1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
15021482	San Clemente	Santiago de Compostela	2023/2024

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	2023/2024	6	140	168

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

Profesorado responsable

Profesorado asignado ao módulo	SONIA MARÍA OTERO FERNÁNDEZ
Outro profesorado	

Estado: Pendente de supervisión inspector

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

O desenrolo 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 desenrolan en canto a espazos,
instalacións, alumnado, 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 identificar técnicas e prácticas de tratamento seguro da información, recoñecendo e valorando a súa importancia en distintos contornos de traballo que manexen diferentes sistemas operativos.
Dáselle ó módulo unha orientación fundamentalmente práctica, usando as ferramentas software máis utilizadas hoxe en día nas empresas do entorno, de maneira que os alumnos adquiran os coñecementos adecuados ás características do ámbito produtivo.

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.	Explicación dos conceptos básicos da seguridade informática.	20	10
2	Seguridade no entorno físico	Comprender a importancia da seguridade no entorno físico.	30	18
3	Seguridade no hardware. Almacenamento e recuperación dos datos	Xestionar dispositivos de almacenamento describindo os procedementos efectuados e aplicando técnicas para asegurar a integridade da información.	31	19
4	Sistemas de identificación. Criptografía	Asegurar a privacidade da información transmitida en redes informáticas describindo vulnerabilidades e instalando software específico. Coñecer o concepto de criptografía e comprender o funcionamento das suas diferentes técnicas.	31	19
5	Ameazas e seguridade do software	Recoñecer e valorar incidencias, determinando as suas causas e describindo as accions correctoras para resolvelas.	28	17
6	Redes seguras	Recoñecer e analizar cambios tecnolóxicos para elexir novas alternativas e manterse actualizado dentro do sector.	28	17

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Introdución á seguridade informática.	20

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
RA2 - Aplica medidas de seguridade pasiva en sistemas informáticos, recoñecendo as necesidades de acordo coas características do contorno.	NO
RA6 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e analiza as repercusións do seu incumprimento.	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.
CA2.6 Valorouse a importancia de establecer unha política de contrasinais.
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.
CA6.5 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.

4.1.e) Contidos

Contidos
Seguridade física e lóxica. Políticas de seguridade. 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.

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Seguridade no entorno físico	30

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
RA2 - Aplica medidas de seguridade pasiva en sistemas informáticos, recoñecendo as necesidades de acordo coas características do contorno.	NO
RA3 - Xestiona dispositivos de almacenaxe aplicando os procedementos e as técnicas adecuadas para asegurar a integridade da información.	NO
RA5 - Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico.	NO
RA6 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e analiza as repercusións do seu incumprimento.	NO

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

Criterios de avaliación
CA1.1 Valorouse a importancia de manter a información segura.
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.
CA2.6 Valorouse a importancia de establecer unha política de contrasinais.
CA2.7 Valoráronse as vantaxes do uso de sistemas biométricos.
CA3.1 Interpretouse a documentación técnica relativa á política de almacenaxe.
CA5.1 Identificouse a necesidade de inventariar e controlar os servizos de rede.
CA6.1 Describiuse a lexislación sobre protección de datos de carácter persoal.

4.2.e) Contidos

Contidos
Políticas de seguridade.
Localización e protección física dos equipamentos e dos servidores.
Auditorías de seguridade.
Manual de seguridade e plans de continxencia.
Lexislación sobre os servizos da sociedade da información e o correo electrónico.
Normas ISO sobre xestión de seguridade da información.

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Seguridade no hardware. Almacenamento e recuperación dos datos	31

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.	NO
RA3 - Xestiona dispositivos de almacenaxe aplicando os procedementos e as técnicas adecuadas para asegurar a integridade da información.	SI
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
CA2.3 Verificouse o funcionamento dos sistemas de alimentación ininterrompida.
CA2.4 Seleccionáronse os puntos de aplicación dos sistemas de alimentación ininterrompida.
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.
CA3.5 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.
CA3.8 Identificáronse as características dos medios de almacenaxe remotos e extraíbles.
CA3.9 Utilizáronse medios de almacenaxe remotos e extraíbles.
CA3.10 Creáronse e restauráronse imaxes de respaldo de sistemas en funcionamento.
CA4.7 Aplicáronse técnicas de recuperación de datos.

4.3.e) Contidos

Contidos
Sistemas de alimentación ininterrompida. Almacenaxe da información: rendemento, dispoñibilidade e accesibilidade. Almacenaxe redundante e distribuída. Almacenaxe remota e extraíble.

Contidos
Copias de seguridade e imaxes de respaldo. Medios de almacenaxe.

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Sistemas de identificación. Criptografía	31

4.4.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
RA2 - Aplica medidas de seguridade pasiva en sistemas informáticos, recoñecendo as necesidades de acordo coas características do contorno.	NO

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

Criterios de avaliación
CA1.4 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.).
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.

4.4.e) Contidos

Contidos
Criptografía. Sistemas biométricos de identificación. Identificación dixital: sinatura electrónica e certificado dixital.

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Ameazas e seguridade do software	28

4.5.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.	NO
RA4 - Aplica mecanismos de seguridade activa atendendo ás necesidades do sistema informático.	NO
RA5 - Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico.	NO
RA6 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e analiza as repercusións do seu incumprimento.	NO

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

Criterios de avaliación
CA2.6 Valorouse a importancia de establecer unha política de contrasinais.
CA4.1 Seguíronse plans de continxencia para actuar ante fallos de seguridade.
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.
CA4.4 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.
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.
CA5.7 Describíronse e utilizáronse sistemas de identificación como a sinatura electrónica, o certificado dixital, etc.
CA6.4 Contrastouse a obriga de pór ao dispor das persoas os datos persoais que lles atinxen.

4.5.e) Contidos

Contidos
Política de contrasinais. Recuperación de datos.

Contidos
Monitorización de sistemas.
Software malicioso: clasificación. Ferramentas de protección e desinfección.
Actualización de sistemas e aplicacións.
Métodos para asegurar a privacidade da información transmitida.
0Análise dos rexistros (logs) dun sistema para identificar ataques reais ou potenciais á seguridade.
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.
Utilización de devasas (firewalls) en equipamentos e en servidores.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Redes seguras	28

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
RA6 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e analiza as repercusións do seu incumprimento.	NO

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

Criterios de avaliación
CA5.8 Instalouse e configurouse unha devasa (firewall) nun equipamento ou nun servidor.
CA6.6 Contrastáronse as normas sobre xestión de seguridade da información.
CA6.7 Comprendeuse a necesidade de coñecer e respectar a normativa aplicable.

4.6.e) Contidos

Contidos
Listas de control de acceso. Sistemas de seguridade nas telecomunicacións: correo, www, ftp, p2p, etc. Publicidade e correo non desexados. Utilización de devasas (firewalls) en equipamentos e en servidores.

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

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

Existen tres sesións de avaliación onde se emitirá unha nota (con cifras enteiras do 1 ao 10) segundo os pesos de avaliación expresados para cada unidade didáctica e os seus contidos.

Para o cálculo da nota terase en conta:

1. Proba de avaliación, que poderá ser escritas ou prácticas co ordenador: probas individuais acerca dos contidos estudados nunha ou varias unidades didácticas. Poden conter preguntas teóricas de tipo test, respostas curtas ou desenvolvemento, así como esixir a resolución de exercicios e supostos prácticos, podendo estes ser realizados en papel ou no ordenador. (90% da nota).

2. Entrega das tarefas propostas na aula virtual. (10% da nota). Tódalas tarefas propostas deberán ser entregadas en tempo e forma, asi coma ter o calificativo de APTAS pra poder ser avaliadas e formar parte do 10% da nota final.

A nota resultante en cada unha das avaliacións será a do redondeo matemático a un numero enteiro (do 1 ao 10) tras aplicar as porcentaxes descritas, sempre e cando se acade un mínimo de 5 nas probas ou proba de avaliación. De non ser o caso, a nota resultante será a da proba escrita. Para superar o módulo en cada avaliación é preciso obter unha nota resultante igual ou superior a 5.

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

Faise una media ponderada atendendo ao peso asignado a cada unha das UDs que se imparten en cada avaliación.

Pode requerirse para a preparación e organización das probas que o alumnado CONFIRME a intención de realizar éstas con polo menos con anterioridade de 48h á súa realización. De requerirse, e de non confirmarse por parte do alumno a súa participación nestas probas de avaliación, podería ter unha condición de NON APTO na proba de avaliación.

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

Ó tratarse dun módulo a distancia, o alumnado que non alcance os mínimos exixibles en cada unidade de traballo terá abertas as unidades didácticas na plataforma de formación a distancia.

Tamén terán á súa disposición os foros especificos onde poderán facer preguntas a través da mensaxería tanto ao profesorado coma a outros compañeiros e compañeiras.

Se o precisan e así o requiren, entregaránselle actividades de reforzo que incidan naqueles aspectos sobre os que atopen máis dificultades.

E como todo o resto do alumnado, terán as horas asinadas para titorías para a resolución das dúbidas, tanto de maneira presencial como telemática

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

Ao ser unha ensinanza a distancia non hai perda de dereito a avaliación continua e como tal non se contempla a existencia dunha proba extraordinaria.

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

Considerando que a programación é un documento que se elabora ao comezo do curso escolar estará sempre aberta a calquera modificación baseándonos en diferentes factores que se inclúen no proceso de ensinanza-aprendizaxe.
Avaliaremos os procesos de avaliación, técnicas e métodos, temporalización e momentos de aplicación, os recursos dos que dispoñemos e a metodoloxía.
Unidades didácticas
Máis polo miudo, ao remate de cada unidade didáctica analizaremos:
- contidos: na programación do vindeiro curso incluiranse novas actividades para aqueles contidos que supuxeron maior dificultade de aprendizaxe para o alumnado.
Engadiranse tamén os contidos de ampliación tratados, se houbo algún. Terase en conta tamén o cambio de aqueles contidos que se deciden impartir noutra unidade didáctica.
- actividades: eliminaranse da nova programación as actividades que non se realizaron por considerarse redundantes ou innecesarias, e incorporaranse todas as novas que o docente considerou necesarias para acadar os obxectivos da unidade, así como a modificación das xa existentes.
- recursos: na programación vindeira incluiranse os recursos empregados que non se tiveran en conta ao facer a programación actual. Aqueles non usados indicarase que son opcionais.
Se algún recurso necesario non se puido empregar por non existir no centro, solicitarase a súa compra nunha reunión de departamento. Na programación do curso seguinte comprobarase a dispoñibilidade dese recurso para incluílo ou non na mesma.
- metodoloxía: a metodoloxía empregada para o desenvolvemento de cada unidade didáctica traballo baséase principalmente na exposición por parte do docente da parte teórica e de exemplos de actividades, e a realización do alumnado de tarefas e traballos sobre os contidos expostos.
Se houbo algún cambio na metodoloxía que fixo que o alumnado acadase os obxectivos da UD de xeito máis doado, incorporarase á nova programación.
- temporalización: o número de sesións asignadas axustaranse ao tempo real empregado na unidade didáctica.
Avaliacións
Además, ao remate de cada trimestre, revisarase o proceso de avaliación, axustando o tipo e número de instrumentos de avaliación e en consecuencia as porcentaxes e xeito de calcular as cualificacións parciais e final.

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

Terase en conta que a lexislación vixente indica explicitamente que a metodoloxía (flexible, adaptada as circunstancias persoais e favorecedora do autoaprendizaxe) a utilizar (e polo tanto, enténdese por extensión que a programación didáctica) ha de ser acorde ás circunstancias persoais do

alumnado que asiste ó réxime de formación a distancia.
O procedemento para a realización da avaliación inicial será o que segue:
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. Realización dunha sesión de avaliación inicial (preceptiva) conxunta co equipo docente á luz da antedita información e calquera outra que xurda na reunión.
Elaboración dun informe de orientación individual e posibles medidas de atención a diversidade para o alumnado que se estime que o precisa para o correcto seguimento das actividades formativas. O equipo docente do ciclo acorda que se pode ampliar a data de entrega de tarefas e realización de exames en Platega segundo a dispoñibilidade de tempo do alumnado o requira.

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

As medidas de reforzo educativo serán sempre consensuadas co resto do equipo docente do ciclo e o coordinador da informática a distancia e serán personalizadas para as necesidades detectadas para un alumno ou alumna. Incluirán:
Eliminación, adaptación ou reelaboración de certas actividades de ensino aprendizaxe que presenten especial dificultade por parte do discente.
Proposta de repetir, baixo supervisión directa do profesor, certas actividades especialmente problemáticas.
Aumento do prazo de entrega de tarefas e da realización dos exames en Platega.
Calquera outra que poda axudar a que a alumna/o responda globalmente aos obxectivos programados.

9. Aspectos transversais

9.a) Programación da educación en valores

Tendo en conta que unha das nosas metas e a formación integral dos alumnos/as, 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, respecto a Lei de protección de datos de carácter persoal, 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 virtual.
Educación do consumidor: Hai diversidade de empresas de informática e diversidade de produtos de software. 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 con criterio.

9.b) Actividades complementarias e extraescolares

As actividades extraescolares para este módulo son as mesmas que as que se propoñan polo departamento de informática para todo o alumnado, así como aquelas que podan ser de interese promovidas polo centro. Todas estas actividades serán informadas na Web do centro.