferramentas como docker, vagrant, compose
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.

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Instalación e configuración de tornalumes.	20

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

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

Criterios de avaliación
0CA1.10 Empregáronse sistema de control de versións para o correcto emprego dos artefactos xerados nunha contorna de ciberseguridade e, nun contexto máis amplo, de toda a actividade da operación dun sistema informático.
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.

4.4.e) Contidos

Contidos
Creación de escenarios de ciberseguridade empregando ferramentas como docker, vagrant, compose

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.

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Instalación e configuración dun servidor proxy.	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
RA5 - Implanta servidores proxy, aplicando criterios de configuración que garantan o funcionamento seguro do servizo.	SI

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

Criterios de avaliación
0CA1.10 Empregáronse sistema de control de versións para o correcto emprego dos artefactos xerados nunha contorna de ciberseguridade e, nun contexto máis amplo, de toda a actividade da operación dun sistema informático.
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.

Criterios de avaliación
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.

4.5.e) Contidos

Contidos
Creación de escenarios de ciberseguridade empregando ferramentas como docker, vagrant, compose
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.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Implantación de soluciones de alta disponibilidad.	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
RA6 - Implanta solucións de alta dispoñibilidade empregando técnicas de virtualización, e configura os contornos de proba.	SI

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

Criterios de avaliación
0CA1.10 Empregáronse sistema de control de versións para o correcto emprego dos artefactos xerados nunha contorna de ciberseguridade e, nun contexto máis amplo, de toda a actividade da operación dun sistema informático.
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.

4.6.e) Contidos

Contidos
Creación de escenarios de ciberseguridade empregando ferramentas como docker, vagrant, compose
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.

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Lexislación e normas sobre seguridade.	13

4.7.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

4.7.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.

Criterios de avaliación
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.

4.7.e) Contidos

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

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

Os CRITERIOS e INSTRUMENTOS de avaliación da adquisición do resultados de aprendizaxe serán os seguintes:

ACTIVIDADES PRÁCTICAS REALIZADAS DURANTE O CURSO

1. Realización de actividades prácticas ou traballos. Realizaranse por defecto de xeito individual e a súa autoría debe ser do propio alumno e quedar acreditada. Consistirán no desenvolvemento das tarefas propostas polo profesorado. Cada exercicio individualmente avaliable será identificado e ponderado para a posterior obtención da calificación dos exercicios prácticos aplicando unha MEDIA ARITMÉTICA PONDERADA.

Cada exercicio será avaliado coa escala de valoración seguinte (A, B, C, D, E):

E) Traballo ou práctica non entregada.
D) Traballo ou práctica entregada en prazo ordinario ou extraordinario pero que NON ACADA significativamente o esperado no plantexado polo profesorado.

C) Traballo ou práctica entregada en prazo ordinario ou extraordinario pero contén especificacións non satisfeitas. Funciona parcialmente e que non sería unha solución admitida nun ámbito profesional.
B) Traballo ou práctica entregada en prazo extraordinario que CUMPRE con TODAS as especificacións e requisitos plantexados polo profesorado.
A) Traballo ou práctica entregada en prazo ordinario que CUMPRE con TODAS as especificacións e requisitos plantexados polo profesorado.

Os correspondentes valores numéricos nunha escala do 0 ao 10 son:

A/A+ -> 10 puntos
B -> 6 puntos
C -> 3 puntos
D -> 1 puntos
E -> 0 puntos

Poderíase facer mención especial (A+) a unha actividade ou traballo ou práctica entregada en prazo ordinario que profundiza e vai máis aló do plantexado polo profesorado, ou denota excepcionalidade polo valor que aporta na súa resolución, ou destaque pola suá apropiada documentación, ou que conteña algunha característica que pode aportar valor ó conxunto dos alumnos do módulo. Esta mención non ten efecto sobre a calificación alcanzada.

A nota obtida neste apartado será o 30% da nota final da avaliación. As prácticas non entregadas no PRAZO ORDINARIO deberán entregarse igualmente nun novo PRAZO EXTRAORDINARIO (por defecto 1 semana antes do exame da 3ª avaliación se non se indica outra data) e non superarán a valoración de 3 puntos. A nota na citada escala de valoración coma a súa extrapolación na escala de 0 sobre 10 será comunicada ó alumno previo exame trimestral de evaluación e será PROVISIONAL. Disporá de 48h a partir de dita comunicación para expor calquera obxección á nota asignada ó exercicio práctico. A nota obtida en cada actividade práctica será DEFINITIVA cando o alumno DEMOSTRE A SÚA AUTORÍA aprobeitando as datas de exámes no centro, desenvolvendo durante a proba posibles modificacións na súa actividades que demostre que a domina ou exposicións orales sobre a mesma que certifiquen que o alumno comprendeas e é quen de modificalas. Pode eximirse ao alumno desta proba de autoría se o docente considera acreditada a autoría baseándose en evidencias documentais (consultas, control de versións, seguimento do desenvolvemento da práctica, etc).

PROBAS ESCRITAS E/OU PRÁCTICAS EN CADA AVALIACIÓN:

2. Probas escritas e/ou prácticas a modo de exames. Realizarase unha proba escrita e/ou práctica por avaliación. En devandita proba procurarase a proporcionalidade entre as cuestións suscitadas e o tempo dedicado no aula ás unidades de traballo ás que correspondan, tanto na súa

aprendizaxe teórica como práctica, logo será obxecto de exame: TODO O PRESENTADO DURANTE O MÓDULO ATA ESE MOMENTO (materiais, recursos, prácticas), incluindo probas e actividades de avaliacións previas.

Serán evaluadas cunha nota numérica entre 0 e 10. Nun mesmo exame, póderase dividir en diferentes partes. O sistema de puntuación e valoración de cada parte, como os mínimos necesarios serán expresados claramente por escrito xunto a proba. Pódese eximir de partes da proba ós alumnos que xa demostrasen ter sobrada competencia na mesma en avaliacións previas, asumindo a calificación que acadaron nelas. Será necesario por parte do docente evidencias documentais para facer dita exención.

A nota obtida neste apartado será o 70% da nota da avaliación trimestral. Cómpre ter unha nota igual ou superior a 5 sobre 10 nesta proba a modo de exame para acadar a condición de APTO na avaliación. Nesta proba tamén realizarase as probas de autoría das actividades prácticas.

RESUMO CUALIFICACIÓN POR AVALIACION:

-- Proba escrita e/ou práctica da avaliación : 70%
-- Actividades Prácticas realizadas ata ese momento dende o principio de curso: 30%
-- A avaliación considerase aprobada cando a NOTA MEDIA PONDERADA (proba escrita e actividadas prácticas) sexa igual ou superior a 5 sobre 10.

NOTAL FINAL NA AVALIACIÓN CONTINUA:

- A nota final do módulo corresponderá exclusivamente á nota final do último exame realizado na 3a Evaluación e as das partes exentas se as houbera (nun 70%); E a nota das prácticas feitas durante todo o curso (nun 30%), extrapoladas nunha escala de 1 a 10.

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, obtendo a calificación acadada na 3ª avaliación.
- Realizarán esta proba os alumnos que non acadaron a condición de APTO na avaliación continua ou que perderan o seu dereito de evaluación

continuada por calquera razón.
- As actividades prácticas realizadas durante o curso NON serán obxeto de avaliación nin serán consideradas na nota final desta convocatoria extraordinaria.
- Será unha proba teórico-práctica. A nota final será exclusivamente referida a esta proba nunha escala de 1 a 10.

As probas presenciais de avaliación parcial e final deberán realizarse no IES San Clemente o día e hora fixados. A información concernente a estas probas estará na plataforma de formación con suficiente antelación. Poderá ser necesario, protocolos organizativos, manifestar a presencia ou ausencia ás mesmas usando os mecanismos indicados para elo.

NOTAS ADICIONÁIS:

- Empregaranse Git y GitLab para a realización y consigna das prácticas y exercicios prácticos de exame. Isto é acorde ao Criterio de Avaliación "Empregáronse sistema de control de versións para o correcto emprego dos artefactos xerados nunha contorna de ciberseguridade e, nun contexto máis amplo, de toda a actividade da operación dun sistema informático".

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

Como se trata dun modulo a distancia o alumno terá abertas as unidades didácticas e os recursos complementarios de cada unidade, e se creara un foro para que se prepararen a recuperación. Además tamén poderá facer preguntas a través da aula virtual e poderá recibir tutorías persoais a través da plataforma de videoconferencia WebEx ou Meet, pero non presenciais (agás casos excepcionáis) debido á situación sociosanitaria derivada da pandemia do COVID-19.

O alumnado que non supere a avaliación final deberá recuperar os contidos non superados mediante unha proba escrita final máis a entrega dos traballos fináis de tema non superados.

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

Como o alumnado e do réxime a distancia, non existe a perda de dereito de evaluación continua, polo que non se pode aplicar a este módulo.

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

O seguemento da programación didáctica realizarase una vez tódalas semanas para así poder comprobar se a temporización é a correcta, ou se as actividades foron realistas na súa concepción teórica.

A avaliación da propia práctica docente será utilizada como realimentación para ter unha visión máis global de cómo se está a realizar.

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

O procedemento para a realización da avaliación inicial será o que segue:

a)Preguntas no foro para saber, información das circunstancias persoais de cada alumna/o (formación previa, intereses, motivacións, recursos dispoñibles, experiencias previas, ...) e análise das respostas por parte do profesorado que integra o equipo docente do grupo.

b)Realización dunha sesión de avaliación inicial a través do módulo de Titoría.

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

As medidas para estudantes con necesidades especiais serán facilitarlle as directrices especiales dacordo cas instruccions da orientadora do centro e adaptarle a metodoloxía didáctica.

9. Aspectos transversais

9.a) Programación da educación en valores

Tendo en conta que unha das nosas metas e a formación integral do alumnado, terase en conta a transversalidade dos valores. Estes concíbense como o conxunto de contidos pertencentes a campos do coñecemento moi diversos, que deben ser abordados cun enfoque interdisciplinario e que se aprecian de maneira integrada tanto nos obxectivos como nos contidos de tódolos módulos que conforman o currículo.

Educación ambiental: Evitar proxectos empresariais non respectuosos co media ambiente e o perigo de determinados residuos informáticos.
Educación moral e cívica: Axustarse a lexislación todo o relacionado, por exemplo, o respecto da propiedade intelectual do software, o uso adecuado da Internet...

Educación para a paz e a convivencia: Promoverase como principio fundamental o respecto mutuo e o respecto a regras de convivencia no día a día da aula.
Educación do consumidor: Hai diversidade de empresas comerciais e diversidade de produtos. O consumidor ten a posibilidade de elixir de acordo a uns criterios. A posibilidade de elección entre software libre e propietario. Esixir unha documentación correcta e adecuada as empresas subministradoras. Aprendizaxe para a toma de decisións.

Ademais dos contidos, incorpórase no módulo a formación noutras áreas prioritarias relativas a: Tecnoloxías da Información e a Comunicación (en adiante TIC), idiomas dos Países da Unión Europea, o traballo en equipo, etc.

Por tratarse dun módulo pertencente a un ciclo formativo da familia de Informática, impartido a distancia, as tecnoloxías TICs están plenamente integradas na actividade docente. Neste sentido potenciarase o seu uso mediante PLATEGA, plataforma na que o alumnado poderá dispor, entre outra
documentación, de apuntes, documentos, artigos, respostas ás preguntas máis frecuentes, exercicios propostos e/ou resoltos, e tamén enlaces na rede con documentación sobre os temas tratados.
En canto aos idiomas dos Países da Unión Europea, fomentarase a súa familiarización ao facilitar vídeos, escritos, documentos, bibliografías, etc. nestes idiomas, en particular en inglés, así como promover no alumnado a consulta de páxinas en Internet en distintos idiomas. O traballo en equipo potenciarase mediante a proposta de exercicios a realizar en grupos de dous ou máis, nas titorías presenciais, procurando que os compoñentes do grupo teñan que involucrarse e colaborar na súa execución. Por outra banda, o profesorado debe tamén axudar a inculcar uns valores ao seu alumnado, esta educación en valores realízase mediante temas transversais e intenta favorecer a tolerancia, a convivencia e o multiculturalismo, tanto dentro como fóra da aula. O educador pode crear no foro un ambiente de diálogo, de debate, de invitación á reflexión que axude a propagar e asentar os anteditos valores. Todas as unidades didácticas poranse en contacto con algún destes temas sempre que pola súa afinidade o fagan posible.

9.b) Actividades complementarias e extraescolares

Todas as actividades propostas polo Departamento de Orientación que vaian dirixidas ao alumnado dos ciclos de informática e tódalas actividades propostas polo Departamento de Informática.

O departamento deixa aberta a porta á asistencia a conferencias e seminarios, que ou ben se planifiquen polo departamento ou ben vaian xurdindo no ámbito social e sexan consideradas de interese.

Hai que ter en conta que calquera actividade proposta non tería carácter obrigatorio dado que estamos dentro do réxime de distancia.

10.Outros apartados

10.1) Adaptación á situación sociosanitaria

Neste módulo, ó ser de tipo "Distancia" preséntanse soamente os seguintes cambios:
- Non haberá tutorías presenciais agás casos excepcionáis, polo que sustituiranse por tutorías telemáticas por medio de Cisco WebEx ou Meet.
- O examen farase en quendas para reducir o alumnado na aula e utilizaranse mamparas separadoras.