1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
36019475	de Rodeira	Cangas	2018/2019

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	2018/2019	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	30	20
2	Conceptos Básicos de Seguridade Informática	Introducción do concepto de seguridade informática e descrición das vulnerabilidades do sistema	6	5
3	Ataques a Sistemas Informáticos e Medidas Preventivas	Tipos de Ameazas e Ataques. Medidas. Seguridade Física e Lóxica	30	20
4	Técnicas de Acceso Remoto e Seguridade Perimetral	Medidas de Seguridade Activa e Pasiva	6	10
5	Firewalls	Descrición de en qué consiste o análise forense e de algunhas das ferramentas empregadas	15	10
6	Proxys	Descrición do proceso e das ferramentas necesarias para a realización dun plan de Seguridade Informática	15	10
7	Solucións de Alta Dispoñibilidade	Descrición das redes WiFi e a súa seguridade	21	20
8	Lexislación e Normativa	Introducción ao cifrado de información e ás infraestructuras de chave pública	3	5

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Introducción á Virtualización	30

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.
CA6.3.1 Avaliaronse as posibilidades da virtualización nos sistemas 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

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.

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Conceptos Básicos 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.
CA1.3 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.
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.

4.2.e) Contidos

Contidos
Fiabilidade, confidencialidade, integridade e dispoñibilidade. Elementos vulnerables no sistema informático: hardware, software e datos. Análise das principais vulnerabilidades dun sistema informático. Riscos potenciais dos servizos de rede. Software para detección de vulnerabilidades. Intentos de penetración: tipoloxía.

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Ataques a Sistemas Informáticos e Medidas Preventivas	30

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
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

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

Criterios de avaliación
CA1.2 Describíronse as diferenzas entre seguridade física e lóxica.
CA1.5 Adoptáronse políticas de contrasinais.
CA1.6 Valoráronse as vantaxes do uso de sistemas biométricos.
CA1.7 Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información.
CA1.9 Identificáronse as fases da análise forense ante ataques a un sistema.
0CA1.10 Comprendeuse o fundamento técnico das vulnerabilidades máis comúns e se estableceron medidas paliativas.
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.
CA2.6 Utilizáronse técnicas de cifraxe, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas.
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.
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.
CA3.7 Instalouse, configurouse e integrouse na pasarela un servidor remoto de autenticación.

4.3.e) Contidos

Contidos
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. Seguridade lóxica: Criptografía. Listas de control de acceso. Establecemento de políticas de contrasinais. Sistemas biométricos de identificación. Políticas de almacenamento. Medios de almacenamento. Análise forense en sistemas informáticos: obxectivo. Recollida e análise de incidencias. Ferramentas empregadas na análise forense. Ataques e contramedidas en sistemas informáticos. 0Técnicas de cifraxe da información: clave pública e clave privada; certificados dixitais; sinaturas. Monitorización do tráfico en redes: captura e análise; aplicacións. Seguridade nos protocolos para comunicacións sen fíos. 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. Copias de seguridade e imaxes de respaldo. Recuperación de datos. Actualización de sistemas e aplicacións. Servidores de acceso remoto: Protocolos de autenticación. Configuración de parámetros de acceso. Servidores de autenticación.

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Técnicas de Acceso Remoto e Seguridade Perimetral	6

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
CA1.8 Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.
CA2.7 Avaliáronse as medidas de seguridade dos protocolos usados en redes de comunicación.
CA3.1 Describíronse escenarios típicos de sistemas con conexión a redes públicas en que cumpra fortificar a rede interna.
CA3.2 Clasificáronse as zonas de risco dun sistema, segundo criterios de seguridade perimetral.
CA3.3 Identificáronse os protocolos seguros de comunicación e os seus ámbitos de uso.
CA3.4 Configuráronse redes privadas virtuais mediante protocolos seguros a distintos niveis.
CA3.5 Implantouse un servidor como pasarela de acceso á rede interna desde localizacións remotas.
CA3.6 Identificáronse e configuráronse os métodos posibles de autenticación no acceso de usuarios remotos a través da pasarela.

4.4.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.

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Firewalls	15

4.5.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

4.5.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.

4.5.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.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Proxys	15

4.6.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

4.6.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.

4.6.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.

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Solucións de Alta Dispoñibilidade	21

4.7.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

4.7.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.
CA6.4 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.

4.7.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.

4.8.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
8	Lexislación e Normativa	3

4.8.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

4.8.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.

4.8.e) Contidos

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

5. Mínimos exixibles para alcanzar a avaliación positiva e 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, 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