



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
MP5022	Bastionado de redes e sistemas	2024/2025	6	160	192

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

Profesorado responsable

Profesorado asignado ao módulo	JAVIER GARCIA RAJOY
Outro profesorado	

Estado: Pendente de supervisión equipo directivo

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

O módulo profesional MP5022: "Bastionado de redes e sistemas" adáptase ao contexto produtivo de Vilagarcía de Arousa, un entorno caracterizado pola presenza de sectores clave como o portuario, a loxística, o comercio e o turismo. Neste sentido, o currículo deste módulo debe enfocarse en proporcionar as competencias necesarias para garantir a seguridade das infraestruturas tecnolóxicas e redes de comunicación utilizadas nestes sectores estratéxicos.

Características destacadas do ámbito produtivo en Vilagarcía de Arousa:

Sector portuario e loxístico: A presenza dun porto de importancia no transporte marítimo require profesionais capacitados para bastionar redes e sistemas críticos empregados na xestión de mercadorías, control de tráfico marítimo e almacenamento.

Sector comercial e industrial: Empresas locais e multinacionais demandan solucións seguras para o intercambio de datos, control de accesos e protección fronte a ameazas cibernéticas.

Sector turístico: A crecente dixitalización dos servizos turísticos esixe garantir a seguridade das transaccións electrónicas, redes wifi públicas e bases de datos de clientes.

Adaptación do currículo:

Prácticas específicas: Deseño de infraestruturas seguras para redes en empresas loxísticas, portos e hoteis, simulación de ataques e resposta ante incidentes.

Colaboracións: Promover convenios con empresas locais e organismos públicos para a realización de proxectos reais de bastionado.

Enfoque tecnolóxico: Uso de ferramentas e estándares actuais, como sistemas de detección de intrusións (IDS/IPS), control de accesos e bastionado de servidores.

Sensibilización en ciberseguridade: Promover unha cultura de ciberseguridade adaptada ás necesidades dos sectores clave da rexión.

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	Diseño de planes de securización		28	14
2	Configuración de sistemas de control de acceso y autenticación de personas		27	14
3	Administración de credenciales de acceso a sistemas informáticos		27	14



U.D.	Título	Descrición	Duración (sesións)	Peso (%)
4	Diseño de redes de computadores seguras		27	14
5	Configuración de dispositivos y sistemas informáticos		27	14
6	Configuración de dispositivos para la instalación de sistemas informáticos		28	15
7	Configuración de los sistemas informáticos		28	15

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Diseño de planes de securización	28

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Deseña plans de securización incorporando boas prácticas para o bastionado de sistemas e redes	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 Identifícanse os activos, as ameazas e as vulnerabilidades da organización
CA1.2 Avaliáronse as medidas de seguridade actuais
CA1.3 Elaborouse unha análise de risco da situación actual en ciberseguridade da organización
CA1.4 Priorizáronse as medidas técnicas de seguridade para implantar na organización, tendo tamén en conta os principios da economía circular
CA1.5 Deseñouse e elaborouse un plan de medidas técnicas de seguridade para implantar na organización, apropiadas para garantir un nivel de seguridade adecuado en función dos riscos da organización



Criterios de avaliación
CA1.6 Identifícaronse as mellores prácticas con base en estándares, guías e políticas de securización adecuadas para o bastionado dos sistemas e das redes da organización

4.1.e) Contidos

Contidos
Análise de riscos. Principios da economía circular na industria 4.0. Plan de medidas técnicas de seguridade. Políticas de securización máis habituais. Guías de boas prácticas para a securización de sistemas e redes. Estándares de securización de sistemas e redes. Caracterización de procedementos, instrucións e recomendacións. Niveis, escalados e protocolos de atención a incidencias.

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Configuración de sistemas de control de acceso y autenticación de personas	27

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

Resultado de aprendizaxe do currículo	Completo
RA2 - Configura sistemas de control de acceso e autenticación de persoas preservando a confidencialidade e a privacidade dos datos	SI



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

Criterios de avaliación
CA2.1 Definíronse os mecanismos de autenticación con base en diversos factores (físicos, inherentes e baseados no coñecemento)
CA2.2 Definíronse protocolos e políticas de autenticación baseados en contrasinais e frases de paso, con base nas vulnerabilidades e nos tipos de ataques principais
CA2.3 Definíronse protocolos e políticas de autenticación baseados en certificados dixitais e tarxetas intelixentes, con base nas vulnerabilidades e nos tipos de ataques principais
CA2.4 Definíronse protocolos e políticas de autenticación baseados en tokens, OTP, etc., con base nas vulnerabilidades e nos tipos de ataques principais
CA2.5 Definíronse protocolos e políticas de autenticación baseados en características biométricas, segundo as vulnerabilidades e os tipos de ataques principais

4.2.e) Contidos

Contidos
Mecanismos de autenticación. Tipos de factores.
Autenticación baseada en distintas técnicas.

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Administración de credenciales de acceso a sistemas informáticos	27

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

Resultado de aprendizaxe do currículo	Completo
RA3 - Administra credenciais de acceso a sistemas informáticos aplicando os requisitos de funcionamento e seguridade establecidos	SI

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

Criterios de avaliación
CA3.1 Identifícanse os tipos de credenciais máis utilizados
CA3.2 Xeráronse e utilizáronse diferentes certificados dixitais como medio de acceso a un servidor remoto
CA3.3 Comprobase a validez e a autenticidade dun certificado dixital dun servizo web
CA3.4 Comparáronse certificados dixitais válidos e inválidos por diferentes motivos
CA3.5 Instalouse e configurouse un servidor seguro para a administración de credenciais tipo RADIUS (remote access dial in user service)

4.3.e) Contidos

Contidos
Xestión de credenciais. Infraestruturas de clave pública (PKI). Acceso por medio de sinatura electrónica. Xestión de accesos. Sistemas de xestión de acceso á rede NAC (network access control). Xestión de contas privilexiadas. Protocolos RADIUS e TACACS, servizo KERBEROS, etc.

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Diseño de redes de computadores seguras	27



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

Resultado de aprendizaxe do currículo	Completo
RA4 - Deseña redes de computadores tendo en conta os requisitos de seguridade	SI

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

Criterios de avaliación
CA4.1 Incrementouse o nivel de seguridade dunha rede local plana segmentándoa fisicamente e utilizando técnicas e dispositivos de enrutamento
CA4.2 Optimizouse unha rede local plana utilizando técnicas de segmentación lóxica (VLAN)
CA4.3 Adaptouse un segmento dunha rede local xa operativa utilizando técnicas de subnetting para incrementar a súa segmentación respectando os direccionamentos existentes
CA4.4 Configuráronse as medidas de seguridade adecuadas nos dispositivos que dan acceso a unha rede sen fíos (enrutadores, puntos de acceso, etc.)
CA4.5 Estableceuse un túnel seguro de comunicacións entre dúas sedes xeograficamente separadas

4.4.e) Contidos

Contidos
Segmentación de redes.
Subnetting.
Redes virtuais (VLAN).
Zona desmilitarizada (DMZ).
Seguridade en redes sen fíos (WPA2, WPA3, etc.).
Protocolos de rede seguros (IPSec, etc.).



4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Configuración de dispositivos y sistemas informáticos	27

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

Resultado de aprendizaxe do currículo	Completo
RA5 - Configura dispositivos e sistemas informáticos cumprindo os requisitos de seguridade	SI

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

Criterios de avaliación
CA5.1 Configúranse dispositivos de seguridade perimetral acordes a unha serie de requisitos de seguridade
CA5.2 Detectáronse erros de configuración de dispositivos de rede mediante a análise de tráfico
CA5.3 Identifícanse comportamentos non desexados nunha rede a través da análise dos rexistros (logs) dunha devasa
CA5.4 Puxéronse en práctica contramedidas fronte a comportamentos non desexados nunha rede
CA5.5 Caracterizáronse, instaláronse e configúranse ferramentas de monitorización

4.5.e) Contidos

Contidos
Seguridade perimetral. Firewalls de próxima xeración.
0Redes privadas virtuais (VPN) e túneles (protocolo IPSec).
Monitorización de sistemas e dispositivos.
Ferramentas de monitorización (IDS e IPS).
Xestores de eventos e información de seguridade (SIEM).



Contidos
Solucións de centros de operación de rede, e centros de seguridade de rede: NOC e SOC. Seguridade de portais e aplicativos web. Solucións WAF (web application firewall). Seguridade do posto de traballo e endpoint fixo e móbil. AntiAPT; antimalware. Seguridade de contornos Cloude. Solucións CASB. Seguridade do correo electrónico Solucións DLP (data loss prevention). Ferramentas de almacenamento de logs. Protección ante ataques de denegación de servizo distribuído (DDoS). Configuración segura de devasas, enrutadores e proxies.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Configuración de dispositivos para la instalación de sistemas informáticos	28

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

Resultado de aprendizaxe do currículo	Completo
RA6 - Configura dispositivos para a instalación de sistemas informáticos reducindo ao mínimo as probabilidades de exposición a ataques	SI

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

Criterios de avaliación
CA6.1 Configurouse a BIOS para incrementar a seguridade do dispositivo e o seu contido, reducindo ao mínimo as probabilidades de exposición a ataques
CA6.2 Preparouse un sistema informático para a súa primeira instalación, tendo en conta as medidas de seguridade necesarias
CA6.3 Configurouse un sistema informático para que un actor malicioso non poida alterar a secuencia de arranque con fins de acceso ilexítimo



Criterios de avaliación
CA6.4 Instalouse un sistema informático utilizando as súas capacidades de cifraxo do sistema de ficheiros, para evitar a extracción física de datos
CA6.5 Particionouse o sistema de ficheiros do sistema informático para reducir ao mínimo os riscos de seguridade

4.6.e) Contidos

Contidos
Precaucións previas á instalación dun sistema informático: illamento, configuración do control de acceso á BIOS, bloqueo da orde de arranque dos dispositivos, etc.
Seguridade no arranque do sistema informático; configuración do arranque seguro.
Seguridade dos sistemas de ficheiros, cifraxo, partición, etc.

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Configuración de los sistemas informáticos	28

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

Resultado de aprendizaxe do currículo	Completo
RA7 - Configura sistemas informáticos reduciendo ao mínimo as probabilidades de exposición a ataques	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 Enumeráronse e elimináronse os programas, os servizos e os protocolos innecesarios que foran instalados por defecto no sistema
CA7.2 Configuráronse as características propias do sistema informático para imposibilitar o acceso ilexítimo mediante técnicas de explotación de procesos
CA7.3 Incrementouse a seguridade do sistema de administración remoto SSH e outros



Criterios de avaliación
CA7.4 Instalouse e configurouse un sistema de detección de intrusos nun host (HIDS) no sistema informático
CA7.5 Instaláronse e configuráronse sistemas de copias de seguridade

4.7.e) Contidos

Contidos
Redución do número de servizos, Telnet, RSSH, TFTP, etc. Hardening de procesos (eliminación de información de depuración en caso de erros, aleatorización da memoria virtual para evitar exploits, etc.). Eliminación de protocolos de rede innecesarios (ICMP, etc.). Securización dos sistemas de administración remota. Sistemas de prevención e protección fronte a virus e intrusionés (antivirus, HIDS, etc.). Configuración de actualizacións e parches automáticos. Sistemas de copias de seguridade. Shadow IT e políticas de seguridade en contornos SaaS.

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

Mínimos esixibles para alcanzar unha avaliación positiva

- Dominio dos conceptos fundamentais: O alumnado deberá demostrar, a través das actividades propostas (presentación, traballo ou exame), un coñecemento básico e funcional dos contidos impartidos na unidade.
- Resolución de actividades prácticas: As tarefas prácticas deberán realizarse cun nivel de calidade suficiente para demostrar a comprensión dos procedementos e técnicas ensinadas.
- Participación activa: O alumnado deberá participar nas actividades, demostrando compromiso, interese e colaboración.
- Cumprimento dos prazos: As entregas de traballos e a realización de presentacións deberán facerse dentro dos prazos establecidos.
- Aplicación de boas prácticas: En todas as actividades, o alumnado deberá aplicar as boas prácticas relacionadas coa unidade (como configuracións seguras, documentación técnica ou análise de riscos).



Métodos de cualificación

Presentación oral ou práctica:

- Calidade da exposición.
- Claridade na explicación dos conceptos.
- Capacidade para responder preguntas relacionadas co tema.
- Uso de recursos axeitados para apoiar a presentación (diapositivas, demostracións).

Traballo práctico:

- Adecuación do traballo aos requisitos plantexados.
- Nivel de detalle e precisión na documentación presentada.
- Funcionalidade e seguridade das configuracións ou sistemas desenvolvidos.
- Creatividade e orixinalidade na solución proposta.

Exame teórico ou práctico:

- Resolución correcta das preguntas ou exercicios plantexados.
- Capacidade para analizar e resolver problemas relacionados cos contidos da unidade.
- Aplicación dos coñecementos adquiridos a situacións prácticas.

Notas adicionais

- Aprobado: Para obter unha avaliación positiva, o alumnado debe alcanzar, como mínimo, un 5 na conxunción dos métodos elixidos para a avaliación (poden usarse un o varios de forma simultanea).
- Recuperación: No caso de non alcanzar o mínimo, poderase realizar unha recuperación baseada nas áreas onde se detectase maior dificultade (presentación, traballo ou exame).
- Flexibilidade: As ponderacións dos criterios poderán axustarse segundo as características específicas de cada unidade, priorizando as actividades prácticas nas máis orientadas ao ámbito técnico.

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

Identificación das áreas de mellora:



Analizar os resultados da avaliación inicial para identificar as áreas nas que o alumnado non acadou os mínimos esixibles.
Avaliar cales son os criterios de cualificación que non se alcanzaron, como presentación, traballo práctico ou exame.

Definición dos obxectivos das actividades de recuperación:

Establecer obxectivos claros e específicos para cada actividade de recuperación, orientados a reforzar os contidos nos que o alumnado amosou máis dificultades.
Garantir que as actividades permitan demostrar que se adquiriron os coñecementos ou habilidades necesarias para superar a unidade.

Deseño das actividades:

Presentación:

Solicitar unha presentación sobre un tema específico da unidade para avaliar a comprensión conceptual e a capacidade de comunicación.
Establecer un guión ou estrutura que o alumnado debe seguir.

Traballo práctico:

Propor tarefas prácticas relacionadas cos obxectivos da unidade, adaptadas ás áreas non superadas.
Por exemplo: configurar un sistema operativo seguro, implementar políticas de control de acceso ou realizar a segmentación dunha rede.

Exame:

Deseñar un exame teórico ou práctico que avalíe os contidos principais da unidade.
Incluir exercicios prácticos ou casos reais que permitan demostrar a aplicación dos coñecementos adquiridos.

Proporcionar orientación e apoio:

Ofrecer ao alumnado material adicional ou guías específicas para facilitar a preparación das actividades de recuperación.
Realizar tutorías individuais ou en pequenos grupos para resolver dúbidas.

Avaliación das actividades de recuperación:

Corrixir as actividades de recuperación utilizando os mesmos criterios de cualificación que na avaliación inicial.
Valorar se o alumnado acadou os mínimos esixibles para superar a unidade.

Comunicación dos resultados:

Informar ao alumnado dos resultados das actividades de recuperación, destacando os aspectos mellorados e sinalando posibles áreas de reforzo adicional.
Proporcionar feedback claro e construtivo.

Documentación e rexistro:



Gardar os resultados das actividades de recuperación como evidencia do proceso de avaliación.
Rexistrar no sistema ou no expediente académico os resultados finais.

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

A recuperación poderá conter algunha o varias partes:

Parte teórica:

Preguntas curtas, de desenvolvemento ou tipo test que avalíen o coñecemento dos conceptos teóricos.

Parte práctica :

Resolución de casos prácticos, problemas ou tarefas que permitan avaliar as habilidades técnicas adquiridas.

É necesario obter un 5 en global.

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

Mediante a aplicación de seguimento e tomando os seguintes puntos en conta:

1. Establecemento dun plan de seguimento

Definir os obxectivos e indicadores clave para avaliar o cumprimento da programación e a calidade da práctica docente.

Identificar ferramentas e métodos para realizar o seguimento (por exemplo: rexistro de sesións, enquisas ao alumnado, reunións de coordinación).

2. Revisión periódica da programación

Temporalización:

Establecer puntos de control ao longo do curso (por exemplo: ao remate de cada unidade didáctica ou trimestre).

Análise:

Comprobar se se están cumprindo os prazos e obxectivos establecidos na programación.

Revisar a adecuación dos contidos, actividades e avaliacións ao nivel do alumnado.



3. Avaliación do progreso do alumnado

Recollida de datos:

Analizar os resultados obtidos polo alumnado nas actividades, traballos e exames para detectar áreas de mellora.

Identificar patróns ou dificultades comúns que poidan indicar necesidade de axustes na programación.

Enquisas e feedback:

Solicitar opinións do alumnado sobre as actividades e metodoloxías empregadas para valorar a súa eficacia e impacto.

4. Reflexión sobre a práctica docente

Autocrítica:

Avaliar o propio desempeño docente en canto á comunicación, organización e capacidade para motivar ao alumnado.

Análise de incidencias:

Identificar problemas ou desviacións ocorridas durante o desenvolvemento da programación (falta de tempo, recursos inadecuados, etc.) e buscar solucións.

5. Coordinación e reunións do equipo docente

Realizar reunións periódicas con outros docentes para:

Comparar avances e retos comúns no cumprimento das programacións.

Compartir boas prácticas e propostas de mellora.

Revisar criterios de avaliación e adaptar o plan se fose necesario.

6. Axustes na programación

Realizar modificacións na programación en función das conclusións extraídas do seguimento:

Redefinir actividades ou contidos que non resulten eficaces.

Adaptar os prazos ou métodos de avaliación en función do nivel e progresión do alumnado.

Incorporar novas ferramentas ou metodoloxías que melloren o proceso de ensino-aprendizaxe.

7. Avaliación final da programación e da práctica docente



Análise global:

Ao remate do curso, realizar unha avaliación integral sobre o cumprimento da programación e a efectividade da práctica docente.

Documentación:

Elaborar un informe que inclúa os logros, incidencias e propostas de mellora para o próximo curso.

Feedback:

Recolle opinións do alumnado e dos compañeiros docentes sobre o desenvolvemento da programación e as metodoloxías empregadas.

8. Incorporación de melloras para cursos futuros

Integrar as conclusións obtidas no seguimento e avaliación da práctica docente para optimizar as programacións seguintes.

Realizar formación continua para mellorar competencias docentes e metodolóxicas.

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

1. Definición de obxectivos da avaliación inicial

Determinar os obxectivos principais da avaliación inicial, que poden incluír:

Identificar o nivel de coñecementos previos do alumnado.

Detectar posibles carencias formativas que poidan interferir no desenvolvemento das unidades didácticas.

Adaptar a programación para atender as necesidades reais do grupo.

2. Deseño da avaliación inicial

Ferramentas e métodos:

Elaborar actividades e probas axeitadas ao nivel do alumnado, como:

Test de coñecementos previos.

Actividades prácticas básicas relacionadas cos contidos do módulo.

Preguntas abertas para avaliar a comprensión dos conceptos iniciais.



Incluir tanto aspectos teóricos como prácticos, dependendo dos obxectivos de aprendizaxe do módulo.

Temporalización:

Realizar a avaliación inicial durante as primeiras sesións do curso, garantindo que os resultados poidan empregarse para adaptar a programación.

3. Recollida de datos

Solicitar ao alumnado que complete as actividades ou probas deseñadas.

Observar o comportamento e actitude do alumnado durante as tarefas para detectar habilidades, dificultades ou posibles desintereses.

4. Análise dos resultados

Cualitativa:

Analizar os coñecementos previos detectados e valorar a capacidade do alumnado para afrontar os contidos do módulo.

Identificar patróns comúns que indiquen carencias ou fortalezas no grupo.

Cuantitativa:

Clasificar os resultados segundo niveis de competencia (por exemplo: básico, intermedio, avanzado).

5. Adaptación da programación

En función dos resultados obtidos:

Modificar a programación inicial para reforzar os contidos nos que o alumnado mostre máis carencias.

Propor actividades de apoio ou reforzo para os estudantes con maior dificultade.

Adaptar o ritmo das sesións ao nivel global do grupo, sen comprometer os obxectivos finais do módulo.

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

1. Identificación das necesidades do alumnado

Analizar as áreas específicas nas que o alumnado presenta dificultades, a través de:

Resultados das actividades e avaliacións realizadas.



Observación directa durante as sesións prácticas e teóricas.

Feedback proporcionado polo propio alumnado.

Identificar patróns que indiquen carencias comúns ou particulares (conceptuais, procedimentais ou de actitude).

2. Deseño dun plan de reforzo personalizado

Adaptación de contidos:

Seleccionar e reforzar os conceptos básicos ou fundamentais que sirvan de alicerce para avanzar nos obxectivos programados.

Temporalización:

Dedicar sesións específicas de reforzo, de forma individual ou en pequenos grupos.

Compatibilizar o reforzo co desenvolvemento da programación para evitar atrasos no progreso do grupo.

9. Aspectos transversais

9.a) Programación da educación en valores

1. Integración da educación en valores na programación

A educación en valores debe estar integrada de forma transversal en todas as unidades didácticas, adaptándose ás actividades teóricas e prácticas.

Priorizar valores fundamentais como:

Responsabilidade: Cumprir prazos e compromisos nas tarefas asignadas.

Colaboración: Promover o traballo en equipo e o respecto polos compañeiros.

Integridade: Fomentar a ética profesional, especialmente no uso de ferramentas tecnolóxicas.

Sustentabilidade: Sensibilizar sobre o impacto ambiental das tecnoloxías e prácticas profesionais.

2. Metodoloxía para a educación en valores

Exemplos prácticos: Utilizar casos reais ou simulados que permitan reflexionar sobre dilemas éticos ou sociais no ámbito profesional (por exemplo, uso indebido de datos persoais).

Traballo colaborativo: Desenvolver actividades en grupo que fomenten o respecto polas ideas alleas e a resolución de conflitos de forma constructiva.

Reflexión crítica: Propoñer debates ou dinámicas que permitan analizar cuestións como a ciberseguridade, o respecto á privacidade e a igualdade de acceso ás tecnoloxías.



9.b) Actividades complementarias e extraescolares

Non se contemplan actividades extraescolares