# Programación de proba libre de módulos profesionais

## 1. Identificación da programación

### Centro educativo

| Código | Centro | Concello | Ano académico |
|---|---|---|---|
| 15021482 | IES San Clemente | Santiago de Compostela | 2012/2013 |

### Ciclo formativo

| Código da familia profesional | Familia profesional | Código do ciclo formativo | Ciclo formativo | Grao | Réxime |
|---|---|---|---|---|---|
| IFC | Informática e comunicacións | CMIFC01 | Ciclos formativos de grao medio | | LIBRE |

### Módulo profesional

| Código MP | Nome | Horas |
|---|---|---|
| MP0226 | Seguridade informática | 140 |

### Profesorado responsable

| |
|---|
| JOSEFA PAULOS LAREO |

## 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.<br>▪ CA1.2. Clasificouse a información no ámbito da seguridade.<br>▪ CA1.3. Describíronse as diferenzas entre seguridade física e lóxica.<br>▪ CA1.4. Identificáronse as principais técnicas criptográficas. |

| |
|---|
| ▪ CA1.5. Recoñeceuse a necesidade de integrar técnicas criptográficas na almacenaxe e na transmisión da información.<br>▪ CA1.6. Identificáronse os fundamentos criptográficos dos protocolos seguros de comunicación (clave pública, clave privada, etc.).<br>▪ CA1.7. Recoñeceuse a necesidade de facer unha análise de riscos e a posta en marcha dunha política de seguridade.<br>▪ 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.<br>▪ CA2.2. Identificouse a necesidade de protexer fisicamente os sistemas informáticos.<br>▪ CA2.3. Verificouse o funcionamento dos sistemas de alimentación ininterrompida.<br>▪ CA2.4. Seleccionáronse os puntos de aplicación dos sistemas de alimentación ininterrompida.<br>▪ CA2.5. Esquematizáronse as características dunha política de seguridade baseada en listas de control de acceso.<br>▪ CA2.6. Valorouse a importancia de establecer unha política de contrasinais.<br>▪ CA2.7. Valoráronse as vantaxes do uso de sistemas biométricos. |
| ▪ CA3.1. Interpretouse a documentación técnica relativa á política de almacenaxe.<br>▪ CA3.2. Tivéronse en conta factores inherentes á almacenaxe da información (rendemento, dispoñibilidade, accesibilidade, etc.).<br>▪ CA3.3. Clasificáronse e enumeráronse os principais métodos de almacenaxe, incluídos os sistemas en rede.<br>▪ CA3.4. Describíronse as tecnoloxías de almacenaxe redundante e distribuída.<br>▪ CA3.5. Seleccionáronse estratexias para a realización de copias de seguridade.<br>▪ CA3.6. Tívose en conta a frecuencia e o esquema de rotación.<br>▪ CA3.7. Realizáronse copias de seguridade seguindo diversas estratexias.<br>▪ CA3.8. Identificáronse as características dos medios de almacenaxe remotos e extraíbles.<br>▪ CA3.9. Utilizáronse medios de almacenaxe remotos e extraíbles.<br>▪ CA3.10. Creáronse e restauráronse imaxes de respaldo de sistemas en funcionamento. |
| ▪ CA4.1. Seguíronse plans de continxencia para actuar ante fallos de seguridade.<br>▪ CA4.2. Clasificáronse os principais tipos de software malicioso.<br>▪ CA4.3. Empregáronse ferramentas que examinan a integridade do sistema, e ferramentas de control e seguimento de accesos.<br>▪ CA4.4. Realizáronse actualizacións periódicas dos sistemas para corrixir posibles vulnerabilidades.<br>▪ CA4.5. Verificouse a orixe e a autenticidade das aplicacións que se instalan nos sistemas.<br>▪ CA4.6. Instaláronse, probáronse e actualizáronse aplicacións específicas para a detección e a eliminación de software malicioso.<br>▪ CA4.7. Aplicáronse técnicas de recuperación de datos. |
| ▪ CA5.1. Identificouse a necesidade de inventariar e controlar os servizos de rede.<br>▪ CA5.2. Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas e nos roubos de información.<br>▪ CA5.3. Deduciuse a importancia de reducir o volume de tráfico xerado pola publicidade e o correo non desexado.<br>▪ CA5.4. Aplicáronse medidas para evitar a monitorización de redes con cables.<br>▪ CA5.5. Identificáronse as ameazas na navegación por internet.<br>▪ CA5.6. Clasificáronse e valoráronse as propiedades de seguridade dos protocolos usados en redes sen fíos.<br>▪ CA5.7. Describíronse e utilizáronse sistemas de identificación como a sinatura electrónica, o certificado dixital, etc. CA5.8. Instalouse e configurouse unha devasa (firewall) nun equipamento ou nun servidor. |
| ▪ CA6.1. Describiuse a lexislación sobre protección de datos de carácter persoal.<br>▪ CA6.2. Determinouse a necesidade de controlar o acceso á información persoal almacenada.<br>▪ CA6.3. Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.<br>▪ CA6.4. Contrastouse a obriga de pór ao dispor das persoas os datos persoais que lles atinxen.<br>▪ CA6.5. Describiuse a lexislación sobre os servizos da sociedade da información e o comercio electrónico.<br>▪ CA6.6. Contrastáronse as normas sobre xestión de seguridade da información.<br>▪ 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 |
|---|
| ▪ 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. |

### 2.2.2 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 manter a información segura.<br>▪ CA1.2. Clasificouse a información no ámbito da seguridade.<br>▪ CA1.3. Describíronse as diferenzas entre seguridade física e lóxica.<br>▪ CA1.4. Identificáronse as principais técnicas criptográficas.<br>▪ CA1.5. Recoñeceuse a necesidade de integrar técnicas criptográficas na almacenaxe e na transmisión da información.<br>▪ CA1.6. Identificáronse os fundamentos criptográficos dos protocolos seguros de comunicación (clave pública, clave privada, etc.).<br>▪ CA1.7. Recoñeceuse a necesidade de facer unha análise de riscos e a posta en marcha dunha política de seguridade.<br>▪ 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.<br>▪ CA2.2. Identificouse a necesidade de protexer fisicamente os sistemas informáticos.<br>▪ CA2.3. Verificouse o funcionamento dos sistemas de alimentación ininterrompida.<br>▪ CA2.4. Seleccionáronse os puntos de aplicación dos sistemas de alimentación ininterrompida.<br>▪ CA2.5. Esquematizáronse as características dunha política de seguridade baseada en listas de control de acceso.<br>▪ CA2.6. Valorouse a importancia de establecer unha política de contrasinais.<br>▪ CA2.7. Valoráronse as vantaxes do uso de sistemas biométricos. |
| ▪ CA3.1. Interpretouse a documentación técnica relativa á política de almacenaxe.<br>▪ CA3.2. Tivéronse en conta factores inherentes á almacenaxe da información (rendemento, dispoñibilidade, accesibilidade, etc.).<br>▪ CA3.3. Clasificáronse e enumeráronse os principais métodos de almacenaxe, incluídos os sistemas en rede.<br>▪ CA3.4. Describíronse as tecnoloxías de almacenaxe redundante e distribuída.<br>▪ CA3.5. Seleccionáronse estratexias para a realización de copias de seguridade.<br>▪ CA3.6. Tívose en conta a frecuencia e o esquema de rotación.<br>▪ CA3.7. Realizáronse copias de seguridade seguindo diversas estratexias.<br>▪ CA3.8. Identificáronse as características dos medios de almacenaxe remotos e extraíbles.<br>▪ CA3.9. Utilizáronse medios de almacenaxe remotos e extraíbles.<br>▪ CA3.10. Creáronse e restauráronse imaxes de respaldo de sistemas en funcionamento. |
| ▪ CA4.1. Seguíronse plans de continxencia para actuar ante fallos de seguridade.<br>▪ CA4.2. Clasificáronse os principais tipos de software malicioso.<br>▪ CA4.3. Empregáronse ferramentas que examinan a integridade do sistema, e ferramentas de control e seguimento de accesos.<br>▪ CA4.4. Realizáronse actualizacións periódicas dos sistemas para corrixir posibles vulnerabilidades.<br>▪ CA4.5. Verificouse a orixe e a autenticidade das aplicacións que se instalan nos sistemas.<br>▪ CA4.6. Instaláronse, probáronse e actualizáronse aplicacións específicas para a detección e a eliminación de software malicioso.<br>▪ CA4.7. Aplicáronse técnicas de recuperación de datos. |
| ▪ CA5.1. Identificouse a necesidade de inventariar e controlar os servizos de rede.<br>▪ CA5.2. Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas e nos roubos de información.<br>▪ CA5.3. Deduciuse a importancia de reducir o volume de tráfico xerado pola publicidade e o correo non desexado.<br>▪ CA5.4. Aplicáronse medidas para evitar a monitorización de redes con cables.<br>▪ CA5.5. Identificáronse as ameazas na navegación por internet.<br>▪ CA5.6. Clasificáronse e valoráronse as propiedades de seguridade dos protocolos usados en redes sen fíos.<br>▪ CA5.7. Describíronse e utilizáronse sistemas de identificación como a sinatura electrónica, o certificado dixital, etc. CA5.8. Instalouse e configurouse unha devasa (firewall) nun equipamento ou nun servidor. |
| ▪ CA6.1. Describiuse a lexislación sobre protección de datos de carácter persoal.<br>▪ CA6.2. Determinouse a necesidade de controlar o acceso á información persoal almacenada.<br>▪ CA6.3. Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.<br>▪ CA6.4. Contrastouse a obriga de pór ao dispor das persoas os datos persoais que lles atinxen.<br>▪ CA6.5. Describiuse a lexislación sobre os servizos da sociedade da información e o comercio electrónico.<br>▪ CA6.6. Contrastáronse as normas sobre xestión de seguridade da información.<br>▪ CA6.7. Comprendeuse a necesidade de coñecer e respectar a normativa aplicable. |

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

*MINIMOS EXIXIBLES*

BC1. Tratamento seguro da información

- Seguridade física e lóxica.
- Criptografía.
- Políticas de seguridade.

BC2. Medidas de seguridade física e ambiental

- Localización e protección física dos equipamentos e dos servidores.
- Sistemas de alimentación ininterrompida.

BC3. Dispositivos de almacenaxe

- Almacenaxe da información: rendemento, dispoñibilidade e accesibilidade.
- Almacenaxe redundante e distribuída.
- Almacenaxe remota e extraíble.
- Copias de seguridade e imaxes de respaldo.
- Medios de almacenaxe.

BC4. Mecanismos de seguridade lóxica

- Listas de control de acceso.
- Política de contrasinais.
- Sistemas biométricos de identificación.
- Recuperación de datos.
- Monitorización de sistemas.
- Auditorías de seguridade.
- Software malicioso: clasificación. Ferramentas de protección e desinfección.
- Actualización de sistemas e aplicacións.
- Manual de seguridade e plans de continxencia.

BC5. Medidas de seguridade en redes

- Métodos para asegurar a privacidade da información transmitida.
- Identificación dixital: sinatura electrónica e certificado dixital.
- Monitorización do tráfico en redes con cables.
- Seguridade en redes sen fíos.
- Riscos potenciais dos servizos de rede.
- Sistemas de seguridade nas telecomunicacións: correo, www, ftp, p2p, etc.
- Publicidade e correo non desexados.
- Fraudes informáticas e roubos de información.
- Utilización de devasas (firewalls) en equipamentos e en servidores.
- Análise dos rexistros (logs) dun sistema para identificar ataques reais ou potenciais á seguridade.

BC6. Cumprimento da lexislación e das normas sobre seguridade

- Lexislación sobre protección de datos.
- Lexislación sobre os servizos da sociedade da información e o correo electrónico.
- Normas ISO sobre xestión de seguridade da información.

*CRITERIOS DE CUALIFICACIÓN*

*PRIMEIRA PARTE DA PROBA:*

Esta primeira parte da proba será avaliada de cero a dez puntos, para a súa superación as persoas candidatas deberán obter unha puntuación igual ou superior a cinco puntos.

Cada reposta ben contestada terá unha determinada puntuación positiva e cada 3 preguntas erróneas se eliminará unha correcta.

A puntuación positiva/negativa exacta de cada pregunta se especificará detalladamente no exame, en función do tipo de pregunta que sexa.

*SEGUNDA PARTE DA PROBA:*

Esta segunda parte da proba será avaliada 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.

Se valorará positivamente o uso das ferramentas máis idóneas segundo a situación ou suposto a resolver, así coma a claridade e limpeza nas solucións propostas.

A solución ós supostos deberá cumprir correctamente o enunciado proposto, e probarase a súa validez mediante diferentes casos de proba verificando cada un deles de xeito adecuado.

# 4. Características da proba e instrumentos necesarios para o seu desenvolvemento

## 4.1 Primeira parte da proba

Terá carácter eliminatorio e consistirá na realización dunha proba escrita de carácter teórico que constará de diferentes cuestións tipo test onde haberá unha única resposta correcta e/ou pequenas preguntas para contestar de xeito breve e razoado.

Para o desenvolvemento desta primeira parte a persoa aspirante soamente disporá de papel e un bolígrafo de cor azul ou negro. Non se permitirá ningún outro material. Non se correxirá ningún exercicio feito con lápiz ou haber empregado algún tipo de tinta correctora.

O aspirante deberá identificar claramente a súa proba, en caso contrario non se correxirá.

Queda totalmente prohibido o emprego de teléfonos móbiles ou calqueira outro dispositivo similar, deberán estar totalmente apagados e nunca visibles.

## 4.2 Segunda parte da proba

As persoas aspirantes que superen a primeira parte da proba realizarán a segunda, que tamén terá carácter eliminatorio e 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.

Para o desenvolvemento desta segunda parte a persoa aspirante disporá de papel, bolígrafo (azul ou negro), un ordenador con todo o software necesario para a realización dos exercicios. Nos equipos haberá o Sistema Operativo Windows 7 Enterprise así coma Ubuntu. As prácticas serán levadas a cabo en máquinas virtuais Oracle VM VirtualBox.

Non se poderá empregar ningún outro tipo de material que non sexa aceptado polo profesor.

O aspirante deberá identificar claramente a súa proba, en caso contrario non se correxirá.

Queda totalmente prohibido o emprego de teléfonos móbiles ou calqueira outro dispositivo similar, deberán estar totalmente apagados e nunca visibles.