1. Identificación da programación

Centro educativo

Código	Centro	Concello	Ano académico
15021482	San Clemente	Santiago de Compostela	2023/2024

Ciclo formativo

Código da familia profesional	Familia profesional	Código do ciclo formativo	Ciclo formativo	Grao	Réxime
IFC	Informática e comunicacións	CSIFC01	Administración de sistemas informáticos en rede	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
MP0378	Seguridade e alta dispoñibilidade	2023/2024	6	105	126

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

Profesorado responsable

Profesorado asignado ao módulo	MANUEL GONZÁLEZ REGAL
Outro profesorado	

Estado: Pendente de supervisión departamento

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

- Este módulo profesional contén a formación necesaria para seleccionar e utilizar técnicas e ferramentas específicas de seguridade informática no ámbito da administración de sistemas. Ademais, ha servir para coñecer arquitecturas de alta dispoñibilidade e utilizar ferramentas de virtualización na implantación de servizos de alta dispoñibilidade.
- As funcións da administración segura de sistemas abranguen aspectos como:
  * Coñecemento e correcta manipulación de todos os elementos que forman o compoñente físico e lóxico dos equipamentos.
  * Adopción de prácticas seguras consonte os plans de seguridade física e lóxica do sistema.
  * Coñecemento e uso de técnicas seguras de acceso remoto a un sistema, tanto en modo usuario como en modo administrativo.
  * Selección e aplicación de técnicas e ferramentas de seguridade activa que actúen como medidas preventivas ou paliativas ante ataques a ao sistema.
  * Instalación e configuración de ferramentas de protección perimetral, tornalumes e servidores proxy.
  * Instalación e configuración de servizos de alta dispoñibilidade que garantan a continuidade de servizos e a dispoñibilidade de datos.
  * Coñecemento e aplicación da lexislación no ámbito do tratamento dixital da información.
- As actividades profesionais asociadas a estas funcións aplícanse en:
  * Mantemento de equipamentos (hardware e software).
  * Administración de sistemas en pequenas e medianas empresas.
  * Persoal técnico de administración de sistemas en centros de procesamento de datos.
  * Persoal técnico de apoio en empresas especializadas en seguridade informática.
- A formación do módulo contribúe a alcanzar os seguintes obxectivos xerais:
  * Seleccionar sistemas de protección e recuperación, analizando as súas características funcionais, para pór en marcha solucións de alta dispoñibilidade.
  * Identificar condicións de equipamentos e instalacións, interpretando plans de seguridade e especificacións de fábrica, para supervisar a seguridade física.
  * Aplicar técnicas de protección contra ameazas externas, así como tipificalas e avalialas, para asegurar o sistema.
  * Aplicar técnicas de protección contra perdas de información, analizando plans de seguridade e necesidades de uso para asegurar os datos.
  * Establecer a planificación de tarefas, analizando actividades e cargas de traballo do sistema, para xestionar o mantemento.
  * Identificar os cambios tecnolóxicos, organizativos, económicos e laborais na actividade propia, analizando as súas implicacións no ámbito de traballo, para resolver problemas e manter unha cultura de actualización e innovación.
- A formación do módulo contribúe a alcanzar as seguintes competencias profesionais, persoais e sociais:
  * Mellorar o rendemento do sistema configurando os dispositivos de hardware consonte os requisitos de funcionamento.
  * Avaliar o rendemento dos dispositivos de hardware identificando posibilidades de mellora segundo as necesidades de funcionamento.
  * Pór en práctica solucións de alta dispoñibilidade, analizando as opcións do mercado, para protexer e recuperar o sistema ante situacións imprevistas.
  * Supervisar a seguridade física segundo especificacións de fábrica e o plan de seguridade, para evitar interrupcións na prestación de servizos do sistema.
  * Asegurar o sistema e os datos segundo as necesidades de uso e as condicións de seguridade establecidas, para previr fallos e ataques externos.
  * Diagnosticar as disfuncións do sistema e adoptar as medidas correctivas para restablecer a súa funcionalidade.
  * Xestionar e/ou realizar o mantemento dos recursos da súa área (programando e verificando ou seu cumprimento), en función das cargas de traballo e o plan de mantemento.
  * Manter o espírito de innovación e actualización no ámbito de ou seu traballo para adaptarse aos cambios tecnolóxicos e organizativos de ou seu ámbito profesional.
  * Xestionar a propia carreira profesional, analizando as oportunidades de emprego, de autoemprego e de aprendizaxe.
  * Participar de xeito activo na vida económica, social e cultural, con actitude crítica e responsable.

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	Introdución á Seguridade da Información	Introdución á Seguridade da Información	8	6
2	LSSI-CE	Lei Serv. Soc. Infor. e Comercio Elect.	4	3
3	LOPD	Lei Org. Protección de datos	9	7
4	Seguridade defensiva	Medidas de seg. Física e lóxica	10	8
5	Seguridade nas redes	Introducción ás medidas de seg. en rede	20	16
6	Firewalls	Firewalls	16	13
7	Proxys	Proxys	12	10
8	Acceso Remoto	Técnicas de acceso remoto seguro	8	6
9	Auditorías e Seguridade Ofensiva	Técnicas de seg. Ofensiva e auditorías	6	5
10	Criptoloxía. Lei Sinatura dixital	Cifrado, lei sinatura dixital, dni-e.	6	5
11	Alta dispoñibilidade	Sistemas de alta dispoñibilidade	27	21

4. Por cada unidade didáctica

4.1.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
1	Introdución á Seguridade da Información	8

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.	NO
RA7 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia.	NO

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 Valorouse a importancia de asegurar a privacidade, a coherencia e a dispoñibilidade da información nos sistemas informáticos.
CA1.2 Describíronse as diferenzas entre seguridade física e lóxica.
CA1.3 Clasificáronse os tipos principais de vulnerabilidade dun sistema informático, segundo a súa tipoloxía e a súa orixe.
CA1.4 Contrastouse a incidencia das técnicas de enxeñaría social nas fraudes informáticas.
CA1.9 Identificáronse as fases da análise forense ante ataques a un sistema.
CA7.1 Describiuse a lexislación sobre protección de datos de carácter persoal.
CA7.2 Determinouse a necesidade de controlar o acceso á información persoal almacenada.
CA7.6 Contrastáronse as normas sobre xestión de seguridade da información.
CA7.7 Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable.

4.1.e) Contidos

Contidos
Fiabilidade, confidencialidade, integridade e dispoñibilidade.
Elementos vulnerables no sistema informático: hardware, software e datos.
Análise das principais vulnerabilidades dun sistema informático.
Tipos de ameazas: físicas e lóxicas.
Análise forense en sistemas informáticos: obxectivo. Recollida e análise de incidencias.
Ferramentas empregadas na análise forense.

4.2.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
2	LSSI-CE	4

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

Resultado de aprendizaxe do currículo	Completo
RA7 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia.	NO

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

Criterios de avaliación
CA7.5 Describiuse a lexislación actual sobre os servizos da sociedade da información e o comercio electrónico.
CA7.7 Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable.

4.2.e) Contidos

Contidos
Lexislación sobre protección de datos e sobre os servizos da sociedade da información e o correo electrónico.

4.3.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
3	LOPD	9

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.	NO
RA7 - Recoñece a lexislación e a normativa sobre seguridade e protección de datos, e valora a súa importancia.	NO

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

Criterios de avaliación
CA1.5 Adoptáronse políticas de contrasinais.
CA7.1 Describiuse a lexislación sobre protección de datos de carácter persoal.
CA7.2 Determinouse a necesidade de controlar o acceso á información persoal almacenada.
CA7.3 Identificáronse as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.
CA7.4 Contrastouse o deber de pór ao dispor das persoas os datos persoais que lles atinxen.
CA7.7 Comprendeuse a necesidade de coñecer e respectar a normativa legal aplicable.

4.3.e) Contidos

Contidos
Seguridade lóxica: Criptografía. Listas de control de acceso. Establecemento de políticas de contrasinais. Sistemas biométricos de identificación. Políticas de almacenamento. Medios de almacenamento. Copias de seguridade e imaxes de respaldo. Recuperación de datos. Lexislación sobre protección de datos e sobre os servizos da sociedade da información e o correo electrónico.

4.4.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
4	Seguridade defensiva	10

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.	NO
RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.	NO

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

Criterios de avaliación
CA1.6 Valoráronse as vantaxes do uso de sistemas biométricos.
CA2.1 Clasificáronse os principais tipos de ameazas lóxicas contra un sistema informático.
CA2.2 Verificouse a orixe e a autenticidade das aplicacións instaladas nun equipamento, así como o estado de actualización do sistema operativo.
CA2.3 Identificouse a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.
CA2.4 Analizáronse diversos tipos de ameazas, ataques e software malicioso, en contornos de execución controlados.
CA2.5 Implantáronse aplicacións específicas para a detección de ameazas e a eliminación de software malicioso.

4.4.e) Contidos

Contidos
Pautas e prácticas seguras. Seguridade física e ambiental: Localización e protección física dos equipamentos e dos servidores. Sistemas de alimentación ininterrompida. Seguridade lóxica: Criptografía. Listas de control de acceso. Establecemento de políticas de contrasinais. Sistemas biométricos de identificación. Políticas de almacenamento. Medios de almacenamento. Ataques e contramedidas en sistemas informáticos. Clasificación dos ataques. Ferramentas preventivas e paliativas: instalación e configuración. Actualización de sistemas e aplicacións.

4.5.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
5	Seguridade nas redes	20

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.	NO
RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.	NO

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

Criterios de avaliación
CA1.8 Recoñeceuse a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.
CA2.7 Avaliáronse as medidas de seguridade dos protocolos usados en redes de comunicación.
CA2.8 Recoñeceuse a necesidade de inventariar e controlar os servizos de rede que se executan nun sistema.
CA2.9 Describíronse os tipos e as características dos sistemas de detección de intrusións.

4.5.e) Contidos

Contidos
Análise forense en sistemas informáticos: obxectivo. Recollida e análise de incidencias.
Ferramentas empregadas na análise forense.
Monitorización do tráfico en redes: captura e análise; aplicacións.
Seguridade nos protocolos para comunicacións sen fíos.
Sistemas de detección de intrusións.
Seguridade na conexión con redes públicas.
Elementos básicos da seguridade perimetral: encamiñador fronteira; tornalumes; redes privadas virtuais.
Perímetros de rede. Zonas desmilitarizadas.
Arquitectura débil e forte de subrede protexida.

4.6.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
6	Firewalls	16

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

Resultado de aprendizaxe do currículo	Completo
RA4 - Implanta tornalumes (firewalls) para asegurar un sistema informático, analiza as súas prestacións e controla o tráfico cara á rede interna.	SI

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

Criterios de avaliación
CA4.1 Describíronse as características, os tipos e as funcións dos tornalumes.
CA4.2 Clasificáronse os niveis en que se realiza a filtraxe de tráfico.
CA4.3 Configuráronse filtros nun tornalumes a partir dunha listaxe de regras de filtraxe.
CA4.4 Revisáronse os rexistros de sucesos de tornalumes, para verificar que as regras se apliquen correctamente.
CA4.5 Interpretouse a documentación técnica de distintos tornalumes hardware nos idiomas máis empregados pola industria.
CA4.6 Probáronse distintas opcións para implementar tornalumes, tanto de software como de hardware.
CA4.7 Diagnosticáronse problemas de conectividade nos clientes provocados polos tornalumes.
CA4.8 Planificouse a instalación de tornalumes para limitar os accesos a determinadas zonas da rede.
CA4.9 Elaborouse documentación relativa á instalación, configuración e uso de tornalumes.

4.6.e) Contidos

Contidos
Utilización de tornalumes. Filtraxe de paquetes de datos. Tipos de tornalumes: características e funcións principais: Uso das características de tornalumes incorporadas no sistema operativo. Implantación de tornalumes en sistemas libres e propietarios. Instalación e configuración. Tornalumes hardware. Regras de filtraxe de tornalumes. Probas de funcionamento: sondaxe. Rexistros de sucesos nos tornalumes.

4.7.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
7	Proxys	12

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

Resultado de aprendizaxe do currículo	Completo
RA5 - Implanta servidores proxy, aplicando criterios de configuración que garantan o funcionamento seguro do servizo.	SI

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

Criterios de avaliación
CA5.1 Identificáronse os tipos de proxy, as súas características e as súas funcións principais.
CA5.2 Instalouse e configurouse un servidor proxy cache.
CA5.3 Configuráronse os métodos de autenticación no proxy.
CA5.4 Configurouse un proxy en modo transparente.
CA5.5 Utilizouse o servidor proxy para establecer restricións de acceso web.
CA5.6 Arranxáronse problemas de acceso desde os clientes ao proxy.
CA5.7 Realizáronse probas de funcionamento do proxy, monitorizando a súa actividade con ferramentas gráficas.
CA5.8 Configurouse un servidor proxy en modo inverso.
CA5.9 Elaborouse documentación relativa á instalación, a configuración e o uso de servidores proxy.

4.7.e) Contidos

Contidos
Tipos de proxy: características e funcións.
Instalación de servidores proxy.
Instalación e configuración de clientes proxy.
Configuración do almacenamento na cache dun proxy.
Configuración de filtros.
Métodos de autenticación nun proxy.
Proxy inverso.
Encadeamento e xerarquías.
Probas de funcionamento.

4.8.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
8	Acceso Remoto	8

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

Resultado de aprendizaxe do currículo	Completo
RA3 - Implanta técnicas seguras de acceso remoto a un sistema informático, para o que interpreta e aplica o plan de seguridade.	SI

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

Criterios de avaliación
CA3.1 Describíronse escenarios típicos de sistemas con conexión a redes públicas en que cumpra fortificar a rede interna.
CA3.2 Clasificáronse as zonas de risco dun sistema, segundo criterios de seguridade perimetral.
CA3.3 Identificáronse os protocolos seguros de comunicación e os seus ámbitos de uso.
CA3.4 Configuráronse redes privadas virtuais mediante protocolos seguros a distintos niveis.
CA3.5 Implantouse un servidor como pasarela de acceso á rede interna desde localizacións remotas.
CA3.6 Identificáronse e configuráronse os métodos posibles de autenticación no acceso de usuarios remotos a través da pasarela.
CA3.7 Instalouse, configurouse e integrouse na pasarela un servidor remoto de autenticación.

4.8.e) Contidos

Contidos
Redes privadas virtuais. VPN. Beneficios e desvantaxes con respecto ás liñas dedicadas. VPN a nivel de enlace. VPN a nivel de rede. SSL e IPSec. VPN a nivel de aplicación. SSH. Servidores de acceso remoto: Protocolos de autenticación. Configuración de parámetros de acceso. Servidores de autenticación.

4.9.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
9	Auditorías e Seguridade Ofensiva	6

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.	NO
RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.	NO

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

Criterios de avaliación
CA1.9 Identificáronse as fases da análise forense ante ataques a un sistema.
CA2.3 Identificouse a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.
CA2.4 Analizáronse diversos tipos de ameazas, ataques e software malicioso, en contornos de execución controlados.
CA2.8 Recoñeceuse a necesidade de inventariar e controlar os servizos de rede que se executan nun sistema.

4.9.e) Contidos

Contidos
Análise forense en sistemas informáticos: obxectivo. Recollida e análise de incidencias.
Ferramentas empregadas na análise forense.
Ataques e contramedidas en sistemas informáticos.
Riscos potenciais dos servizos de rede. Software para detección de vulnerabilidades.
Intentos de penetración: tipoloxía.
Clasificación dos ataques.
Anatomía de ataques e análise de software malicioso.
Realización de auditorías de seguridade.

4.10.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
10	Criptoloxía. Lei Sinatura dixital	6

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

Resultado de aprendizaxe do currículo	Completo
RA1 - Adopta pautas e prácticas de tratamento seguro da información, e recoñece a vulnerabilidade dun sistema informático e a necesidade de o asegurar.	NO
RA2 - Implanta mecanismos de seguridade activa, para o que selecciona e executa contramedidas ante ameazas ou ataques ao sistema.	NO

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

Criterios de avaliación
CA1.7 Aplicáronse técnicas criptográficas no almacenamento e na transmisión da información.
CA2.6 Utilizáronse técnicas de cifraxe, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas.

4.10.e) Contidos

Contidos
Seguridade lóxica: Criptografía. Listas de control de acceso. Establecemento de políticas de contrasinais. Sistemas biométricos de identificación. Políticas de almacenamento. Medios de almacenamento. 0Técnicas de cifraxe da información: clave pública e clave privada; certificados dixitais; sinaturas.

4.11.a) Identificación da unidade didáctica

N.º	Título da UD	Duración
11	Alta dispoñibilidade	27

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

Resultado de aprendizaxe do currículo	Completo
RA6 - Implanta solucións de alta dispoñibilidade empregando técnicas de virtualización, e configura os contornos de proba.	SI

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

Criterios de avaliación
CA6.1 Analizáronse supostos e situacións en que cumpra pór en marcha solucións de alta dispoñibilidade.
CA6.2 Identificáronse solucións de hardware para asegurar a continuidade no funcionamento dun sistema.
CA6.3 Avaliáronse as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.
CA6.4 Implantouse un servidor redundante que garanta a continuidade de servizos en casos de caída do servidor principal.
CA6.5 Implantouse un balanceador de carga á entrada da rede interna.
CA6.6 Implantáronse sistemas de almacenamento redundante sobre servidores e dispositivos específicos.
CA6.7 Avaliouse a utilidade dos sistemas de clúster para aumentar a fiabilidade e a produtividade do sistema.
CA6.8 Analizáronse solucións de futuro para un sistema con demanda crecente.
CA6.9 Esquematizáronse e documentáronse solucións para supostos con necesidades de alta dispoñibilidade.

4.11.e) Contidos

Contidos
Definición e obxectivos. Análise de configuracións de alta dispoñibilidade. Funcionamento ininterrompido. Integridade de datos e recuperación de servizo. Servidores redundantes. Sistemas de clústers. Balanceadores de carga. Instalación e configuración de solucións de alta dispoñibilidade. Virtualización de sistemas. Posibilidades da virtualización de sistemas. Ferramentas para a virtualización. Configuración e uso de máquinas virtuais. Alta dispoñibilidade e virtualización. Simulación de servizos con virtualización. Análise e optimización Virtualización en contornos de produción.

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

CRITERIOS DE CUALIFICACIÓN:

Probas:

- A medida que o curso avanza, as unidades didácticas vanse facendo máis complexas e moitas delas baséanse nas anteriores. Como norma xeral, realizarase unha proba por cada dúas unidades de traballo; sen embargo, o número de unidades de traballo podería aumentar ou diminuír se fose o máis indicado para obter mellores resultados no proceso de ensinanza-aprendizaxe.
- Estas probas constarán de forma xeral de dúas partes:

* Escrita sobre contidos teóricos das unidades.
* Práctica simulando unha situación real de traballo, onde o alumno deberá demostrar o dominio dos contidos e procedementos adquiridos para levar a cabo a tarefa dunha forma axeitada e nun tempo adecuado.

- En cada parte figurará a puntuación asignada a cada pregunta.
- No enunciado informarase da puntuación mínima necesaria en cada parte para acadar o aprobado na proba.
- Como norma xeral a puntuación máxima dunha proba será 10, estando o aprobado nun 5 (traballando con ata 3 decimais) sempre que se chegue ó aprobado en cada parte. É dicir, hai que aprobar as dúas partes para que a proba se considere aprobada.

Traballos de investigación en grupo ou individuais:

- Consistirán na investigación e/ou exposición por parte dun alumno ou dun grupo de alumnos ó resto dos seus compañeiros.
- O traballo versará sobre un tema concreto proposto polo profesor, ó que os alumnos poden suxerir ideas.
- Haberá traballos de reforzo que non sumarán para a nota de avaliación pero que sí son de entrega obrigatoria.
- Valorarase:

  * A consecución dos obxectivos a acadar no traballo e a súa forma de implementación.
  * Os contidos do traballo.
  * A capacidade de investigación.
  * A comprensión.
  * A capacidade de explicación
  * Nivel de dificultade do traballo.

- En cada traballo o profesor indicará os obxectivos a acadar, a puntuación máxima e a e a puntuación necesaria para acadar a superación na proba. Así como o peso do mesmo en relación á nota da avaliación.
- Todos os traballos son de entrega obrigatoria, salvo que o profesor indique o contrario. Non entregar o traballo en tempo e forma, conlevará a consideración de suspenso (non superado).
- Como norma xeral a puntuación máxima dunha proba será 10 estando o aprobado nun 5, traballando con ata 3 decimais.

Traballo diario na aula e asistencia:

- O profesor proporcionará enunciados de exercicios que terán que resolver os alumnos. Algúns serán traballos a entregar ou ben a ensinar na aula ó profesor para que este verifique o seu correcto funcionamento.
- Cada traballo entregado será puntuado, corrixido e entregado de novo ó alumno para que rectifique os fallos cometidos, e se lle explicarán aqueles conceptos ou procedementos que non teña claros.
- Haberá traballos de reforzo que non sumarán para a nota de avaliación pero que si son de entrega obrigatoria.

Proxecto final:
- En función da marcha do curso e se o tempo o permite, plantexarase na última parte de mesmo, ó alumnado un proxecto de fin de curso consistente nun traballo,
eminentemente práctico, onde teña que aplicar tanto os coñecementos coma os procedementos adquiridos ó longo de curso.
- Este proxecto ten o mesmo carácter que un exame práctico.

Avaliación:
- En cada avaliación haberá de forma xeral:
  * Dúas ou máis probas.
  * Un o máis traballos.

Avaliación positiva:
- Para ter unha avaliación positiva nunha avaliación é preciso superar todas e cada unha das probas e traballos. No caso de non superar todas as probas ou traballos, a avalación considerase como non superada.
- De superar todas as probas e traballos a avaliación considerase aprobada.
- De forma xeral, no caso de aprobar a avaliación o cálculo da nota seguirá o seguinte criterio:
  * as probas un 90% da nota da avaliación.
  * os traballos prácticos un 10% da nota da avaliación.
  * Esta porcentaxe será comunicada ó alumnado, e no caso de que a marcha da clase así o suxira poderá modificarse, comunicándollo ó alumnado con suficiente antelación.

Avaliación negativa:
- No caso de non superar algunha das probas nunha avaliación, o alumno/a terá antes da sesión de avaliación unha proba personalizada, onde terá a oportunidade de recuperar aquelas probas pendentes.
- No caso de traballos non superados, o profesor asignará ó alumno unha serie de tarefas para entregar nunha data anterior á sesión de avaliación.
- A nota que aparecerá na avaliación será a menor das puntuacións obtidas nas probas.

- Para ó alumnado que ó chegar ó mes de marzo/abril teña partes pendentes (probas non superadas):
  * haberá unha proba final personalizada por alumno, onde poderá recuperar aquelas partes da asignatura que teña suspensas.
  * no caso de traballos non superados, o profesor asignará ó alumno unha serie de tarefas para entregar.
- De superar esta proba/traballos, considerarase que o alumno superou a asignatura.
- No caso de non superar esta proba/traballos, considerase que o alumno non superou a asignatura.
- Para aqueles alumnos que superaron o módulo, a nota final será o promedio das notas das avaliacións xunto coa nota da proba final.
- Para o alumnado que non superou o módulo, a nota final reflictirá a nota da proba final. Nesta situación non se calculan medias coas notas recibidas en partes superadas.

Alumnado NEE:
- No caso do alumnado con NEE, valorarase a súa situación e procederase á adaptación das probas/traballos.

MINIMOS ESIXIBLES:
Unidade Didáctica 1: Introdución á Seguridade da Información
- Valorar a importancia de asegurar a privacidade, a coherencia e a dispoñibilidade da información nos sistemas informáticos.
- Describir as diferenzas entre seguridade física e lóxica.
- Clasificar os tipos principais de vulnerabilidade dun sistema informático, segundo a súa tipoloxía e a súa orixe.
- Contrastar a incidencia das técnicas de enxeñaría social nas fraudes informáticas.
- Identificar as fases da análise forense ante ataques a un sistema. Coñecer e entender as fases dun ataque. A Cyber Kill Chain e matriz MITRE ATT&CK.

- Describir a lexislación sobre protección de datos de carácter persoal.
- Determinar a necesidade de controlar o acceso á información persoal almacenada.
- Contrastar as normas sobre xestión de seguridade da información.
- Comprender a necesidade de coñecer e respectar a normativa legal aplicable.

Unidade Didáctica 2: LSSI-CE

- Describir a lexislación actual sobre os servizos da sociedade da información e o comercio electrónico.
- Comprender a necesidade de coñecer e respectar a normativa legal aplicable.

Unidade Didáctica 3: LOPD

- Describir a lexislación sobre protección de datos de carácter persoal.
- Determinar a necesidade de controlar o acceso á información persoal almacenada.
- Identificar as figuras legais que interveñen no tratamento e no mantemento dos ficheiros de datos.
- Contrastar o deber de pór ao dispor das persoas os datos persoais que lles atinxen.
- Adoptar políticas de contrasinais.

Unidade Didáctica 4: Seguridade defensiva

- Valorar as vantaxes do uso de sistemas biométricos.
- Clasificar os principais tipos de ameazas lóxicas contra un sistema informático.
- Verificar a orixe e a autenticidade das aplicacións instaladas nun equipamento, así como o estado de actualización do sistema operativo.
- Identificar a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles. A Cyber Kill Chain e matriz MITRE ATT&CK
- Analizar diversos tipos de ameazas, ataques e software malicioso, en contornos de execución controlados.
- Implantar aplicacións específicas para a detección de ameazas e a eliminación de software malicioso.

Unidade Didáctica 5: Seguridade nas redes

- Recoñer a necesidade de establecer un plan integral de protección perimetral, nomeadamente en sistemas conectados a redes públicas.
- Avaliar as medidas de seguridade dos protocolos usados en redes de comunicación.
- Recoñer a necesidade de inventariar e controlar os servizos de rede que se executan nun sistema.
- Describir os tipos e as características dos sistemas de detección de intrusións.
- Instalar e usar sniffers para analizar capturas de rede e detectar intrusións seguindo os pasos dunha análise forense.

Unidade Didáctica 6: Firewalls

- Describir as características, os tipos e as funcións dos tornalumes.
- Clasificar os niveis en que se realiza a filtraxe de tráfico.
- Configurar filtros nun tornalumes a partir dunha listaxe de regras de filtraxe.
- Revisar os rexistros de sucesos de tornalumes, para verificar que as regras se apliquen correctamente.
- Interpretara documentación técnica de distintos tornalumes hardware nos idiomas máis empregados pola industria.
- Probar distintas opcións para implementar tornalumes, tanto de software como de hardware.
- Diagnosticar problemas de conectividade nos clientes provocados polos tornalumes.
- Planificar a instalación de tornalumes para limitar os accesos a determinadas zonas da rede.
- Elaborar documentación relativa á instalación, configuración e uso de tornalumes.

Unidade Didáctica 7: Proxys

- Identificar os tipos de proxy, as súas características e as súas funcións principais.
- Instalar e configurar un servidor proxy cache.
- Configurar os métodos de autenticación no proxy.
- Configurar un proxy en modo transparente.
- Utilizar o servidor proxy para establecer restricións de acceso web.
- Arranxar problemas de acceso desde os clientes ao proxy.
- Realizar probas de funcionamento do proxy, monitorizando a súa actividade con ferramentas gráficas.

- Configurar un servidor proxy en modo inverso. Configurar o proxy para funcionar como terminador ssl.
- Elaborar documentación relativa á instalación, a configuración e o uso de servidores proxy.

Unidade Didáctica 8: Acceso Remoto

- Describir escenarios típicos de sistemas con conexión a redes públicas en que cumpra fortificar a rede interna.
- Clasificar as zonas de risco dun sistema, segundo criterios de seguridade perimetral.
- Identificar os protocolos seguros de comunicación e os seus ámbitos de uso.
- Configurar redes privadas virtuais mediante protocolos seguros a distintos niveis.
- Implantar un servidor como pasarela de acceso á rede interna desde localizacións remotas.
- Identificar e configurar os métodos posibles de autenticación no acceso de usuarios remotos a través da pasarela.
- Instalar, configurar e integrar na pasarela un servidor remoto de autenticación.
- Instalar, configurar e manexar o acceso seguro mediante SSH e certificados dixitais,

Unidade Didáctica 9: Auditorías e Seguridade Ofensiva

- Identificar a anatomía dos ataques máis habituais, así como as medidas preventivas e paliativas dispoñibles.
- Analizar diversos tipos de ameazas, ataques e software malicioso, en contornos de execución controlados.
- Coñecer e executar as distintas fases das que se compoñen as metodoloxías de auditoría máis empregados hoxe en día.
- Recoñecer a necesidade de inventariar e controlar os servizos de rede que se executan nun sistema.

Unidade Didáctica 10: Criptoloxía. Lei Sinatura dixital

- Aplicar técnicas criptográficas no almacenamento e na transmisión da información.
- Utilizar técnicas de cifraxe, sinaturas e certificados dixitais nun contorno de traballo baseado no uso de redes públicas.

Unidade Didáctica 11: Alta dispoñibilidade

- Analizar supostos e situacións en que cumpra pór en marcha solucións de alta dispoñibilidade.
- Identificar solucións de hardware para asegurar a continuidade no funcionamento dun sistema.
- Avaliar as posibilidades da virtualización de sistemas para pór en práctica solucións de alta dispoñibilidade.
- Implantar un servidor redundante que garanta a continuidade de servizos en casos de caída do servidor principal.
- Implantar un balanceador de carga á entrada da rede interna.
- Implantar sistemas de almacenamento redundante sobre servidores e dispositivos específicos.
- Avaliar a utilidade dos sistemas de clúster para aumentar a fiabilidade e a produtividade do sistema.
- Analizar solucións de futuro para un sistema con demanda crecente.
- Esquematizar e documentar solucións para supostos con necesidades de alta dispoñibilidade.

6. Procedemento para a recuperación das partes non superadas

6.a) Procedemento para definir as actividades de recuperación

- No caso de non superar algunha das probas nunha avaliación, o alumno/a terá antes da sesión de avaliación unha proba personalizada, onde terá a oportunidade de recuperar aquelas partes pendentes.
- No caso de traballos non superados, o profesor asignará ó alumno unha serie de tarefas para entregar nunha data anterior á sesión de avaliación.
- A nota que aparecerá na avaliación será a menor das puntuacións obtidas nas probas. Nesta situación non se calculan medias coas notas recibidas en partes superadas.

- Para ó alumnado que ó chegar ó mes de marzo/abril teña partes pendentes (non superadas):
  * haberá unha proba final personalizada por alumno, onde poderá recuperar aquelas partes da asignatura que teña suspensas.
  * no caso de traballos non superados, o profesor asignará ó alumno unha serie de tarefas para entregar.
- De superar esta proba/traballos, considerarase que o alumno superou a asignatura.
- No caso de non superar esta proba/traballos, considerase que o alumno non superou a asignatura.

- Para aqueles alumnos que superaron o módulo, a nota final será o promedio das notas das avaliacións xunto coa nota da proba final.
- Para o alumnado que non superou o módulo, a nota final reflictirá a nota da proba final. Nesta situación non se calculan medias coas notas recibidas en partes superadas.

- Para ó alumnado que ó chegar ó mes de abril teña partes suspensas e non as supere:
 * Haberá actividades de recuperación presenciais onde faranse traballos e actividades de repaso de todas as unidades didácticas.
 * Haberá unha proba escrita e/ou práctica final personalizada por alumno de recuperación. Esta proba final poderá dividirse en varias probas ó longo do trimestre de considerarse oportuno para favorecer o estudo do alumnado
 * O profesor asignará ó alumno unha serie de tarefas para entregar. Algunhas destas tarefas contarán para a nota final e outras non; de ser o caso, informarase ó alumnado do peso da tarefa na nota
 * De superar todas as probas e traballos a avaliación considerarase que o alumno superou a asignatura, obtendo unha nota como resultado da aplicación do seguinte criterio:
  - as probas suporán un 90% da nota da avaliación.
  - os traballos prácticos un 10% da nota da avaliación.
 * Estas porcentaxe poderá cambiar en base ó número e tipoloxía das probas/traballos. Informarase ó alumnado das porcentaxes.
 * No caso de non ter superado todas e cada unha desta/s proba/s e traballos, considerase que o alumno non superou a asignatura.
 * A nota que aparecerá na avaliación será a media anteriormente sinalada; e no caso de dividirse a proba final en varias ó longo do trimestre, a menor das puntuacións obtidas nas probas.

Alumnado NEE:
- No caso do alumnado con NEE, valorarase a súa situación e procederase á adaptación das probas/traballos.

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

- Esta proba consistirá de:
 * Unha proba con:
  - parte escrita na que se incluirán contidos conceptuais das unidades didácticas.
  - parte práctica de duración adecuada para que o alumno poida demostrar o dominio dos conceptos e procedementos indicados anteriormente.
 * Presentación e defensa ante o profesor, dun ou varios traballos indicados polo profesor.
- O contido destas probas poderá ser diferente ás probas plantexadas ó resto do alumnado que non perdeu a avaliación continua.

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

Considerando que a programación é un documento que se elabora ó comezo do curso escolar estará sempre aberta a calquera modificación baseándonos en diferentes factores que se inclúen no proceso de ensinanza-aprendizaxe. Avaliaranse os procesos de avaliación, técnicas e métodos, temporalización e momentos de aplicación, os recursos dos que dispoñemos e a metodoloxía.
Unidades didácticas:
Máis polo miudo, ó remate de cada unidade didáctica analizaremos:

Contidos:
- Na programación do vindeiro curso incluiranse novas actividades para aqueles contidos que supuxeron maior dificultade de aprendizaxe para o alumnado.
- Engadiranse tamén os contidos de ampliación tratados, se houbo algún. Terase en conta tamén o cambio daqueles contidos que se deciden

impartir noutra unidade de traballo.
Actividades:
- Eliminaranse da nova programación as actividades que non se realizaron por considerarse redundantes ou innecesarias, e incorporaranse todas as novas que o docente considerou necesarias para acadar os obxectivos da unidade, así como a modificación das xa existentes.
Recursos:
- Na programación vindeira incluiranse os recursos empregados que non se tiveran en conta ao facer a programación actual. Aqueles non usados indicarase que son opcionais.
- Se algún recurso necesario non se puido empregar por non existir no centro, solicitarase a súa compra nunha reunión de departamento. Na programación do curso seguinte comprobarase a dispoñibilidade dese recurso para incluílo ou non na mesma.
Metodoloxía:
- A metodoloxía empregada para o desenvolvemento de cada unidade de traballo baséase principalmente na exposición por parte do docente da parte teórica e de exemplos de actividades, e a realización do alumnado de tarefas e traballos sobre os contidos expostos.
- Se houbo algún cambio na metodoloxía que fixo que o alumnado acadase os obxectivos da UT de xeito máis doado, incorporarase á nova programación.
Temporalización:
- O número de sesións asignadas axustaranse ao tempo real empregado na unidade de traballo.
Avaliacións
- Ó remate de cada trimestre, revisarase o proceso de avaliación, axustando o tipo e número de instrumentos de avaliación e en consecuencia as porcentaxes e o xeito de calcular as cualificacións parciais e final.

8. Medidas de atención á diversidade

8.a) Procedemento para a realización da avaliación inicial

- Ao comezo do curso, cubrirase un formulario onde se reflictan os seguintes aspectos recollidos desde o comezo do curso académico e ata a data de avaliación:
  * Coñecementos teóricos.
  * Destrezas e habilidades prácticas.
  * Resultados nos controis.
  * Traballos entregados.
  * Relación co resto do grupo.
  * Relación co profesor do módulo.
  * Comportamento xeral na clase.
  * Puntualidade e asistencia.
- Esta proba non será cualificable e só se terán en conta os resultados para adecuar o nivel de partida do proceso de ensino-aprendizaxe á realidade do grupo e/ou adoptar as medidas de reforzo que se consideren oportunas.

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

Medidas de reforzo:
- As medidas de reforzo teñen como obxectivo intentar axudar a superar algunha unidade de traballo a aqueles alumnos que non acadaron os obxectivos mínimos esixibles.
- Cada caso será analizado de forma particular, e as actividades teórico/prácticas serán indicadas o alumno para o seu desenrolo.

Medidas de ampliación:

- As medidas de ampliación teñen como obxectivo atender ás demandas de aqueles alumnos que superan amplamente ós obxectivos do módulo.
- As medidas de ampliación poden ser:
  * Investigación por parte do alumno de temas non tratados na aula.
  * Profundización en temas tratados.
  * Realización de traballos/tarefas adicionais.
- Todas estas tarefas estarán supervisadas e orientadas polo profesor, personalizando as tarefas según a situación especial de cada alumno..

9. Aspectos transversais

9.a) Programación da educación en valores

Os temas transversais que se atopan en todas as unidades de traballo son:

* Coñecemento e respecto pola normativa TIC legal vixente; en especial a Lei de Protección de Datos de Carácter Persoal (LOPD).
* Manexo da lingua inglesa para poder empregar manuais escritos nesta lingua, xa que ademais do castelán, é a lingua máis empregada en manuais técnicos informáticos.
* Aprendizaxe permanente ao longo da vida.
* Entendemento da importancia que ten o movemento de Software Libre no desenvolvemento da carreira profesional de cada alumno/a, no contorno produtivo de Galicia e as súas implicacións sociais.

Educación en valores

* A educación en valores na Formación Profesional está dirixida ao desenvolvemento da cultura profesional. A sociedade require algo máis que persoas adestradas para a función específica do mundo do traballo. Necesita profesionais con motivacións e capacidades para a actividade creadora e independente, tanto no desempeño laboral como investigador, ante os desafíos do coñecemento e información científico-técnica e da realización do seu ideal social e humano.
* A formación integral e especializada son dous piares da profesionalidade.
* A personalidade profesional maniféstase a través do conxunto de rasgos presentes no individuo, na actividade profesional, nos marcos de determinada comunidade e contexto.
* Por todo isto o profesorado fomentará:
  - O amor á actividade profesional.
  - O sentido de respecto socioprofesional.
  - O estilo de busca profesional creativo-innovador.
  - A comunicación interpersoal. Compañerismo.
  - Elevar a calidade profesional na solución de problemas.
  - Responsabilidade.
  - Honestidade.

9.b) Actividades complementarias e extraescolares

- Conferencias con expertos do sector.
- Participación en concursos de retos de ciberseguridade.