

1. Identificación da programación
Centro educativo

Código	Centro	Concello	Ano académico
15021482	San Clemente	Santiago de Compostela	2024/2025

Ciclo formativo

Código da familia profesional	Familia profesional	Código do ciclo formativo	Ciclo formativo	Grao	Réxime
IFC	Informática e comunicacións	CE3IFC005000	Ciberseguridade en contornos das tecnoloxías da información	Ciclos formativos de grao superior	Réxime xeral-ordinario

Módulo profesional e unidades formativas de menor duración (*)

Código MP/UF	Nome	Curso	Sesións semanais	Horas anuais	Sesións anuais
MP5022	Bastionado de redes e sistemas	2024/2025	7	160	192

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

Profesorado responsable

Profesorado asignado ao módulo	JAVIER FERNÁNDEZ PEÓN
Outro profesorado	

Estado: Pendente de supervisión equipo directivo

2. Concreción do currículo en relación coa súa adecuación ás características do ámbito produtivo

O desenrolo curricular deste módulo profesional fíxose tomando como referencia o Centro educativo IES San Clemente que cumpre as condicións establecidas pola L.O.E. e os Reais Decretos que a desenrolan en canto a espazos, instalacións, alumado, etc.

Se o contextualizamos para o entorno da cidade de Santiago de Compostela, no entorno do Centro encóntranse varias empresas de servizos informáticos onde é previsible que poidan desenrolar a súa carreira profesional. Sen embargo dado o carácter específico do Curso de Especialización no que se enmarca o presente módulo debemos o ámbito produtivo ampliarse a calquera empresa prestadora de servizos informáticos ou relacionada cas TICs nas que a capacitación en Ciberseguridade é fundamental.

3. Relación de unidades didácticas que a integran, que contribuirán ao desenvolvemento do módulo profesional, xunto coa secuencia e o tempo asignado para o desenvolvemento de cada unha

U.D.	Título	Descrición	Duración (sesións)	Peso (%)
1	Deseño de plans de securización	Deseña plans de securización incorporando boas prácticas para o bastionado de sistemas e redes	7	5
2	Configuración de sistemas de control de acceso e autenticación de persoas	Configura sistemas de control de acceso e autenticación preservando a confidencialidade e privacidade	7	5
3	Administración de credenciais de acceso a sistemas informáticos	Administra credenciais de acceso a sistemas informáticos aplicando os requisitos de funcionamento e seguridade establecidos	30	15
4	Deseño de redes de computadoras seguras	Deseña redes de computadoras contemplando os requisitos de seguridade	40	20
5	Configuración de dispositivos e sistemas informáticos	Configura dispositivos e sistemas informáticos cumprindo os requisitos de seguridade	40	20
6	Configuración de dispositivos para a instalación de sistemas informáticos	Configura dispositivos para a instalación de sistemas informáticos minimizando as probabilidades de exposición a ataques	24	10
7	Configuración dos sistemas informáticos	Configura sistemas informáticos minimizando as probabilidades de exposición a ataques	44	25

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Deseño de plans de securización	7

4.1.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA1 - Deseña plans de securización incorporando boas prácticas para o bastionado de sistemas e redes	SI

4.1.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA1.1 Identificáronse os activos, as ameazas e as vulnerabilidades da organización
CA1.2 Avaliáronse as medidas de seguridade actuais
CA1.3 Elaborouse unha análise de risco da situación actual en ciberseguridade da organización
CA1.4 Priorizáronse as medidas técnicas de seguridade para implantar na organización, tendo tamén en conta os principios da economía circular
CA1.5 Deseñouse e elaborouse un plan de medidas técnicas de seguridade para implantar na organización, apropiadas para garantir un nivel de seguridade adecuado en función dos riscos da organización
CA1.6 Identificáronse as mellores prácticas con base en estándares, guías e políticas de securización adecuadas para o bastionado dos sistemas e das redes da organización

4.1.e) Contidos

Contidos
Análise de riscos.
Principios da economía circular na industria 4.0.
Plan de medidas técnicas de seguridade.
Políticas de securización máis habituais.
Guías de boas prácticas para a securización de sistemas e redes.
Estándares de securización de sistemas e redes.
Caracterización de procedementos, instrucións e recomendacións.

Contidos
Niveis, escalados e protocolos de atención a incidencias.

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	Configuración de sistemas de control de acceso e autenticación de persoas	7

4.2.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA2 - Configura sistemas de control de acceso e autenticación de persoas preservando a confidencialidade e a privacidade dos datos	SI

4.2.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA2.1 Definíronse os mecanismos de autenticación con base en diversos factores (físicos, inherentes e baseados no coñecemento)
CA2.2 Definíronse protocolos e políticas de autenticación baseados en contrasinais e frases de paso, con base nas vulnerabilidades e nos tipos de ataques principais
CA2.3 Definíronse protocolos e políticas de autenticación baseados en certificados dixitais e tarxetas intelixentes, con base nas vulnerabilidades e nos tipos de ataques principais
CA2.4 Definíronse protocolos e políticas de autenticación baseados en tokens, OTP, etc., con base nas vulnerabilidades e nos tipos de ataques principais
CA2.5 Definíronse protocolos e políticas de autenticación baseados en características biométricas, segundo as vulnerabilidades e os tipos de ataques principais

4.2.e) Contidos

Contidos
Mecanismos de autenticación. Tipos de factores.
Autenticación baseada en distintas técnicas.

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	Administración de credenciais de acceso a sistemas informáticos	30

4.3.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA3 - Administra credenciais de acceso a sistemas informáticos aplicando os requisitos de funcionamento e seguridade establecidos	SI

4.3.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA3.1 Identifícanse os tipos de credenciais máis utilizados
CA3.2 Xeráronse e utilizáronse diferentes certificados dixitais como medio de acceso a un servidor remoto
CA3.3 Comprobase a validez e a autenticidade dun certificado dixital dun servizo web
CA3.4 Comparáronse certificados dixitais válidos e inválidos por diferentes motivos
CA3.5 Instalouse e configurouse un servidor seguro para a administración de credenciais tipo RADIUS (remote access dial in user service)

4.3.e) Contidos

Contidos
Xestión de credenciais.
Infraestruturas de clave pública (PKI).

Contidos
<p>Acceso por medio de sinatura electrónica.</p> <p>Xestión de accesos. Sistemas de xestión de acceso á rede NAC (network access control).</p> <p>Xestión de contas privilexiadas.</p> <p>Protocolos RADIUS e TACACS, servizo KERBEROS, etc.</p>

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Deseño de redes de computadoras seguras	40

4.4.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA4 - Deseña redes de computadores tendo en conta os requisitos de seguridade	SI

4.4.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA4.1 Incrementouse o nivel de seguridade dunha rede local plana segmentándoa fisicamente e utilizando técnicas e dispositivos de enrutamento
CA4.2 Optimizouse unha rede local plana utilizando técnicas de segmentación lóxica (VLAN)
CA4.3 Adaptouse un segmento dunha rede local xa operativa utilizando técnicas de subnetting para incrementar a súa segmentación respectando os direccionamentos existentes
CA4.4 Configuráronse as medidas de seguridade adecuadas nos dispositivos que dan acceso a unha rede sen fíos (enrutadores, puntos de acceso, etc.)
CA4.5 Estableceuse un túnel seguro de comunicacións entre dúas sedes xeograficamente separadas

4.4.e) Contidos

Contidos
Segmentación de redes.
Subnetting.
Redes virtuais (VLAN).
Zona desmilitarizada (DMZ).
Seguridade en redes sen fíos (WPA2, WPA3, etc.).
Protocolos de rede seguros (IPSec, etc.).

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Configuración de dispositivos e sistemas informáticos	40

4.5.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA5 - Configura dispositivos e sistemas informáticos cumprindo os requisitos de seguridade	SI

4.5.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA5.1 Configúranse dispositivos de seguridade perimetral acordes a unha serie de requisitos de seguridade
CA5.2 Detectáronse erros de configuración de dispositivos de rede mediante a análise de tráfico
CA5.3 Identifícanse comportamentos non desexados nunha rede a través da análise dos rexistros (logs) dunha devasa
CA5.4 Puxéronse en práctica contramedidas fronte a comportamentos non desexados nunha rede

Criterios de avaliación

CA5.5 Caracterizáronse, instaláronse e configuráronse ferramentas de monitorización

4.5.e) Contidos

Contidos

Seguridade perimetral. Firewalls de próxima xeración.

0Redes privadas virtuais (VPN) e túneles (protocolo IPSec).

Monitorización de sistemas e dispositivos.

Ferramentas de monitorización (IDS e IPS).

Xestores de eventos e información de seguridade (SIEM).

Solucións de centros de operación de rede, e centros de seguridade de rede: NOC e SOC.

Seguridade de portais e aplicativos web. Solucións WAF (web application firewall).

Seguridade do posto de traballo e endpoint fixo e móbil. AntiAPT; antimalware.

Seguridade de contornos Cloude. Solucións CASB.

Seguridade do correo electrónico

Solucións DLP (data loss prevention).

Ferramentas de almacenamento de logs.

Protección ante ataques de denegación de servizo distribuído (DDoS).

Configuración segura de devasas, enrutadores e proxies.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Configuración de dispositivos para a instalación de sistemas informáticos	24

4.6.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA6 - Configura dispositivos para a instalación de sistemas informáticos reducindo ao mínimo as probabilidades de exposición a ataques	SI

4.6.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA6.1 Configúrase a BIOS para incrementar a seguridade do dispositivo e o seu contido, reducindo ao mínimo as probabilidades de exposición a ataques
CA6.2 Prepara-se un sistema informático para a súa primeira instalación, tendo en conta as medidas de seguridade necesarias
CA6.3 Configúrase un sistema informático para que un actor malicioso non poida alterar a secuencia de arranque con fins de acceso ilexítimo
CA6.4 Instálase un sistema informático utilizando as súas capacidades de cifrado do sistema de ficheiros, para evitar a extracción física de datos
CA6.5 Particiónase o sistema de ficheiros do sistema informático para reducir ao mínimo os riscos de seguridade

4.6.e) Contidos

Contidos
Precaucións previas á instalación dun sistema informático: illamento, configuración do control de acceso á BIOS, bloqueo da orde de arranque dos dispositivos, etc.
Seguridade no arranque do sistema informático; configuración do arranque seguro.
Seguridade dos sistemas de ficheiros, cifrado, partición, etc.

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Configuración dos sistemas informáticos	44

4.7.b) Resultados de aprendizaxe do currículo que se tratan

Resultado de aprendizaxe do currículo	Completo
RA7 - Configura sistemas informáticos reduciendo ao mínimo as probabilidades de exposición a ataques	SI

4.7.d) Criterios de avaliación que se aplicarán para a verificación da consecución dos obxectivos por parte do alumnado

Criterios de avaliación
CA7.1 Enumeráronse e elimináronse os programas, os servizos e os protocolos innecesarios que foran instalados por defecto no sistema
CA7.2 Configuráronse as características propias do sistema informático para imposibilitar o acceso ilexítimo mediante técnicas de explotación de procesos
CA7.3 Incrementouse a seguridade do sistema de administración remoto SSH e outros
CA7.4 Instalouse e configurouse un sistema de detección de intrusos nun host (HIDS) no sistema informático
CA7.5 Instaláronse e configuráronse sistemas de copias de seguridade

4.7.e) Contidos

Contidos
Redución do número de servizos, Telnet, RSSH, TFTP, etc.
Hardening de procesos (eliminación de información de depuración en caso de erros, aleatorización da memoria virtual para evitar exploits, etc.).
Eliminación de protocolos de rede innecesarios (ICMP, etc.).
Securización dos sistemas de administración remota.
Sistemas de prevención e protección fronte a virus e intrusións (antivirus, HIDS, etc.).

Contidos

Configuración de actualizacións e parches automáticos.

Sistemas de copias de seguridade.

Shadow IT e políticas de seguridade en contornos SaaS.

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

Para o módulo de Bastionado de Redes e Sistemas será preciso aprobar as dúas avaliación, cunha nota de 5 ou superior en cada unha, para superar con éxito o módulo.

As probas poden realizarse en ordenador.

A proba final constará dun exame teórico-práctico onde o alumno deberá de aprobar con 5 puntos sobre 10. Será necesario entregar todas as prácticas obrigatorias do curso para superar con éxito o módulo.

EXAME DE AVALIACIÓN:

Realizara un exame teórico/práctico por avaliación. O exame pode incluír unha parte práctica a realizar no ordenador.

A nota do exame será entre 0 e 10.

NOTA DE CADA AVALIACIÓN

É imprescindible ter superado cada apartado do exame para poder aprobar a avaliación.

É imprescindible acadar un 5 sobre 10 para aprobar cada avaliación

A nota final da avaliación será un número enteiro entre 1 e 10.

NOTA FINAL DO CURSO

Calcularase como a media das notas de cada avaliación.

Será o valor enteiro entre 1 e 10 máis próximo á nota media.

É imprescindible ter aprobado tódalas avaliacións, no caso de ter unha avaliación suspensa a nota final non poderá ser maior de 4.

6. Procedemento para a recuperación das partes non superadas**6.a) Procedemento para definir as actividades de recuperación**

Durante o período que abarca dende a segunda avaliación ata a proba do exame final o alumnado que non acade os mínimos requiridos poderán realizar actividades complementarias co obxecto de acadar os mínimos exixidos.

Poderanse propor actividades de reforzo para os alumnos que non superasen as avaliacións, consistentes na realización de exercicios prácticos, teóricos e explicacións complementarias sobre as unidades didácticas non superadas, empregando a plataforma Mestre do IES San Clemente.

Permitirase entregar de novo as tarefas que non se entregaran no prazo establecido ou acadasen unha nota baixa.

Poderán optar a avaliación da parte non superada (avaliación ou unidade didáctica, segundo se considere preciso) na proba final, no remate do curso.

Atención especial para a resolución de dúbidas, tanto en clase como en horas de titoría.

6.b) Procedemento para definir a proba de avaliación extraordinaria para o alumnado con perda de dereito a avaliación continua

Non aplica

7. Procedemento sobre o seguimento da programación e a avaliación da propia práctica docente

Durante o curso irase actualizando, revisando e modificando a programación. Avaliarase a práctica docente tendo en conta a interacción co alumnado e os resultados que se obteñen.

O procedemento para a seguimento da programación didáctica será o que continúa:

En reunión de departamento, cunha frecuencia mensual dunha reunión por mes, revisarase o cumprimento da programación e se corraxirá o que se estime oportuno: secuenciación/temporalización de actividades, substitución de actividades por outras, etc.

Teranse en conta especialmente os informes e observacións do profesor titor do ciclo. Tamén revisarase a coordinación co resto do equipo docente do grupo. Cara o curso académico seguinte, a programación reflectirá as correccións feitas froito do traballo anterior.

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

Farase unha sesión de avaliación inicial do alumnado para determinarl o nivel de coñecementos do mesmo. Ao tratarse dun Curso de Especialización ó que o alumnado accede cunha titulación mínima de Técnico de Grado Superior será avaliación de ámbito puramente técnico enfocada a determinar a capacitación técnica para así poder establecer un punto de partida o máis homoxéneo posible. Ao comezo das actividades lectivas falarase co profesor ou a profesora que se encarguen da titoría para coñecer a información dispoñible sobre as características xerais do grupo ou sobre as circunstancias especificamente académicas ou persoais con incidencia educativa, conforme ao informe que se elaborou o primeiro curso do ciclo.

No caso de detectarse casos de necesidades educativas especiais en cursos anteriores, proporase realizar unha sesión de avaliación inicial do equipo docente, recoller nunha acta os acordos necesarios e entregar unha copia na xefatura de estudos.

8.b) Medidas de reforzo educativo para o alumnado que non responda globalmente aos obxectivos programados

Os contidos teórico-prácticos e a realización de tarefas propostas diríxense ao conxunto do alumnado. Porén, prevese un tempo, que será concretado polo profesorado segundo a marcha real das clases, para adicalo á atención diferente que requiren os niveis fóra da media.

Para o alumnado por baixo da media o profesorado tratará con especial atención os problemas que se lles presenten, deténdose nos puntos onde se detectou dificultade na comprensión, e propondrá exercicios de reforzo dos conceptos vistos, abondando nos puntos cruciais.

Para o alumnado por riba da media poderase propor, se así se estima, exercicios de maior dificultade que os presentados ao conxunto do alumnado, a busca de información para a ampliación de temas xa tratados, e o tratamento de temas de interese relacionados aínda que non incluídos nos contidos do módulo.

- Atención especial aos alumnos con deficiencias de comprensión e seguimento de contidos.
- Coordinación de accións co Departamento de Orientación naqueles casos que se considere necesario.

9. Aspectos transversais

9.a) Programación da educación en valores

Recordarase ao alumnado as conmemoracións que se produzan ao longo do curso:

- * Día Universal da infancia
- * Día Internacional contra a Violencia de Xénero.
- * Constitución e Estatuto de autonomía de Galicia.
- * Día Internacional das Persoas con Discapacidade.
- * Día da Declaración Universal dos Dereitos Humanos.
- * Día Escolar da non Violencia e da Paz.
- * Día Internacional da Muller.
- * Día Mundial dos Dereitos do Consumidor.

- * Semana da Prensa.
- * Día Mundial da Saúde.
- * Semana do libro.
- * Día de Europa.
- * Semana das Letras Galegas.
- * Día Mundial do Ambiente

9.b) Actividades complementarias e extraescolares

Tódalas actividades propostas polo Departamento de Informática. O departamento deixa aberta a porta á asistencia a conferencias e seminarios, que ou ben se planifiquen polo departamento ou ben vaian xurdindo no ámbito social e sexan consideradas de interese.