

**1. Identificación da programación****Centro educativo**

Código	Centro	Concello	Ano académico
15006778	Rodolfo Ucha Piñeiro	Ferrol	2017/2018

Ciclo formativo

Código da familia profesional	Familia profesional	Código do ciclo formativo	Ciclo formativo	Grao	Réxime
IFC	Informática e comunicacións	CMIFC01	Sistemas microinformáticos e redes	Ciclos formativos de grao medio	Réxime de proba libre

Módulo profesional e unidades formativas de menor duración (*)

Código MP/UF	Nome	Curso	Sesións semanais	Horas anuais	Sesións anuais
MP0226	Seguridade informática	2017/2018	0	140	0

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

Profesorado responsable

Profesorado asignado ao módulo	MARÍA BELÉN BALDONEDO DEL RÍO
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 - Identifica técnicas e prácticas de tratamento seguro da información, e recoñece e valora a súa importancia en distintos contornos de traballo.
RA2 - Aplica medidas de seguridade pasiva en sistemas informáticos, recoñecendo as necesidades de acordo coas características do contorno.
RA3 - Xestiona dispositivos de almacenaxe aplicando os procedementos e as técnicas adecuadas para asegurar a integridade da información.
RA4 - Aplica mecanismos de seguridade activa atendendo ás necesidades do sistema informático.
RA5 - Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico.
RA6 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e analiza as repercusións do seu incumprimento.

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 manter a información segura.
CA1.2 Clasificouse a información no ámbito da seguridade.
CA1.3 Describíronse as diferenzas entre seguridade física e lóxica.
CA1.4 Identificáronse as principais técnicas criptográficas.
CA1.5 Recoñeceuse a necesidade de integrar técnicas criptográficas na almacenaxe e na transmisión da información.
CA1.6 Identificáronse os fundamentos criptográficos dos protocolos seguros de comunicación (clave pública, clave privada, etc.).
CA1.7 Recoñeceuse a necesidade de facer unha análise de riscos e a posta en marcha dunha política de seguridade.
CA1.8 Establecéronse as normas básicas para incluír nun manual de seguridade informática.
CA2.1 Definíronse as características do emprazamento e as condicións ambientais dos equipamentos e dos servidores.
CA2.2 Identificouse a necesidade de protexer fisicamente os sistemas informáticos.
CA2.3 Verificouse o funcionamento dos sistemas de alimentación ininterrompida.
CA2.4 Seleccionáronse os puntos de aplicación dos sistemas de alimentación ininterrompida.
CA2.5 Esquematizáronse as características dunha política de seguridade baseada en listas de control de acceso.
CA2.6 Valorouse a importancia de establecer unha política de contrasinais.
CA2.7 Valoráronse as vantaxes do uso de sistemas biométricos.
CA3.1 Interpretouse a documentación técnica relativa á política de almacenaxe.
CA3.2 Tivéronse en conta factores inherentes á almacenaxe da información (rendemento, dispoñibilidade, accesibilidade, etc.).



Criterios de avaliación do currículo
CA3.3 Clasifícanse e enumeráronse os principais métodos de almacenaxe, incluídos os sistemas en rede.
CA3.4 Descríbense as tecnoloxías de almacenaxe redundante e distribuída.
CA3.5 Seleccionáronse estratexias para a realización de copias de seguridade.
CA3.6 Tívoise en conta a frecuencia e o esquema de rotación.
CA3.8 Identifícanse as características dos medios de almacenaxe remotos e extraíbles.
CA4.1 Seguíronse plans de continxencia para actuar ante fallos de seguridade.
CA4.2 Clasifícanse os principais tipos de software malicioso.
CA5.1 Identifícase a necesidade de inventariar e controlar os servizos de rede.
CA5.2 Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas e nos roubos de información.
CA5.3 Deduciuse a importancia de reducir o volume de tráfico xerado pola publicidade e o correo non desexado.
CA5.5 Identifícanse as ameazas na navegación por internet.
CA5.6 Clasifícanse e valoráronse as propiedades de seguridade dos protocolos usados en redes sen fíos.
CA5.7 Descríbense e utilízanse sistemas de identificación como a sinatura electrónica, o certificado dixital, etc.
CA6.1 Descríbiuse a lexislación sobre protección de datos de carácter persoal.
CA6.2 Determinouse a necesidade de controlar o acceso á información persoal almacenada.
CA6.3 Identifícanse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.
CA6.4 Contrastouse a obriga de pór ao dispor das persoas os datos persoais que lles atinxen.
CA6.5 Descríbiuse a lexislación sobre os servizos da sociedade da información e o comercio electrónico.
CA6.6 Contrastáronse as normas sobre xestión de seguridade da información.
CA6.7 Comprendeuse a necesidade de coñecer e respectar a normativa aplicable.

2.2. Segunda parte da proba

2.2.1. Resultados de aprendizaxe do currículo que se tratan

Resultados de aprendizaxe do currículo
RA3 - Xestiona dispositivos de almacenaxe aplicando os procedementos e as técnicas adecuadas para asegurar a integridade da información.
RA4 - Aplica mecanismos de seguridade activa atendendo ás necesidades do sistema informático.
RA5 - Asegura a privacidade da información transmitida en redes informáticas, para o que identifica vulnerabilidades e instala software específico.



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
CA3.7 Realizáronse copias de seguridade seguindo diversas estratexias.
CA3.9 Utilizáronse medios de almacenaxe remotos e extraíbles.
CA3.10 Creáronse e restauráronse imaxes de respaldo de sistemas en funcionamento.
CA4.3 Empregáronse ferramentas que examinan a integridade do sistema, e ferramentas de control e seguimento de accesos.
CA4.4 Realizáronse actualizacións periódicas dos sistemas para corrir posibles vulnerabilidades.
CA4.5 Verificouse a orixe e a autenticidade das aplicacións que se instalan nos sistemas.
CA4.6 Instaláronse, probáronse e actualizáronse aplicacións específicas para a detección e a eliminación de software malicioso.
CA4.7 Aplicáronse técnicas de recuperación de datos.
CA5.4 Aplicáronse medidas para evitar a monitorización de redes con cables.
CA5.7 Descríronse e utilízanse sistemas de identificación como a sinatura electrónica, o certificado dixital, etc.
CA5.8 Instalouse e configurouse unha devasa (firewall) nun equipamento ou nun servidor.

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

Mínimos exixibles:

- Para acadar a avaliación positiva na proba teórica, considéranse como mínimos exixibles os criterios de avaliación 1.8, 3.3, 3.4, 3.5 e 5.6 indicados no punto 2.1.2.
- Para acadar a avaliación positiva na proba práctica, considéranse como mínimos exixibles os criterios de avaliación 3.7, 4.3, 4.5, 4.6 e 5.8 indicados no punto 2.2.2.

Criterios de cualificación:

- Cada proba puntuarase de 0 a 10, sen decimais.
- Para superar cada proba e preciso acadar o 50% da nota da mesma.
- E preciso superar a proba teórica para poder realizar a proba práctica.
- A cualificación final correspondente da proba 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.
- No caso de realizar preguntas de tipo test nas probas, penalizaranse as repostas incorrectas, anulando unha resposta correcta por cada x número de repostas incorrectas (este número X de repostas incorrectas indicaranse no enunciado da proba, xa que está será proporcional o número de preguntas test formuladas).
- Cada exercicio da proba práctica, para poder ser valorado, ten que realizar as función solicitadas e sen erros.
- Para superar a proba práctica ten que demostrar ter acadado os mínimos esixidos en cada unha das unidades formativas que compoñen o módulo.

4. Características da proba e instrumentos para o seu desenvolvemento

4.a) Primeira parte da proba

Características da proba

- Consistirá nunha proba teórica sobre os contidos citados na UD1 do punto 2.b.
- A proba será de carácter presencial e será realizada de forma individual.
- A proba consistirá nunha serie de preguntas que poderán ser: tipo test ou cuestións a desenvolver por escrito
- No caso de preguntas de tipo test penalizaranse as repostas incorrectas, anulando unha resposta correcta por cada x número de repostas incorrectas (este número X de repostas incorrectas indicaranse no enunciado da proba, xa que está será proporcional o número de preguntas test formuladas).
- A proba terá unha duración mínima dunha hora e máxima de tres horas.
- A proba valorase sobre 10. Para poder superar a proba e preciso acadar o 50% da nota.

Instrumentos necesario para o seu desenvolvemento: papel e bolígrafo azul ou negro.

4.b) Segunda parte da proba

Características da proba

- A proba será de carácter práctico, presencial e será realizada de forma individual.
- A proba estará composta por varios exercicios prácticos nos que se lle pedirá ao aspirante que demostre os coñecementos prácticos aos que se refire na UD2 do punto 2.b.
- Na proba pode ter que instalar aplicacións en diferentes sistemas operativos propietarios, libres, monoposto e en rede e utilizar máquinas virtuais con emuladores do tipo VirtualBox.
- A proba terá unha duración mínima de dúas horas e máxima de tres horas.
- Poderánselle pedir a entrega de capturas de pantalla dos procesos levados a cabo para realizar as tarefas solicitadas na proba.

Instrumentos necesario para o seu desenvolvemento:

- Papel.
- Bolígrafo azul ou negro.
- Emulador de máquinas virtuais.
- Máquinas virtuais de sistemas operativos propietarios e libres.
- Imaxes ISO dos sistemas operativos propietarios ou libres.
- Outro software preciso para a realización dos exercicios da proba.