

1. Identificación da programación
Centro educativo

Código	Centro	Concello	Ano académico
27015773	Muralla Romana	Lugo	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 de proba libre

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	0	105	0

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

Profesorado responsable

Profesorado asignado ao módulo	EUGENIO VÁZQUEZ BLANCO, MARÍA BELÉN LÓPEZ RUÍZ
Outro profesorado	

Estado: Pendente de supervisión inspector

2. Resultados de aprendizaxe e criterios de avaliación

2.1. Primeira parte da proba

2.1.1. Resultados de aprendizaxe do currículo que se tratan

Resultados de aprendizaxe do currículo
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.
RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade.
RA4 - Implanta tornalumes (firewalls) para asegurar un sistema informático, analiza as súas prestacións e controla o tráfico cara á rede interna.
RA5 - Implanta servidores proxy, aplicando criterios de configuración que garantan o funcionamento seguro do servizo.
RA6 - Implanta solucións de alta dispoñibilidade empregando técnicas de virtualización, e configura os contornos de proba.
RA7 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia.

2.1.2. Criterios de avaliación que se aplicarán para a verificación da consecución dos resultados de aprendizaxe por parte do alumnado

Criterios de avaliación do currículo
CA1.1 Valorouse a importancia de asegurar a privacidade, a coherencia e a dispoñibilidade da información nos sistemas informáticos.
CA1.2 Descríronse as diferenzas entre seguridade física e lóxica.
CA1.3 Clasifícanse os tipos principais de vulnerabilidade dun sistema informático, segundo a súa tipoloxía e a súa orixe.
CA1.4 Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas.
CA1.6 Valoráronse as vantaxes do uso de sistemas biométricos.
CA1.8 Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.

Crterios de avaliación do currículo

CA1.9 Identificáronse as fases da análise forense ante ataques a un sistema.

CA2.1 Clasificáronse os principais tipos de ameazas lóxicas contra un sistema informático.

CA2.3 Identificouse a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.

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.

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.

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.

CA5.1 Identificáronse os tipos de proxy, as súas características e as súas funcións principais.

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.

CA6.8 Analizáronse solucións de futuro para un sistema con demanda crecente.

CA6.9 Esquematzáronse e documentáronse solucións para supostos con necesidades de alta dispoñibilidade.

CA7.1 Describiuse a lexislación sobre protección de datos de carácter persoal.

Crterios de avaliación do currículo
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.

2.2. Segunda parte da proba

2.2.1. Resultados de aprendizaxe do currículo que se tratan

Resultados de aprendizaxe do currículo
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.
RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade.
RA4 - Implanta tornalumes (firewalls) para asegurar un sistema informático, analiza as súas prestacións e controla o tráfico cara á rede interna.
RA5 - Implanta servidores proxy, aplicando criterios de configuración que garantan o funcionamento seguro do servizo.
RA6 - Implanta solucións de alta dispoñibilidade empregando técnicas de virtualización, e configura os contornos de proba.

2.2.2. Criterios de avaliación que se aplicarán para a verificación da consecución dos resultados de aprendizaxe por parte do alumnado

Criterios de avaliación do currículo
CA1.1 Valorouse a importancia de asegurar a privacidade, a coherencia e a dispoñibilidade da información nos sistemas informáticos.
CA1.5 Adoptáronse políticas de contrasinais.
CA1.7 Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información.
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.
CA2.6 Utilizáronse técnicas de cifraxo, 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.
CA3.4 Configuráronse redes privadas virtuais mediante protocolos seguros a distintos niveis.
CA3.5 Implantouse un servidor como pasarela de acceso á rede interna desde localizacións remotas.
CA3.6 Identificáronse e configuráronse os métodos posibles de autenticación no acceso de usuarios remotos a través da pasarela.
CA3.7 Instalouse, configurouse e integrouse na pasarela un servidor remoto de autenticación.
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.

Crterios de avaliación do currículo

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.

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.

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.

3. Mínimos exigibles para alcanzar a avaliación positiva e os criterios de cualificación

Tódolos criterios de avaliación son esixibles.

A primeira proba terá carácter eliminatorio. O profesor ou a profesora do módulo profesional cualificará esta primeira parte da proba de cero a dez puntos. Para a súa superación as persoas candidatas deberán obter unha puntuación igual ou superior a cinco puntos.

O profesor ou a profesora do módulo profesional cualificará a segunda parte da proba de cero a dez puntos. Para a súa superación as persoas candidatas deberán obter unha puntuación igual ou superior a cinco puntos. As persoas que non superen a primeira parte da proba serán cualificadas cun cero nesta segunda parte.

A cualificación final será a media aritmética das cualificacións obtidas en cada unha das partes, expresada con números enteiros, redondeada á unidade máis próxima. No caso das persoas aspirantes que suspendan a segunda parte da proba, a puntuación máxima que poderá asignarse será de catro puntos.

4. Características da proba e instrumentos para o seu desenvolvemento

4.a) Primeira parte da proba

Proba escrita con preguntas de contestación breve que se desenvolverán en dúas sesións de 50 minutos como máximo e versará sobre unha mostra suficientemente significativa dos criterios de avaliación establecidos na programación para esta parte.

4.b) Segunda parte da proba

A segunda parte da proba consistirá no desenvolvemento de un ou de varios supostos prácticos que versarán sobre unha mostra suficientemente significativa dos criterios de avaliación establecidos na programación para esta parte. Durará como máximo 3 sesións de 50 minutos e desenvolverase nunha aula de ordenadores en rede con sistema operativo Windows 10 como anfitrión e virtualización Virtualbox con hóspedes Ubuntu e Windows.