



Període de compleció 2025

MÒDUL PROFESSIONAL: M1

PROFESSOR/S RESPONSABLE/S: Francesc Bertó i Xavier Munté

- **Contingut a considerar per la prova:**
 - UF1: Instal·lació, configuració i explotació del sistema informàtic: Instal·lació i configuració de Windows 10 i Ubuntu 18.04 o superior.
 - UF2: Implantació de programari específic: organització i configuració de fitxers, discos, scripts i dominis
 - UF3: Gestió de la informació i de recursos en una xarxa: Documentació tècnica i gestió d'incidències amb FOG.
 - UF4: Seguretat, rendiment i recursos: Seguretat de dades, supervisió de sistemes operatius, directives de seguretat i auditories.

- **Format de la prova:** Qüestionari de respostes múltiples. En el cas de no haver presentat les pràctiques en el seu moment, caldrà fer també una prova pràctica de la Unitat Formativa no superada.

Continguts en l'espai Moodle del curs 2023-2024:

<https://www.vidalibarraquer.net/moodle2324/course/view.php?id=3324>



Període de compleció 2025

MÒDUL PROFESSIONAL: M03-ASIXC Programació bàsica

PROFESSOR/S RESPONSABLE/S: Joan Cervós

- **Contingut a considerar per la prova:**
 - UF1: Programació estructurada
 - Introducció a la programació en Python: imprimir per pantalla, literals, operadors, variables
 - Entrada per teclat, conversió de dades
 - Operacions amb cadenes
 - Estructures condicionals
 - Estructures iteratives (bucles)
 - Llistes: operacions, recorregut, índexs
 - UF2: Disseny modular
 - Funcions
 - Llistes de llistes
 - Tuples i diccionaris
 - Llistes amb diccionaris, diccionaris amb llistes
 - UF3: Fonaments de gestió de fitxers
 - Operacions: lectura i escriptura
 - Fitxers de text
 - Fitxers CSV
- **Format de la prova:** Cada UF consistirà en la realització d'un o més programes en Python, amb ordinador i entorn de programació, en què s'hauran d'aplicar els conceptes del temari.



Els conceptes inclosos en les diferents unitats formatives són necessaris en les unitats formatives posteriors.





Període de compleció 2025

MÒDUL PROFESSIONAL: M06-ASIXC Administració de sistemes operatius

PROFESSOR/S RESPONSABLE/S: José María Rojano

- **Contingut a considerar per la prova:**
 - UF1: Administració avançada de sistemes operatius
 - Administració de servei de directori
 - Instal·lació, configuració i ús de serveis d'accés i administració remota
 - Administració de servidors d'impressió:
 - Administració de processos del sistema
 - Integració de sistemes operatius en xarxa lliures i propietaris
 - UF2: Automatització de tasques i llenguatges de guions
 - Informació del sistema
 - Aplicació de llenguatge: «scripting» en sistemes operatius lliures i propietaris
- **Format de la prova:** Cada UF consistirà en la realització d'un qüestionari, amb ordinador, en que s'hauran de conèixer tant els conceptes teòrics com pràctics del temari.





Període de compleció 2025

MÒDUL PROFESSIONAL: M07 - ASIXC Planificació i administració de xarxes.

PROFESSOR/S RESPONSABLE/S: Xavi Abillà i Joan Cervós

- **Contingut a considerar per la prova:**

- UF1:

1. Caracterització de xarxes:

- 1.1 Terminologia: xarxes LAN, MAN i WAN, topologies, arquitectures, protocols.
- 1.2 Sistemes de numeració decimal, hexadecimal i binari. Conversió entre sistemes.
- 1.3 Arquitectura de xarxes.
- 1.4 1.4 Encapsulat de la informació.
- 1.5 El model OSI.
- 1.6 El model TCP/IP.
- 1.7 Les tecnologies Ethernet.
- 1.8 El model OSI i Ethernet.
- 1.9 Tipus de cablatge Ethernet.

- 2 Integració d'elements en una xarxa:

- 2.1 Els medis físics.
- 2.2 Ample de banda i tasa de transferència.
- 2.3 Els cables metàl·lics (coaxial, STP i UTP).
- 2.4 Factors físics que afecten la transmissió.
- 2.5 La connexió sense fils. Els espectres d'ona de microones i radio. Tipologies. Associació i autenticació a la WLAN.
- 2.6 Adreçament.
- 2.7 Dominis de col·lisió i de difusió.
- 2.8 Adreces IPv4 i màscares de xarxa.
- 2.9 Adreçament dinàmic (DHCP).
- 2.10 Adaptadors.
- 2.11 Adaptadors amb fil: instal·lació i configuració.
- 2.12 Adaptadors sense fil: instal·lació i configuració.

- UF2:

- 3.- Configuració i administració de commutadors:

- 3.1 Segmentació de la xarxa. Avantatges que presenta.
- 3.2 Commutadors i dominis de col·lisió i de difusió.
- 3.3 Segmentació de xarxes.
- 3.4 Formes de connexió al commutador per a la seva configuració.
- 3.5 Configuració del commutador.
- 3.6 Configuració estàtica i dinàmica de la taula d'adreces MAC.

4. Configuració i administració bàsica d'encaminadors:

- 4.1 Els encaminadors a la LAN i a les WAN.
- 4.2 Components de l'encaminador.
- 4.3 Formes de connexió a l'encaminador per a la seva configuració inicial.



- 4.4 Comandes per a la configuració de l'encaminador.
- 4.5 Comandes per a l'administració de l'encaminador.
- 4.6 Configuració de l'encaminament estàtic.
- 4.7 Definició i ubicació de les llistes de control d'accés (ACLs).

- **UF3:**

- 5. Configuració de xarxes virtuals.
 - 5.1 El disseny de xarxes locals en tres capes (nucli, distribució i accés).
 - 5.2 Implantació i configuració de xarxes virtuals.
 - 5.3 Definició d'enllaços troncal als commutadors i encaminadors.
El protocol IEEE802.1Q.
- 6. Configuració i administració de protocols dinàmics:
 - 6.1 Protocols encaminadors i protocols d'encaminament.
 - 6.2 Protocols d'encaminament interior i exterior.
 - 6.3 L'encaminament sense classe.
 - 6.4 La subdivisió de xarxes i l'ús de màscares de longitud variable (VLM).
 - 6.5 El protocol RIPv2; comparació amb RIPv1.
 - 6.6 Configuració i administració de RIPv1.
 - 6.7 Configuració i administració de RIPv2.
- 7. Configuració de l'accés a Internet des d'una LAN:
 - 7.1 Adreçament intern i adreçament extern..
 - 7.2 Origen NAT i destinació NAT.
 - 7.3 NAT estàtic, dinàmic, de sobrecàrrega (PAT) i invers.
 - 7.4 Configuració de NAT.
 - 7.5 Diagnòstic d'incidències de NAT.
 - 7.6 Configuració de PAT.

- **Format de la prova:**

- Qüestionari del Moodle que poden incloure preguntes de teòrico-pràctics i exercicis de Packet Tracer a resoldre.

Període de compleció 2025

MÒDUL PROFESSIONAL: M08-ASIXC Servers en xarxa i Internet

PROFESSOR/S RESPONSABLE/S: Albert Galera

- **Contingut a considerar per la prova:**

UF1: DNS & DHCP

- DHCP

- Windows (Servei bàsic inclòs a Windows Server) + comprovacions
- Linux (Servei bàsic isc-dhcp-server sense seguretat) + (recerca de forma teòrica de com es pot aplicar mesures de seguretat al servei)

- DNS

- Windows (Servei bàsic sense seguretat) + comprovacions
- Linux (Servei bàsic bind9) + servidor esclau / transferència de zones + opcional (DNSSEC)

UF2: FTP & WEB

- FTP

- Windows (Servei bàsic filezilla Server sense seguretat amb diferents formes de funcionament actiu/passiu) + comprovacions + opcions bàsiques de seguretat del propi servei + FTP passiu amb SSL
- Linux (Servei bàsic vsftpd sense seguretat amb usuaris) + engabament usuaris + control accés a usuaris i recursos

- WEB

- Windows (Servei bàsic IIS sense seguretat) + comprovacions + https + directoris virtuals, virtualhost i control d'accés bàsic
- Linux (Servei bàsic apache2 sense seguretat) + virtualhost multisites + restriccions d'accés per autenticació + https

UF3: Correu & Missatgeria

- Windows (Servei bàsic hmailServer sense seguretat) + comprovacions + SMTP relay + seguretat 1 (Autenticació obligatòria per enviar correus + Filtrat d'IPs i llistes negres (Anti-spam) + Protecció contra ús indegut) + seguretat 2 (TLS per a xifrar connexions de correu) + opcional (DKIM + xifrat extrem a extrem)
- Linux (Servei bàsic dovecot & postfix) + comprovacions + SMTP AUTH + Filtrat IP (ip ranges) i Llistes negres (anti spam) + SMTP RELAYER (opcional) + TLS per SMTP + TLS per IMAP i POP3 (opcional) + Signatura digital (DKIM) (opcional) + Xifrat d'extrem a extrem (opcional)
- Missatgeria configuració bàsica del servidor i el client amb linux i Windows (*ejabberd*)





UF4: Serveis de video i audio

- Configuracions bàsiques del servidor i el client amb linux (nginx + icecast) per lograr streaming d'àudio i video.
- **Format de la prova:** Cada UF consistirà en la realització d'un exàmen en el que es mesclaran conceptes teòrics i pràctics d'implementació de serveis. Els conceptes inclosos en les diferents unitats formatives són necessaris en les unitats formatives posteriors.



Període de compleció 2025

MÒDUL PROFESSIONAL: M11

PROFESSOR/S RESPONSABLE/S: Ferran Ballesté

- **Contingut a considerar per la prova:**
 - UF2: Seguretat activa i accés remot.
 - Pràctiques d'OpenStego, OpenVPN, OSSEC i preguntes generals relacionades amb la seguretat activa i accés remot.
 - UF3: Tallafocs i servidors intermediaris.
 - Pràctiques de Shorewall, iptables i preguntes generals sobre tallafocs i proxy servers.
 - UF4: Alta disponibilitat i virtualització.
 - Pràctiques d'OwnCloud, Docker, Linux Containers i preguntes generals de disponibilitat i fiabilitat d'un sistema.

Continguts en l'espai Moodle del curs 2023-2024.

- **Format de la prova:** La prova avaluarà els coneixements adquirits en les Unitats Formatives UF2, UF3 i UF4 a través de tres qüestionaris independents (un per UF). El format principal de cada qüestionari serà de respostes múltiples, tot i que podran incloure altres tipus de preguntes. No és necessari entregar les pràctiques, però poden sortir preguntes relacionades amb els continguts treballades en elles.

Es recomana repassar les proves i qüestionaris realitzades anteriorment.





Període de compleció 2025

MÒDUL PROFESSIONAL: M14-ASIXC Projecte d'Administració de Sistemes Informàtics en Xarxa

PROFESSOR/S RESPONSABLE/S: Cristina Pallàs, Joan Cervós

- **Contingut a considerar per la prova:**
 - Disseny d'una xarxa segura
 - Disseny físic
 - Disseny lògic
 - Serveis
 - Seguretat
 - Simulació utilitzant GNS3
 - Seguretat en dispositius IoT:
 - Integrar en la xarxa una aplicació utilitzant dispositius IoT
 - Obtenció de dades dels sensors
 - Control d'actuadors
 - Ús d'un simulador IoT
 - Les especificacions detallades del projecte estaran disponibles al Moodle.
- **Format de la prova:** L'alumne haurà de lliurar la documentació i producte corresponent al projecte proposat i fer-ne una defensa oral de 15 minuts.





Període de compleció 2025

MÒDUL PROFESSIONAL: M16 Ciberseguretat i hacking ètic

PROFESSOR/S RESPONSABLE/S: Cristina Pallás Bruned

- **Contingut a considerar per la prova:**
 - **UF2: Hacking ètic**
 - 1. Anàlisi de la seguretat:
 - 1.1. Introducció al Hacking ètic.
 - 1.2. Normativa vigent:
 - 1.2.1. Codi penal.
 - 1.2.2. Llei orgànica de protecció de dades (LOPD).
 - 1.2.3. Llei de serveis de la societat de la informació i el comerç electrònic.
 - 1.3. Riscos i límits de la utilització de dades.
 - 1.4. Comprovació de protocols de seguretat. Auditories.
 - 1.5. Recollida d'informació tècnica (sistemes, serveis, infraestructures i altres).
 - 1.6. Anàlisi de vulnerabilitats (sistemes, serveis, infraestructures i altres).
 - 1.7. Explotació de vulnerabilitats (sistemes, serveis, infraestructures i altres).
 - 1.8. Realització d'informes i propostes de millora.
- **Format de la prova:** Es realitzarà una prova amb contingut teòric i pràctic.
 - Consistirà en un qüestionari i una prova pràctica dels continguts de la UF2.



Període de compleció 2025

MÒDUL PROFESSIONAL: M17 Seguretat en sistemes, xarxes i serveis

PROFESSOR/S RESPONSABLE/S: Xavi Abillà i Jordi Sánchez

- **Contingut a considerar per la prova:**
 - UF1: Implementació de funcionament segur per dispositius mòbils i IoT:
 - Arquitectura dels dispositius mòbils.
 - Sistemes operatius mòbils: instal·lació i configuració.
 - Assegurament dels serveis als dispositius mòbils.
 - Arquitectura dels dispositius IoT.
 - Sistemes operatius per IoT: instal·lació i configuració.
 - Assegurament dels serveis a IoT.
 - Posada en servei i recuperació del funcionament dels dispositius.
 - UF2: Assegurament als serveis de xarxa:
 - Assegurament i actualització de serveis.
 - Vulnerabilitats i assegurament del servei DNS.
 - Vulnerabilitats i assegurament del servei web.
 - Vulnerabilitats i assegurament del servei FTP.
 - Vulnerabilitats i assegurament del servei de correu.
 - Vulnerabilitats i assegurament del servei de VoIP.
 - Documentació: Aspectes a incloure.
 - UF3: Solucions de seguretat web:
 - Principals amenaces de seguretat web.
 - Eines en seguretat web.
 - Tipus d'injeccions (SQL, path, arxius, codi, altres).
 - Gestió segura de les sessions i autenticacions.
 - Referència a objectes de forma directa i indirecta.
 - Configuració i creació d'aplicacions web segures.
 - Realització d'informes d'amenaces i solucions.
 - UF4: Seguretat dels canals de comunicació i de enrutament:
 - Principis de la seguretat en xarxes.
 - Seguretat al switch.
 - Seguretat a les xarxes inalàmbriques.
 - Seguretat del router i de l'enrutament.
 - Seguretat dels equips terminals.
 - Denegació de servei: atacs i mitigació.
 - Riscos en altres xarxes.
- **Format de la prova:** Es realitzarà una prova amb contingut teòric i pràctic.
 - Consistirà en un qüestionari i una prova pràctica dels continguts de les UFs.