1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
36019402	Pazo da Mercé	Neves (As)	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 xeral-ordinario

Módulo profesional e unidades formativas de menor duración (*)

Código MP/UF	Nome	Curso	Sesións semanais	Horas anuais	Sesións anuais
MP0226	Seguridade informática	2023/2024	8	140	168

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

Profesorado responsable

Profesorado asignado ao módulo	MARÍA ESTHER FERREIRO FERNÁNDEZ
Outro profesorado	

Estado: Pendente de supervisión inspector

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

O módulo "Seguridade Informática" pertence ao ciclo de Formación Profesional de grao medio de Sistemas Microinformáticos e Redes, que ten unha duración de 2.000 horas ao longo de 2 cursos académicos, ao que lle corresponde o título de Técnico en sistemas microinformáticos e redes. Este módulo impártese durante o segundo curso, no segundo trimestre.
O desenvolvemento curricular de este módulo ten como referencia de partida o Real Decreto 1691/2007, do 14 de decembro (BOE nº 3446 do 17 de xaneiro de 2008), onde se establece o currículo do ciclo Sistemas Microinformáticos e Redes.

O ámbito produtivo no que se atopa o centro caracterízase pola abundancia de PEMEs. Polo tanto, na concreción do currículo do ciclo terase en conta esta circunstancia para incidir nas tecnoloxías e infraestruturas máis utilizadas neste tipo de empresas, así como as coñecementos e habilidades que se poden demandar na actividade laboral.

As ocupacións e os postos de traballo máis salientables son os seguintes:
* Técnico/a instaladora/a ou reparador/a de equipamentos informáticos.
* Técnico/a de soporte informático.
* Técnico/a de redes de datos.
* Reparador/a de periféricos de sistemas microinformáticos.
* Comercial de microinformática.
* Operador/a de teleasistencia.
* Operador/a de sistemas.

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 (%)	Resultados de aprendizaxe					
					MP0226_00					
					RA1	RA2	RA3	RA4	RA5	RA6
1	Introdución á seguridade informática	Nesta unidade aprenderanse os conceptos básicos de seguridade informática.	12	6	X					
2	Criptografía e identificación dixital	Nesta unidade estudaranse as principais técnicas critográficas para asegurar a confidencialidade da información, as técnicas para a comprobación da súa integridade e aquelas que nos permiten identificar dixitalmente ao emisor.	32	19	X				X	
3	Seguridade pasiva: Hardware e almacenamento	Esta unidade trata todo o relacionado coa seguridade física nun centro de procesamento de datos: localización, condicións medioambientais, sistemas de control de acceso; así como as técnicas de alimentación ininterrompida e o almacenamento redundante e distribuído.	22	13		X	X			
4	Seguridade pasiva: Recuperación de datos	Esta unidade trata as técnicas de prevención de perda da información e recuperación da mesma.	25	14			X	X		
5	Seguridade activa no sistema	Nesta unidade trátanse as técnicas para evitar accesos non desexados ao sistema.	27	16	X	X		X	X	
6	Seguridade activa en redes	Esta unidade trata dos protocolos que aportan seguridade á hora de conectarse a unha rede ou a outro equipo da rede.	20	12					X	
7	Seguridade perimetral: devasas e proxies	Esta unidade trata sobre a utilidade das devasas para controlar a entrada e saída de datos nunha rede, así coma os proxies para regular os accesos desde a rede interna a Internet.	20	12					X	
8	Lexislación e normativa sobre seguridade informática	Esta unidade trata en profundidade a lexislación e normativa que afecta á seguridade informática.	10	8						X
		Total:	168							

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Introdución á seguridade informática	12

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Identifica técnicas e prácticas de tratamento seguro da información, e recoñece e valora a súa importancia en distintos contornos de traballo.	NO

4.1.c) Obxectivos específicos da unidade didáctica

Obxectivos específicos	Act	Título das actividades	Duración (sesións)
1.2 Diferenciar entre a seguridade física e lóxica 1.3 Diferenciar a seguridade pasiva e activa 1.1 Valorar a importancia de manter a información segura. 1.4 Identificar as propiedades da seguridade informática (CIA e outras) 1.5 Coñecer os principios da seguridade inofrmática 1.6 Clasificar a información no ámbito da seguridade. 1.7 Analizar os obxectivos dos ataques informáticos 1.8 Identificar as ferramentas da seguridade informática 1.9 Coñecer os conceptos que identifican as fraxilidades na seguridade 1.10 Diferenciar entre ataques pasivos e activos 1.11 Coñecer os elementos relevantes dunha política de seguridade 1.12 Saber os elementos a desenvolver nun plan de continxencia 1.13 Coñecer organismos relacionados coa seguridade	1	INTRODUCIÓN Á SEGURIDADE INFORMATICA	12,0
		TOTAL	**12**

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

Criterios de avaliación	Instrumentos de avaliación	Mínimos exixibles	Peso cualificación (%)
CA1.1 Valorouse a importancia de manter a información segura.	• PE.1 - Exame escrito a final da UD	S	15
CA1.2 Clasificouse a información no ámbito da seguridade.	• PE.2 - Exame escrito a final da UD	S	15
CA1.3 Describíronse as diferenzas entre seguridade física e lóxica.	• PE.3 - Exame escrito a final da UD	S	20

Criterios de avaliación	Instrumentos de avaliación	Mínimos exixibles	Peso cualificación (%)
CA1.7 Recoñeceuse a necesidade de facer unha análise de riscos e a posta en marcha dunha política de seguridade.	• PE.4 - Exame escrito a final da UD	S	10
CA1.8 Establecéronse as normas básicas para incluír nun manual de seguridade informática.	• PE.5 - Exame escrito a final da UD	N	15
CA1.9 Describíronse as diferenzas entre seguridade activa e pasiva.	• PE.6 - Exame escrito a final da UD	S	20
CA1.10 Coñécense organismos relacionados coa Ciberseguridade	• PE.7 - Exame escrito a final da UD	N	5
		TOTAL	100

4.1.e) Contidos

Contidos
Valoración da importancia de manter a información segura
Conceptos básicos sobre seguridade informática
Obxectivos da seguridade informática
Recoñecemento da necesidade de facer un análise de riscos
Descrición das diferenzas entre seguridade activa e pasiva
Seguridade física e lóxica.
Políticas de seguridade.
Obxectivos e medidas a tomar para garantir a seguridade
Planificación dun documento de política de seguridade
Organismos relacionados coa Ciberseguridade

4.1.f) Actividades de ensino e aprendizaxe, e de avaliación, con xustificación de para que e de como se realizarán, así como os materiais e os recursos necesarios para a súa realización e, de ser o caso, os instrumentos de avaliación

Que e para que	Como			Con que	Como e con que se valora	Duración (sesións)
Actividade (título e descrición)	Profesorado (en termos de tarefas)	Alumnado (tarefas)	Resultados ou produtos	Recursos	Instrumentos e procedementos de avaliación	

Que e para que	Como			Con que	Como e con que se valora	Duración (sesións)
Actividade (título e descrición)	**Profesorado (en termos de tarefas)**	**Alumnado (tarefas)**	**Resultados ou produtos**	**Recursos**	**Instrumentos e procedementos de avaliación**	
INTRODUCIÓN Á SEGURIDADE INFORMÁTICA - Conceptos básicos da seguridade informática	• Explicar os conceptos básicos da seguridade informática • Analizar co grupo as respostas do cuestionario e resolver as dúbidas que aparezan	• Analizar a política de contrasinais dalgunha institución. • Comprobación de contrasinais con comprobador en liña. • Comparativa antivirus en liña. • Resolver cuestións sobre os aspectos básicos da seguridade informática.	• Cuestións resoltas • Informes sobre o análise de vulnerabilidades	• Canón de proxección • Aula virtual • Equipos informáticos coa capacidade de execución de máquinas virtuais • Acceso a Internet	• PE.1 - Exame escrito a final da UD • PE.2 - Exame escrito a final da UD • PE.3 - Exame escrito a final da UD • PE.4 - Exame escrito a final da UD • PE.5 - Exame escrito a final da UD • PE.6 - Exame escrito a final da UD • PE.7 - Exame escrito a final da UD	12,0
					TOTAL	**12,0**

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Criptografía e identificación dixital	32

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

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

4.2.c) Obxectivos específicos da unidade didáctica

Obxectivos específicos	Act	Título das actividades	Duración (sesións)
1.2 Recoñecer a necesidade de integrar técnicas criptográficas na almacenaxe e na transmisión da información. 1.3 Identificar os fundamentos criptográficos dos protocolos seguros de comunicación (clave pública, clave privada, etc.). 1.4 Describir e utilizar sistemas de identificación como a sinatura electrónica, o certificado dixital, etc. 1.1 Identificar as principais técnicas criptográficas.	1	Técnicas criptográficas	25,0
2.1 Describir e utilizar sistemas de identificación como a sinatura electrónica, o certificado dixital, etc.	2	Sistemas de identificación dixital	7,0
		TOTAL	32

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

Criterios de avaliación	Instrumentos de avaliación	Mínimos exixibles	Peso cualificación (%)
CA1.4 Identificáronse as principais técnicas criptográficas.	• PE.1 - Cuestionarios	S	30
CA1.5 Recoñeceuse a necesidade de integrar técnicas criptográficas na almacenaxe e na transmisión da información.			0
CA1.5.1 Analizáronse os obxectivos da criptografía para a protección de datos	• PE.2 - Cuestionarios	S	15
CA1.6 Identificáronse os fundamentos criptográficos dos protocolos seguros de comunicación (clave pública, clave privada, etc.).	• PE.3 - Cuestionarios	S	20
CA5.6 Clasificáronse e valoráronse as propiedades de seguridade dos protocolos usados en redes sen fíos.	• PE.4 - Cuestionarios	N	5
CA5.7 Describíronse e utilizáronse sistemas de identificación como a sinatura electrónica, o certificado dixital, etc.	• LC.1 - Informes sobre casos prácticos	S	30
		TOTAL	100

4.2.e) Contidos

Contidos
Criptografía. Técnicas criptográficas

Contidos
Sistemas de identificación dixital
Conceptos básicos sobre criptografía
Métodos para asegurar a privacidade da información transmitida.
Identificación dixital: sinatura electrónica e certificado dixital.

4.2.f) Actividades de ensino e aprendizaxe, e de avaliación, con xustificación de para que e de como se realizarán, así como os materiais e os recursos necesarios para a súa realización e, de ser o caso, os instrumentos de avaliación

Que e para que	Como			Con que	Como e con que se valora	Duración (sesións)
Actividade (título e descrición)	Profesorado (en termos de tarefas)	Alumnado (tarefas)	Resultados ou produtos	Recursos	Instrumentos e procedementos de avaliación	
Técnicas criptográficas - Nesta actividade analizarase a necesidade de encriptar mensaxes, contrasinais, documentos, etc. Estudaranse distintos métodos de encriptación, tanto clásicos coma modernos. Aprenderase o funcionamento e as aplicacións dos sistemas de cifrado de clave simétrica e asimétrica para protexer a almacenaxe e a transmisión da información.	• Explicación dos sistemas de cifrado. • Avaliar o informe realizado polo alumnado. • Avaliar o informe realizado polo alumnado	• Realización de exercicios sobre sistemas de cifrado antigos. • Cifrar documentos con GPG usando cifrado simétrico e asimétrico e facer un informe do traballo realizado. • Calcular o Hash de documentos e analizar o seu resultado. Facer un informe do traballo realizado.	• Informes • Documentos cifrados e asinados	• Canón de proxección • Aula virtual • Equipos informáticos coa capacidade de execución de máquinas virtuais • Acceso a Internet	• PE.1 - Cuestionarios • PE.2 - Cuestionarios • PE.3 - Cuestionarios	25,0
Sistemas de identificación dixital - Nesta actividade aprenderase o funcionamento dunha infraestrutura PKI, dos certificados dixitais e do seu uso nas identidades dixitais.	• Avaliar os informes realizados polo alumnado.	• Explicación dos sistemas de sinatura e certificados dixitais. • Procura de certificados no navegador. • Sinatura de documentos con GPG. Informe do traballo realizado. • Creación de certificado autoasinado. Informe do traballo realizado. • Emprego dos programas da administración electrónica para a sinatura de documentos e xeración e sinatura de facturas electrónicas. Informe do traballo realizado.	• Exercicios resoltos • Informes	• Canón de proxección • Aula virtual • Equipos informáticos coa capacidade de execución de máquinas virtuais • Acceso a Internet	• LC.1 - Informes sobre casos prácticos • PE.4 - Cuestionarios	7,0
					TOTAL	**32,0**

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Seguridade pasiva: Hardware e almacenamento	22

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.	NO

4.3.c) Obxectivos específicos da unidade didáctica

Obxectivos específicos	Act	Título das actividades	Duración (sesións)
1.1 Definir as características do emprazamento dos equipos e dos servidores. 1.2 Definir as condicións ambientais dos equipos e dos servidores. 1.3 Identificar a necesidade de protexer fisicamente os sistemas informáticos. 1.4 Esquematizar as características dunha política de seguridade baseada en listas de control de acceso. 1.5 Valorar a importancia de establecer unha política de contrasinais. 1.6 Describir os sistemas biométricos. 1.7 Analizar as vantaxes e inconvenientes de cada sistema biométrico. 1.8 Seguir plans de continxencia para actuar ante fallos de seguridade física.	1	Seguridade física e ambiental	8,0
2.1 Identificar os tipos de sistemas de alimentación ininterrompida. 2.2 Identificar o modo de funcionamento do sistema de alimentación ininterrompida. 2.3 Seleccionar o sistema de alimentación ininterrompida acorde ao sistema. 2.4 Seleccionar puntos de aplicación dos sistemas de alimentación ininterrompida.	2	Hardware de protección física	5,0
3.1 Interpretar a documentación técnica relativa á política de almacenaxe. 3.2 Ter en conta factores inherentes á almacenaxe da información (rendemento, dispoñibilidade, accesibilidade, etc.). 3.3 Clasificar os principais métodos de almacenaxe, incluídos os sistemas en rede. 3.4 Enumerar os principais métodos de almacenaxe, incluídos os sistemas en rede 3.5 Describir a tecnoloxía de almacenaxe redundante e distribuída. 3.6 Utilizar medios de almacenaxe redundantes e distribuídos. 3.7 Identificar as características dos medios de almacenaxe remotos e extraíbles. 3.8 Utilizar medios de almacenaxe remotos.	3	Almacenamento de información	9,0

TOTAL	**22**

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

Criterios de avaliación	Instrumentos de avaliación	Mínimos exixibles	Peso cualificación (%)
CA2.1 Definíronse as características do emprazamento e as condicións ambientais dos equipamentos e dos servidores.	• TO.1 - Informe sobre un caso práctico	S	15
CA2.2 Identificouse a necesidade de protexer fisicamente os sistemas informáticos.	• PE.1 - Cuestionarios	S	5
CA2.3 Verificouse o funcionamento dos sistemas de alimentación ininterrompida.	• TO.2 - Observación directa	N	5
CA2.4 Seleccionáronse os puntos de aplicación dos sistemas de alimentación ininterrompida.	• PE.2 - Cuestionarios	S	10
CA3.2 Tivéronse en conta factores inherentes á almacenaxe da información (rendemento, dispoñibilidade, accesibilidade, etc.).	• PE.3 - Cuestionarios	S	10
CA3.3 Clasificáronse e enumeráronse os principais métodos de almacenaxe, incluídos os sistemas en rede.	• PE.4 - Cuestionarios	S	15
CA3.4 Describíronse as tecnoloxías de almacenaxe redundante e distribuída.	• PE.5 - Cuestionarios	S	15
CA3.8 Identificáronse as características dos medios de almacenaxe remotos e extraíbles.	• PE.6 - Cuestionarios	S	10
CA3.9 Utilizáronse medios de almacenaxe remotos e extraíbles.	• TO.3 - Observación directa e informes sobre casos prácticos	N	5
CA3.11 Utilizáronse medios de almacenaxe redundantes e distribuídos.	• TO.4 - Observación directa e informes sobre casos prácticos	S	10
	TOTAL		**100**

4.3.e) Contidos

Contidos
Localización e protección física dos equipamentos e dos servidores.
Sistemas de alimentación ininterrompida.
Almacenaxe da información: rendemento, dispoñibilidade e accesibilidade.
Almacenaxe redundante e distribuída.
Almacenaxe remota e extraíble.

4.3.f) Actividades de ensino e aprendizaxe, e de avaliación, con xustificación de para que e de como se realizarán, así como os materiais e os recursos necesarios para a súa realización e, de ser o caso, os instrumentos de avaliación

Que e para que	Como			Con que	Como e con que se valora	Duración (sesións)
Actividade (título e descrición)	Profesorado (en termos de tarefas)	Alumnado (tarefas)	Resultados ou produtos	Recursos	Instrumentos e procedementos de avaliación	

Que e para que	Como			Con que	Como e con que se valora	Duración (sesións)
Actividade **(título e descrición)**	**Profesorado (en termos de tarefas)**	**Alumnado (tarefas)**	**Resultados ou produtos**	**Recursos**	**Instrumentos e procedementos de avaliación**	
Seguridade física e ambiental - Esta actividade trata as características da situación física e condicións ambientais e da contorna dos CPD, así coma os protocolos de actuación cara as posibles incidencias físicas e métodos de control de acceso. Nela tratarase tamén os distintos sistemas de seguridade física que se poden implantar nun CPD.	• Explicación da necesidade de aplicación de mecanismos para a seguridade física dos sistemas informáticos. • Descrición das ameazas naturais e da contorna que poden afectar ao correcto funcionamento dos equipos informáticos, así como as medidas de prevención a levar a cabo. • Exposición dos factores a ter en conta para a correcta localización dun CPD. • Descrición de modelos de CPD que non se deben seguir. • Explicación dos distintos sistemas de protección física. • Descrición de como levar a cabo un plan de continxencia física.	• Identificación de ameazas que poden afectar a un sistema informáticos. • Localización do CPD no centro de ensino. • Resumo das innovacións na construción dun CPD. • Identificación de medidas de prevención e protección de lumes. • Elaboración dun cuestionario de afondamento. • Elaboración do plan de continxencia físico do centro de ensino.	• Cuestionario resolto na aula virtual • Informes • Equipo coa ferramenta de xestión do SAI instalada e configurada • Cámara IP instalada e configurada	• Canón de proxección • Aula virtual • Equipos con capacidade para a execución de máquinas virtuais • Acceso a Internet • Cámaras IP • Equipos con fontes de alimentación e tarxetas de rede redundantes	• PE.1 - Cuestionarios • TO.1 - Informe sobre un caso práctico	8,0
Hardware de protección física - Esta actividade trata da necesidade de uso e os tipos de sistemas de alimentación ininterrompida para manter a subministración eléctrica en caso de fallo total na rede eléctrica.	• Explicación do concepto de SAI xunto cos elementos que o compoñen . • Explicación doutras características de interese para a elección dun SAI. • Explicación dos tres tipos de SAI segundo a forma de funcionamento.	• Cálculo da potencia dun SAI. • Selección dun SAI en función dunhas condicións especificadas. • Comparativa das características de distintos tipos de SAIs. • Selección online dun SAI de servidor en función dunha configuración dada. • Instalación e monitorización dun SAI.	• Cuestións resoltas • SAI seleccionado • Táboa comparativa das características de diversos SAIs. • SAI instalado e configurado.	• Canón de proxección • Aula virtual. • Ordenador persoal, con navegador web e conexión a Internet. • Máquinas virtuais Windows ou GNU/Linux. • Software necesario para a realización das tarefas. • SAI.	• PE.2 - Cuestionarios • TO.2 - Observación directa	5,0

Que e para que	Como			Con que	Como e con que se valora	Duración (sesións)
Actividade (título e descrición)	**Profesorado (en termos de tarefas)**	**Alumnado (tarefas)**	**Resultados ou produtos**	**Recursos**	**Instrumentos e procedementos de avaliación**	
Almacenamento de información - Esta actividade trata sobre as tecnoloxías de almacenamento da información. Nela trataranse as distintas técnicas que se poden utilizar para levar a cabo este almacenamento, onde se verán técnicas redundantes, distribuídas e remotas. Así mesmo trataranse os factores que se deben valorar na seguridade da información e que afectan ao seu almacenamento.	• Analizar co grupo as respostas do cuestionario e resolver as dúbidas que aparezan • Analizar co grupo a solución do exercicio e resolver as dúbidas que aparezan • Avaliar o informe realizado polo alumnado • Avaliar o informe realizado polo alumnado • Avaliar mediante a observación directa o traballo realizado polo alumnado • Avaliar os informes realizados polo alumnado	• Ler un texto sobre os sistemas de almacenamento redundante e en rede • Resolver un cuestionario sobre os sistemas de almacenamento redundante e en rede • Resolver un exercicio de simulación sobre o funcionamento dos sistemas RAID5 • Realizar a configuración de sistemas RAID sobre Windows nun caso práctico e realizar un informe do traballo realizado • Realizar a configuración de sistemas RAID sobre Linux nun caso práctico e realizar un informe do traballo realizado • Levar a cabo no taller a configuración dun sistema de almacenamento RAID por hardware • Realizar a configuración de sistemas NAS e facer informes do traballo realizado	• Cuestionario resolto • Informes • Máquinas virtuais Windows e Linux con sistemas RAID configurados • Equipo con sistema RAID por hardware configurado • Sistemas NAS configurados	• Aula virtual • Equipos informáticos coa capacidade de execución de máquinas virtuais • Acceso a Internet • Libro de texto • Sistemas NAS • Equipos informáticos com controladoras RAID	• PE.3 - Cuestionarios • PE.4 - Cuestionarios • PE.5 - Cuestionarios • PE.6 - Cuestionarios • TO.3 - Observación directa e informes sobre casos prácticos • TO.4 - Observación directa e informes sobre casos prácticos	9,0
					TOTAL	**22,0**

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Seguridade pasiva: Recuperación de datos	25

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

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

4.4.c) Obxectivos específicos da unidade didáctica

Obxectivos específicos	Act	Título das actividades	Duración (sesións)
1.2 Realizar e restaurar copias de seguridade do sistema 1.1 Identificar os distintos tipos de copias de seguridade 1.3 Describir unha política de copias de seguridade	1	Copias de seguridade en Windows e Linux	8,0
2.1 Recuperar datos perdidos dun disco 2.2 Recoñecer a necesidade do borrado físico para garantir a confidencialidade dos datos eliminados	2	Ferramentas de recuperación de datos	7,0
3.1 Realizar e restaurar imaxes do sistema, xeneralizándoas para distinto tipo de hardware 3.2 Utilizar CDs de arranque para recuperar datos co sistema operativo danado	3	Ferramentas de recuperación do sistema	10,0
		TOTAL	**25**

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

Criterios de avaliación	Instrumentos de avaliación	Mínimos exixibles	Peso cualificación (%)
CA3.1 Interpretouse a documentación técnica relativa á política de almacenaxe.	• PE.1 - Cuestionarios	N	5
CA3.5 Seleccionáronse estratexias para a realización de copias de seguridade.	• PE.2 - Cuestionarios	S	20
CA3.6 Tívose en conta a frecuencia e o esquema de rotación.	• PE.3 - Cuestionarios	S	20
CA3.7 Realizáronse copias de seguridade seguindo diversas estratexias.	• LC.1 - Informes sobre casos prácticos	S	25
CA3.10 Creáronse e restauráronse imaxes de respaldo de sistemas en funcionamento.	• LC.2 - Informe sobre un caso práctico	S	20
CA4.7 Aplicáronse técnicas de recuperación de datos.	• LC.3 - Informe sobre un caso práctico	S	10
		TOTAL	**100**

4.4.e) Contidos

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

4.4.f) Actividades de ensino e aprendizaxe, e de avaliación, con xustificación de para que e de como se realizarán, así como os materiais e os recursos necesarios para a súa realización e, de ser o caso, os instrumentos de avaliación

Que e para que	Como			Con que	Como e con que se valora	Duración (sesións)
Actividade (título e descrición)	Profesorado (en termos de tarefas)	Alumnado (tarefas)	Resultados ou produtos	Recursos	Instrumentos e procedementos de avaliación	
Copias de seguridade en Windows e Linux - Copias de seguridade en Windows e Linux	• Analizar co grupo as respostas do cuestionario e resolver as dúbidas que aparezan • Avaliar o informe realizado polo alumnado	• Ler un texto sobre as copias de seguridade • Resolver un cuestionario sobre copias de seguridade • Facer copias de seguridade sobre sistemas Windows e Linux e realizar un informe do traballo realizado	• Cuestionario resolto • Informes • Máquinas virtuais configuradas para a realización de copias de seguridade	• Libro de texto • Aula virtual • Equipos con capacidade para a execución de máquinas virtuais • Acceso a Internet	• LC.3 - Informe sobre un caso práctico • PE.1 - Cuestionarios • PE.2 - Cuestionarios • PE.3 - Cuestionarios	8,0
Ferramentas de recuperación de datos - Ferramentas de recuperación de datos perdidos accidentalmente	• Explicación dos procesos de borrado e recuperación de datos nun sistema informático • Avaliar o informe realizado polo alumnado	• Recuperar datos borrados sobre unha máquina virtual e facer o borrado físico de ficheiros, e realizar un informe do traballo realizado	• Informes	• Aula virtual • Equipos con capacidade para a execución de máquinas virtuais • Acceso a Internet	• LC.1 - Informes sobre casos prácticos • LC.3 - Informe sobre un caso práctico	7,0
Ferramentas de recuperación do sistema - Ferramentas de recuperación do sistema operativo	• Avaliar o informe realizado polo alumnado • Avaliar o informe realizado polo alumnado • Avaliar o informe realizado polo alumnado	• Ler un texto sobre as principais técnicas e ferramentas de recuperación do sistema operativo • Resolver un cuestionario sobre técnicas de recuperación do sistema operativo • Facer usando máquinas virtuais unha imaxe dun sistema Windows e restauralo sobre outra máquina e realizar un informe do traballo realizado • Definir e utilizar puntos de restauración con unha máquina virtual con Windows e realizar un informe do traballo realizado • Utilizar un CD de arranque para recuperar os datos dun sistema corrupto e realizar un informe do traballo realizado	• Cuestionario resolto • Informes	• Libro de texto • Aula virtual • Equipos con capacidade para a execución de máquinas virtuais • Acceso a Internet	• LC.2 - Informe sobre un caso práctico • LC.3 - Informe sobre un caso práctico	10,0
					TOTAL	**25,0**

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Seguridade activa no sistema	27

4.5.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
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

4.5.c) Obxectivos específicos da unidade didáctica

Obxectivos específicos	Act	Título das actividades	Duración (sesións)
1.1 Identificar os distintos métodos de autenticación existentes e as vantaxes e inconvenientes de cada un 1.2 Subsistemas onde é necesario un control de acceso (BIOS, xestor de arranque...)	1	Métodos de autenticación	8,0
2.1 Establecer permisos aos datos e ao sistema aos usuarios xa autenticados 2.2 Configurar a seguridade dos usuarios e dos grupos utilizando ACL. 2.3 Encriptado de datos nos sistemas de almacenamento 2.4 Utilidade do establecemento de cotas de disco	2	Control de acceso aos recursos	7,0
3.1 Rexistro de actividade como ferramenta de seguridade do sistema 3.2 Métodos de actualización dos software para manter a seguridade do sistema 3.3 Auditorias de seguridade	3	Actualización e monitorización do sistema	7,0
4.1 Identificar as accións e/ou tipos de software que pode ameazar o sistema e as técnicas de protección que se poden utilizar 4.2 Instalación e uso de software antimalware	4	Software malicioso e ferramentas antimalware	5,0
		TOTAL	**27**

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

Criterios de avaliación	Instrumentos de avaliación	Mínimos exixibles	Peso cualificación (%)
CA1.5 Recoñeceuse a necesidade de integrar técnicas criptográficas na almacenaxe e na transmisión da información.			0
CA1.5.2 Coñécense técnicas para a encriptación de datos en sistemas de almacenamento	• LC.1 - Informes sobre casos prácticos	S	5
CA2.5 Esquematizáronse as características dunha política de seguridade baseada en listas de control de acceso.	• PE.1 - Cuestionario	N	5

Criterios de avaliación	Instrumentos de avaliación	Mínimos exixibles	Peso cualificación (%)
CA2.6 Valorouse a importancia de establecer unha política de contrasinais.	• LC.2 - Informes sobre casos prácticos	S	15
CA2.7 Valoráronse as vantaxes do uso de sistemas biométricos.	• LC.3 - Informes sobre casos prácticos	N	5
CA4.1 Seguíronse plans de continxencia para actuar ante fallos de seguridade.	• LC.4 - Informe sobre caso práctico	N	5
CA4.2 Clasificáronse os principais tipos de software malicioso.	• LC.5 - Informe sobre caso práctico	S	10
CA4.3 Empregáronse ferramentas que examinan a integridade do sistema, e ferramentas de control e seguimento de accesos.	• LC.6 - Informe sobre caso práctico	S	10
CA4.4 Realizáronse actualizacións periódicas dos sistemas para corrixir posibles vulnerabilidades.	• LC.7 - Informe sobre caso práctico	S	10
CA4.5 Verificouse a orixe e a autenticidade das aplicacións que se instalan nos sistemas.	• LC.8 - Informe sobre caso práctico	N	5
CA4.6 Instaláronse, probáronse e actualizáronse aplicacións específicas para a detección e a eliminación de software malicioso.	• LC.9 - Informe sobre caso práctico	S	10
CA5.2 Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas e nos roubos de información.	• PE.2 - Cuestionario	S	10
CA5.3 Deduciuse a importancia de reducir o volume de tráfico xerado pola publicidade e o correo non desexado.	• PE.3 - Cuestionario	S	5
CA5.5 Identificáronse as ameazas na navegación por internet.	• PE.4 - Cuestionario	S	5
		TOTAL	**100**

4.5.e) Contidos

Contidos
Criptografía.
Técnicas de encriptación de datos en sistemas de almacenamento
Listas de control de acceso.
0Actualización de sistemas e aplicacións.
Manual de seguridade e plans de continxencia.
Política de contrasinais.
Autenticación centralizada
Control de acceso aos sistemas
Sistemas biométricos de identificación.
Monitorización de sistemas.
Auditorías de seguridade.
Software malicioso: clasificación. Ferramentas de protección e desinfección.
0Análise dos rexistros (logs) dun sistema para identificar ataques reais ou potenciais á seguridade.
Publicidade e correo non desexados.
Fraudes informáticas e roubos de información.

4.5.f) Actividades de ensino e aprendizaxe, e de avaliación, con xustificación de para que e de como se realizarán, así como os materiais e os recursos necesarios para a súa realización e, de ser o caso, os instrumentos de avaliación

Que e para que	Como			Con que	Como e con que se valora	Duración (sesións)
Actividade (título e descrición)	Profesorado (en termos de tarefas)	Alumnado (tarefas)	Resultados ou produtos	Recursos	Instrumentos e procedementos de avaliación	
Métodos de autenticación - Instalar e manexar diversos métodos de autenticación do sistema (por contrasinal, certificado dixital ou elementos biométricos). Realizar ataques contra os contrasinais do sistema	• Analizar co grupo as respostas do cuestionario e resolver as dúbidas que aparezan • Avaliar o informe realizado polo alumnado • Avaliar o informe realizado polo alumnado	• Ler un texto sobre as técnicas de autenticación dispoñibles nos sistemas informáticos • Resolver un cuestionario sobre técnicas de autenticación • Configurar e probar distintos métodos de autenticación no sistema e facer un informe do traballo realizado • Crackear os contrasinais dos usuarios almacenados o sistema operativo utilizando un dicionario e facer un informe do traballo realizado	• Cuestionario resolto • Informes	• Aula virtual • Libro de texto • Equipos informáticos coa capacidade de execución de máquinas virtuais • Acceso a Internet	• LC.2 - Informes sobre casos prácticos • LC.3 - Informes sobre casos prácticos	8,0
Control de acceso aos recursos - Determinar os métodos de control de acceso aos distintos recursos do sistema	• Analizar co grupo as respostas do cuestionario e resolver as dúbidas que aparezan • Avaliar o informe realizado polo alumnado	• Ler un texto sobre técnicas de cifrado do disco • Resolver un cuestionario sobre técnicas de cifrado do disco • Cifrar carpetas e particións con distintas ferramentas sobre sistemas Windows e Linux e facer un informe do traballo realizado	• Cuestionario resolto • Informes	• Libro de texto • Aula virtual • Equipos informáticos coa capacidade de execución de máquinas virtuais • Acceso a Internet	• LC.1 - Informes sobre casos prácticos • PE.1 - Cuestionario	7,0
Actualización e monitorización do sistema - Configurar e aplicar actualizacións e técnicas de monitorización tanto en Windows como en Linux	• Avaliar o informe realizado polo alumnado • Avaliar o informe realizado polo alumnado	• Aplicar as actualizacións sobre o sistema operativo e as aplicacións instaladas e facer un informe do traballo realizado • Manexar ferramentas de análise do rexistro sobre Windows e Linux e facer un informe do traballo realizado	• Informes	• Aula virtual • Acceso a Internet • Equipos informáticos coa capacidade de execución de máquinas virtuais	• LC.4 - Informe sobre caso práctico • LC.6 - Informe sobre caso práctico • LC.7 - Informe sobre caso práctico • LC.8 - Informe sobre caso práctico	7,0

Que e para que	Como			Con que	Como e con que se valora	Duración (sesións)
Actividade (título e descrición)	**Profesorado (en termos de tarefas)**	**Alumnado (tarefas)**	**Resultados ou produtos**	**Recursos**	**Instrumentos e procedementos de avaliación**	
Software malicioso e ferramentas antimalware - Instalar algún antivirus gratuíto e analizar as súas funcionalidades principais	• Avaliar o informe realizado polo alumnado	• Instalar unha ferramenta de detección e eliminación de malware sobre un sistema e elaborar un informe sobre as súas características principais	• Informes	• Aula virtual • Acceso a Internet • Equipos informáticos coa capacidade de execución de máquinas virtuais	• LC.5 - Informe sobre caso práctico • LC.6 - Informe sobre caso práctico • LC.9 - Informe sobre caso práctico • PE.2 - Cuestionario • PE.3 - Cuestionario • PE.4 - Cuestionario	5,0
					TOTAL	**27,0**

4.6.a) Identificación da unidade didáctica

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

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

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

4.6.c) Obxectivos específicos da unidade didáctica

Obxectivos específicos	Act	Título das actividades	Duración (sesións)
1.1 Recoñecer os riscos na transmisión da información a través da rede	1	Ataques sobre as conexións en rede	5,0
2.1 Coñecer e manexar os elementos de seguridade na navegación por Internet e no uso do correo electrónico	2	Seguridade no acceso a Internet	5,0
3.1 Instalar e configurar mecanismos de seguridade tanto en redes cableadas como en redes sen fíos	3	Conexións remotas seguras	7,0
4.1 Instalar e configurar mecanismos de seguridade en redes sen fíos	4	Seguridade en redes WiFi	3,0
		TOTAL	**20**

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

Criterios de avaliación	Instrumentos de avaliación	Mínimos exixibles	Peso cualificación (%)
CA5.1 Identificouse a necesidade de inventariar e controlar os servizos de rede.	• PE.1 - Cuestionarios	S	80
CA5.4 Aplicáronse medidas para evitar a monitorización de redes con cables.	• LC.1 - Informes sobre casos prácticos	N	20
		TOTAL	**100**

4.6.e) Contidos

Contidos
Métodos para asegurar a privacidade da información transmitida.
Monitorización do tráfico en redes con cables.
Seguridade en redes sen fíos.
Riscos potenciais dos servizos de rede.
Sistemas de seguridade nas telecomunicacións: correo, www, ftp, p2p, etc.

4.6.f) Actividades de ensino e aprendizaxe, e de avaliación, con xustificación de para que e de como se realizarán, así como os materiais e os recursos necesarios para a súa realización e, de ser o caso, os instrumentos de avaliación

Que e para que	Como			Con que	Como e con que se valora	Duración (sesións)
Actividade (título e descrición)	**Profesorado (en termos de tarefas)**	**Alumnado (tarefas)**	**Resultados ou produtos**	**Recursos**	**Instrumentos e procedementos de avaliación**	
Ataques sobre as conexións en rede - Realización de ataques de sniffing e spoofing nunha LAN	• Avaliar o informe realizado polo alumnado	• Realizar ataques de sniffing e spoofing sobre conexión de redes de equipos da LAN e facer un informe do traballo realizado	• Informe	• Aula virtual • Equipos con capacidade para a execución de máquinas virtuais	• PE.1 - Cuestionarios	5,0
Seguridade no acceso a Internet - Seguridade nos navegadores e clientes de email	• Analizar co grupo as respostas do cuestionario e resolver as dúbidas que aparezan • Avaliar o informe realizado polo alumnado	• Ler un texto sobre os riscos ao navegar por Internet e ler correo electrónico • Resolver un cuestionario sobre a seguridade no acceso a Internet • Realizar un informe sobre as principais funcionalidades dos navegadores web máis usados en relación coa seguridade	• Cuestionario resolto • Informe	• Aula virtual • Libro de texto • Equipos con capacidade para a execución de máquinas virtuais • Acceso a Internet	• LC.1 - Informes sobre casos prácticos • PE.1 - Cuestionarios	5,0
Conexións remotas seguras - Conexións SSH e VPN	• Avaliar o informe realizado polo alumnado	• Configurar a seguridade nas conexións remotas por SSH e facer un informe do traballo realizado • Configurar unha conexión por VPN e facer un informe do traballo realizado • Avaliar o informe realizado polo alumnado	• Informes	• Aula virtual • Equipos con capacidade para a execución de máquinas virtuais • Acceso a Internet	• LC.1 - Informes sobre casos prácticos • PE.1 - Cuestionarios	7,0
Seguridade en redes WiFi - Protocolos de seguridade nas WiFi	• Avaliar o informe realizado polo alumnado	• Configurar redes WiFi con medidas de seguridade avanzadas como WPA2 Empresarial e un portal cautivo e facer un informe do traballo realizado	• Informe	• Aula virtual • Ordenadores con interfaces WiFi • Puntos de acceso sen fíos • Acceso a Internet	• PE.1 - Cuestionarios	3,0
					TOTAL	**20,0**

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Seguridade perimetral: devasas e proxies	20

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

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

4.7.c) Obxectivos específicos da unidade didáctica

Obxectivos específicos	Act	Título das actividades	Duración (sesións)
1.1 Analizar a necesidade de asegurar o perímetro da rede da organización. 1.2 Identificar as características, vantaxes, funcións e tipos de devasas (tornalumes ou firewall) 1.3 Revisar as arquitecturas de rede con devasas. 1.4 Instalar e configurar unha devasa nun equipamento ou nun servidor.	1	Devasas	10,0
2.1 Identificar as características e as funcións pricipais dun proxy así coma os tipos de proxy existentes. 2.2 Configurar o equipo para empregar un proxy.	2	Proxies	10,0
		TOTAL	**20**

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

Criterios de avaliación	Instrumentos de avaliación	Mínimos exixibles	Peso cualificación (%)
CA5.8 Instalouse e configurouse unha devasa (firewall) nun equipamento ou nun servidor.			0
CA5.8.1 Indentificáronse os pasos necesarios para a configuración dun firewall	• TO.1 - Observación directa ou dos informes entregados.	S	30
CA5.8.2 Instalouse e configurouse un firewall nun servidor	• TO.2 - Observación directa ou dos informes entregados.	N	20
CA5.8.3 Instalouse e configurouse un firewall nun router	• TO.3 - Observación directa ou dos informes entregados.	N	20
CA5.9 Describíronse e identificáronse as características, os tipos e as funcións dun Proxy	• TO.4 - Observación directa ou dos informes entregados.	S	30
		TOTAL	**100**

4.7.e) Contidos

Contidos
Descrición e identificación as características, os tipos e as funcións das devasas a nivel de aplicación (Proxy)
Utilización de devasas (firewalls) en equipamentos e en servidores.
Descrición e identificación das características, os tipos e as funcións das devasas.

4.7.f) Actividades de ensino e aprendizaxe, e de avaliación, con xustificación de para que e de como se realizarán, así como os materiais e os recursos necesarios para a súa realización e, de ser o caso, os instrumentos de avaliación

Que e para que	Como			Con que	Como e con que se valora	Duración (sesións)
Actividade (título e descrición)	Profesorado (en termos de tarefas)	Alumnado (tarefas)	Resultados ou produtos	Recursos	Instrumentos e procedementos de avaliación	
Devasas - Nesta actividade analizarase a necesidade de asegurar o perímetro da rede da organización. Estudaranse as características, vantaxes, funcionalidades e tipos de devasas (tornalumes ou firewall), así como as arquitecturas de rede con devasas máis comúns.	• Análise do concepto de seguridade perímetral e explicación das características, vantaxes, funcións e tipos de devasas (tornalumes ou firewall) • Explicación das regras de filtraxe e as boas prácticas a seguir á hora de configurar un firewall. • Explicación do funcionamento do sistema de filtraxe netfilter/iptables que permite implementar un firewall • Demostración de como configurar un firewall con netfilter/iptables nun sistema Linux de propósito xeral. • Explicación das funcionalidades de Gufw, ferramenta gráfica de configuración de Netfilter.	• Regras do firewall • Explicación das arquitecturas de rede con devasas. • Deseño dunha zona DMZ • Regras con iptables • Configuración das regras do firewall empregando iptables • Instalación e configuración de Gufw	• Regras con iptables analizadas • Informe coas regras do firewall • Gufw instalado e configurado	• Canón de proxección • Aula virtual. • Ordenador persoal, con navegador web e conexión a Internet. • Máquinas virtuais Windows ou GNU/Linux. • Software necesario para a realización das tarefas.	• TO.1 - Observación directa ou dos informes entregados. • TO.2 - Observación directa ou dos informes entregados. • TO.3 - Observación directa ou dos informes entregados.	10,0
Proxies	• Explicación das características e funcións principais dos proxys. • Explicación dos tipos de proxys e do descubremento autoático dos mesmos.	• Funcionalidade do proxy. • Configuración manual do proxy nos navegadores.	• Proxy configurado. • Navegadores configurados.	• Canón de proxección. • Aula virtual. • Ordenador persoal, con navegador web e conexión a Internet. • Máquinas virtuais Windows ou GNU/Linux. • Software necesario para a realización das tarefas.	• TO.4 - Observación directa ou dos informes entregados.	10,0
					TOTAL	**20,0**

4.8.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
8	Lexislación e normativa sobre seguridade informática	10

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

Resultado de aprendizaxe do currículo	Completo
RA6 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e analiza as repercusións do seu incumprimento.	SI

4.8.c) Obxectivos específicos da unidade didáctica

Obxectivos específicos	Act	Título das actividades	Duración (sesións)
1.1 Describir a lexislación sobre protección de datos de carácter persoal. 1.2 Determinar a necesidade de controlar o acceso á información persoal almacenada. 1.3 Identificar as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos. 1.4 Contrastar a obriga de pór ao dispor das persoas os datos persoais que lles atinxen. 1.5 Describir a lexislación sobre os servizos da sociedade da información e o comercio electrónico. 1.6 Contrastar as normas sobre xestión de seguridade da información. 1.7 Comprender a necesidade de coñecer e respectar a normativa aplicable.	1	Lexislación e normativa sobre seguridade informática.	10,0
		TOTAL	**10**

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

Criterios de avaliación	Instrumentos de avaliación	Mínimos exixibles	Peso cualificación (%)
CA6.1 Describiuse a lexislación sobre protección de datos de carácter persoal.	• PE.1 - Exame escrito a final de trimestre e revisión de informes.	S	25
CA6.2 Determinouse a necesidade de controlar o acceso á información persoal almacenada.	• PE.2 - Exame escrito a final de trimestre e revisión de informes.	S	15
CA6.3 Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.	• PE.3 - Exame escrito a final de trimestre e revisión de informes.	N	10
CA6.4 Contrastouse a obriga de pór ao dispor das persoas os datos persoais que lles atinxen.	• PE.4 - Exame escrito a final de trimestre e revisión de informes.	S	15
CA6.5 Describiuse a lexislación sobre os servizos da sociedade da información e o comercio electrónico.	• PE.5 - Exame escrito a final de trimestre e revisión de informes.	N	10
CA6.6 Contrastáronse as normas sobre xestión de seguridade da información.	• PE.6 - Exame escrito a final de trimestre e revisión de informes.	N	10
CA6.7 Comprendeuse a necesidade de coñecer e respectar a normativa aplicable.	• PE.7 - Exame escrito a final de trimestre e revisión de informes.	S	15
		TOTAL	**100**

4.8.e) Contidos

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

4.8.f) Actividades de ensino e aprendizaxe, e de avaliación, con xustificación de para que e de como se realizarán, así como os materiais e os recursos necesarios para a súa realización e, de ser o caso, os instrumentos de avaliación

Que e para que	Como			Con que	Como e con que se valora	Duración (sesións)
Actividade (título e descrición)	Profesorado (en termos de tarefas)	Alumnado (tarefas)	Resultados ou produtos	Recursos	Instrumentos e procedementos de avaliación	
Lexislación e normativa sobre seguridade informática. - Nesta actividade recoñecerase a lexislación e a normativa sobre a protección de datos, a lexislación sobre os servizos da sociedade da información e o comercio electrónico e revisaranse as normas ISO sobre xestión de seguridade da información. Ademais, analizarase as repercusións do seu incumprimento.	• Explicación da Lei de Proteción de Datos. • Explicación dos diferentes tipos de comercio electrónico, do concepto de prestador de servizos da sociedade da información e da obriga do deber de información xeral. • Explicación das normas sobre a xestión da seguridade da información.	• Implatanción da Lei de Proteción de Datos nunha empresa. • Análise das sancións impostas por incumprimento da Lei de Proteción de Datos en varios supostos. • Prácticas consistente na análise da normativa revisada. • Práctica consistente na análise dos pasos a seguir para conseguir a certificación ISO27001.	• Informes	• Canón de proxección. • Aula virtual. • Ordenador persoal, con navegador web e conexión a Internet. • Software necesario para a realización das tarefas.	• PE.1 - Exame escrito a final de trimestre e revisión de informes. • PE.2 - Exame escrito a final de trimestre e revisión de informes. • PE.3 - Exame escrito a final de trimestre e revisión de informes. • PE.4 - Exame escrito a final de trimestre e revisión de informes. • PE.5 - Exame escrito a final de trimestre e revisión de informes. • PE.6 - Exame escrito a final de trimestre e revisión de informes. • PE.7 - Exame escrito a final de trimestre e revisión de informes.	10,0
					TOTAL	**10,0**

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

Os mínimos exixibles para alcanzar a avaliación positiva son os determinados no Decreto 27/2010, do 25 de febreiro, polo que se establece o currículo do ciclo formativo de grao medio correspondente ao título de técnico en sistemas microinformáticos e redes, e sinalados ao longo desta programación, en cada unha das unidades didácticas que a compoñen.

En cada UD obterase unha cualificación de 0 a 10 utilizando os criterios de avaliación e debe obterse un 5 para aprobar.

Realizaranse traballos para cada UD que deberán entregarse na aula virtual e que implican ao conxunto dos CA de cada UD.

En todos os casos, o traballo na clase que derive nunha entrega na aula virtual (que terá unha corrección conxunta na clase ou unha entrega das solucións), ponderará un 10% en cada UD.

Estes traballos puntuaranse como 10 sempre que a entrega sexa en tempo e forma (indicarase na aula virtual) e o contido se corresponda cos enunciados solicitados.

No caso de que algún traballo non estea feito en tempo e forma poderase entregar ata 1 semana antes do día da avaliación oficial do centro, neste caso, a nota destes traballo será 0, pero poderase aprobar a UD se se obtén no exame un 5 sobre 9.

Se despois da semana antes da avaliación non se entregan algún dos traballos ou algunha das entregas non teñen relación co enunciado, a avaliación da UD será suspensa.

Os exercicios entregados na aula virtual poderán ser materia de exame, e poderá solicitarse a entrega parcial ou total dun traballo entregado para a súa avaliación exhaustiva. O alumnado é responsable de subir a AV as tarefas corrixidas para afrontar unha posible pregunta no exame correspondente.

Cada UD poderase avaliar segundo un exame escrito ou un exame práctico ou unha combinación dos dous tipos. O peso de cada tipo de exame na avaliación de cada UD pode variar en función da súa dificultade e da súa relación cos CA correspondente. Deberase informar ao alumnado do peso en cada avaliación.

Para superar unha avaliación parcial, será necesario ter unha cualificación mínima de 5 en cada unha das unidades avaliadas ata ese momento, aínda que se gardará a nota das UD aprobadas ata a avaliación final.

A nota da avaliación final calcularase coas cualificacións das UD realizadas e ponderadas polo seu peso dentro do módulo. Por conseguinte, esta xa será a nota final do módulo, cumprindo o establecido na Orde do 12 de xullo de 2011 pola que se regula a avaliación e a acreditación académica do alumnado que cursa as ensinanzas de formación profesional inicial.

O alumnado que non superase algunha das UD, deberá seguir o procedemento para recuperar as partes suspensas segundo o que se establece no seguinte punto.

Para superar a avaliación final, será necesario ter unha cualificación mínima de 5 en cada unha das UD e todas as practicas entregadas en tempo e forma. A nota da avaliación final formarase coas cualificacións das UD ponderadas polo seu peso dentro do módulo.

AVISO: se un alumno copia obterá unha cualificación de 0 puntos.

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

Naquelas unidades didácticas nas que non se acadaran os mínimos esixibles establecidos nesta programación, seguirase o procedemento seguinte:

Analizaranse, conxuntamente co/a alumno/a, aqueles criterios de avaliación e contidos para os que non se cumplen os mínimos esixibles.

Proporanse as oportunas actividades de recuperación, que poderán incluír tarefas xa desenvolvidas como outras novas, co fin de acadar os mínimos esixibles da unidade.

As novas tarefas que se propoñan ao alumnado terán un nivel máis gradual no seu desenvolvemento, co obxectivo de facilitar a adquisición das habilidades requiridas nos criterios de avaliación.

As actividades de recuperación para o alumnado que non supere o módulo no segundo trimestre realizaranse ao longo do terceiro trimestre e incidirán na parte máis práctica do módulo, xa que consistirán na resolución por parte do alumnado das actividades xa realizadas durante o curso (incidindo especialmente nas probas de avaliación parciais realizadas) e/ou novas actividades similares propostas polo profesor.

Finalizadas estas actividades, o alumno ou alumna deberá superar unha proba de recuperación daquelas avaliacións non superadas, na que deberá obter unha cualificación mínima de 5 para recuperar o módulo. Para aprobar o módulo será imprescindible ter entregada todas as prácticas en tempo e forma indicadas pola docente.

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

Para o alumnado que perda o dereito a avaliación continua ou non supere o proceso ordinario de avaliación, a avaliación final extraordinaria do módulo consistirá na realización de varias probas co obxectivo de comprobar que este acade os contidos mínimos recollidos nesta programación.

As probas que deberá realizar serán as seguintes:

- Unha proba escrita para avaliar aqueles criterios que nesta programación teñen asignado como instrumento de avaliación o de proba escrita.
- Unha proba práctica no ordenador para aqueles criterios que nesta programación teñen asignado como instrumento de avaliación o de lista de cotexo aplicada sobre un informe feito a partir do traballo realizado sobre máquinas virtuais.
- Unha proba práctica na que realizará a instalación e configuración de distintos elementos de seguridade informática manexados: Cámaras de videovixilancia, SAIs, RAID, sistemas de almacenamento externos, dispositivos redundantes, dispositivos de autenticación e control de acceso e routers-firewall.

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

- O seguimento da programación de cada módulo farase a través da aplicación web Xestión das programacións, da Consellería de Educación (https://www.edu.xunta.es/programacions/).

- Cada vez que se inicie/remate unha unidade anotaranse as datas de inicio/fin na aplicación e por cada unidade, tamén se indicará a data en que é avaliada, sesións realizadas, grao de cumprimento, e todas aquelas observacións que o profesorado estime oportunas.

- Dende o departamento establécese un calendario para a realización do seguimento das programacións

- O profesor recollerá a temporalización real das distintas unidades didácticas, co obxectivo de poder corrixir no propio curso os desfases detectados fronte a temporalización prevista e precisar mellor a temporalización das unidades en vindeiros cursos académicos.

-Día a día, farase un seguimento das actividades na app Additio.

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

Farase unha avaliación inicial de coñecementos xerais de Seguridade Informática para coñecer o nivel de coñecementos técnicos e de costumes na xestión da seguridade dos dispositivos cotiáns que xestiona cada persoa

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

- Realizar de novo diferentes actividades e cuestionarios na aula virtual no centro, fora do horario de clases.
- Resolver actividades extra propostas na aula virtual, fora do horario de clases.
- Resolver as probas de recuperación dos distintos trimestres.

9. Aspectos transversais

9.a) Programación da educación en valores

En particular, ao longo de todo o proceso de ensino-aprendizaxe transmitiráselle ao alumnado:

- Fomentar o traballo en equipo
- Evitar os condicionantes de xénero nos exercicios, nos exemplos e nos traballos en grupo.
- A necesidade de respectar o material existente no taller, tanto hardware como software.
- A obrigatoriedade do cumprimento da normativa vixente en canto ao non emprego de copias ilegais de software.
- A necesidade de manter a confidencialidade dos datos que así o requiran e respectar a propiedade intelectual.
- A necesidade de manter un clima de respeto cara aos compañeiros e ao profesor.

9.b) Actividades complementarias e extraescolares

Realizarase unha visita ao CESGA en Santiago de Compostela para que o alumnado teña contacto con un CPD para observar a infraestructura e analizar todas as medidas de seguridade que ten implementadas.
Ademais, o Departamento de Informática programará otras actividades extraescolares ao longo do curso nas que se participará. de forma activa.

10.Outros apartados

10.1) Modificación da ensinanza motivada pola situación sanitaria (COVID-19)

No caso de que a situación sanitaria provocada polo COVID-19 non permita a ensinanza semipresencial e haxa que pasar a ensinanza telemática para todo o alumnado tomaranse as seguintes medidas e pautas:

* Utilizarase a aplicación de Cisco, Webex para realizar clases online, a aula virtual para a entrega de exercicios, e o correo como apoio a comunicación entre o alumando e a docente.

* Usarase a plataforma de almacenamento Drive para o intercambio de software ou documentación que non sexa apropiada para ser posta na aula virtual.

* O horario de conexión online para impartir as clases será espello do horario presencial.

10.2) Lingua de impartición do módulo

A lingua galega será a utilizada para impartir as clases e na que estará o material de estudo/prácticas e documentación.
Poderá haber documentación en otras linguas como o castelán e inglés xa que moita da documentación existente utiliza estes idiomas.

10.3) Transparencia

Tan pronto como sexa posible, farase un resumo da programación ao alumnado indicándolles os obxectivos do módulo, as unidades didácticas nas que se divide o módulo e cómo se van desenvolver as clases, indicándoselles os criterios de cualificación que se van aplicar para obter a nota.
A programación estará a disposición dos alumnos na aula virtual e na web do instituto.

10.4) Secuencia dos contidos

As unidades didácticas poderanse impartir en un orde diferente ao indicado na programación por motivo xustificados.