



1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
36019669	Armando Cotarelo Valledor	Vilagarcía de Arousa	2024/2025

Ciclo formativo

Código da familia profesional	Familia profesional	Código do ciclo formativo	Ciclo formativo	Grao	Réxime
IFC	Informática e comunicacións	CE3IFC005000	Ciberseguridade en contornos das tecnoloxías da información	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
MP5025	Hacking ético	2024/2025	5	120	144

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

Profesorado responsable

Profesorado asignado ao módulo	GUSTAVO ADOLFO IGLESIAS BELLO
Outro profesorado	

Estado: Pendente de supervisión equipo directivo



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 Armando Cotarelo Valledor e o ámbito produtivo da súa zona de influencia.

Os alumnos aos que está destinado pertencen ó curso de Especialización E3IFC005000 - LOOIFP | Ciberseguridade en contornos das tecnoloxías da información, que segue o Real Decreto 479/2020, de 7 de abril do currículo do Curso de especialización en ciberseguridade en contornos das tecnoloxías da información.

A competencia xeral deste curso de especialización consiste en definir e implementar estratexias de seguridade nos sistemas de información realizando diagnósticos de ciberseguridade, identificando vulnerabilidades e implementando as medidas necesarias para mitígalas aplicando a normativa vixente e estándares do sector, seguindo os protocolos de calidade, de prevención de riscos laborais e respecto ambiental.

As ocupacións e postos de traballo máis relevantes son os seguintes:

- * Experto en ciberseguridade.
- * Auditor de ciberseguridade.
- * Consultor de ciberseguridade.
- * Hacker ético.

- A formación do módulo contribúe a alcanzar os seguintes obxectivos xerais:

- * Combinar técnicas de hacking ético interno e externo para detectar vulnerabilidades que permitan eliminar e mitigar os riscos asociados.
- * Revisar e actualizar procedementos de acordo con normas e estándares actualizados para o correcto cumprimento normativo en materia de ciberseguridade e de protección de datos persoais.
- * Desenvolver manuais de información, utilizando ferramentas ofimáticas e de deseño asistido por computador para elaborar documentación técnica e administrativa.
- * Analizar e utilizar os recursos e oportunidades de aprendizaxe relacionados coa evolución científica, tecnolóxica e organizativa do sector e as tecnoloxías da información e a comunicación, para manter o espírito de actualización e adaptarse a novas situacións laborais e persoais.
- * Desenvolver a creatividade e o espírito de innovación para responder os retos que se presentan nos procesos e na organización do traballo e da vida persoal.
- * Avaliar situacións de prevención de riscos laborais e de protección ambiental, propoñendo e aplicando medidas de prevención persoais e colectivas, de acordo coa normativa aplicable nos procesos de traballo, para garantir contornas seguras.
- * Identificar e propoñer as accións profesionais necesarias para dar resposta á accesibilidade universal e ao «deseño para todas as persoas».
- * Identificar e aplicar parámetros de calidade nos traballos e actividades realizados no proceso de aprendizaxe, para valorar a cultura da avaliación e da calidade e ser capaces de supervisar e mellorar procedementos de calidade.

- A formación do módulo contribúe a alcanzar as seguintes competencias profesionais, persoais e sociais:

- * Detectar vulnerabilidades en sistemas, redes e aplicacións, avaliando os riscos asociados.
- * Elaborar documentación técnica e administrativa cumprindo coa lexislación vixente, respondendo os requisitos establecidos.
- * Adaptarse ás novas situacións laborais, mantendo actualizados os coñecementos científicos, técnicos e tecnolóxicos relativos á súa contorna profesional, xestionando a súa formación e os recursos existentes



na aprendizaxe ao longo da vida.

* Resolver situacións, problemas ou continxencias con iniciativa e autonomía no ámbito da súa competencia, con creatividade, innovación e espírito de mellora no traballo persoal e no dos membros do equipo.

* Xerar contornas seguras no desenvolvemento do seu traballo e o do seu equipo, supervisando e aplicando os procedementos de prevención de riscos laborais e ambientais, de acordo co establecido pola normativa e os obxectivos da organización.

* Supervisar e aplicar procedementos de xestión de calidade, de accesibilidade universal e de «deseño para todas as persoas», nas actividades profesionais incluídas nos procesos de produción ou prestación de servizos.

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	Introducción ao Hacking Ético		15	5
2	Recopilación da información (Footprinting)		25	15
3	Enumeración dos servizos (Fingerprinting)		25	15
4	Hacking de aplicacións Web		25	15
5	Hacking de redes y sistemas informáticos		22	20
6	Mantemento do acceso, escalada de privilegios y pivotaxe		17	15
7	Hacking de redes inalámbricas		15	15

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Introducción ao Hacking Ético	15



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

Resultado de aprendizaxe do currículo	Completo
RA1 - Determina ferramentas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético	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 Definiuse a terminoloxía esencial do hacking ético
CA1.2 Identificáronse os conceptos éticos e legais fronte ao cibercrimo
CA1.3 Definíronse o alcance e as condicións dun test de intrusión
CA1.4 Identificáronse os elementos esenciais de seguridade: confidencialidade, autenticidade, integridade e dispoñibilidade
CA1.5 Identificáronse as fases dun ataque seguidas por un atacante
CA1.6 Analizáronse e definíronse os tipos vulnerabilidades
CA1.7 Analizáronse e definíronse os tipos de ataque
CA1.8 Determináronse e caracterizáronse as vulnerabilidades existentes

4.1.e) Contidos

Contidos
Elementos esenciais do hacking ético.
Diferenzas entre hacking, hacking ético, tests de penetración e hacktivismo.
Recolección de permisos e autorizacións previas a un test de intrusión.
Auditorías de caixa negra e de caixa branca.
Documentación de vulnerabilidades.



4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Recopilación da información (Footprinting)	25

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Determina ferramentas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético	NO

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

Criterios de avaliación
CA1.9 Determináronse as ferramentas de monitorización adecuadas dispoñibles no mercado en función do tipo de organización

4.2.e) Contidos

Contidos
ClearNet, Deep Web, Dark Web, Darknets. Coñecemento, diferenzas e ferramentas de acceso: Tor. ZeroNet; FreeNet.
Fase de recoñecemento (footprinting).

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Enumeración dos servizos (Fingerprinting)	25

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

Resultado de aprendizaxe do currículo	Completo
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO
RA3 - Ataca e defende redes e sistemas en contornos de proba, e consegue acceso a información e a sistemas de terceiros	NO



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

Criterios de avaliación
CA2.7 Realizáronse informes sobre as vulnerabilidades detectadas
CA3.1 Compilouse información sobre a rede e sobre sistemas obxectivo mediante técnicas pasivas

4.3.e) Contidos

Contidos
Clasificación de ferramentas de seguridade e hacking.
Análise e colleita de datos en redes sen fíos.
Fase de escaneo (fingerprinting).

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Hacking de aplicacións Web	25

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

Resultado de aprendizaxe do currículo	Completo
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO
RA3 - Ataca e defende redes e sistemas en contornos de proba, e consegue acceso a información e a sistemas de terceiros	NO
RA5 - Ataca e defende aplicacións web en contornos de proba, e consegue acceso a datos ou funcionalidades non autorizadas	SI



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

Criterios de avaliación
CA2.6 Utilizáronse técnicas de ?equipo vermello e azul?
CA3.1 Compilouse información sobre a rede e sobre sistemas obxectivo mediante técnicas pasivas
CA5.1 Identifícaronse os sistemas de autenticación web, destacando as súas debilidades e as súas fortalezas
CA5.2 Realizouse un inventario de equipamentos, protocolos, servizos e sistemas operativos que proporcionan o servizo dunha aplicación web
CA5.3 Analizouse o fluxo das interaccións realizadas entre o navegador e a aplicación web durante o seu uso normal
CA5.4 Examináronse manualmente aplicacións web na procura das vulnerabilidades máis habituais
CA5.5 Usáronse ferramentas de procuras e explotación de vulnerabilidades web
CA5.6 Realizouse a procura e a explotación de vulnerabilidades web mediante ferramentas software

4.4.e) Contidos

Contidos
ClearNet, Deep Web, Dark Web, Darknets. Coñecemento, diferenzas e ferramentas de acceso: Tor. ZeroNet; FreeNet.
Fase de recoñecemento (footprinting).
Fase de escaneo (fingerprinting).
Monitorización de tráfico.
Manipulación e inxección de tráfico.
Negación de credenciais en aplicacións web.
Colleita de información.
Automatización de conexións a servidores web (exemplo: Selenium).



Contidos
Análise de tráfico a través de proxies de intercepción. Procura de vulnerabilidades habituais en aplicacións web. Ferramentas para a explotación de vulnerabilidades web.

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Hacking de redes y sistemas informáticos	22

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

Resultado de aprendizaxe do currículo	Completo
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO
RA3 - Ataca e defende redes e sistemas en contornos de proba, e consegue acceso a información e a sistemas de terceiros	SI

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 Utilizáronse técnicas de ?equipo vermello e azul?
CA3.1 Compilouse información sobre a rede e sobre sistemas obxectivo mediante técnicas pasivas
CA3.2 Creouse un inventario de equipamentos, contas de usuario e potenciais vulnerabilidades da rede e sistemas obxectivo, mediante técnicas activas
CA3.3 Interceptouse tráfico de rede de terceiros para procurar información sensible
CA3.4 Realizouse un ataque de intermediario lendo, inserindo e modificando a vontade o tráfico intercambiado por dous extremos remotos
CA3.5 Comprometéronse sistemas remotos explotando as súas vulnerabilidades



4.5.e) Contidos

Contidos
Fases do hacking. Modo infraestrutura, ad-hoc e monitor. Monitorización de tráfico. Interceptación de comunicacións utilizando distintas técnicas. Manipulación e inxección de tráfico. Ferramentas de procura e explotación de vulnerabilidades. Enxeñaría social. Phising. Escalada de privilexios.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Mantemento do acceso, escalada de privilegios y pivotaxe	17

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

Resultado de aprendizaxe do currículo	Completo
RA4 - Consolida e utiliza sistemas comprometidos garantindo accesos futuros	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 Administráronse sistemas remotos a través de ferramentas de liña de comandos
CA4.2 Comprometéronse contrasinais a través de ataques de dicionario, táboas rainbow e forza bruta contra as súas versións encriptadas



Criterios de avaliación
CA4.3 Accedeuse a sistemas adicionais a través de sistemas comprometidos
CA4.4 Instaláronse portas traseiras para garantir accesos futuros aos sistemas comprometidos

4.6.e) Contidos

Contidos
Administración de sistemas de maneira remota. Ataques e auditorías de contrasinais. Pivotaxe na rede. Instalación de portas traseiras con troianos (RAT, Remote Access Trojan).

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Hacking de redes inalámbricas	15

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

Resultado de aprendizaxe do currículo	Completo
RA2 - Ataca e defende comunicacións sen fíos en contornos de proba, e consegue acceso a redes para demostrar as súas vulnerabilidades	NO

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

Criterios de avaliación
CA2.1 Configúranse os modos de funcionamento das tarxetas de rede sen fíos
CA2.2 Descríbense as técnicas de encriptación das redes sen fíos e os seus puntos vulnerables



Criterios de avaliación
CA2.3 Detectáronse redes sen fíos e capturouse tráfico de rede como paso previo ao seu ataque
CA2.4 Accedeuse a redes sen fíos vulnerables
CA2.5 Caracterizáronse outros sistemas de comunicación sen fíos e as súas vulnerabilidades

4.7.e) Contidos

Contidos
Comunicación sen fíos. Análise e colleita de datos en redes sen fíos. Técnicas de ataque e exploración de redes sen fíos. Ataques a outros sistemas sen fíos. Realización de informes de auditoría e presentación de resultados.

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

Mínimos exixibles:

Os mínimos exixibles de cada unidade son os estipulados no apartado 4c desta programación.

Cotas de nota

A cota máxima que é posibel acadar en calqueira calificación é de 10.

As tarefas, traballos, actividades e/ou probas de calqueira índole avaliable, e con obriga de presentación, se non se fixera a devandita actividade e/ou probas, permancerá coma "non presentado", co a cualificación de 0 a efectos de cálculos de avaliación.

En todos os casos, a avaliación final mínima será de "1", advertindo que a cualificación de "0" utilizarase pra os caulculos de medias parciais.

Superación de cada unidade:



-Para cada unidade didáctica realizaranse unha serie de actividades, traballos e/ou probas de calquera índole para avaliar os coñecementos adquiridos polo alumnado, tal como se recolle no apartado 4 desta programación.

-A realización de cada unha das actividades, tarefas ou traballos que non teñan carácter de obriga, axuda a obtención da nota global. Non entregar algunha, non terá implicacións pra superar a unidade, pero terase en conta que as actividades son o 20% da nota da unidade.

-As entregas terán que facerse dentro do prazo estipulado, de non ser así, contará como non entregado.

-Cando se realicen probas teórico-prácticas, estas son de obrigada realización e terán, en conxunto (por se fose mais de unha), un peso do 80% na nota da unidade; o 20% restante da nota da unidade, pertence as chamadas actividades, traballos ou prácticas-laboratorios, non sendo estas de obrigado cumprimento. As probas exame teórico-prácticas poderán incluír unha unidade ou varias.

-De non superar unha ou varias avaliacións, esta/s terá/n que ser recuperada/s nas datas estipuladas polo docente, no exame final do curso.

Traballos, actividades, tarefas ou prácticas (20% da nota):

-A nota dos traballos será individual, e o alumnado deberá defendelos ante o docente respondendo unha serie de cuestións referentes as partes do mesmo. A nota de cada parte depende das respostas dadas e, de non ser respondidas correctamente, dita parte pode ser considerada como non superada.

Superación de cada avaliación:

-Para a nota da avaliación teranse en conta as notas das actividades impartidas nesa avaliación, xunto co proba/s-exame/s da avaliación.

-A nota de cada avaliación obterase: un 80% a proba/s exame/s en media ponderada distes (mínimo un 4,8 puntos [0-10] en cada proba para poder facer media ponderada) xunto co 20% das tarefas, actividades prácticas ou laboratorios incluídos na avaliación. Dita ponderación é a estipulada no apartado 3 desta programación.

Autoría de actividades, tarefas, probas ou traballos:

-calesqueira das probas/traballos/tarefas/actividades a realizar por os alumnos ou as alumnas, ben sexan teóricas ou prácticas e actividades na casa, etc. poderá ser verificada a autoría das mesmas por parte do profesor en calquera momento da celebración ou realización da proba/traballo/tarefa/actividade ou ben con posterioridade a ésta. Se o resultado é copia ou falsificación ou calquera outro método de suplantación da autoría (uso de ferramentas de intelixencia artificial non autorizadas, ferramentas de internet non autorizadas, etc) a nota global da proba/traballo/tarefa/actividade será a nota mínima da mesma.

Superación do módulo:

-A nota final do módulo será a nota ponderada de todas as unidades didácticas seguindo os pesos estipulados no apartado 3 desta programación.

De detectarse calquer comportamento incorrecto como copiar traballos, actividades, tarefas ou probas: contará/n como non superada/s, e o alumno terá que recuperala; se fose unha proba teórico-práctica, o exercicio será anulado acadando a calificación de 0 no mesmo.

O docente pode esixir a defensa total ou parcial de calquera actividade mediante unha serie de preguntas individuais. De non ser respondidas correctamente, a actividade, tarefa, práctica, proba ou exercicio (no caso das probas teórico-prácticas) pode ser considerada como non superada, obtendo a calificación de 0.



6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

Recuperación durante o curso:

O alumnado que non supere algunha das avaliacións, poderá optar a recuperala no exame final do curso nas datas estipuladas polo docente.

No caso de ter non superada algunha avaliación e ter tamén nesa avaliación, algunha actividade ou traballo suspenso ou non entregado, o alumnado poderá que realizar a entrega dos mesmos no prazo estipulado polo docente e sempre antes das probas do exame final nas datas estipuladas polo docente.

A nota será calculada seguindo os mesmos criterios establecidos no apartado 5 desta programación, cambiando a nota anterior da proba, actividade ou traballo pola nota da recuperación se esta é maior ca anterior.

Exame final:

O alumnado que non supere algunha das unidades do módulo fará unha proba teórico-práctica de recuperación. Dita proba estará dividida por avaliacións ven diferenciadas.

A nota final do módulo será a nota ponderada de todas as unidades didácticas seguindo os pesos estipulados no apartado 3 desta programación.

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

Para superar o módulo deberán someterse a unha proba final antes da avaliación de xuño. Dita proba será teórico-práctica e estará dividida por avaliacións ven diferenciadas que terá que superar cun mínimo de 5 sobre 10 en cada unha delas.

A nota final será calculada seguindo a ponderación estipulada no apartado 3 desta programación.

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

O seguimento da programación realizarase na aplicación web da Xunta para as programacións.

No que respecta a avaliación da programación, esta se avaliará mediante os seguintes procedementos:

-En reunións de equipo docente, de departamento e xuntas de avaliación, ao longo do curso, nas que se realizará o seguimento e control da programación, tomando as medidas oportunas se fose o caso.

-Memoria fin de curso, na que, entre outros temas, se recolle a porcentaxe da programación impartida e as causas de non impartir o previsto, así coma a realización de modificacións na mesma e as propostas de mellora para o seguinte curso académico.



8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

Ao comezo do módulo farase unha proba escrita e/ou oral ao alumnado que conterá cuestións sinxelas sobre aspectos que se desenvolverán ao longo do módulo, así como información xeral da formación do alumnado. Esta proba permitirá avaliar os coñecementos previos que o alumnado poda ter sobre o contido que se verá no módulo co fin de adaptar o proceso de ensino-aprendizaxe á realidade do grupo.

Esta proba non terá asociada unha nota, senón que servirá soamente para facer unha valoración dos coñecementos iniciais que ten o alumnado. Tamén se levará a cabo ao longo das actividades que se desenvolverán ao longo das primeiras semanas, unha observación detallada do comportamento, actitudes e aptitudes do alumnado.

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

Para o alumnado que teña dificultades e/ou non acade os mínimos realizaranse actividades de reforzo e faranse explicacións individuais na titoría presencial se o precisase e así o solicitare a alumna ou alumno.

Cos alumnos cunha maior capacidade de aprendizaxe, programaranse actividades adicionais, de maior dificultade, incluíndo conceptos, tecnoloxías e ferramentas que non entran dentro desta programación pero que complementan o módulo. Estas actividades poden estar guiadas ou ter un carácter de descubrimento e investigación autónoma pola súa parte.

Para os alumnos que presenten algunha discapacidade, seguiranse as directrices que facilite o departamento de orientación para cada caso individual.

9. Aspectos transversais

9.a) Programación da educación en valores

No ámbito da informática é moi común que se traballe en equipo, polo que é necesario fomentar unha serie de valores para que o alumnado teña unha relación profesional sana cos seus actuais e futuros compañeiros.

Por isto, ademais dos coñecementos propios do módulo, teranse en conta aspectos máis persoais, actitudes, normas e técnicas para o desenvolvemento integral da persoa. Estes valores serán tratados de forma transversal durante todo o curso sempre que sexa posible nesta impartida a distancia.

Traballo en equipo e colaboración, durante todo o curso sempre que sexa posible nesta modalidade impartida a distancia:

- Promoverase o traballo colaborativo, en equipo, onde cada un aporta o que sabe, de tal forma que o alumnado resolva as dúbidas dos demais e compartan os coñecementos adquiridos, tanto no módulo coma de fontes externas.

- Fomentarase a participación do alumnado nas explicacións mediante preguntas nos foros e preguntas nas titorías presenciais, para que perdan o medo a falar en grupo.



-Nas posibles actividades en grupo, fomentárase e prestarase especial atención ao reparto equitativo das tarefas e que se fagan por motivos de coñecementos, non por interese ou discriminación. En caso de detectar calquer problema ou alumnado que non colabora, tomaranse medidas para evitar que o resto do equipo se vexa afectado.

Convivencia:

- Cortárase de raíz calquer comentario, conversación ou frase que poida resultar ofensiva para unha persoa ou colectivo, xa sexa en broma ou non.
- Correxírase calquer tipo de conducta que poida resultar dañina física ou psicolóxicamente para outra persoa, grupo ou colectivo.
- Porase en coñecemento do equipo de orientación e responsables do centro calquer tipo de comportamento que haxa que controlar e se tomarán as medidas necesarias para correxilo.

Autonomía e aprendizaxe autónomo:

- Fomentárase a capacidade de cada alumno para buscar información na rede mediante traballos de investigación.
- Cando teñan que instalar algunha ferramenta ou tecnoloxía, remitírase ao manual oficial. Desta forma acostúmbanse a buscar e acceder a sitios oficiais.
- De cando en cando, diante do alumnado farase unha búsqueda na web dalgunha dúbida para acostumalos a realízalas eles o día de mañá.

Pensamento crítico e lóxico:

- Fomentárase a participación do alumnado na toma de decisións activa mediante actividades de elección libre e valoración de tecnoloxías e ferramentas dende distintos puntos de vista.

Boas prácticas:

- Correxíranse todas aquelas malas prácticas de programación que se detecten, ofrecendo alternativas máis óptimas.
- Promóvese a reutilización de código, uso de métodos auxiliares e utilidades do propio linguaxe que facilitan a programación e lexibilidade.
- Fomentárase a documentación do código, tanto interna como externa.
- Deixáranse de lado tecnoloxías obsoletas explicando as razóns polas que non se usan, para que o alumnado comprenda ditas razóns.

Seguridade:

- En toda actividade térase en conta a normativa vixente en protección de datos para o tratamento correcto dos datos manexados.
- Teráse en conta a seguridade e os problemas que poidan acarrear o uso de certas tecnoloxías e, na medida do posible evítanse as obsoletas ou inseguras.

Inglés:

- Posto que a maioría da documentación atópase neste idioma, fomentárase o aprendizaxe de dito idioma e mencionárase en inglés os nomes que sexan orixinais dese idioma.
- Se o alumnado non comprende o inglés, tradúcese diante del, para que vaia aprendendo certos conceptos.

Posto de traballo:



- O uso do ordenador nunha mala postura e a mala colocación dos periféricos pode acarrear problemas físicos, polo que intentarase corregir as malas posicións e incitarase a colocar correctamente o teclado e o rato para evitar dores e lesións.
- A colocación dos monitores tamén terase en conta, xa que pode acarrear problemas posturais.
- Ademais ao alumno váiselle valorar a organización do seu posto de traballo, que teña todo ordenado e o use para as cosas que debe.

9.b) Actividades complementarias e extraescolares

Realizaranse as actividades extraescolares acordadas no departamento e no centro durante o curso. Estas quedarán reflexadas na memoria do departamento e no Plan Xeral Anual do centro.

10.Outros apartados

10.1) Publicidade da programación

A programación daráselle a coñecer ao alumnado mediante a plataforma de educación a distancia utilizada ao longo do desenvolvemento do módulo. Desta forma, o alumnado terá dispoñible, en calquera momento, un enlace ao documento pdf coa programación de alumnado xerada pola aplicación de elaboración de programacións.