1 Programación do módulo de Seguridade Informática

1.1 Sumario

1.2 Identificación da programación

1.2.1 Identificación do centro

- **Código do centro**: 36019402
- **Nome do centro**: IES Pazo da Mercé
- **Concello do centro**: As Neves
- **Curso académico**: 2011-2012

1.2.2 Identificación do ciclo

- **Código da familia profesional**: IFC
- **Nome da familia profesional**: Informática e comunicacións
- **Código do ciclo**: CMIFC01
- **Nome do ciclo**: Sistemas microinformáticos e redes
- **Grao**: Medio
- **Réxime**: Xeral-ordinario

1.2.3 Identificación do módulo profesional e unidades formativas

- **Código do módulo**: MP0226
- **Nome do módulo**: Seguridade informática
- **Curso**: 2º
- **Sesións semanais**: 8
- **Horas anuais**: 140
- **Sesións anuais**: 168

1.2.4 Profesorado responsable da programación

- **Elabora a programación**: Antonio de Andrés Lema
- **Imparte o módulo**: Antonio de Andrés Lema

1.3 Obxectivos xerais do módulo

Os obxectivos específicos a acadar coa impartición do módulo son os seguintes:

- Coñecer os riscos dun sistema informático e as técnicas de seguridade que se poden aplicar.
- Coñecer a lexislación relativa á seguridade dos sistemas informáticos.
- Manexar os criterios e dispositivos de seguridade básicos nun CPD.
- Manexar sistemas de alimentación ininterrompida.
- Manexar sistemas de almacenamento redundante e distribuído.
- Coñecer os elementos que dotan ao sistema de tolerancia aos fallos.

- Realizar copias de seguridade e imaxes do sistema.
- Coñecer e manexar os elementos dunha PKI.
- Coñecer e manexar os elementos de seguridade no sistema operativo.
- Coñecer e manexar os elementos de seguridade na navegación por Internet e no uso do correo electrónico.
- Instalar e configurar mecanismos de seguridade tanto en redes cableadas como en redes sen fíos.
- Instalar e configurar un firewall.

1.4 Concreción do currículo ás características do ámbito produtivo

O módulo ?Seguridade Informática? pertence ao ciclo de Formación Profesional de grao medio ?Sistemas Microinformáticos e Redes?, que ten unha duración de 2.000 horas ao longo de 2 cursos académicos, ao que lle corresponde o título de ?Técnico en sistemas microinformáticos e redes?. Este módulo impártese durante o segundo curso.

O desenvolvemento curricular de este módulo ten como referencia de partida o Real Decreto 1691/2007, do 14 de decembro (BOE nº 3446 do 17 de xaneiro de 2008), onde se establece o currículo do ciclo ?Sistemas Microinformáticos e Redes?.

1.5 Desenvolvemento curricular das unidades didácticas

1.5.1 Unidade didáctica 1: Introdución á seguridade informática

1.5.1.1 Obxectivos didácticos

- Coñecer os riscos dun sistema informático e as técnicas de seguridade que se poden aplicar (Actividades 1, 2, 3 e 5).
- Distinguir os distintos tipos de seguridade non sistemas informáticos (Actividade 5).
- Coñecer a lexislación relativa á seguridade dos sistemas informáticos (Actividade 6).

1.5.1.2 Contidos

- Obxectivos da seguridade informática.
- Seguridade física e lóxica.
- Seguridade activa e pasiva.
- Ameazas e fraudes nos sistemas de información.
- Lexislación relacionada coa seguridade da información.

1.5.1.3 Actividades

- **Actividade 1**: Utilizar a ferramenta sfc para verificar a integridade do ficheiros protexidos en Windows.
- **Actividade 2**: Utilizar as ferramentas nmap e Zenmap para detectar vulnerabilidades dos sistemas informáticos.
- **Actividade 3**: Consultar boletíns de vulnerabilidades de sistemas operativos.
- **Actividade 4**: Analizar a principal lexislación sobre a seguridade da información (LOPD e LSSI) e resolver cuestións prácticas sobre as mesmas.
- **Actividade 5**: Resolver cuestións sobre os contidos da unidade.

1.5.1.4 Resultados de aprendizaxe e criterios de avaliación

Nesta unidade didáctica abórdanse os seguintes resultados de aprendizaxe e criterios de avaliación definidos no currículo do ciclo:

- **RA1**: CA1.1, CA1.2, CA1.3, CA1.7, CA1.8
- **RA6**: CA6.1, CA6.2, CA6.3, CA6.4, CA6.5, CA6.6, CA6.7

1.5.2 Unidade didáctica 2: Seguridade pasiva: Hardware e almacenamento

1.5.2.1 Obxectivos didácticos

- Manexar os criterios e dispositivos de seguridade básicos nun CPD (Actividades 1, 2 e 9).
- Manexar sistemas de alimentación ininterrompida (Actividade 3).
- Manexar sistemas de almacenamento redundante e distribuído (Actividades 4, 5, 6 e 9).
- Coñecer os elementos que dotan ao sistema de tolerancia aos fallos (Actividade 7).
- Instalar e configurar servizos en clúster (Actividade 8).

1.5.2.2 Contidos

- Ubicación e protección física:
    - ♦ Factores para elixir a ubicación do CPD.
    - ♦ Sistemas de control de acceso.
    - ♦ Sistemas de videovixilancia: Sistemas PoE.
    - ♦ Sistemas de climatización e protección no CPD.
- Sistemas de alimentación ininterrompida.
- Almacenamento redundante e distribuído:
    - ♦ Sistemas RAID.
    - ♦ Almacenamento externo:
        - ◊ *Network Attached Storage*.
        - ◊ *Storage Area Network*.
- Sistemas tolerantes a fallos.
- Clusters de servidores.

1.5.2.3 Actividades

- **Actividade 1**: Configurar unha cámara de videovixilancia IP e a súa conexión a un sitch PoE.
- **Actividade 2**: Analizar vantaxes e inconvenientes sobre diferentes ubicacións e configuracións para un CPD.
- **Actividade 3**: Instalar e configurar SAIs: Cambiar as baterías, monitorizar o seu estado e configurar accións en caso de esgotamento das baterías.
- **Actividade 4**: Configurar almacenamentos RAID hardware e software con Windows e Linux.
- **Actividade 5**: Resolver exercicios prácticos sobre o funcionamento dos sistemas RAID.
- **Actividade 6**: Instalar e configurar sistemas de almacenamento externos e de rede.
- **Actividade 7**: Montar un equipo con fonte de alimentación e tarxeta de rede redundantes.
- **Actividade 8**: Configurar equipos en clúster.
- **Actividade 9**: Resolver cuestións sobre os contidos da unidade.

1.5.2.4 Resultados de aprendizaxe e criterios de avaliación

Nesta unidade didáctica abórdanse os seguintes resultados de aprendizaxe e criterios de avaliación definidos no currículo do ciclo:

- **RA2**: CA2.1, CA2.2, CA2.3, CA2.4, CA2.5
- **RA3**: CA3.1, CA3.2, CA3.3, CA3.4, CA3.8, CA3.9

1.5.3 Unidade didáctica 3: Seguridade pasiva: Recuperación de datos

1.5.3.1 Obxectivos didácticos

- Realizar e restaurar copias de seguridade do sistema (Actividades 1 e 6).
- Recuperar datos dun disco perdidos (Actividade 2).
- Realizar e restaurar imaxes do sistema, xeneralizándoas para distinto tipo de hardware (Actividades 3, 4 e 5).

1.5.3.2 Contidos

- Tipos de copias de seguridade.
- Realizar copias de seguridade en Windows e Linux.
- Modos de recuperación fronte a perdas no sistema operativo.
- Ferramentas para a recuperación de datos perdidos.
- Creación e restauración de imaxes do sistema:
    - ♦ Servizo de preparación do sistema para a creación de imaxes en Windows: O sysprep.
- Políticas de copias de seguridade.

1.5.3.3 Actividades

- **Actividade 1**: Facer copias de seguridade en Windows e Linux.
- **Actividade 2**: Instalar e utilizar algunha ferramenta de recuperación de datos perdidos (Recuva).
- **Actividade 3**: Crear imaxes do sistema e restauralas utilizando Clonezilla.
- **Actividade 4**: Manexas ferramentas de recuperación do sistema operativo.
- **Actividade 5**: Usar o *sysprep* en Windows.

- **Actividade 6**: Resolver cuestións sobre os contidos da unidade.

1.5.3.4 Resultados de aprendizaxe e criterios de avaliación

Nesta unidade didáctica abórdanse os seguintes resultados de aprendizaxe e criterios de avaliación definidos no currículo do ciclo:

- **RA3**: CA3.2, CA3.5, CA3.6, CA3.7, CA3.10
- **RA4**: CA4.7

1.5.4 Unidade didáctica 4: Criptografía e métodos de cifrado

1.5.4.1 Obxectivos didácticos

- Distinguir os elementos e técnicas dos sistemas de cifrado (Actividades 1, 3 e 4).
- Coñecer e manexar os elementos dunha PKI (Actividades 2 e 3).
- Utilizar Openssl para a xestión de certificados dixitais (Actividade 2).

1.5.4.2 Contidos

- Técnicas de criptografía: Cifrado simétrico e asimétrico.
- Funcións hash e sinatura dixital.
- Certificados dixitais.
- Infraestrutura de chave pública (PKI).

1.5.4.3 Actividades

- **Actividade 1**: Cifrado e sinatura de documentos con GPG.
- **Actividade 2**: Xenerar certificados dixitais con openssl e con Windows Server.
- **Actividade 3**: Utilizar certificados dixitais para o cifrado e sinatura de correo electrónico e documentos.
- **Actividade 4**: Resolver cuestións sobre os contidos da unidade.

1.5.4.4 Resultados de aprendizaxe e criterios de avaliación

Nesta unidade didáctica abórdanse os seguintes resultados de aprendizaxe e criterios de avaliación definidos no currículo do ciclo:

- **RA1**: CA1.4, CA1.5, CA1.6
- **RA5**: CA5.7

1.5.5 Unidade didáctica 5: Seguridade activa no sistema

1.5.5.1 Obxectivos didácticos

- Coñecer e manexar os elementos de seguridade no sistema operativo (Actividades 1, 2, 4, 5, 6 e 9).
- Instalar e configurar dispositivos de autenticación de usuarios (Actividade 3).
- Identificar as accións e/ou tipos de software que pode ameazar o sistema e as técnicas de protección que se poden utilizar (Actividade 1, 2, 4, 5, 6, 7, 8 e 9).

1.5.5.2 Contidos

- Seguridade no acceso á elementos críticos do sistema: BIOS, xestor de arranque e particións do disco.
- Autenticación dos usuarios:
    - ♦ Políticas de contrasinais.
    - ♦ Sistemas biométricos.
    - ♦ Sistemas de bloqueo de equipos.
    - ♦ Sistemas de tarxeta con certificado dixital.
- Vulnerabilidades do sistema, bugs e instalación de actualizacións.
- Monitorización do sistema operativo.
- Conxelación dos datos do disco.
- Software que vulnera a seguridade do sistema e medidas de actuación:
    - ♦ Tipos de software malicioso: Virus, troiano, bomba lóxica, *cracker*, *dialer*, *keylogger*, *spyware*, etc.

- ♦ Antivirus: Tipos e técnicas de análise.

1.5.5.3 Actividades

- **Actividade 1**: Configurar restricións de acceso por medio de contrasinal á BIOS e ao xestor de arranque.
- **Actividade 2**: Cifrar particións dun disco, con Windows e Linux.
- **Actividade 3**: Instalar e manexar diversos de autenticación do sistema (por contrasinal, certificado dixital ou elementos biométricos).
- **Actividade 4**: Configurar e aplicar as actualizacións tanto en Windows como en Linux.
- **Actividade 5**: Utilizar diferentes ferramentas de monitorización dos accesos no sistema operativo.
- **Actividade 6**: Manexar algunha ferramenta de conxelación do sistema.
- **Actividade 7**: Facer unha wiki cos distintos tipos de software malicioso e as técnicas de defensa existentes.
- **Actividade 8**: Instalar algún antivirus gratuíto e analizar as súas funcionalidades principais.
- **Actividade 9**: Resolver cuestións sobre os contidos da unidade.

1.5.5.4 Resultados de aprendizaxe e criterios de avaliación

Nesta unidade didáctica abórdanse os seguintes resultados de aprendizaxe e criterios de avaliación definidos no currículo do ciclo:

- **RA1**: CA1.5
- **RA4**: CA4.1, CA4.2, CA4.3, CA4.4, CA4.5, CA4.6
- **RA5**: CA5.7

1.5.6 Unidade didáctica 6: Seguridade activa en redes

1.5.6.1 Obxectivos didácticos

- Coñecer e manexar os elementos de seguridade na navegación por Internet e no uso do correo electrónico (Actividades 2 e 3).
- Instalar e configurar mecanismos de seguridade tanto en redes cableadas como en redes sen fíos (Actividades 1, 4, 5 e 6).

1.5.6.2 Contidos

- Protocolos seguros: HTTPS, SSH e NX.
- Seguridade nos navegadores web: Configuración de niveis de seguridade en distintos navegadores, almacenamento de contrasinais e datos de formularios, xestión da caché do navegador, manexo do historial, almacenamento de certificados dixitais, bloqueador de ventás emerxentes, xestión de *cookies*, administración de complementos e plugins.
- Seguridade no acceso ao correo electrónico: Criterios de seguridade na configuración do cliente de correo e protección ante *spam*, *phishing*, *hoax*, etc.
- Control dos servizos de rede.
- As redes privadas virtuais (VPN).
- Ferramentas de auditoría de redes.
- Seguridade en redes WIFI: Protocolos WEP e WPA.

1.5.6.3 Actividades

- **Actividade 1**: Conectarse a un equipo remoto utilizando ssh e o protocolo NX.
- **Actividade 2**: Analizar a configuración de seguridade dos principais navegadores web; Internet Explorer e Mozilla Firefox.
- **Actividade 3**: Instalar e configurar clientes de correo electrónico; Windows Mail, Thunderbird.
- **Actividade 4**: Configurar unha VPN entre equipos da aula.
- **Actividade 5**: Instalar redes WIFI e configurar os protocolos de seguridade.
- **Actividade 6**: Resolver cuestións sobre os contidos da unidade.

1.5.6.4 Resultados de aprendizaxe e criterios de avaliación

Nesta unidade didáctica abórdanse os seguintes resultados de aprendizaxe e criterios de avaliación definidos no currículo do ciclo:

- **RA1**: CA1.5
- **RA2**: CA2.6, CA2.7
- **RA5**: CA5.1, CA5.2, CA5.3, CA5.4, CA5.5, CA5.6, CA5.7

1.5.7 Unidade didáctica 7: Seguridade de alto nivel en redes: O firewall

1.5.7.1 Obxectivos didácticos

- Instalar e configurar un firewall (Actividades 1, 2 e 3).

1.5.7.2 Contidos

- Características e funcións do firewall.
- Tipos de firewalls.
- Filtrado de paquetes.
- Instalación e configuración de firewalls.
- Arquitecturas de rede con firewalls.
- Monitorización do firewall.

1.5.7.3 Actividades

- **Actividade 1**: Instalar e configurar o firewall con Windows e con Linux.
- **Actividade 2**: Configurar un router firewall baixo os requisitos indicados polo profesor.
- **Actividade 3**: Resolver cuestións sobre os contidos da unidade.

1.5.7.4 Resultados de aprendizaxe e criterios de avaliación

Nesta unidade didáctica abórdanse os seguintes resultados de aprendizaxe e criterios de avaliación definidos no currículo do ciclo:

- **RA5**: CA5.8

1.5.8 Unidade didáctica 8: Comprensión de textos e vocabulario técnico en Inglés

O carácter fortemente cambiante e dinámico do contorno profesional da informática e as novas tecnoloxías fai imprescindible que o alumno adquira a capacidade de comprender de forma autónoma textos e documentos de diversas fontes e en diferentes formatos que lle permitan adaptarse a novos sistemas, ferramentas, etc. É por iso que nesta unidade tratarase de aumentar a capacidade do alumnado de extraer a información útil dos textos, fundamentalmente de carácter técnico, que lle permita levar a cabo unha formación continua na carreira profesional unha vez rematado o ciclo formativo.

A xustificación desta unidade basease ademais no plan lector do centro e na asignación dentro do mesmo de unha sesión de lectura semanal para todo ao alumnado, que será englobada dentro da unidade.

Por outra banda, o manexo do vocabulario técnico en inglés relativo ao módulo permite ao alumnado manexar documentos, manuais, aplicativos, etc. que en moitas ocasións atópanse unicamente neste idioma, e aumenta polo tanto a autonomía do alumno no seu traballo.

1.5.8.1 Obxectivos didácticos

- Extraer información da lectura de documentos técnicos, manuais, etc (Actividade 1).
- Manexar o vocabulario técnico en inglés relativo as tecnoloxías, ferramentas, procesos, etc. abordadas no módulo (Actividades 2 e 3).

1.5.8.2 Actividades

- **Actividade 1: Resolver cuestións sobre diversas lecturas propostas polo profesor**
  - **Duración**: 2 sesións.
  - **Tarefas do profesorado**: Ofrecer ao alumnado unha serie de lecturas para que seleccionar para logo presentar unha serie de cuestións sobre o lido.
  - **Tarefas do alumnado**: Ler o texto seleccionado e resolver as cuestións que se lle presentan.
  - **Recursos necesarios**: Aula virtual.
  - **Instrumentos de avaliación**: Cuestionario na aula virtual do centro, que corrixe de forma automática os resultados de cada alumno.

- **Actividade 2: Elaborar glosarios de termos técnicos en inglés e resolver cuestións sobre os termos incluídos**
  - **Duración**: 2 sesións.
  - **Tarefas do profesorado**: Propoñer ao alumnado diversos termos en inglés para que elabore un glosario de termos relacionados

co módulo.
    - **Tarefas do alumnado**: Buscar o significado dos termos e elaborar con eles o glosario.
    - **Recursos necesarios**: Aula virtual.
    - **Instrumentos de avaliación**: Glosario na aula virtual do centro.

- **Actividade 3: Manexar ferramentas en inglés e analizar os termos máis relevantes**
    - **Duración**: 1 sesión.
    - **Tarefas do profesorado**: O profesor proporá utilizar durante períodos do curso as ferramentas de traballo en inglés (sistema operativo, aplicacións, etc.) e resolverá co grupo o significado das palabras máis relevantes.
    - **Tarefas do alumnado**: Manexar as ferramentas en inglés e buscar o significado das palabras máis relevantes.
    - **Recursos necesarios**: Equipos informáticos.
    - **Instrumentos de avaliación**: Folla de cálculo no que o profesor anotará a cualificación do traballo de cada alumno.

1.5.8.3 Resultados de aprendizaxe e criterios de avaliación

Nesta unidade didáctica abórdanse os seguintes criterios de avaliación:

- Obtívose información de documentos técnicos e manuais.
- Utilizouse o vocabulario técnico en inglés para comprender documentos te?nicos e manuais.

1.6 Contidos mínimos

Os contidos mínimos imprescindibles para a superación do módulo son os seguintes:

- Riscos dun sistema informático e as técnicas de seguridade que se poden aplicar.
- Tipos de técnicas de seguridade.
- Lexislación relativa á seguridade dos sistemas informáticos.
- Criterios e dispositivos de seguridade básicos nun CPD.
- Sistemas de alimentación ininterrompida.
- Sistemas de almacenamento redundante e distribuído.
- Sistemas tolerantes a fallos.
- Realizar copias de seguridade en Windows e Linux.
- Creación e restauración de imaxes do sistema.
- Técnicas de criptografía: Cifrado simétrico e asimétrico.
- Elementos dunha PKI.
- Seguridade no acceso á elementos críticos do sistema: BIOS, xestor de arranque e particións do disco.
- Autenticación dos usuarios: políticas e sistemas de autenticación.
- Software que vulnera a seguridade do sistema e medidas de actuación.
- Seguridade nos navegadores web e no acceso ao correo electrónico.
- As redes privadas virtuais (VPN).
- Seguridade en redes WIFI: Protocolos WEP e WPA.
- Instalación e configuración de firewalls.

1.7 Metodoloxía

Con respecto á metodoloxía didáctica a seguir na impartición do módulo, cabe destacar os seguintes aspectos:

- No comezo de cada unidade de traballo, exporanse na clase os conceptos e obxectivos fundamentais da mesma.

- Nas distintas sesións da ensino-aprendizaxe, o profesor introducirá os novos conceptos buscando sempre a implicación do alumnado no establecemento de debates para aclarar no máximo posible estes conceptos. Para favorecelo, o profesor presentará durante a explicación cuestións que propicien o razoamento dos alumnos e alumnas. Tentarase desta forma aclarar todas as dúbidas que poidan aparecer sobre os temas abordados. As explicacións apoiaranse no uso do libro de texto e de material que o profesorado ofrecerá ao alumnado a través da ferramenta de *e-learning* implantada na aula virtual do centro.

- No desenvolvemento da unidade, os alumnos e alumnas realizarán diferentes actividades prácticas sobre os conceptos e procesos expostos, que variarán segundo a unidade. Moitas destas actividades serán realizadas na aula virtual do centro, incluíndo diversos cuestionarios sobre os contidos fundamentais das distintas unidades didácticas.

- En ocasións, os alumnos realizarán traballos en grupos, propostos polo profesor.

1.8 Temporalización

Na seguinte táboa recóllense as sesións (de 50 minutos) adicadas a cada unha das unidades didácticas nas que se distribúen os contidos do módulo:

Unidade didáctica	Sesións
U.D. 1: Introdución á seguridade informática	10
U.D. 2: Seguridade pasiva: Hardware e almacenamento	30
U.D. 3: Seguridade pasiva: Recuperación de datos	30
U.D. 4: Criptografía e métodos de cifrado	20
U.D. 5: Seguridade activa no sistema	25
U.D. 6: Seguridade activa en redes	30
U.D. 7: Seguridade de alto nivel en redes: O firewall	16
U.D. 9: Comprensión de textos e vocabulario técnico en Inglés	7

1.9 Avaliación

1.9.1 Instrumentos de avaliación

- No comezo do módulo, o profesor realizará unha **avaliación inicial** que permitirá coñecer o nivel de coñecementos previos do alumnado e poder adaptar o ritmo desenvolvemento das clases e realización das actividades.
- No desenvolvemento e/ou remate da unidade didáctica, o alumnado resolverá unha serie de cuestións sobre os contidos e actividades realizadas, que serán despois resoltos na clase co obxectivo de clarificar todos os erros que se cometidos. Este instrumento permitirá aplicar en cada unidade didáctica os criterios de avaliación establecidos para a mesma.
- En ocasións, o alumnado realizará actividades de investigación para elaborar presentacións ou artigos sobre algúns dos contidos da unidade, con obxecto de fomentar así a súa autonomía e capacidade de análise e síntese de información. Aplicaranse nestas actividades os criterios de avaliación expostos no apartado anterior.
- Nas distintas actividades prácticas de instalación e configuración realizadas polo alumnado aplicaranse tamén os criterios de avaliación recollidos en cada unha das unidades didácticas.
- Na unidade 8, o alumnado realizará diversas actividades que consistirán na lectura de textos propostos polo profesor e a resolución de cuestións sobre os mesmos, así como a resolución de cuestións e casos prácticos sobre o manexo de vocabulario técnico en inglés.
- Ao remate de cada trimestre o alumnado realizará unha proba que incluirá diversas cuestións e actividades prácticas na que se aplicarán todos os criterios de avaliación definidos para as unidades abordadas no mesmo.

1.9.2 Sistemas de cualificación

A nota final formarase da seguinte forma:

Parte	Porcentaxe
Participación en clase e prácticas	30%
Probas das unidades didácticas e probas finais dos trimestres	70%

Tendo en conta as seguintes consideracións:

- Será necesario obter unha cualificación mínima de 4,5 na proba final do trimestre para poder superar cada unha das avaliacións. De non alcanzar esta cualificación, o alumno deberá realizar unha proba de recuperación da mesma.

- Para poder obter a puntuación correspondente á participación en clase e prácticas, o alumno/a debe mostrar respecto e bo uso de todo o material posto á súa disposición para a realización das mesmas, xa que a incorporación ao mundo laboral require do alumno unha actitude positiva neste aspecto. Os deterioros intencionados ou substraccións do material suporán a perda da puntuación deste apartado.

A cualificación final da avaliación será un número enteiro de 1 a 10, resultado de redondear os resultado obtidos seguindo a táboa. Considéranse aprobados aqueles alumnos que obteñan unha cualificación igual ou superior a 5.

1.9.3 Plan extraordinario de avaliación

Para o alumnado que perda o dereito a avaliación continua ou non supere o proceso ordinario de avaliación, a avaliación final extraordinaria do módulo consistirá na realización de varias probas co obxectivo de comprobar que este acade os contidos mínimos recollidos nesta programación. As probas que deberá realizar serán as seguintes:

- Unha proba escrita na que o alumno ou alumna debe demostrar a adquisición dos contidos incluídos nas distintas unidades didácticas.
- Unha proba práctica na que realizará a instalación e configuración de distintos elementos de seguridade informática manexados: Cámaras de videovixilancia, SAIs, RAID, sistemas de almacenamento externos, dispositivos redundantes, dispositivos de autenticación e control de acceso e routers-firewall.
- Unha proba práctica no ordenador na que deberá resolver actividades das unidades 2 á 7.

1.10 Actividades de recuperación

As actividades de recuperación para o alumnado que non supere o módulo no segundo trimestre realizaranse ao longo do terceiro trimestre e incidirán na parte máis práctica do módulo, xa que consistirán na resolución por parte do alumnado das actividades xa realizadas durante o curso e/ou novas actividades similares propostas polo profesor.

1.11 Atención ao alumnado con necesidades educativas especiais

Durante o desenvolvemento do curso prestarase especial atención ao alumnado que presente necesidades educativas especiais ou algún grao de discapacidade, mediante unha secuenciación diferenciada das unidades didácticas, a realización dun maior número de actividades graduadas en dificultade e poñendo á súa disposición os recursos necesarios para a consecución dos obxectivos didácticos fixados nas distintas unidades.

1.12 Seguimento e avaliación da programación

No desenvolvemento do curso, farase uso de diversos mecanismos para facer un seguimento e avaliación do planificado na presente programación:

- De xeito continuo, o profesor avaliará na clase a medida en que o alumnado acada de forma xeral os obxectivos fixados nas distintas unidades didácticas. En consecuencia, poderase decidir incidir en determinados contidos e/ou actividades, aumentando se se considera necesario o número de sesións adicadas a unha determinada unidade.
- Ao remate de cada trimestre, o alumnado cubrirá unha enquisa na que valorará diversos aspectos do desenvolvemento do módulo, como a metodoloxía utilizada, as actividades realizadas, os recursos usados, os contidos expostos, etc. O resultado destas enquisas serán utilizados para aplicar as correccións que se consideren oportunas no propio desenvolvemento do curso, así como en vindeiros cursos académicos.
- O profesor recollerá a temporalización real das distintas unidades didácticas, co obxectivo de poder corrixir no propio curso os desfases detectados fronte a temporalización prevista e precisar mellor a temporalización das unidades en vindeiros cursos académicos.

1.13 Materiais e recursos didácticos

O desenvolvemento do módulo apoiarase no libro de texto editado pola editorial MCGraw-Hill para este módulo, ademais do material que o profesor proporcionará ao alumnado a través da aula virtual.

Cada alumno ou alumna contará con un ordenador para realizar as actividades das clases, e o profesor con un ordenador con canón proxector para expoñer os contidos das mesmas.

Para a realización das prácticas, farase uso do seguinte material:

- SAIs con capacidade de monitorización dende o ordenador.

- Cámaras de videovixilancia IP e switch PoE.
- Discos duros e controladora RAID.
- Discos duros de rede NAS.
- Fontes de alimentación e tarxetas de rede redundantes.
- Dispositivos de autenticación baseados en certificados dixitais e elementos biométricos.
- Puntos de acceso e equipos con tarxetas de rede sen fíos.
- Routers-firewall.