1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
15021482	San Clemente	Santiago de Compostela	2021/2022

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	2021/2022	0	105	0

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

Profesorado responsable

Profesorado asignado ao módulo	INÉS VALIÑO RIELO,MANUEL GONZÁLEZ REGAL,ADÁN AMORÍN VIDE (Subst.),LAURA PÉREZ SÁNCHEZ (Subst.)
Outro profesorado	

Estado: Pendente de supervisión departamento

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 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.
CA1.8 Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.
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.
CA2.8 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.
CA3.6 Identificáronse e configuráronse os métodos posibles de autenticación no acceso de usuarios remotos a través da pasarela.
CA4.1 Describíronse as características, os tipos e as funcións dos tornalumes.

Criterios de avaliación do currículo
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.
CA6.2 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.
CA6.7 Avaliouse a utilidade dos sistemas de clúster para aumentar a fiabilidade e a produtividade do sistema.
CA6.9 Esquematizáronse e documentáronse solucións para supostos con necesidades de alta dispoñibilidade.
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.

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
CA1.5 Adoptáronse políticas de contrasinais.
CA1.7 Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información.

Criterios de avaliación do currículo
CA2.2 Verificouse a orixe e a autenticidade das aplicacións instaladas nun equipamento, así como o estado de actualización do sistema operativo.
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 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.
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.
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.
CA6.1 Analizáronse supostos e situacións en que cumpra pór en marcha solucións 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.

Criterios de avaliación do currículo
CA6.6 Implantáronse sistemas de almacenamento redundante sobre servidores e dispositivos específicos.
CA6.8 Analizáronse solucións de futuro para un sistema con demanda crecente.

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

Os contidos mínimos imprescindibles para a superación do módulo son os que fan referencia aos seguintes puntos:

- Fiabilidade, confidencialidade, integridade e dispoñibilidade.
- Elementos vulnerables no sistema informático: hardware, software e datos.
- Análise das principais vulnerabilidades dun sistema informático.
- Pautas e prácticas seguras.
- Tipos de ameazas: físicas e lóxicas.
- Identificar as fases da análise forense ante ataques a un sistema. Coñecer e entender as fases dun ataque. A Cyber Kill Chain e matriz MITRE ATT&CK.
- 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.
- Ataques e contramedidas en sistemas informáticos.
- Técnicas 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.
- Riscos potenciais dos servizos de rede. Software para detección de vulnerabilidades.
- Intentos de penetración: tipoloxía.
- Sistemas de detección de intrusións.
- Clasificación dos ataques.
- Ferramentas preventivas e paliativas: instalación e configuración.
- Copias de seguridade e imaxes de respaldo.
- Recuperación de datos.
- Actualización de sistemas e aplicacións.
- Seguridade na conexión con redes públicas.
- Elementos básicos da seguridade perimetral: encamiñador fronteira; tornalumes; redes priva das virtuais.
- Perímetros de rede. Zonas desmilitarizadas.
- Arquitectura débil e forte de subrede protexida.
- Servidores de acceso remoto.
- Protocolos de autenticación.
- Configuración de parámetros de acceso.
- Servidores de autenticación.
- SSH.
- Tipos de tornalumes.

- Regras de filtraxe de tornalumes.
- Probas de funcionamento: sondaxe.
- Rexistros de sucesos nos tornalumes.
- Tipos de proxy.
- Configuración de filtros.
- Métodos de autenticación nun proxy.
- Proxy inverso.
- Solucións de alta dispoñibilidade.
- Virtualización de sistemas.
- Ferramentas para a virtualización. Configuración e uso de máquinas virtuais e contedores linux LXC/LXD.
- Lexislación sobre protección de datos e sobre os servizos da sociedade da información e o correo electrónico.

A nota total de cada unha das partes da proba indicarase nunha escala de cero (0) a dez (10) puntos.

A avaliación positiva acadarase despois de superar no proceso de avaliación as dúas partes (teórica e práctica) da proba, tendo cada unha delas carácter eliminatorio. A persoa aspirante terá que acadar como mínimo unha nota de cinco (5) puntos en cada unha das partes para obter dita valoración positiva.

Cualificación:
- En caso de superar as dúas partes, a cualificación final será a media aritmética das cualificacións obtidas en cada unha das partes, expresada con números enteiros entre un e dez, redondeada á unidade máis próxima.
- As persoas candidatas que non superen a primeira parte da proba; e polo tanto non accedan á realización da segunda parte da proba, serán cualificadas nesta segunda parte con cero puntos. A cualificación final será a media aritmética das dúas probas.
- No caso das persoas aspirantes que superando a primeira parte suspendan a segunda parte da proba, a cualificación final será a puntuación obtida na proba non superada.

4. Caracteríticas da proba e instrumentos para o seu desenvolvemento

4.a) Primeira parte da proba

Consistirá nunha proba escrita que poderá combinar preguntas tipo test, de resposta curta e de exposición. As preguntas tipo test puntuarán en negativo en caso de erro ou estar en branco (o peso de cada parte e a valoración negativa comunicarase as persoas candidatas ao inicio da proba).
A proba abordará a maior parte dos contidos sinalados nesta programación.
Os instrumentos necesarios serán papel e bolígrafo de cor azul ou negra; non se permitirán cintas nin fluídos correctores e tampouco será corrixido ningún exercicio feito a lapis.
Aqueles exercicios que non estean perfectamente identificados non serán corrixidos.
Queda totalmente prohibido o uso de teléfono móbil ou calquera dispositivo electrónico, tendo que estar estes totalmente apagados e debidamente gardados.

4.b) Segunda parte da proba

Consistirá na resolución de distintas cuestións nun suposto práctico onde os sistemas informáticos serán virtualizados mediante a ferramenta de virtualización Oracle VM Virtualbox e contedores linux LXC/LXD. Os aspirantes deben ser quen de configurar, para logo dar resposta as cuestións propostas. Os sistemas operativos cos que se traballará serán Ubuntu/Debian e Windows nas versións servidor e/ou desktop. Nalgúns casos as respostas serán dadas mediante capturas de pantalla.

A proba abordará contidos sinalados nesta programación; o número de contidos virá determinado polo tempo dispoñible, que é limitado e non permite o tratamento completo de tódolos contidos.

Aqueles exercicios que non estean perfectamente identificados non serán corrixidos.

Queda totalmente prohibido o uso de teléfono móbil ou calquera dispositivo electrónico non proporcionado polo centro ou expresamente autorizado, tendo que estar estes totalmente apagados e debidamente gardados.