

PROGRAMACIÓN LOOIFP

Versión Alumnado

Centro educativo

Código	Centro	Concello	Ano académico
36015159	IES Chan do Monte	Marín	2025/2026

Datos da programación

Ensinanza	Ciclo formativo/Curso de especialización	Grao		
Graos D: Ciclos formativos	D3IFC000100 - Administración de sistemas informáticos en rede	A		
Módulo				
MP0378 - Seguridade e alta dispoñibilidade (2º)				
Tipo de oferta	Modalidade	Réxime dual	Grupo	
Réxime xeral-ordinario	Presencial	Xeral	A	
Sesiões semanais	Horas anuais	Duración Sesiões	Sesiões anuais	Sesiões centro
5	137	50	164	85

Profesorado responsable

Docentes
Gores Fandiño, Rosendo David

Contido	Páxina
Concreción do currículo en relación coa súa adecuación ás características do ámbito produtivo.	3
Relación e secuencia de unidades didácticas	3
Asignación de elementos curriculares ás unidades didácticas.	4
Procedemento de avaliación inicial.	14
Criterios de cualificación e recuperación	14
Procedemento de seguimento, recuperación e avaliación das materias pendentes	16
Procedemento para definir a proba de avaliación extraordinaria para o alumnado con perda de dereito á avaliación continua	16
Medidas de reforzo educativo para o alumnado que non responda globalmente aos obxectivos programados.	16
Programación da educación en valores.	17
Actividades complementarias e extraescolares.	17
Procedemento sobre o seguimento da programación e a avaliación da propia práctica docente.	17
Outros apartados.	17

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

O ámbito produtivo do Instituto son empresas PEME que se adican á consultoría e a distintos servizos informáticos e/ou a programación nos diferentes ámbitos da informática (web, programación a medida, etc.).

Neste módulo de Seguridade Informática e Alta Disponibilidade tratarase de orientar aos alumnos/as para axudar a mellorar a seguridade e a posta en funcionamento de sistemas de alta dispoñibilidade de estas empresas.

No currículo especificase, nas orientacións pedagóxicas do módulo, as funcións que obterán os alumnos/as ao aprobar este módulo.

Tamén no currículo, nas competencias profesionais, persoais e sociais especificanse varias habilidades e capacidades que terán os alumnos/as.

En concreto destacar as seguintes:

- Pór en práctica solucións de alta dispoñibilidade, analizando as opcións do mercado, para protexer e recuperar o sistema ante situacións imprevistas
 - Supervisar a seguridade física segundo especificacións de fábrica e o plan de seguridade, para evitar interrupcións na prestación de servizos do sistema.
 - Asegurar o sistema e os datos segundo as necesidades de uso e as condicións de seguridade establecidas, para previr fallos e ataques externos.
 - Administrar usuarios de acordo coas especificacións de explotación, para garantir os accesos e a dispoñibilidade dos recursos do sistema.
 - Diagnosticar as disfuncións do sistema e adoptar as medidas correctivas para restablecer a súa funcionalidade.
 - Xestionar e/ou realizar o mantemento dos recursos da súa área (programando e verificando o seu cumprimento), en función das cargas de traballo e o plan de mantemento.

Relación e secuencia de unidades didácticas

UD	Título	Descrición	% Peso materia	Nº sesións
1	Introdución á seguridade informática.		8	7
2	Seguridade física.		8	7
3	Criptografía.		8	7
4	Seguridade Lóxica. Servidor.		8	7
5	Seguridade Lóxica. Seguridade Perimetral.		8	7
6	Implantación de firewalls.		15	14
7	Implantación de proxys.		13	8
8	Sistemas de alta dispoñibilidade. Clusters.		8	7
9	Virtualización.		8	7
10	Análisis forense.		8	7
11	Lexislación.		8	7

Asignación de elementos curriculares ás unidades didácticas.

UD	Título da UD	Duración
1	Introdución á seguridade informática.	7

Criterios de avaliación
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e reconece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.
CA1.1 - Valorouse a importancia de asegurar a privacidade, a coherencia e a dispoñibilidade da información nos sistemas informáticos.
CA1.2 - Describíronse as diferenzas entre seguridade física e lóxica.
CA1.5 - Adoptáronse políticas de contrasinais.
CA1.6 - Valoráronse as vantaxes do uso de sistemas biométricos.
RA7 - Reconece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia.
CA7.2 - Determinouse a necesidade de controlar o acceso á información persoal almacenada.
CA7.7 - Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable.

Lenda: IA: Instrumento de Avaliación, %: Peso orientativo; PE: Proba escrita, LC:Lista de cotexo, TO:Táboa de observación, OU: outro

Contidos
BC1 - Adopción de pautas de seguridade informática
Fiabilidade, confidencialidade, integridade e dispoñibilidade.
Elementos vulnerables no sistema informático: hardware, software e datos.
Análise das principais vulnerabilidades dun sistema informático.
Pautas e prácticas seguras.

UD	Título da UD	Duración
2	Seguridade física.	7

Criterios de avaliación
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e reconece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.
CA1.5 - Adoptáronse políticas de contrasinais.
CA1.6 - Valoráronse as vantaxes do uso de sistemas biométricos.
CA1.8 - Reconeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.

Lenda: IA: Instrumento de Avaliación, %: Peso orientativo; PE: Proba escrita, LC:Lista de cotexo, TO:Táboa de observación, OU: outro

Contidos
BC1 - Adopción de pautas de seguridade informática
Tipos de ameazas: físicas e lóxicas.
Seguridade física e ambiental: Localización e protección física dos equipamentos e dos servidores. Sistemas de alimentación ininterrompida.

UD	Título da UD	Duración
3	Criptografía.	7

Criterios de avaliación
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e reconece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.
CA1.7 - Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información.
CA1.9 - Identificáronse as fases da análise forense ante ataques a un sistema.
RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.
CA2.6 - Utilizáronse técnicas de cifraxo, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas.

Lenda: IA: Instrumento de Avaliación, %: Peso orientativo; PE: Proba escrita, LC:Lista de cotexo, TO:Táboa de observación, OU: outro

Contidos
BC1 - Adopción de pautas de seguridade informática

Contidos
Pautas e prácticas seguras.
Seguridade lóxica: Criptografía. Listas de control de acceso. Establecemento de políticas de contrasinais. Sistemas biométricos de identificación. Políticas de almacenamento. Medios de almacenamento.
BC2 - Implantación de mecanismos de seguridade activa
Seguridade na conexión con redes públicas.
Técnicas de cifraxa da información: clave pública e clave privada; certificados dixitais; sinaturas.

UD	Título da UD	Duración
4	Seguridade Lóxica. Servidor.	7

Criterios de avaliación
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e reconece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.
CA1.3 - Clasifícanse os tipos principais de vulnerabilidade dun sistema informático, segundo a súa tipoloxía e a súa orixe.
CA1.4 - Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas.
CA1.5 - Adoptáronse políticas de contrasinais.
RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.
CA2.1 - Clasifícanse os principais tipos de ameazas lóxicas contra un sistema informático.
CA2.2 - Verifícase a orixe e a autenticidade das aplicacións instaladas nun equipamento, así como o estado de actualización do sistema operativo.
CA2.3 - Identifícase a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.
CA2.4 - Analizáronse diversos tipos de ameazas, ataques e software malicioso, en contornos de execución controlados.
CA2.5 - Implantáronse aplicacións específicas para a detección de ameazas e a eliminación de software malicioso.
CA2.7 - Avaliáronse as medidas de seguridade dos protocolos usados en redes de comunicación.
CA2.8 - Recoñeceuse a necesidade de inventariar e controlar os servizos de rede que se executan nun sistema.
CA2.9 - Describíronse os tipos e as características dos sistemas de detección de intrusións.

Lenda: IA: Instrumento de Avaliación, %: Peso orientativo; PE: Proba escrita, LC:Lista de cotexo, TO:Táboa de observación, OU: outro

Contidos
BC1 - Adopción de pautas de seguridade informática
Análise das principais vulnerabilidades dun sistema informático.
Tipos de ameazas: físicas e lóxicas.
Seguridade lóxica: Criptografía. Listas de control de acceso. Establecemento de políticas de contrasinais. Sistemas biométricos de identificación. Políticas de almacenamento. Medios de almacenamento.
BC2 - Implantación de mecanismos de seguridade activa
Ataques e contramedidas en sistemas informáticos.
Clasificación dos ataques.
Anatomía de ataques e análise de software malicioso.
Realización de auditorías de seguridade.
Ferramentas preventivas e paliativas: instalación e configuración.
Copias de seguridade e imaxes de respaldo.
Recuperación de datos.
Actualización de sistemas e aplicacións.

UD	Título da UD	Duración
5	Seguridade Lóxica. Seguridade Perimetral.	7

Criterios de avaliación
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e reconece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.
CA1.8 - Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.
RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.
CA2.7 - Avaliáronse as medidas de seguridade dos protocolos usados en redes de comunicación.
CA2.8 - Recoñeceuse a necesidade de inventariar e controlar os servizos de rede que se executan nun sistema.
CA2.9 - Describíronse os tipos e as características dos sistemas de detección de intrusións.
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e

Criterios de avaliación
aplica o plan de seguridade.
CA3.1 - Describíronse escenarios típicos de sistemas con conexión a redes públicas en que cumpra fortificar a rede interna.
CA3.2 - Clasificáronse as zonas de risco dun sistema, segundo criterios de seguridade perimetral.
CA3.3 - Identificáronse os protocolos seguros de comunicación e os seus ámbitos de uso.
CA3.4 - Configuráronse redes privadas virtuais mediante protocolos seguros a distintos niveis.
CA3.5 - Implantouse un servidor como pasarela de acceso á rede interna desde localizacións remotas.
CA3.6 - Identificáronse e configuráronse os métodos posibles de autenticación no acceso de usuarios remotos a través da pasarela.
CA3.7 - Instalouse, configurouse e integrouse na pasarela un servidor remoto de autenticación.

Lenda: IA: Instrumento de Avaliación, %: Peso orientativo; PE: Proba escrita, LC:Lista de cotexo, TO:Táboa de observación, OU: outro

Contidos
BC2 - Implantación de mecanismos de seguridade activa
Ferramentas preventivas e paliativas: instalación e configuración.
Monitorización do tráfico en redes: captura e análise; aplicacións.
Seguridade nos protocolos para comunicacións sen fíos.
Riscos potenciais dos servizos de rede. Software para detección de vulnerabilidades.
Intentos de penetración: tipoloxía.
Sistemas de detección de intrusións.
BC3 - Implantación de técnicas de acceso remoto. Seguridade perimetral
Elementos básicos da seguridade perimetral: encamiñador fronteira; tornalumes; redes privadas virtuais.
Perímetros de rede. Zonas desmilitarizadas.
Arquitectura débil e forte de subrede protexida.
Redes privadas virtuais. VPN. Beneficios e desvantaxes con respecto ás liñas dedicadas. VPN a nivel de enlace. VPN a nivel de rede. SSL e IPsec. VPN a nivel de aplicación. SSH.
Servidores de acceso remoto: Protocolos de autenticación. Configuración de parámetros de acceso. Servidores de autenticación.

UD	Título da UD	Duración
6	Implantación de firewalls.	14

Criterios de avaliación
RA4 - Implanta tornalumes (firewalls) para asegurar un sistema informático, analiza as súas prestacións e controla o tráfico cara á rede interna.
CA4.1 - Describíronse as características, os tipos e as funcións dos tornalumes.
CA4.2 - Clasificáronse os niveis en que se realiza a filtraxe de tráfico.
CA4.3 - Planificouse a instalación de tornalumes para limitar os accesos a determinadas zonas da rede.
CA4.4 - Configuráronse filtros nun tornalumes a partir dunha listaxe de regras de filtraxe.
CA4.5 - Revisáronse os rexistros de sucesos de tornalumes, para verificar que as regras se apliquen correctamente.
CA4.6 - Probáronse distintas opcións para implementar tornalumes, tanto de software como de hardware.
CA4.7 - Diagnosticáronse problemas de conectividade nos clientes provocados polos tornalumes.
CA4.8 - Elaborouse documentación relativa á instalación, configuración e uso de tornalumes.

Lenda: IA: Instrumento de Avaliación, %: Peso orientativo; PE: Proba escrita, LC:Lista de cotexo, TO:Táboa de observación, OU: outro

Contidos
BC4 - Instalación e configuración de tornalumes
Utilización de tornalumes.
Filtraxe de paquetes de datos.
Tipos de tornalumes: características e funcións principais: Uso das características de tornalumes incorporadas no sistema operativo. Implantación de tornalumes en sistemas libres e propietarios. Instalación e configuración. Tornalumes hardware.
Regras de filtraxe de tornalumes.
Probas de funcionamento: sondaxe.
Rexistros de sucesos nas devasas.

UD	Título da UD	Duración
7	Implantación de proxys.	8

Criterios de avaliación

RA5 - Instala servidores proxy, aplicando criterios de configuración que garantan o funcionamento seguro do servizo.
CA5.1 - Identifícanse os tipos de proxy, as súas características e as súas funcións principais.
CA5.2 - Instalouse e configúrase un servidor proxy cache.
CA5.3 - Configúranse os métodos de autenticación no proxy.
CA5.4 - Configúrase un proxy en modo transparente.
CA5.5 - Utilízase o servidor proxy para establecer restricións de acceso web.
CA5.6 - Arranxáronse problemas de acceso desde os clientes ao proxy.
CA5.7 - Realízanse probas de funcionamento do proxy, monitorizando a súa actividade con ferramentas gráficas.
CA5.8 - Configúrase un servidor proxy en modo inverso.
CA5.9 - Elaborouse documentación relativa á instalación, a configuración e o uso de servidores proxy.

Lenda: IA: Instrumento de Avaliación, %: Peso orientativo; PE: Proba escrita, LC:Lista de cotexo, TO:Táboa de observación, OU: outro

Contidos

BC5 - Instalación e configuración de servidores proxy
Tipos de proxy: características e funcións.
Instalación de servidores proxy.
Instalación e configuración de clientes proxy.
Configuración do almacenamento na cache dun proxy.
Configuración de filtros.
Métodos de autenticación nun proxy.
Proxy inverso.

Contidos
Encadeamento e xerarquías.
Probas de funcionamento.

UD	Título da UD	Duración
8	Sistemas de alta dispoñibilidade. Clusters.	7

Criterios de avaliación
RA6 - Implanta solucións de alta dispoñibilidade empregando técnicas de virtualización, e configura os contornos de proba.
CA6.1 - Analizáronse supostos e situacións en que cumpra pór en marcha solucións de alta dispoñibilidade.
CA6.2 - Identificáronse solucións de hardware para asegurar a continuidade no funcionamento dun sistema.
CA6.4 - Implantouse un servidor redundante que garanta a continuidade de servizos en casos de caída do servidor principal.
CA6.5 - Implantouse un balanceador de carga á entrada da rede interna.
CA6.6 - Implantáronse sistemas de almacenamento redundante sobre servidores e dispositivos específicos.
CA6.7 - Avaliouse a utilidade dos sistemas de clúster para aumentar a fiabilidade e a produtividade do sistema.
CA6.8 - Analizáronse solucións de futuro para un sistema con demanda crecente.
CA6.9 - Esquematzáronse e documentáronse solucións para supostos con necesidades de alta dispoñibilidade.

Lenda: IA: Instrumento de Avaliación, %: Peso orientativo; PE: Proba escrita, LC:Lista de cotexo, TO:Táboa de observación, OU: outro

Contidos
BC6 - Implantación de solucións de alta dispoñibilidade
Definición e obxectivos.
Análise de configuracións de alta dispoñibilidade. Funcionamento ininterrompido. Integridade de datos e recuperación de servizo. Servidores redundantes. Sistemas de clústers. Balanceadores de carga.
Computación na nube.
Instalación e configuración de solucións de alta dispoñibilidade.

UD	Título da UD	Duración
9	Virtualización.	7

Criterios de avaliación
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade.
CA3.5 - Implantouse un servidor como pasarela de acceso á rede interna desde localizacións remotas.
RA4 - Implanta tornalumes (firewalls) para asegurar un sistema informático, analiza as súas prestacións e controla o tráfico cara á rede interna.
CA4.6 - Probáronse distintas opcións para implementar tornalumes, tanto de software como de hardware.
RA6 - Implanta solucións de alta dispoñibilidade empregando técnicas de virtualización, e configura os contornos de proba.
CA6.3 - Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.

Lenda: IA: Instrumento de Avaliación, %: Peso orientativo; PE: Proba escrita, LC:Lista de cotexo, TO:Táboa de observación, OU: outro

Contidos
BC6 - Implantación de solucións de alta dispoñibilidade
Computación na nube.
Virtualización de sistemas. Posibilidades da virtualización de sistemas. Ferramentas para a virtualización. Configuración e uso de máquinas virtuais. Alta dispoñibilidade e virtualización. Simulación de servizos con virtualización. Análise e optimización
Virtualización en contornos de produción.

UD	Título da UD	Duración
10	Analisis forense.	7

Criterios de avaliación
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e reconece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.
CA1.9 - Identificáronse as fases da análise forense ante ataques a un sistema.
RA7 - Reconece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia.

Criterios de avaliación
CA7.3 - Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.
CA7.4 - Contrastouse o deber de pór ao dispor das persoas os datos persoais que lles atinxen.
CA7.7 - Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable.

Lenda: IA: Instrumento de Avaliación, %: Peso orientativo; PE: Proba escrita, LC:Lista de cotexo, TO:Táboa de observación, OU: outro

Contidos
BC1 - Adopción de pautas de seguridade informática
Análise forense en sistemas informáticos: obxectivo. Recollida e análise de incidencias.
Ferramentas empregadas na análise forense.
BC7 - Lexislación e normas sobre seguridade
Lexislación sobre protección de datos e sobre os servizos da sociedade da información e o correo electrónico.
Normas de seguridade e cumprimento normativo na nube.

UD	Título da UD	Duración
11	Lexislación.	7

Criterios de avaliación
RA7 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia.
CA7.1 - Describiuse a lexislación sobre protección de datos de carácter persoal.
CA7.2 - Determinouse a necesidade de controlar o acceso á información persoal almacenada.
CA7.3 - Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.
CA7.4 - Contrastouse o deber de pór ao dispor das persoas os datos persoais que lles atinxen.
CA7.5 - Describiuse a lexislación actual sobre os servizos da sociedade da información e o comercio electrónico.
CA7.6 - Contrastáronse as normas sobre xestión de seguridade da información.

Criterios de avaliación

CA7.7 - Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable.

Lenda: IA: Instrumento de Avaliación, %: Peso orientativo; PE: Proba escrita, LC:Lista de cotexo, TO:Táboa de observación, OU: outro

Contidos

BC7 - Lexislación e normas sobre seguridade

Lexislación sobre protección de datos e sobre os servizos da sociedade da información e o correo electrónico.

Normas de seguridade e cumprimento normativo na nube.

Procedemento de avaliación inicial.

Realización de proba escrita onde se pretende averiguar a motivación do alumnado para escoller este ciclo, cales son as expectativas de aprendizaxe e cales son as expectativas de traballo que teñen unha vez que rematen o ciclo.

Tamén se lles preguntará preguntas sinxelas relacionadas coa materia do módulo Seguridade Informática e Alta Dispoñibilidade (Cifrado, clave privada, clave pública, firewall, proxy, LOPDGDD,...).

Esta proba valerá para facerme unha idea do que pensan os alumnos/as que opinión teñen sobre o módulo e o ciclo e tamén para ter unha idea dos coñecementos que poidan ter da materia e as diferenzas que hai entre o distinto tipo de alumnado, según proveñan de Bacharelato ou dun ciclo medio de informática e comunicacións.

A finais do primeiro mes de clase 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/a o a un grupo.

Criterios de cualificación e recuperación

Procedemento e criterios de cualificación:

A avaliación do alumnado será continua, e haberase de ter en conta o grao de consecución dos obxectivos específicos deste módulo.

Durante o desenvolvemento das clases, procederase á observación sistemática e pautada do proceso de aprendizaxe de cada alumno/a co fin de avaliar o progreso do mesmo en relación ao grao de consecución dos obxectivos xerais descritos no currículo do ciclo formativo.

Para acadar unha cualificación o máis obxectiva posible en relación ao traballo realizado, empregaranse os seguintes instrumentos de avaliación:

* O traballo dentro da aula e no taller. Comprobarase o traballo individual e en equipo, se resultou óptimo ou deficiente e comprobando se o alumno tivo un talante aberto ás solucións aportadas polos demais (cando é en grupo) por ser máis eficaces. Asemade, valorarase a capacidade para aceptar as críticas ao seu traballo e o tesón á hora de defender as súas solucións. Tratando de evitar a ensinanza mecánica e memorística, fomentarase a participación do alumnado no proceso de aprendizaxe. Valorarase a capacidade para resolver problemas sobre o ordenador, a facilidade de acceso ós manuais técnicos, bibliografía e utilidades de software dispoñible, así como o interese, esforzo persoal e responsabilidade de cada quen.

* A realización, presentación (dentro do prazo previsto) e exposición (no seu caso), das tarefas encomendadas debidamente documentadas. Farase unha recollida puntual de exercicios e realizaranse probas puntuais para obter información sobre capacidades ou destrezas concretas como se describe nas unidades didácticas correspondentes.

* A participación activa na clase propoñendo solucións aos diferentes casos prácticos que se expoñan.

* Probas individuais (exames) sobre os coñecementos teórico-prácticos, que permitirán determinar se un/a alumno/a acadou os obxectivos específicos propostos no deseño curricular do módulo e desenvolvidas nesta programación, e tamén permitirán comprobar que o/a alumno/a fixo o traballo da clase e non o plagiou doutro compañeiro ou de Internet. Estas probas individuais poderanse facer dunha ou varias unidades didácticas na mesma proba e terán un peso na nota obtida polo alumno/a na avaliación dun 90% e serán como se explica a continuación:

->Probas escritas onde se preguntará aos alumnos/as conceptos teóricos relacionados cos traballos feitos na aula. Poderán ser tipo test, de resposta curta e/ou longa sobre un tema.

->Probas prácticas onde os alumnos deberán realizar configuracións (de servizos, equipos ou redes) que xa practicaron na aula ou no taller.

Con estas probas preténdese facer un seguimento individualizado da asimilación de tódolos conceptos impartidos segundo os criterios de avaliación establecidos en cada unidade didáctica ata o momento impartida e o grao de consecución dos obxectivos do módulo.

En cada proba indícarase ao alumno/a que partes corresponden a un CA considerado de OBRIGADO CUMPRIMENTO e debe facer ben esa parte da proba para superala.

Antes de cada avaliación pódese realizar unha proba global que permita valorar o grao de integración de coñecementos que acadou cada un dos alumnos/as.

Nas probas valorarase principalmente a sinxeleza, claridade e comprensión dos procedementos asociados.

A cualificación da avaliación será a media ponderada (indícarase o % de cada unha das probas para a nota total) das notas obtidas nas probas, sempre e cando a nota mínima obtida fose de 4 en cada unha das probas.

Valorándose ademais tódolos aspectos arriba indicados de acordo cos seguintes porcentaxes:

* Un 90% da nota será a nota media (ponderada) obtida nas probas.

* Un 10% estará constituído pola valoración realizada en canto aos aspectos indicados de traballo na aula e participación nos traballos e prácticas propostas sexan en grupo ou individuais.

Normas de integridade e uso de material na realización de probas de avaliación.

Nota: tanto para as probas escritas como as prácticas deberáse seguir as normas para exames publicadas nas NOFC do instituto. A continuación móstranse un resumo das mesmas.

- Material permitido: O profesor/a indicará en cada proba o material que o alumnado pode utilizar. Dependendo da natureza da proba de avaliación, poderase deixar acceso soamente aos materiais proporcionados polo profesor ou ao código dos exercicios e tarefas realizadas polo alumno/a de forma individual. O uso non deste material informarase ao realizar a proba.

- Uso da Intelixencia Artificial (IA): A utilización de ferramentas de IA xenerativa (coma ChatGPT, Copilot ou similares) estará prohibida nas probas de avaliación agas que o profesorado o autorice expresamente para algunha das tarefas que haxa que realizar.

- Defensa da proba: O alumnado deberá estar sempre en disposición de defender a súa proba, de xeito oral ou cunha demostración, para que o profesorado poida verificar a autoría mesma e a comprensión dos procedementos e solucións desenvolvidas.

- Fraude e consecuencias: Non se poderá utilizar calquera outro tipo de material nas probas (apuntes, resúmenes ou calquera nota, así como calquera dispositivo de comunicación coma móbiles, auriculares ou reloxios intelixentes). Se se detectase que durante a proba de avaliación hai un incumprimento destas normas a proba cualificarase con 0 puntos ou, de ser o caso, a parte da proba que se considere que non é de autoría propia do alumno/a que a está a realizar.

Procedemento e criterios de recuperación

O proceso será con dúas probas: unha teórica e outra práctica onde o alumno deberá repetir as probas que realizou durante o curso e non acadou a nota mínima de 4 (so recuperará a parte suspensas).

As probas escritas serán de resposta curta ou longa pero non de tipo test.

As probas prácticas serán semellantes as realizadas durante o curso e as que o alumnado non superou (nota inferior a 4).

Do mesmo xeito que na avaliación ordinaria tanto na proba escrita coma na práctica haberá algunhas preguntas ou partes que se considerarán de OBRIGADO CUMPREMENTO para asuperar esa proba e polo tanto o curso.

As probas teóricas dividiránse en partes (coincidentes coas UD do módulo) e indicárase ao alumnado cales preguntas corresponden a cada parte.

Para considerar a recuperación (tanto a escrita coma a práctica) superada ten que obter unha nota de 5 ou superior en cada unha das partes de cada proba que teña que realizar.

A nota final será a media ponderada das partes que se aprobaron durante o curso e as probas que se fagan nesta recuperación final. Se non aprobábase nada durante o curso a nota será a media ponderada das probas feitas nesta recuperación

Evidentemente, nestas probas segueranse as mesmas normas de realización de exames publicadas nas NOFC.

Procedemento de seguimento, recuperación e avaliación das materias pendentes

Non procede

Procedemento para definir a proba de avaliación extraordinaria para o alumnado con perda de dereito á avaliación continua

Os instrumentos de avaliación neste caso que se empregarán son os seguintes:

Proba escrita: constará de cuestións, problemas e outras tarefas a desenvolver de forma escrita da mesma natureza e 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. Non será de tipo test.

Proba práctica: constará de tarefas e preguntas da mesma natureza e da mesma complexidade cas desenvolvidas ó longo do curso académico polo alumnado avaliado de forma continua, dos contidos desenvolvidos nas diferentes unidades didácticas do módulo.

Para superar o módulo profesional compre acadar unha puntuación de 5 puntos en cada proba. A cualificación final da proba será a media ponderada das puntuacións obtidas en cada unha das dúas probas, escrita e práctica, valorándose a proba escrita un 40% e a proba práctica un 60% sempre e cando se acade un mínimo de 4 en cada unha das partes (teórica e práctica).

Nestas probas tamen se lle indicará ao alumno/a os CA considerados de OBRIGADO CUMPRIMENTO e que debe realizarse correctamente. De non ser así suspenderase o curso aínda que a nota media ponderada estivese por riba de 5 puntos.

Poderanse realizar as probas en días distintos se foxe imposible realizalas nun mesmo día por mor dos horarios ou da duración das probas.

As probas poderán durar ata 5 horas cada unha de elas. Se lle comunicarán o interesado ou interesada as datas e horas das probas coa debida antelación.

O profesor tamén avaliará se a alumna ou alumno reúne os requisitos de profesionalidade, madurez e autonomía suficiente nas devanditas probas..

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

Na avaliación inicial a orientadora do centro informa aos profesorado do curso os casos de alumnos/as que poidan precisar de medidas de reforzo ou axudas individuais na aula para acadar os obxectivos do módulo.

Nesa reunión se valorarán as posibles medidas de reforzo que poidan ser necesarias para cada caso en concreto (dende a adaptación do posto de traballo na aula, adaptación dos contidos para facilitar o estudo, ou axudas en tempo ou procedemento nos exames ou probas a realizar durante o curso).

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 vixente; en especial a Lei de Protección de Datos e Garantía de Dereitos Dixitais (LOPDGDD)

Aprendizaxe permanente ó longo da vida.

Explicar ó 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 os alumnos 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 e alumnas.
- Na Educación Ambiental: Concienciar dos problemas medioambientais producidos polo material informático en desuso e promover hábitos de reutilización e reciclaxe nos materiais empregados.

Actividades complementarias e extraescolares.

Cada curso hai charlas informáticas e seminarios relacionados coa Seguridade Informática (por exemplo CiberGal en Santiago de Compostela) Tentarase asistir a algunha destas charlas e seminarios para complementar os coñecementos adquiridos na clase e ver a evolución da seguridade informática nas empresas do sector.

Tamén procurarase asistir a calquera outra actividade que durante o curso se nos informase que se vaia a realizar e estivese relacionada coa seguridade informática e/ou a alta dispoñibilidade de sistemas.

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

O finalizar cada unidade didáctica, o profesor realizará unha reflexión do proceso de ensino-aprendizaxe de dita unidade co a finalidade de recoller, revisar e analizar o desenrolo de dito proceso, os logros e debilidades dos resultados obtidos a través das distintas fontes e instrumentos de avaliación 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 a temporalización e nos instrumentos de avaliación para así mellorar o proceso de ensino de cada alumno, os rendementos destes, o funcionamento do grupo de clase e a propia práctica docente do profesor.

Outros apartados.

1. Aceso á programación.

A programación está disponible ao alumnado que o solicite ao profesor.

2. Regras de comportamento nos exames

Nas NOFC do instituto descríbense unhas normas de comportamento que o alumnado debe ter nos exames. Estas normas son para evitar que os alumnos/as copien ou fagan calquera trampa no exame. En caso de que se descubra un caso deste tipo o alumno/a será expulsado do exame e a cualificación no mesmo será de 0 puntos.