1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
36019475	de Rodeira	Cangas	2023/2024

Ciclo formativo

Código da familia profesional	Familia profesional	Código do ciclo formativo	Ciclo formativo	Grao	Réxime
IFC	Informática e comunicacións	CSIFC01	Administración de sistemas informáticos en rede	Ciclos formativos de grao superior	Réxime xeral-ordinario

Módulo profesional e unidades formativas de menor duración (*)

Código MP/UF	Nome	Curso	Sesións semanais	Horas anuais	Sesións anuais
MP0378	Seguridade e alta dispoñibilidade	2023/2024	6	105	126

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

Profesorado responsable

Profesorado asignado ao módulo	FRANCISCO JAVIER TABOADA AGUADO
Outro profesorado	

Estado: Pendente de supervisión departamento

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

O contorno productivo está principalmente relacionado coa pesca, como a cria de mexilóns ou a actividade conserveira e o turismo. A situación a carón de Vigo, fai que moita da actividade se desenvolva na industria desta cidade. En relación a este módulo en concreto, a súa xeneralidade fai que os contidos podan adaptarse a calquera tipo de empresa que manteña un sistema informático, e en particular a empresas de servicios informáticos.

3. Relación de unidades didácticas que a integran, que contribuirán ao desenvolvemento do módulo profesional, xunto coa secuencia e o tempo asignado para o desenvolvemento de cada unha

U.D.	Título	Descrición	Duración (sesións)	Peso (%)
1	Introducción á Virtualización	Introducción a virtualización e a súa tipoloxía	24	10
2	Adopción de Pautas de Seguridade Informática	Introducción do concepto de seguridade informática e descrición das vulnerabilidades do sistema	6	5
3	Autenticación e Autorización	Mecanismos de autenticación e autorización	14	15
4	Cifrado da Información	Protección da confidencialidade, integridade e non repudio mediante cifrado	20	15
5	Mecanismos de Seguridade Activa e Pasiva	Bonding, Raid, Clustering e Backups	12	15
6	Seguridade Perimetral	Métodos de acceso e Protección do sistema contra ataques remotos	22	15
7	Firewalls	Descrición de en qué consiste o análise forense e de algunhas das ferramentas empregadas	6	5
8	Proxys	Descrición do proceso e das ferramentas necesarias para a realización dun plan de Seguridade Informática	6	5
9	Solucións de Alta Dispoñibilidade	Garantización da dispoñibilidade en servizos e sistemas	14	10
10	Protección de Datos	Introducción ao cifrado de información e ás infraestructuras de chave pública	2	5

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Introducción á Virtualización	24

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

Resultado de aprendizaxe do currículo	Completo
RA6 - Implanta solucións de alta dispoñibilidade empregando técnicas de virtualización, e configura os contornos de proba.	NO

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

Criterios de avaliación
CA6.3 Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.
CA6.3.2 Crearonse servizos virtualizados basados en Containers
CA6.3.3 Crearonse servizos virtualizados basados en Hypervisores tipo I e tipo II
CA6.3.4 Establecéronse diferentes configuracións de rede entre máquinas virtuais
CA6.3.5 Utilizouse aprovisionamiento lixeiro para o despregue de máquinas virtuais
CA6.3.6 Empregáronse mecanismos de acceso remoto ao almacenamento virtual

4.1.e) Contidos

Contidos
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. Xestión da configuración de rede Xestión do almacenamento

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Adopción de Pautas de Seguridade Informática	6

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.	NO
RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.	NO

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

Criterios de avaliación
CA1.1 Valorouse a importancia de asegurar a privacidade, a coherencia e a dispoñibilidade da información nos sistemas informáticos.
CA1.2 Describíronse as diferenzas entre seguridade física e lóxica.
CA1.3 Clasificáronse 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.
CA1.6 Valoráronse as vantaxes do uso de sistemas biométricos.
CA1.9 Identificáronse as fases da análise forense ante ataques a un sistema.
0CA1.10 Comprendeuse o fundamento técnico das vulnerabilidades máis comúns e se estableceron medidas paliativas.
CA1.11 Comprendeuse o procedemento a seguir nun análise forense e a tipoloxía das súas ferramentas
CA2.1 Clasificáronse os principais tipos de ameazas lóxicas contra un sistema informático.
CA2.2 Verificouse a orixe e a autenticidade das aplicacións instaladas nun equipamento, así como o estado de actualización do sistema operativo.
CA2.3 Identificouse 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.

4.2.e) Contidos

Contidos
0Ferramentas empregadas na análise forense. Fiabilidade, confidencialidade, integridade e dispoñibilidade.

Contidos
Elementos vulnerables no sistema informático: hardware, software e datos.
Análise das principais vulnerabilidades dun sistema informático.
Pautas e prácticas seguras.
Tipos de ameazas: físicas e lóxicas.
Seguridade física e ambiental: Localización e protección física dos equipamentos e dos servidores. Sistemas de alimentación ininterrompida.
Análise forense en sistemas informáticos: obxectivo. Recollida e análise de incidencias.
Ataques e contramedidas en sistemas informáticos.
Monitorización do tráfico en redes: captura e análise; aplicacións.
Riscos potenciais dos servizos de rede. Software para detección de vulnerabilidades.
Intentos de penetración: tipoloxía.
Sistemas de detección de intrusións.
Clasificación dos ataques.
Anatomía de ataques e análise de software malicioso.
Realización de auditorías de seguridade.
Ferramentas preventivas e paliativas: instalación e configuración.
Recuperación de datos.
Actualización de sistemas e aplicacións.

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Autenticación e Autorización	14

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.	NO
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade.	NO

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

Criterios de avaliación
CA1.5 Adoptáronse políticas de contrasinais.
CA1.12 Comprendeuse a diferencia e importancia entre os sistemas MAC e DAC
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.

4.3.e) Contidos

Contidos
Distinguir entre sistemas de autorización discrecional e obrigatorios Seguridade lóxica: Criptografía. Listas de control de acceso. Establecemento de políticas de contrasinais. Sistemas biométricos de identificación. Políticas de almacenamento. Medios de almacenamento. Seguridade nos protocolos para comunicacións sen fíos.

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Cifrado da Información	20

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.	NO
RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.	NO
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade.	NO

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

Criterios de avaliación
CA1.7 Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información.
CA2.6 Utilizáronse técnicas de cifraxe, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas.
CA3.3 Identificáronse os protocolos seguros de comunicación e os seus ámbitos de uso.

4.4.e) Contidos

Contidos
0Técnicas de cifraxe da información: clave pública e clave privada; certificados dixitais; sinaturas.

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Mecanismos de Seguridade Activa e Pasiva	12

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

Resultado de aprendizaxe do currículo	Completo
RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.	NO

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

Criterios de avaliación
0CA2.10 Configuráronse sistemas de copia de seguridade incrementais e/ou diferenciais.
CA2.11 Seleccionouse o sistema de copia de seguridade máis axeitado para cada caso.

4.5.e) Contidos

Contidos
Copias de seguridade e imaxes de respaldo.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Seguridade Perimetral	22

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.	NO
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade.	NO

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

Criterios de avaliación
CA1.8 Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.
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.
CA3.4 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.

4.6.e) Contidos

Contidos
Seguridade na conexión con redes públicas. 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.

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Firewalls	6

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

Resultado de aprendizaxe do currículo	Completo
RA4 - Implanta tornalumes (firewalls) para asegurar un sistema informático, analiza as súas prestacións e controla o tráfico cara á rede interna.	SI

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

Criterios de avaliación
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 Configuráronse filtros nun tornalumes a partir dunha listaxe de regras de filtraxe.
CA4.4 Revisáronse os rexistros de sucesos de tornalumes, para verificar que as regras se apliquen correctamente.
CA4.5 Interpretouse a documentación técnica de distintos tornalumes hardware nos idiomas máis empregados pola industria.
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 Planificouse a instalación de tornalumes para limitar os accesos a determinadas zonas da rede.
CA4.9 Elaborouse documentación relativa á instalación, configuración e uso de tornalumes.

4.7.e) Contidos

Contidos
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 nos tornalumes.

4.8.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
8	Proxys	6

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

Resultado de aprendizaxe do currículo	Completo
RA5 - Implanta servidores proxy, aplicando criterios de configuración que garantan o funcionamento seguro do servizo.	SI

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

Criterios de avaliación
CA5.1 Identificáronse os tipos de proxy, as súas características e as súas funcións principais.
CA5.2 Instalouse e configurouse un servidor proxy cache.
CA5.3 Configuráronse os métodos de autenticación no proxy.
CA5.4 Configurouse un proxy en modo transparente.
CA5.5 Utilizouse o servidor proxy para establecer restricións de acceso web.
CA5.6 Arranxáronse problemas de acceso desde os clientes ao proxy.
CA5.7 Realizáronse probas de funcionamento do proxy, monitorizando a súa actividade con ferramentas gráficas.
CA5.8 Configurouse un servidor proxy en modo inverso.
CA5.9 Elaborouse documentación relativa á instalación, a configuración e o uso de servidores proxy.

4.8.e) Contidos

Contidos
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.
Encadeamento e xerarquías.
Probas de funcionamento.

4.9.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
9	Solucións de Alta Dispoñibilidade	14

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

Resultado de aprendizaxe do currículo	Completo
RA6 - Implanta solucións de alta dispoñibilidade empregando técnicas de virtualización, e configura os contornos de proba.	NO

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

Criterios de avaliación
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.
CA6.3 Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.
CA6.3.1 Avaliaronse as posibilidades da virtualización nos sistemas de alta dispoñibilidade
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 Esquematizáronse e documentáronse solucións para supostos con necesidades de alta dispoñibilidade.

4.9.e) Contidos

Contidos
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. Instalación e configuración de solucións de alta dispoñibilidade.

4.10.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
10	Protección de Datos	2

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

Resultado de aprendizaxe do currículo	Completo
RA7 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia.	SI

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

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

4.10.e) Contidos

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

5.1 Peso dos procedementos e instrumentos de avaliación dos CA na cualificación

Procedementos e instrumentos de avaliación		UD1	UD10	UD2	UD3	UD4	UD5	UD6	UD7	UD8	UD9	Total
		10 %	5 %	5 %	15 %	15 %	15 %	15 %	5 %	5 %	10 %	100,00 %
Proba de coñecementos		0 %	100 %	79 %	10 %	50 %	0 %	0 %	20 %	10 %	40 %	23,45 %
	Proba escrita + modelo de solución	0 %	100 %	79 %	10 %	50 %	0 %	0 %	20 %	10 %	40 %	23,45 %
Proba de desempeño		100 %	0 %	21 %	90 %	50 %	100 %	100 %	80 %	90 %	60 %	76,55 %
	Táboa de indicadores de observación	100 %	0 %	21 %	90 %	50 %	100 %	100 %	80 %	90 %	60 %	76,55 %

Todas as probas	UD1	UD10	UD2	UD3	UD4	UD5	UD6	UD7	UD8	UD9	Total
	10 %	5 %	5 %	15 %	15 %	15 %	15 %	5 %	5 %	10 %	100,00 %
Proba escrita + modelo de solución	0 %	100 %	79 %	10 %	50 %	0 %	0 %	20 %	10 %	40 %	23,45 %
Táboa de indicadores de observación	100 %	0 %	21 %	90 %	50 %	100 %	100 %	80 %	90 %	60 %	76,55 %

Todas as probas	RA1	RA2	RA3	RA4	RA5	RA6	RA7	Total
	10,80 %	24,95 %	29,25 %	5,00 %	5,00 %	20,00 %	5,00 %	100,00 %
Proba escrita + modelo de solución	72,22 %	5,61 %	12,82 %	20,00 %	10,00 %	20,00 %	100,00 %	23,45 %
Táboa de indicadores de observación	27,78 %	94,39 %	87,18 %	80,00 %	90,00 %	80,00 %	0,00 %	76,55 %

5.2 Niveis de logro mínimo dos CA (mínimo esixible)

Criterios ou subcriterios de avaliación	Nivel de logro do mínimo esixible
UD 1. Introducción á Virtualización	
CA 6.3 Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.	
CA 6.3.2 Crearonse servizos virtualizados basados en Containers	si
CA 6.3.3 Crearonse servizos virtualizados basados en Hypervisores tipo I e tipo II	si
CA 6.3.4 Establecéronse diferentes configuracións de rede entre máquinas virtuais	si
CA 6.3.5 Utilizouse aprovisionamiento lixeiro para o despregue de máquinas virtuais	si
CA 6.3.6 Empregáronse mecanismos de acceso remoto ao almacenamento virtual	si
UD 2. Adopción de Pautas de Seguridade Informática	
CA 1.1 Valorouse a importancia de asegurar a privacidade, a coherencia e a dispoñibilidade da información nos sistemas informáticos.	si
CA 1.2 Describíronse as diferenzas entre seguridade física e lóxica.	si
CA 1.3 Clasificáronse os tipos principais de vulnerabilidade dun sistema informático, segundo a súa tipoloxía e a súa orixe.	non
CA 1.4 Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas.	non
CA 1.6 Valoráronse as vantaxes do uso de sistemas biométricos.	non
CA 1.9 Identificáronse as fases da análise forense ante ataques a un sistema.	si
CA 1.10 Comprendeuse o fundamento técnico das vulnerabilidades máis comúns e se estableceron medidas paliativas.	si
CA 1.11 Comprendeuse o procedemento a seguir nun análise forense e a tipoloxía das súas ferramentas	non
CA 2.1 Clasificáronse os principais tipos de ameazas lóxicas contra un sistema informático.	non
CA 2.2 Verificouse a orixe e a autenticidade das aplicacións instaladas nun equipamento, así como o	non

Criterios ou subcriterios de avaliación	Nivel de logro do mínimo esixible
estado de actualización do sistema operativo.	non
CA 2.3 Identificouse a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.	non
CA 2.4 Analizáronse diversos tipos de ameazas, ataques e software malicioso, en contornos de execución controlados.	non
CA 2.5 Implantáronse aplicacións específicas para a detección de ameazas e a eliminación de software malicioso.	non
CA 2.7 Avaliáronse as medidas de seguridade dos protocolos usados en redes de comunicación.	si
CA 2.8 Recoñeceuse a necesidade de inventariar e controlar os servizos de rede que se executan nun sistema.	si
CA 2.9 Describíronse os tipos e as características dos sistemas de detección de intrusións.	si
UD 3. Autenticación e Autorización	
CA 1.5 Adoptáronse políticas de contrasinais.	si
CA 1.12 Comprendeuse a diferencia e importancia entre os sistemas MAC e DAC	si
CA 3.6 Identificáronse e configuráronse os métodos posibles de autenticación no acceso de usuarios remotos a través da pasarela.	si
CA 3.7 Instalouse, configurouse e integrouse na pasarela un servidor remoto de autenticación.	si
UD 4. Cifrado da Información	
CA 1.7 Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información.	si
CA 2.6 Utilizáronse técnicas de cifraxe, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas.	si
CA 3.3 Identificáronse os protocolos seguros de comunicación e os seus ámbitos de uso.	si
UD 5. Mecanismos de Seguridade Activa e Pasiva	
CA 2.10 Configuráronse sistemas de copia de seguridade incrementais e/ou diferenciais.	si
CA 2.11 Seleccionouse o sistema de copia de seguridade máis axeitado para cada caso.	si
UD 6. Seguridade Perimetral	
CA 1.8 Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.	si
CA 3.1 Describíronse escenarios típicos de sistemas con conexión a redes públicas en que cumpra fortificar a rede interna.	si
CA 3.2 Clasificáronse as zonas de risco dun sistema, segundo criterios de seguridade perimetral.	si
CA 3.4 Configuráronse redes privadas virtuais mediante protocolos seguros a distintos niveis.	si
CA 3.5 Implantouse un servidor como pasarela de acceso á rede interna desde localizacións remotas.	si
UD 7. Firewalls	
CA 4.1 Describíronse as características, os tipos e as funcións dos tornalumes.	Coñecer a tipoloxía dos tornalumes
CA 4.2 Clasificáronse os niveis en que se realiza a filtraxe de tráfico.	Distinguir entre os tipos de filtrado
CA 4.3 Configuráronse filtros nun tornalumes a partir dunha listaxe de regras de filtraxe.	Ser capaz de establecer regras no tornalumes para impedir o trafico non desexado
CA 4.4 Revisáronse os rexistros de sucesos de tornalumes, para verificar que as regras se apliquen correctamente.	Ser capaz de detectar fallos na configuración dos tornalumes
CA 4.5 Interpretouse a documentación técnica de distintos tornalumes hardware nos idiomas máis empregados pola industria.	Ser capaz de comprender a documentacion dun tornalumes
CA 4.6 Probáronse distintas opcións para implementar tornalumes, tanto de software como de hardware.	Ser capaz de implantar un tornalumes
CA 4.7 Diagnosticáronse problemas de conectividade nos clientes provocados polos tornalumes.	Ser capaz de detectar e correxir fallos nos servicios debidos a erros no tornalumes
CA 4.8 Planificouse a instalación de tornalumes para limitar os accesos a determinadas zonas da rede.	Ser capaz de planificar un conxunto de reglas para protexer unha rede
CA 4.9 Elaborouse documentación relativa á instalación, configuración e uso de tornalumes.	Dispoñer da documentación das reglas deseñadas para a rede
UD 8. Proxys	

Criterios ou subcriterios de avaliación	Nivel de logro do mínimo esixible
CA 5.1 Identificáronse os tipos de proxy, as súas características e as súas funcións principais.	Coñecer a utilidade e tipoloxías dos proxy
CA 5.2 Instalouse e configurouse un servidor proxy cache.	Ser capaz de instalar e configurar un proxy caché
CA 5.3 Configuráronse os métodos de autenticación no proxy.	Ser capaz de configurar a seguridade dun proxy caché
CA 5.4 Configurouse un proxy en modo transparente.	Ser capaz de configurar un proxy transparente
CA 5.5 Utilizouse o servidor proxy para establecer restricións de acceso web.	Ser capaz de restrinxir o acceso a sitios web mediante o uso dun proxy
CA 5.6 Arranxáronse problemas de acceso desde os clientes ao proxy.	Ser capaz de detectar e correxir os problemas de acceso debidos a un proxy
CA 5.7 Realizáronse probas de funcionamento do proxy, monitorizando a súa actividade con ferramentas gráficas.	Ser capaz de monitorizar o proxy
CA 5.8 Configurouse un servidor proxy en modo inverso.	Ser capaz de configurar un proxy inverso
CA 5.9 Elaborouse documentación relativa á instalación, a configuración e o uso de servidores proxy.	Dispoñer da documentación do traballo de configuración
UD 9. Solucións de Alta Dispoñibilidade	
CA 6.1 Analizáronse supostos e situacións en que cumpra pór en marcha solucións de alta dispoñibilidade.	si
CA 6.2 Identificáronse solucións de hardware para asegurar a continuidade no funcionamento dun sistema.	si
CA 6.3 Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.	
CA 6.3.1 Avaliaronse as posibilidades da virtualización nos sistemas de alta dispoñibilidade	si
CA 6.4 Implantouse un servidor redundante que garanta a continuidade de servizos en casos de caída do servidor principal.	si
CA 6.5 Implantouse un balanceador de carga á entrada da rede interna.	si
CA 6.6 Implantáronse sistemas de almacenamento redundante sobre servidores e dispositivos específicos.	si
CA 6.7 Avaliouse a utilidade dos sistemas de clúster para aumentar a fiabilidade e a produtividade do sistema.	si
CA 6.8 Analizáronse solucións de futuro para un sistema con demanda crecente.	si
CA 6.9 Esquematizáronse e documentáronse solucións para supostos con necesidades de alta dispoñibilidade.	si
UD 10. Protección de Datos	
CA 7.1 Describiuse a lexislación sobre protección de datos de carácter persoal.	si
CA 7.2 Determinouse a necesidade de controlar o acceso á información persoal almacenada.	si
CA 7.3 Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.	si
CA 7.4 Contrastouse o deber de pór ao dispor das persoas os datos persoais que lles atinxen.	sii
CA 7.5 Describiuse a lexislación actual sobre os servizos da sociedade da información e o comercio electrónico.	si
CA 7.6 Contrastáronse as normas sobre xestión de seguridade da información.	si
CA 7.7 Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable.	si

5.3 Peso dos CA na cualificación das UD e pesos das UD na cualificación do módulo

Unidades didácticas e criterios de avaliación	%
UD 1. Introducción á Virtualización	**10 %**
CA 6.3 Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.	0 %
CA 6.3.2 Crearonse servizos virtualizados basados en Containers	20 %
CA 6.3.3 Crearonse servizos virtualizados basados en Hypervisores tipo I e tipo II	20 %
CA 6.3.4 Establecéronse diferentes configuracións de rede entre máquinas virtuais	20 %

Unidades didácticas e criterios de avaliación	%
CA 6.3.5 Utilizouse aprovisionamiento lixeiro para o despregue de máquinas virtuais	20 %
CA 6.3.6 Empregáronse mecanismos de acceso remoto ao almacenamento virtual	20 %
UD 2. Adopción de Pautas de Seguridade Informática	**5 %**
CA 1.1 Valorouse a importancia de asegurar a privacidade, a coherencia e a dispoñibilidade da información nos sistemas informáticos.	10 %
CA 1.2 Describíronse as diferenzas entre seguridade física e lóxica.	10 %
CA 1.3 Clasificáronse os tipos principais de vulnerabilidade dun sistema informático, segundo a súa tipoloxía e a súa orixe.	3 %
CA 1.4 Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas.	3 %
CA 1.6 Valoráronse as vantaxes do uso de sistemas biométricos.	2 %
CA 1.9 Identificáronse as fases da análise forense ante ataques a un sistema.	10 %
CA 1.10 Comprendeuse o fundamento técnico das vulnerabilidades máis comúns e se estableceron medidas paliativas.	10 %
CA 1.11 Comprendeuse o procedemento a seguir nun análise forense e a tipoloxía das súas ferramentas	3 %
CA 2.1 Clasificáronse os principais tipos de ameazas lóxicas contra un sistema informático.	3 %
CA 2.2 Verificouse a orixe e a autenticidade das aplicacións instaladas nun equipamento, así como o estado de actualización do sistema operativo.	3 %
CA 2.3 Identificouse a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.	5 %
CA 2.4 Analizáronse diversos tipos de ameazas, ataques e software malicioso, en contornos de execución controlados.	3 %
CA 2.5 Implantáronse aplicacións específicas para a detección de ameazas e a eliminación de software malicioso.	5 %
CA 2.7 Avaliáronse as medidas de seguridade dos protocolos usados en redes de comunicación.	10 %
CA 2.8 Recoñeceuse a necesidade de inventariar e controlar os servizos de rede que se executan nun sistema.	10 %
CA 2.9 Describíronse os tipos e as características dos sistemas de detección de intrusións.	10 %
UD 3. Autenticación e Autorización	**15 %**
CA 1.5 Adoptáronse políticas de contrasinais.	10 %
CA 1.12 Comprendeuse a diferencia e importancia entre os sistemas MAC e DAC	10 %
CA 3.6 Identificáronse e configuráronse os métodos posibles de autenticación no acceso de usuarios remotos a través da pasarela.	40 %
CA 3.7 Instalouse, configurouse e integrouse na pasarela un servidor remoto de autenticación.	40 %
UD 4. Cifrado da Información	**15 %**
CA 1.7 Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información.	25 %
CA 2.6 Utilizáronse técnicas de cifraxe, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas.	50 %
CA 3.3 Identificáronse os protocolos seguros de comunicación e os seus ámbitos de uso.	25 %
UD 5. Mecanismos de Seguridade Activa e Pasiva	**15 %**
CA 2.10 Configuráronse sistemas de copia de seguridade incrementais e/ou diferenciais.	80 %
CA 2.11 Seleccionouse o sistema de copia de seguridade máis axeitado para cada caso.	20 %
UD 6. Seguridade Perimetral	**15 %**
CA 1.8 Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.	10 %
CA 3.1 Describíronse escenarios típicos de sistemas con conexión a redes públicas en que cumpra fortificar a rede interna.	10 %
CA 3.2 Clasificáronse as zonas de risco dun sistema, segundo criterios de seguridade perimetral.	10 %
CA 3.4 Configuráronse redes privadas virtuais mediante protocolos seguros a distintos niveis.	35 %
CA 3.5 Implantouse un servidor como pasarela de acceso á rede interna desde localizacións remotas.	35 %
UD 7. Firewalls	**5 %**
CA 4.1 Describíronse as características, os tipos e as funcións dos tornalumes.	10 %

Unidades didácticas e criterios de avaliación	%
CA 4.2 Clasificáronse os niveis en que se realiza a filtraxe de tráfico.	10 %
CA 4.3 Configuráronse filtros nun tornalumes a partir dunha listaxe de regras de filtraxe.	15 %
CA 4.4 Revisáronse os rexistros de sucesos de tornalumes, para verificar que as regras se apliquen correctamente.	10 %
CA 4.5 Interpretouse a documentación técnica de distintos tornalumes hardware nos idiomas máis empregados pola industria.	10 %
CA 4.6 Probáronse distintas opcións para implementar tornalumes, tanto de software como de hardware.	10 %
CA 4.7 Diagnosticáronse problemas de conectividade nos clientes provocados polos tornalumes.	10 %
CA 4.8 Planificouse a instalación de tornalumes para limitar os accesos a determinadas zonas da rede.	15 %
CA 4.9 Elaborouse documentación relativa á instalación, configuración e uso de tornalumes.	10 %
UD 8. Proxys	**5 %**
CA 5.1 Identificáronse os tipos de proxy, as súas características e as súas funcións principais.	10 %
CA 5.2 Instalouse e configurouse un servidor proxy cache.	20 %
CA 5.3 Configuráronse os métodos de autenticación no proxy.	10 %
CA 5.4 Configurouse un proxy en modo transparente.	15 %
CA 5.5 Utilizouse o servidor proxy para establecer restricións de acceso web.	10 %
CA 5.6 Arranxáronse problemas de acceso desde os clientes ao proxy.	10 %
CA 5.7 Realizáronse probas de funcionamento do proxy, monitorizando a súa actividade con ferramentas gráficas.	3 %
CA 5.8 Configurouse un servidor proxy en modo inverso.	20 %
CA 5.9 Elaborouse documentación relativa á instalación, a configuración e o uso de servidores proxy.	2 %
UD 9. Solucións de Alta Dispoñibilidade	**10 %**
CA 6.1 Analizáronse supostos e situacións en que cumpra pór en marcha solucións de alta dispoñibilidade.	10 %
CA 6.2 Identificáronse solucións de hardware para asegurar a continuidade no funcionamento dun sistema.	10 %
CA 6.3 Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.	0 %
CA 6.3.1 Avaliaronse as posibilidades da virtualización nos sistemas de alta dispoñibilidade	10 %
CA 6.4 Implantouse un servidor redundante que garanta a continuidade de servizos en casos de caída do servidor principal.	15 %
CA 6.5 Implantouse un balanceador de carga á entrada da rede interna.	15 %
CA 6.6 Implantáronse sistemas de almacenamento redundante sobre servidores e dispositivos específicos.	10 %
CA 6.7 Avaliouse a utilidade dos sistemas de clúster para aumentar a fiabilidade e a produtividade do sistema.	10 %
CA 6.8 Analizáronse solucións de futuro para un sistema con demanda crecente.	10 %
CA 6.9 Esquematizáronse e documentáronse solucións para supostos con necesidades de alta dispoñibilidade.	10 %
UD 10. Protección de Datos	**5 %**
CA 7.1 Describiuse a lexislación sobre protección de datos de carácter persoal.	15 %
CA 7.2 Determinouse a necesidade de controlar o acceso á información persoal almacenada.	15 %
CA 7.3 Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.	15 %
CA 7.4 Contrastouse o deber de pór ao dispor das persoas os datos persoais que lles atinxen.	15 %
CA 7.5 Describiuse a lexislación actual sobre os servizos da sociedade da información e o comercio electrónico.	15 %
CA 7.6 Contrastáronse as normas sobre xestión de seguridade da información.	15 %
CA 7.7 Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable.	10 %

5.4 Peso dos CA na cualificación dos RA e peso dos RA na cualificación do módulo

Resultados de aprendizaxe e criterios de avaliación	%
RA 1. Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.	**10,80 %**
CA 1.1 Valorouse a importancia de asegurar a privacidade, a coherencia e a dispoñibilidade da información nos sistemas informáticos.	4,63 %
CA 1.2 Describíronse as diferenzas entre seguridade física e lóxica.	4,63 %
CA 1.3 Clasificáronse os tipos principais de vulnerabilidade dun sistema informático, segundo a súa tipoloxía e a súa orixe.	1,39 %
CA 1.4 Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas.	1,39 %
CA 1.5 Adoptáronse políticas de contrasinais.	13,89 %
CA 1.6 Valoráronse as vantaxes do uso de sistemas biométricos.	0,93 %
CA 1.7 Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información.	34,72 %
CA 1.8 Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.	13,89 %
CA 1.9 Identificáronse as fases da análise forense ante ataques a un sistema.	4,63 %
CA 1.10 Comprendeuse o fundamento técnico das vulnerabilidades máis comúns e se estableceron medidas paliativas.	4,63 %
CA 1.11 Comprendeuse o procedemento a seguir nun análise forense e a tipoloxía das súas ferramentas	1,39 %
CA 1.12 Comprendeuse a diferencia e importancia entre os sistemas MAC e DAC	13,89 %
RA 2. Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.	**24,95 %**
CA 2.1 Clasificáronse os principais tipos de ameazas lóxicas contra un sistema informático.	0,60 %
CA 2.2 Verificouse a orixe e a autenticidade das aplicacións instaladas nun equipamento, así como o estado de actualización do sistema operativo.	0,60 %
CA 2.3 Identificouse a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.	1,00 %
CA 2.4 Analizáronse diversos tipos de ameazas, ataques e software malicioso, en contornos de execución controlados.	0,60 %
CA 2.5 Implantáronse aplicacións específicas para a detección de ameazas e a eliminación de software malicioso.	1,00 %
CA 2.6 Utilizáronse técnicas de cifraxe, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas.	30,06 %
CA 2.7 Avaliáronse as medidas de seguridade dos protocolos usados en redes de comunicación.	2,00 %
CA 2.8 Recoñeceuse a necesidade de inventariar e controlar os servizos de rede que se executan nun sistema.	2,00 %
CA 2.9 Describíronse os tipos e as características dos sistemas de detección de intrusións.	2,00 %
CA 2.10 Configuráronse sistemas de copia de seguridade incrementais e/ou diferenciais.	48,10 %
CA 2.11 Seleccionouse o sistema de copia de seguridade máis axeitado para cada caso.	12,02 %
RA 3. Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade.	**29,25 %**
CA 3.1 Describíronse escenarios típicos de sistemas con conexión a redes públicas en que cumpra fortificar a rede interna.	5,13 %
CA 3.2 Clasificáronse as zonas de risco dun sistema, segundo criterios de seguridade perimetral.	5,13 %
CA 3.3 Identificáronse os protocolos seguros de comunicación e os seus ámbitos de uso.	12,82 %
CA 3.4 Configuráronse redes privadas virtuais mediante protocolos seguros a distintos niveis.	17,95 %
CA 3.5 Implantouse un servidor como pasarela de acceso á rede interna desde localizacións remotas.	17,95 %
CA 3.6 Identificáronse e configuráronse os métodos posibles de autenticación no acceso de usuarios remotos a través da pasarela.	20,51 %
CA 3.7 Instalouse, configurouse e integrouse na pasarela un servidor remoto de autenticación.	20,51 %
RA 4. Implanta tornalumes (firewalls) para asegurar un sistema informático, analiza as súas prestacións e controla o tráfico cara á rede interna.	**5,00 %**
CA 4.1 Describíronse as características, os tipos e as funcións dos tornalumes.	10,00 %
CA 4.2 Clasificáronse os niveis en que se realiza a filtraxe de tráfico.	10,00 %
CA 4.3 Configuráronse filtros nun tornalumes a partir dunha listaxe de regras de filtraxe.	15,00 %
CA 4.4 Revisáronse os rexistros de sucesos de tornalumes, para verificar que as regras se apliquen correctamente.	10,00 %

Resultados de aprendizaxe e criterios de avaliación	%
CA 4.5 Interpretouse a documentación técnica de distintos tornalumes hardware nos idiomas máis empregados pola industria.	10,00 %
CA 4.6 Probáronse distintas opcións para implementar tornalumes, tanto de software como de hardware.	10,00 %
CA 4.7 Diagnosticáronse problemas de conectividade nos clientes provocados polos tornalumes.	10,00 %
CA 4.8 Planificouse a instalación de tornalumes para limitar os accesos a determinadas zonas da rede.	15,00 %
CA 4.9 Elaborouse documentación relativa á instalación, configuración e uso de tornalumes.	10,00 %
RA 5. Implanta servidores proxy, aplicando criterios de configuración que garantan o funcionamento seguro do servizo.	**5,00 %**
CA 5.1 Identificáronse os tipos de proxy, as súas características e as súas funcións principais.	10,00 %
CA 5.2 Instalouse e configurouse un servidor proxy cache.	20,00 %
CA 5.3 Configuráronse os métodos de autenticación no proxy.	10,00 %
CA 5.4 Configurouse un proxy en modo transparente.	15,00 %
CA 5.5 Utilizouse o servidor proxy para establecer restricións de acceso web.	10,00 %
CA 5.6 Arranxáronse problemas de acceso desde os clientes ao proxy.	10,00 %
CA 5.7 Realizáronse probas de funcionamento do proxy, monitorizando a súa actividade con ferramentas gráficas.	3,00 %
CA 5.8 Configurouse un servidor proxy en modo inverso.	20,00 %
CA 5.9 Elaborouse documentación relativa á instalación, a configuración e o uso de servidores proxy.	2,00 %
RA 6. Implanta solucións de alta dispoñibilidade empregando técnicas de virtualización, e configura os contornos de proba.	**20,00 %**
CA 6.1 Analizáronse supostos e situacións en que cumpra pór en marcha solucións de alta dispoñibilidade.	5,00 %
CA 6.2 Identificáronse solucións de hardware para asegurar a continuidade no funcionamento dun sistema.	5,00 %
CA 6.3 Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.	55,00 %
CA 6.3.1 Avaliaronse as posibilidades da virtualización nos sistemas de alta dispoñibilidade	
CA 6.3.2 Crearonse servizos virtualizados basados en Containers	
CA 6.3.3 Crearonse servizos virtualizados basados en Hypervisores tipo I e tipo II	
CA 6.3.4 Establecéronse diferentes configuracións de rede entre máquinas virtuais	
CA 6.3.5 Utilizouse aprovisionamiento lixeiro para o despregue de máquinas virtuais	
CA 6.3.6 Empregáronse mecanismos de acceso remoto ao almacenamento virtual	
CA 6.4 Implantouse un servidor redundante que garanta a continuidade de servizos en casos de caída do servidor principal.	7,50 %
CA 6.5 Implantouse un balanceador de carga á entrada da rede interna.	7,50 %
CA 6.6 Implantáronse sistemas de almacenamento redundante sobre servidores e dispositivos específicos.	5,00 %
CA 6.7 Avaliouse a utilidade dos sistemas de clúster para aumentar a fiabilidade e a produtividade do sistema.	5,00 %
CA 6.8 Analizáronse solucións de futuro para un sistema con demanda crecente.	5,00 %
CA 6.9 Esquematizáronse e documentáronse solucións para supostos con necesidades de alta dispoñibilidade.	5,00 %
RA 7. Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia.	**5,00 %**
CA 7.1 Describiuse a lexislación sobre protección de datos de carácter persoal.	15,00 %
CA 7.2 Determinouse a necesidade de controlar o acceso á información persoal almacenada.	15,00 %
CA 7.3 Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.	15,00 %
CA 7.4 Contrastouse o deber de pór ao dispor das persoas os datos persoais que lles atinxen.	15,00 %
CA 7.5 Describiuse a lexislación actual sobre os servizos da sociedade da información e o comercio electrónico.	15,00 %
CA 7.6 Contrastáronse as normas sobre xestión de seguridade da información.	15,00 %
CA 7.7 Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable.	10,00 %

5.5 Observacións sobre os criterios de cualificación

Para acadar unha avaliación positiva o alumno debe ter avaliadas de xeito positivas todas e cada unha das unidades de traballo. Unha unidade de traballo será avaliada positivamente cando supera todos e cada un dos criterios de avaliación marcados coma mínimos esixibles. No caso das probas escritas, deberase obter obrigatoriamente UN MÍNIMO DE 5 para que se poda considerar alcanzado o mínimo, antes de sumarlle os resultados obtidos por medio dos outros instrumentos de avaliación establecidos.
A nota final da unidade de traballo se calculará aplicando os pesos indicados a cada un dos criterios de avaliación, e a nota final do módulo será a media de todas as unidades de traballo.

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

Cando un alumno non supere unha unidade, se lle plantexarán exercicios de recuperación de realización obligatoria e terá que superar e si procede unha proba escrita.

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

No caso de perda do dereito a avaliación continua o alumno deberá facer entrega dun traballo que integre a materia impartida e realizar un exercicio escrito sobre a totalidade do temario. A entrega do traballo e a realización do exercicio será na última semana do curso.

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

O finalizar cada unidade didáctica deberá facerse unha valoración sobre:

- O tempo asignado a dita unidade
- O material e recursos empregados
- A materia impartida e o grao de asimilación por parte do alumnado
- Os procedementos seguidos para a explicación da mesma.

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

Sendo unha asignatura de segundo curso, enténdese que o alumno xa posee os coñecementos mínimos de adminstración de sistemas e de redes para a materia. O resto de coñecementos previos non resultan relevantes.

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

Se deseñarán exercicios persoalizados para que o alumno acade, aínda que sexa en grao mínimo, os obxectivos de cada unidade.

9. Aspectos transversais

9.a) Programación da educación en valores

Facilitarase a cooperación entre o alumnado tanto na realización dos traballos como na resolución mutua de dúbidas e fomentarase o coidado do material e o aforro eléctrico e de material (fundamentalmente papel).

9.b) Actividades complementarias e extraescolares

Non se preveen actividades complementarias