

1. Identificación da programación
Centro educativo

Código	Centro	Concello	Ano académico
15021482	San Clemente	Santiago de Compostela	2022/2023

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	2022/2023	0	140	0

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

Profesorado responsable

Profesorado asignado ao módulo	ANA GONZÁLEZ NOVOA, JUAN ANTONIO GESTAL ROMANÍ
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 - 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.
CA2.6 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 Tívoise en conta a frecuencia e o esquema de rotación.

Criterios de avaliación do currículo
CA3.8 Identificáronse as características dos medios de almacenaxe remotos e extraíbles.
CA4.1 Seguíronse plans de continxencia para actuar ante fallos de seguridade.
CA4.2 Clasificáronse os principais tipos de software malicioso.
CA5.1 Identificouse 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 Identificáronse as ameazas na navegación por internet.
CA5.6 Clasificáronse e valoráronse as propiedades de seguridade dos protocolos usados en redes sen fíos.
CA5.7 Descríronse e utilizáronse 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

2.2.1. 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
CA1.2 Clasifícase a información no ámbito da seguridade.
CA1.8 Establecéronse as normas básicas para incluír nun manual de seguridade informática.
CA2.3 Verifícase o funcionamento dos sistemas de alimentación ininterrompida.
CA2.4 Seleccionáronse os puntos de aplicación dos sistemas de alimentación ininterrompida.
CA2.5 Esquematízanse 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.
CA3.2 Tivéronse en conta factores inherentes á almacenaxe da información (rendemento, dispoñibilidade, accesibilidade, etc.).
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.
CA3.7 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.
CA4.1 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 Verifícase 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.
CA5.4 Aplicáronse medidas para evitar a monitorización de redes con cables.
CA5.5 Identificáronse as ameazas na navegación por internet.
CA5.7 Descríbense 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.
CA6.4 Contrastouse a obriga de pór ao dispor das persoas os datos persoais que lles atinxen.

Criterios de avaliación do currículo

CA6.6 Contrastáronse as normas sobre xestión de seguridade da información.

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

A valoración da adquisición dos resultados de aprendizaxe de cada módulo profesional levarase a cabo a través da realización das dúas partes da proba:

Primeira parte. Terá carácter eliminatorio e consistirá nunha proba escrita que versará sobre unha mostra suficientemente significativa dos criterios de avaliación establecidos na programación para esta parte.

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

Segunda parte. As persoas aspirantes que superen a primeira parte da proba realizarán a segunda, que tamén terá carácter eliminatorio e consistirá no desenvolvemento dun ou de varios supostos prácticos que versarán sobre unha mostra suficientemente significativa dos criterios de avaliación establecidos na programación para esta parte.

Esta segunda parte da proba será cualificada 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 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.

4. Características da proba e instrumentos para o seu desenvolvemento**4.a) Primeira parte da proba**

Consistirá nunha proba escrita que poderá contar con preguntas tipo test, de resposta curta e/ou de desenvolvemento. A puntuación de cada pregunta indicárase ao inicio da proba. As preguntas versarán sobre os contidos sinalados na programación. As preguntas tipo test incorrectas restarán, unha pregunta tipo test incorrecta restará unha pregunta correcta.

Os instrumentos necesarios para a realización da proba serán papel e bolígrafo de cor negra ou azul. Non será corrixido ningún exercicio que se realice utilizando ferramentas diferentes ás indicadas, ou que non se cubran segundo as indicacións establecidas no enunciado do exame.

Non se corrixirá ningún exercicio feito con lápiz ou con algún tipo de tinta correctora.

Excluírase as persoas aspirantes que leven a cabo calquera actuación de tipo fraudulento ou incumpran as normas indicadas. Neste caso, o profesor ou a profesora do módulo profesional cualificará esa parte da proba do módulo cun cero.

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

Queda totalmente prohibido o emprego de teléfonos móbiles ou calquera outro dispositivo similar ou electrónico (reloxo digital, etc ...), deberán estar totalmente apagados e nunca visibles.

4.b) Segunda parte da proba

Consistirá na resolución de distintas cuestións nun ou varios supostos práctico onde os sistemas informáticos serán virtualizados mediante a ferramenta de virtualización Oracle VM VirtualBox. Os aspirantes deben ser quen de configurar os sistemas, para logo dar resposta ás cuestións propostas.

Os sistemas operativos cos que se traballará serán Ubuntu e Windows, tanto nas versións desktop como servidor.

Nalgúns casos as respostas ás cuestións serán dadas mediante capturas de pantalla, cos pertinentes comentarios

A proba versará sobre a maior parte dos contidos sinalados na programación.

Para o desenvolvemento desta segunda parte a persoa aspirante disporá de papel, lápiz, bolígrafo (azul ou negro), un ordenador con todo o software necesario para a realización dos exercicios. Nos equipos haberá o Sistema Operativo Windows así coma Ubuntu.

Non se correxirá ningún exercicio feito con lápiz ou con algún tipo de tinta correctora.

Non se permitirá ningún outro material.

Excluírase as persoas aspirantes que leven a cabo calquera actuación de tipo fraudulento ou incumpran as normas indicadas. Neste caso, o profesor ou a profesora do módulo profesional cualificará esa parte da proba do módulo cun cero.

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 ou electrónico (reloxo dixital, etc ...) , deberán estar totalmente apagados e nunca visibles.

Os arquivos empregados deberán poder abriren sen problemas polo profesorado encargado de correxir a proba, en caso contrario o aspirante terá un cero nesa parte. O alumno poderá facer esta comprobación á finalización do exame.