1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
36015159	Chan do Monte	Marín	2022/2023

Ciclo formativo

Código da familia profesional	Familia profesional	Código do ciclo formativo	Ciclo formativo	Grao	Réxime
IFC	Informática e comunicacións	CMIFC01	Sistemas microinformáticos e redes	Ciclos formativos de grao medio	Réxime de adultos

Módulo profesional e unidades formativas de menor duración (*)

Código MP/UF	Nome	Curso	Sesións semanais	Horas anuais	Sesións anuais
MP0226	Seguridade informática	2022/2023	8	140	168

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

Profesorado responsable

Profesorado asignado ao módulo	BENITO SÁNCHEZ MINIÑO,LAURA PÉREZ SÁNCHEZ (Subst.)
Outro profesorado	LAURA PÉREZ SÁNCHEZ

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 de menos de 10 empregados na sua maioría, que se adican á consultoría, a distintos servizos informáticos e/ou a programación nos diferentes ámbitos da informática (web,programación a medida, etc.).
Neste módulo de Seguridade Informática tratarase de orientar as posibles necesidades do entorno produtivo destas empresas para axudarlles á mellora na seguridade informática.

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	Esta UD trata o relativo á seguridade informatica e a súa clasificación. Definirase unha Política de Seguridade e aprenderase a identificar as ameazas, ataques e vulnerabilidades dos sistemas así como os principais mecanismos de protección.	11	5
2	Criptografía	Esta UD trata distintos métodos criptográficos empregados para cifrar e descifrar información, tanto clásicos coma modernos. Así mesmo, aprenderase como cifrar un documento ou un correo electrónico e como xerar e usar as claves públicas e privadas. Outro tema que se tratará serán os distintos sistemas de identificación como os certificados dixitais e firmas dixitais.	26	15
3	Seguridade no hardware e no almacenamento	Esta UD trata todo o relacionado coa seguridade física dun centro de procesamento de datos coma a localización física apropiada, as condicións medioambientais a ter en conta e os sistemas que deben controlar o acceso. Aprenderase tamén cal é o uso, o funcionamento e os tipos dos sistemas de alimentación ininterrompida que evitan que se perda información coa continuación do funcionamento do equipamento. Por último, aplicaranse distintas técnicas para o almacenamento de información redundante e distribuído.	25	15
4	Recuperación de datos	Esta UD trata da necesidade de seguir estratexias para non perder toda a información almacenada nun centro de procesamento de datos, polo tanto aplicaranse distintas técnicas para realizar copias de seguridade, imaxes de respaldo, puntos de restauración e recuperación de datos. A aplicación destas estratexias será tanto nun sistema operativo Windows como nun Linux.	19	10
5	Seguridade activa no sistema	Esta UD trata das técnicas para evitar accesos indesexables de intrusos ao sistema, como son: protección da BIOS, do xestor de arranque, sistemas de autenticación, políticas de contrasinais. Aprenderanse tamén os distintos tipos de software malicioso (virus) e tipos de ataques que se poden realizar a un sistema. Para xestionar o acceso aos datos e ás aplicación instaladas no sistema aprenderase a configurar as listas de control de acceso que determinan as condicións para acceder a un determinado elemento do sistema; a cifrar e descifrar arquivos e particións; a establecer cotas de disco; a actualizar os sistemas operativos e as aplicacións; a verificar a orixe e autenticidade dos programas; etc. Por último aprenderase como monitorizar un sistema para realizar a supervisión de eventos ocorridos no sistema.	32	20
6	Seguridade activa nas redes	Esta UD trata dos protocolos que aportan seguridade á hora de conectarse a unha páxina web ou a outro equipo da rede. Tamén trata de como crear e utilizar as redes privadas virtuais usadas para conectarse a outros equipos da rede a través de internet dun xeito seguro. Aprenderase así mesmo como aplicar a seguridade nas redes de conexión sen fíos así coma dos sistemas de cifrado dispoñibles: WEP e WPA.	20	12
7	Seguridade perimetral. Devasas	Esta UD trata sobre a necesidade de asegurar o perímetro da rede da organización. Estudaranse as características, vantaxes, funcio-nalidades e tipos de devasas (tornalumes ou firewall), así como as arquitecturas de rede con devasas máis comúns.	16	10
8	Seguridade perimetral. Proxys	Esta UD trata as características, as funcións principais e os tipos de proxy existentes e así proceder a configuración dun equipo para empregar un proxy	12	8
9	Lexislación e normativa sobre seguridade informática	Esta UD trata en profundidade a lexislación e normativa que afecta á seguridade informática.	7	5

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

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

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Identifica técnicas e prácticas de tratamento seguro da información, e recoñece e valora a súa importancia en distintos contornos de traballo.	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 manter a información segura.
CA1.2 Clasificouse a información no ámbito da seguridade.
CA1.3 Describíronse as diferenzas entre seguridade física e lóxica.
CA1.7 Recoñeceuse a necesidade de facer unha análise de riscos e a posta en marcha dunha política de seguridade.
CA1.8 Establecéronse as normas básicas para incluír nun manual de seguridade informática.
CA1.9 Describíronse as diferenzas entre seguridade activa e pasiva.

4.1.e) Contidos

Contidos
Seguridade activa e pasiva (CA1.9). Seguridade física e lóxica. Políticas de seguridade.

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Criptografía	26

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Identifica técnicas e prácticas de tratamento seguro da información, e recoñece e valora a súa importancia en distintos contornos de traballo.	NO
RA5 - Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico.	NO

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

Criterios de avaliación
CA1.4 Identificáronse as principais técnicas criptográficas.
CA1.5 Recoñeceuse a necesidade de integrar técnicas criptográficas na almacenaxe e na transmisión da información.
CA1.6 Identificáronse os fundamentos criptográficos dos protocolos seguros de comunicación (clave pública, clave privada, etc.).
CA5.7 Describíronse e utilizáronse sistemas de identificación como a sinatura electrónica, o certificado dixital, etc.

4.2.e) Contidos

Contidos
Criptografía. Identificación dixital: sinatura electrónica e certificado dixital.

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Seguridade no hardware e no almacenamento	25

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

Resultado de aprendizaxe do currículo	Completo
RA2 - Aplica medidas de seguridade pasiva en sistemas informáticos, recoñecendo as necesidades de acordo coas características do contorno.	SI
RA3 - Xestiona dispositivos de almacenaxe aplicando os procedementos e as técnicas adecuadas para asegurar a integridade da información.	NO
RA4 - Aplica mecanismos de seguridade activa atendendo ás necesidades do sistema informático.	NO

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

Criterios de avaliación
CA2.1 Definíronse as características do emprazamento e as condicións ambientais dos equipamentos e dos servidores.
CA2.2 Identificouse a necesidade de protexer fisicamente os sistemas informáticos.
CA2.3 Verificouse o funcionamento dos sistemas de alimentación ininterrompida.
CA2.3.1 Identificáronse os tipos de sistemas de alimentación ininterrompida.
CA2.3.2 Identificouse o modo de funcionamento do sistema de alimentación ininterrompida.
CA2.3.3 Seleccionouse o sistema de alimentación ininterrompida acorde ao sistema.
CA2.3.4 Verificouse o funcionamento dos sistemas de alimentación ininterrompida.
CA2.4 Seleccionáronse os puntos de aplicación dos sistemas de alimentación ininterrompida.
CA2.5 Esquematizáronse as características dunha política de seguridade baseada en listas de control de acceso.
CA2.6 Valorouse a importancia de establecer unha política de contrasinais.
CA2.7 Valoráronse as vantaxes do uso de sistemas biométricos.
CA2.7.1 Describíronse os sistemas biométricos.
CA2.7.2 Analizáronse as vantaxes e inconvintes de cada sistema biométrico.
CA3.1 Interpretouse a documentación técnica relativa á política de almacenaxe.
CA3.2 Tivéronse en conta factores inherentes á almacenaxe da información (rendemento, dispoñibilidade, accesibilidade, etc.).
CA3.3 Clasificáronse e enumeráronse os principais métodos de almacenaxe, incluídos os sistemas en rede.
CA3.4 Describíronse as tecnoloxías de almacenaxe redundante e distribuída.
CA3.8 Identificáronse as características dos medios de almacenaxe remotos e extraíbles.

Criterios de avaliación
CA3.9 Utilizáronse medios de almacenaxe remotos e extraíbles.
CA3.11 Utilizáronse medios de almacenaxe redundantes e distribuídos.
CA4.1 Seguíronse plans de continxencia para actuar ante fallos de seguridade.

4.3.e) Contidos

Contidos
Localización e protección física dos equipamentos e dos servidores.
Sistemas de alimentación ininterrompida.
Esquematización das características dunha política de seguridade baseada en listas de control de acceso (CA2.5).
Valoración da importancia de establecer unha política de contrasinais (CA2.6).
Valoración das vantaxes do uso de sistemas biométricos (CA2.7).
Almacenaxe da información: rendemento, dispoñibilidade e accesibilidade.
Almacenaxe redundante e distribuída.
Almacenaxe remota e extraíble.
Medios de almacenaxe.
Manual de seguridade e plans de continxencia.

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Recuperación de datos	19

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

Resultado de aprendizaxe do currículo	Completo
RA3 - Xestiona dispositivos de almacenaxe aplicando os procedementos e as técnicas adecuadas para asegurar a integridade da información.	NO
RA4 - Aplica mecanismos de seguridade activa atendendo ás necesidades do sistema informático.	NO

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

Criterios de avaliación
CA3.5 Seleccionáronse estratexias para a realización de copias de seguridade.
CA3.6 Tívose en conta a frecuencia e o esquema de rotación.
CA3.7 Realizáronse copias de seguridade seguindo diversas estratexias.
CA3.10 Creáronse e restauráronse imaxes de respaldo de sistemas en funcionamento.
CA4.7 Aplicáronse técnicas de recuperación de datos.
CA4.7.1 Aplicáronse técnicas de recuperación de arquivos e cartafoles.

4.4.e) Contidos

Contidos
Copias de seguridade e imaxes de respaldo.
Copias de seguridade.
Imaxes de respaldo.
Recuperación de datos.
Recuperación de arquivos e cartafoles (CA4.7.1.)

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Seguridade activa no sistema	32

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

Resultado de aprendizaxe do currículo	Completo
RA4 - Aplica mecanismos de seguridade activa atendendo ás necesidades do sistema informático.	NO

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

Criterios de avaliación
CA4.2 Clasificáronse os principais tipos de software malicioso.
CA4.3 Empregáronse ferramentas que examinan a integridade do sistema, e ferramentas de control e seguimento de accesos.
CA4.3.1 Empregáronse ferramentas que examinan a integridade do sistema.
CA4.3.2 Empregáronse ferramentas de control de accesos ao sistema.
CA4.3.3 Empregáronse ferramentas de control de accesos aos datos e ás aplicacións.
CA4.3.4 Empregáronse ferramentas de seguimento de accesos.
CA4.4 Realizáronse actualizacións periódicas dos sistemas para corrixir posibles vulnerabilidades.
CA4.5 Verificouse a orixe e a autenticidade das aplicacións que se instalan nos sistemas.
CA4.6 Instaláronse, probáronse e actualizáronse aplicacións específicas para a detección e a eliminación de software malicioso.
CA4.7 Aplicáronse técnicas de recuperación de datos.
CA4.7.2 Aplicáronse técnicas de recuperación de contrasinais.

4.5.e) Contidos

Contidos
Listas de control de acceso.
Política de contrasinais.
Sistemas biométricos de identificación.
Recuperación de datos.
Recuperación de contrasinais (CA4.7.2)
Monitorización de sistemas.
Auditorías de seguridade.
Software malicioso: clasificación. Ferramentas de protección e desinfección.
Actualización de sistemas e aplicacións.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Seguridade activa nas redes	20

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

Resultado de aprendizaxe do currículo	Completo
RA5 - Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico.	NO

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

Criterios de avaliación
CA5.1 Identificouse a necesidade de inventariar e controlar os servizos de rede.
CA5.2 Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas e nos roubos de información.
CA5.3 Deduciuse a importancia de reducir o volume de tráfico xerado pola publicidade e o correo non desexado.
CA5.4 Aplicáronse medidas para evitar a monitorización de redes con cables.
CA5.5 Identificáronse as ameazas na navegación por internet.
CA5.6 Clasificáronse e valoráronse as propiedades de seguridade dos protocolos usados en redes sen fíos.

4.6.e) Contidos

Contidos
Análise dos rexistros (logs) dun sistema para identificar ataques reais ou potenciais á seguridade.
Métodos para asegurar a privacidade da información transmitida.
Monitorización do tráfico en redes con cables.
Seguridade en redes sen fíos.
Riscos potenciais dos servizos de rede.
Sistemas de seguridade nas telecomunicacións: correo, www, ftp, p2p, etc.
Publicidade e correo non desexados.
Fraudes informáticas e roubos de información.

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Seguridade perimetral. Devasas	16

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

Resultado de aprendizaxe do currículo	Completo
RA5 - Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico.	NO

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

Criterios de avaliación
CA5.8 Instalouse e configurouse unha devasa (firewall) nun equipamento ou nun servidor.

4.7.e) Contidos

Contidos
0Utilización de devasas (firewalls) en equipamentos e en servidores.

4.8.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
8	Seguridade perimetral. Proxys	12

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

Resultado de aprendizaxe do currículo	Completo
RA5 - Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico.	NO

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

Criterios de avaliación
CA5.9 Instalouse e configurouse un proxy nun equipamento ou nun servidor.

4.8.e) Contidos

Contidos
Instalación e configuración dun proxy nun equipamento ou nun servidor (CA5.9).

4.9.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
9	Lexislación e normativa sobre seguridade informática	7

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

Resultado de aprendizaxe do currículo	Completo
RA6 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e analiza as repercusións do seu incumprimento.	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 Describiuse a lexislación sobre protección de datos de carácter persoal.
CA6.2 Determinouse a necesidade de controlar o acceso á información persoal almacenada.
CA6.3 Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.
CA6.4 Contrastouse a obriga de pór ao dispor das persoas os datos persoais que lles atinxen.
CA6.5 Describiuse a lexislación sobre os servizos da sociedade da información e o comercio electrónico.
CA6.6 Contrastáronse as normas sobre xestión de seguridade da información.
CA6.7 Comprendeuse a necesidade de coñecer e respectar a normativa aplicable.

4.9.e) Contidos

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

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

Para proceder á avaliación do alumnado a información referirase aos obxectivos establecidos nesta programación didáctica e aos progresos e dificultades detectados na consecución dos mesmos.

-Mínimos esixibles:
Valorar a importancia de asegurar a privacidade, a coherencia e a dispoñibilidade da información nos sistemas informáticos.
Diferenciar entre seguridade física e lóxica.
Establecer políticas de contrasinais.
Valorar as vantaxes de sistemas biométricos.
Implantar sistemas de almacenamento redundante.
Coñecer a criptografía simétrica e asimétrica e realizar cifrados e descrifrados empregando estas técnicas.
Instalar un certificado dixital.
Coñecer as principais ameazas lóxicas dun sistema informático.
Aplicar medidas de protección no sistema e na rede.
Realizar unha auditoría do sistema informático.
Instalar e empregar redes privadas virtuais.
Instalar e configurar un cortalumes.
Instalar e configurar un proxy.
Comprender e aplicar a LOPD e a LSSI nun sistema informático.

* CRITERIOS DE CUALIFICACIÓN

A avaliación da parte teórica e procedimental efectuarase mediante probas obxectivas escritas e as actividades prácticas empregando o ordenador de clase. Tanto as probas escritas como as prácticas serán cualificadas de 0 a 10.

Doutra banda, os alumnos poderán incrementar a nota final de cada avaliación ata nun punto, mediante actividades de ampliación que serán propostas nas unidades de traballo. Estas non serán obrigatorias e terán un carácter eminentemente práctico e de investigación.

O alumnado deberá superar os mínimos exixidos en cada unidades para obter unha avaliación positiva na mesma. De non superarse todos os criterios mínimos esixibles a nota máxima será un 4.

A nota da primeira avaliación será a media ponderada das 3 primeiras unidades. No caso de non superar algunha unidade didáctica a nota máxima da primeira avaliación será un 4.

A nota final do módulo será a media aritmética ponderada de todas as unidades didácticas. No caso de non superar algunha unidade didáctica a nota máxima do módulo será un 4.

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

En caso de non aprobar unha avaliación, suministraránselles actividades de recuperación relacionadas coas capacidades terminais que o

alumnado non consiga adquirir. Ademais, deberá realizar unha proba de recuperación individual e escrita, que permita recuperar o resto dos contidos procedementais e os conceptuais non superados.

En caso de non recuperar a avaliación mediante o proceso anterior, o alumnado deberá someterse de forma individual a unha proba de avaliación final que se realizará ao final do curso. Esta englobará a totalidade dos criterios de avaliación non superados polo alumnado.

O alumno estará sempre informado sobre a forma de avaliar, os criterios de avaliación, e os coñecementos que se van a analizar.

Para o alumnado que non acceda á FCT por non ter superado o módulo na convocatoria ordinaria, terá un período destinado a súa recuperación que coincidirá co periodo destinado á FCT no último trimestre do curso (abril-xuño).

Para isto o profesor daralle as indicacións oportunas e establecerá unhas horas de titoría, se ten dispoñibilidade, no seu horario semanal nas que solucionar as dúbidas que ao alumno lle poidan xurdir.

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

Os instrumentos de avaliación que se empregarán son os seguintes:
* Proba escrita: constará de cuestións, problemas e outras tarefas a desenvolver de forma escrita, da mesma natureza e, o menos, da mesma complexidade cas desenvolvidas ao longo do curso académico polo alumnado avaliado de forma continua, dos contidos desenvolvidos nas diferentes unidades didácticas do módulo.
* Proba práctica: constará de tarefas e preguntas da mesma natureza e, o menos, da mesma complexidade cas desenvolvidas ao longo do curso académico polo alumnado de forma continua, dos 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 aritmética das puntuacións obtidas en cada proba escrita e práctica, valorándose a proba escrita un 40% e a proba práctica un 60%.
Poderanse realizar as probas en días distintos debido a imposibilidade de realizalas nun mesmo día. As probas poderán durar ata 5 horas cada unha de elas. Se lle comunicarán ao interesado ou interesada as datas e horas das probas coa debida antelación.

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

Ao 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 desenvolvemento de dito proceso, os logros e debilidades dos resultados obtidos a través das distintas fontes e instrumentos de avaliación (observacións, diarios, 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, o rendemento 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, o entorno, a situación previa, a fin de adecuar estratéxicamente o

proceso de ensino-aprendizaxe, introducir adaptacións na programación do módulo, una vez coñecida a realidade dos alumnos e adoptaroutro 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 que mediante as actividades propostas durante as primeiras semanas do inicio curso 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 iso 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 ao longo da vida.
* Explicar ao 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 relacións entre o alumnado 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

Tódalas 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.

Por mor da Covid-19 estas actividades estarán suxeitas a normativa sanitaria vixente en cada momento.

10.Outros apartados

10.1) Acceso á programación

A programación debe ser un documento público e accesible por calquera persoa que requira consuntala. Esta programacíon estará accesible cunha copia impresa que se gardará para a consulta na conserxería do centro.

10.2) Ensino semipresencial e telemático

Para o proceso de ensino-aprendizase vaise utilizar a aula virtual do instituto tanto para a docencia presencial, como para a docencia semipresencial ou a distancia no caso de que fora necesaria.

Na aula virtual estarán a disposición do alumnado todos os recursos e actividades deseñadas para acadar os obxectivos do módulo. Ao ser a plataforma empregada a diario nas clases presenciais, ante calquera cambio de modalidade o alumnado estará familiarizado con esta, o que facilitará a adaptación a nova circunstancia.

Na aula virtual colgarase un diario que permitirá o seguemento do alumnado por parte dos alumnos que non poidan acudir á clase presencial.

Además da aula virtual, no caso de non poder facer as clases presenciais, o ensino apoiarase co uso dos foros, chats e mensaxería dispoñibles no curso, de videoconferencias e do espazo abalar para garantizar a comunicación co alumnado.

O alumnado deberá ter instaladas na súa casa as ferramentas necesarias para facer as tarefas correspondentes as distintas Uds.

As probas de avaliación será presenciales, salvo casos excepcionais.