Programación de proba libre de Seguridade informática

1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
27015773	IES Muralla Romana	Lugo	2013-2014

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	Medio	Libres
IFC	Informática e comunicacións	ZMIFC01	Sistemas microinformáticos e redes	Medio	Libres

Módulo profesional

Código MP	Nome	Horas
MP0226	Seguridade informática	140

Profesorado responsable

Mª Belén López Ruíz
Silvia Quintana Domao

Índice

2. Resultados de aprendizaxe e criterios de avaliación

2.1 Primeira parte da proba

2.1.a 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.b 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.
CA2.1. Definíronse as características da localización e as condicións ambientais dos equipamentos e dos servidores.
CA2.2. Identificouse a necesidade de protexer fisicamente os sistemas informáticos.
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.).
CA3.3. Clasificáronse e enumeráronse os principais métodos de almacenaxe, incluídos os sistemas en rede.
CA3.4. Describíronse as tecnoloxías de almacenaxe redundante e distribuída.
CA3.6. Tívose en conta a frecuencia e o esquema de rotación.
CA3.8. Identificáronse as características dos medios de almacenaxe remotos e extraíbles.
CA4.2. Clasificáronse os principais tipos de software malicioso.
CA5.1. Identificouse a necesidade de inventariar e controlar os servizos de rede.
CA5.4. Aplicáronse medidas para evitar a monitorización de redes con cables.
CA5.5. Identificáronse as ameazas na navegación pola internet.

CA5.6. Clasificáronse e valoráronse as propiedades de seguridade dos protocolos usados en redes sen fíos.
CA5.7. Describíronse sistemas de identificación como a sinatura electrónica, o certificado dixital, etc.
CA6.1. Describiuse a lexislación sobre protección de datos de carácter persoal.
CA6.2. Determinouse a necesidade de controlar o acceso á información persoal almacenada.
CA6.3. Identificáronse 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. Describiuse 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.a 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.

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

Criterios de avaliación do currículo
CA1.8. Establecéronse as normas básicas para incluír nun manual de seguridade informática.
CA2.3. Verificouse o funcionamento dos sistemas de alimentación ininterrompida.
CA2.4. Seleccionáronse os puntos de aplicacióndos sistemas de alimentación ininterrompida.
CA3.5. Seleccionáronse estratexias para a realización de copias de seguridade.
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 apoio de sistemas en funcionamento.
CA4.1. Seguíronse plans de continxencia para actuar ante fallos de seguridade.
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 corrixir 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.
CA5.2. 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.
CA5.4. Aplicáronse medidas para evitar a monitorización de redes con cables.

CA5.7. Utilizáronse sistemas de identificación como a sinatura electrónica, o certificado dixital, etc.
CA5.8. Instalouse e configurouse un tornalumes (firewall) nun equipamento ou nun servidor.

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

Tódolos criterios de avaliación son mínimos 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 necesarios para o seu desenvolvemento

4.1 Primeira parte da proba

Proba escrita con preguntas de contestación breve ou tipo test que desenvolveranse en 2 sesións de 50 minutos como máximo e versará sobre unha mostra suficientemente significativa dos criterios de avaliación establecidos na programación para esta primeira parte.

4.2 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 segunda parte. Durará como máximo 4 sesións de 50 minutos e desenvolverase nun ordenador do departamento con:

- Sistema operativo Windows 7 Professional.
- Máquina virtual con Windows 7 para facer instalacións.

Constará dalgunhas das seguintes operacións:

- Comprobación do funcionamento dun SAI.
- Execución de copias de seguridade.
- Manexo de imaxenes de apoio.
- Instalación e emprego de ferramentas para a detección e eliminación de software malicioso.
- Emprego de sistemas de identificación.
- Instalación e configuración dun firewall.