1 ASIX

**MÒDUL 5: FONAMENTS DE MAQUINARI**

ACTIVITAT 1: Anàlisis d’un CPD

línea horizontal

# 



**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Jacinto López

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

[**Exercici 1 3**](#_xytl2pao16qs)

[a) Què és un CPD? 3](#_5pwvenowtjg1)

[b) Quines són les seves funcionalitats principals? 3](#_wmsf2272wdxb)

[c) Quins són els components físics que ho formen? 3](#_el5ddma0w8p4)

[d) Quin són els components necessaris pels servidors dels CPD? 3](#_7q9hlpoho2xo)

[e) Quins són els components de software necessari? 3](#_mf8ndo6we6d7)

[f) Detalla tots els elements de la infraestructura de xarxa d’un CPD. Adjunta fotos. 3](#_maop1cqsjnpo)

[g) A nivell de seguretat, què podem fer tant a nivell de hardware, i a nivell que les dades siguin disponibles sempre. 6](#_mymaofqan3ke)

[h) Què és l’arquitectura d’alta disponibilitat? Quins nivell hi ha? Explica’ls. 6](#_8jrn1qjcx53t)

[i) Què diferència entre SAI’s i RAID’s. 6](#_8ig5a86gl8y4)

[j) Fes una breu descripció dels riscos que es pot patir amb els CPD’s i quines són les prevencions pertinents. 7](#_7ng3u7jr0cjq)

# Exercici 1

Busca informació del CPD i respon següents preguntes.

#### a) Què és un CPD?

És la instal·lació que centralitza les operacions i la infraestructura de TI d'una organització, on s'emmagatzemen, processen, tracten i difonen dades i aplicacions.

#### b) Quines són les seves funcionalitats principals?

Emmagatzematge de dades.

Tractament i processament de les dades.

Accés a aquesta informació a través d’Internet.

#### c) Quins són els components físics que ho formen?

Computació → Memòria i potència de processament per executar les aplicacions generalment

#### d) Quin són els components necessaris pels servidors dels CPD?

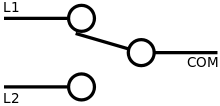
Són els equips de sobretaula, en concret per als servidors CPD processadors, RAM, controladors de xarxa, discs durs, SAI, xips criptogràfics. Són en base a ordinadors de sobretaula ja que han de estar encessos durant un periode de temps elevat.

#### e) Quins són els components de software necessari?

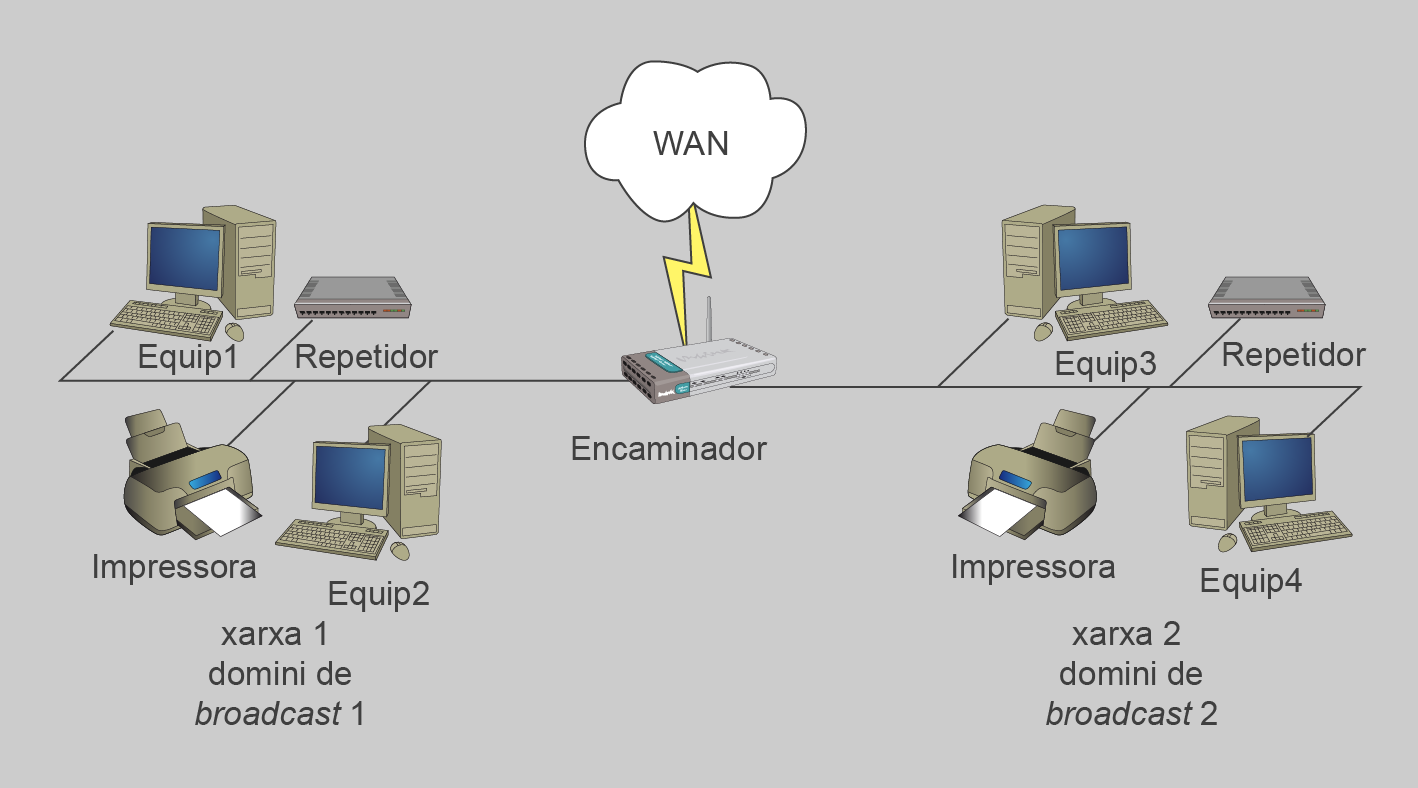
Sistemes operatius, programes de virtualització, programes de gestió de xarxa, programes de gestió de sistemes, programes de seguretat, programes de gestió d’emmagatzematge.

#### f) Detalla tots els elements de la infraestructura de xarxa d’un CPD. Adjunta fotos.

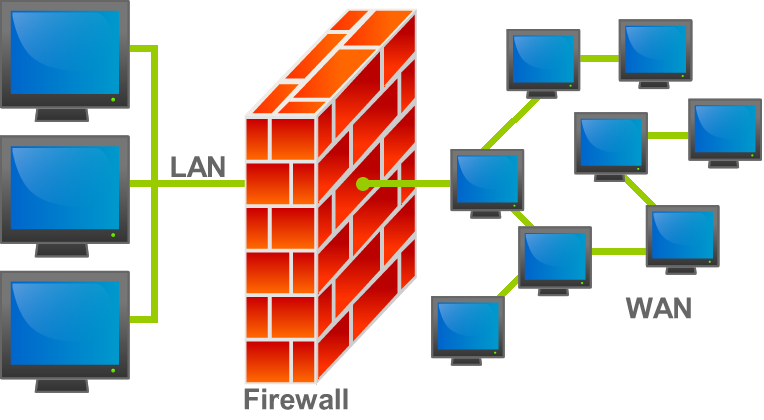
Comutadors, encaminadors, equips de firewall, cablejat estructurat, dispositius de monitorització de xarxa.



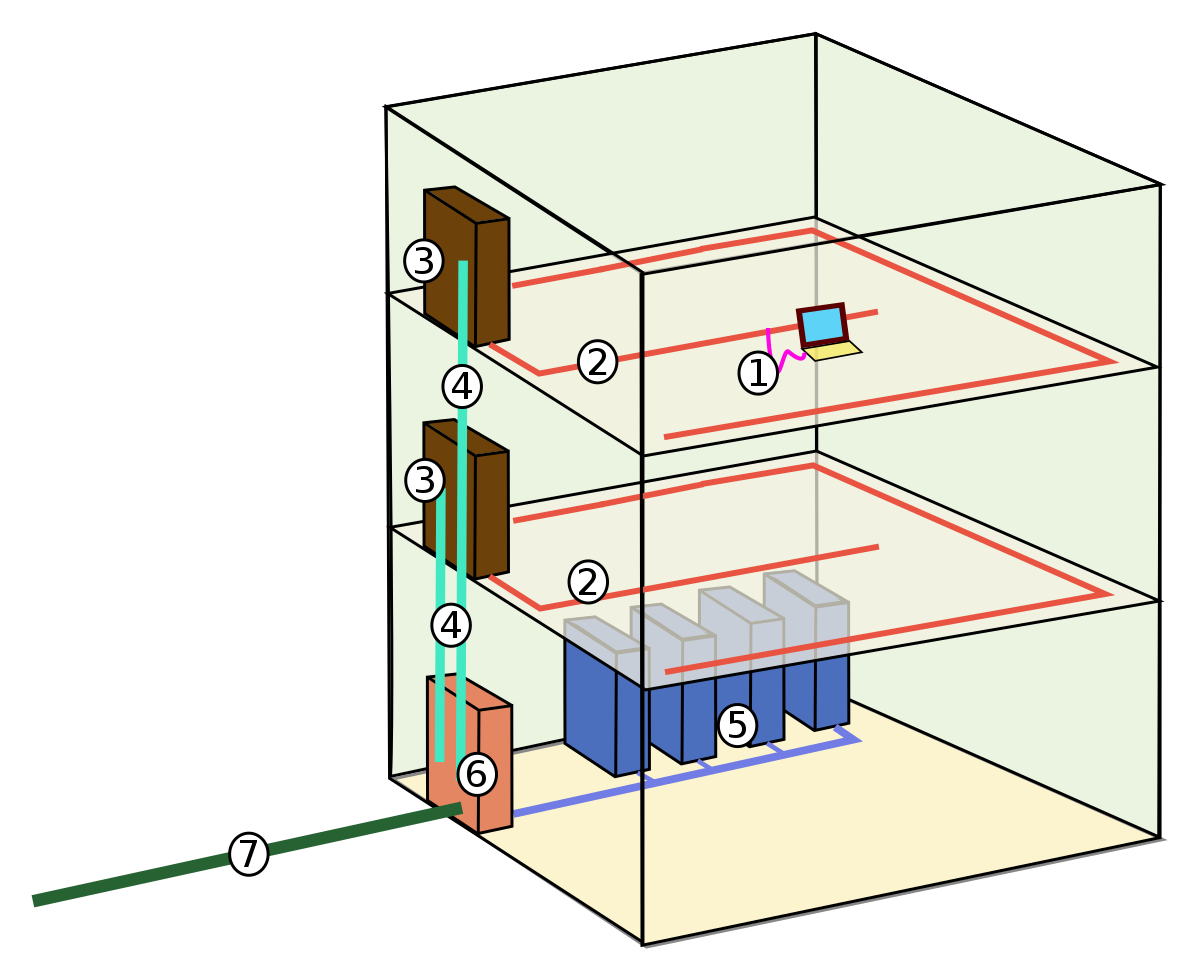
Comutadors



Encaminadors



Equips de firewall



Cablejat estructurat



Dispositius de monitorització de xarxa

#### g) A nivell de seguretat, què podem fer tant a nivell de hardware, i a nivell que les dades siguin disponibles sempre.

SEGURETAT: instal·lar equip físic per protegir servidors com sistemes de control d’accés , també software per protegir dades, com firewall i programes de seguretat. Es poden establir protocols de contingència per recuperació de dades en cas de desastres i accidents, còpies de seguretat de tot tipus.

#### h) Què és l’arquitectura d’alta disponibilitat? Quins nivell hi ha? Explica’ls.

Conjunt de tecnologies i pràctiques que s’utilitzen per garantir que els sistemes sempre estiguin disponibles. Diversos nivells, sistema únic (1 sistema actiu), alta disponibilitat (2 o més sistemes actius) recuperació de desastres (recuperació de dades i aplicacions en cas d’accidents naturals o altres)

#### i) Què diferència entre SAI’s i RAID’s.

Els SAI (Sistema d'Alimentació Ininterrompuda) i els RAID (Redundant Array of Independent Disks) són dues tecnologies diferents que serveixen per a finalitats diferents:

SAI: El SAI és un dispositiu que proporciona energia elèctrica de reserva a un sistema informàtic en cas que es produeixi una interrupció en el subministrament elèctric. Això permet als dispositius connectats continuar funcionant durant un període curt de temps, de manera que es pugui guardar la informació important i apagar els dispositius de manera adequada. Els SAI també protegeixen els dispositius connectats de les sobretensions i altres problemes elèctrics.

RAID: El RAID és una tecnologia que permet connectar diversos discs durs per crear un únic dispositiu de disc dur virtual. El RAID ofereix diverses opcions de configuració, com ara la redundància de dades, la millora del rendiment i la combinació d'ambdós. La redundància de dades és útil perquè, en cas que un disc dur falli, les dades encara es poden recuperar des d'un altre disc dur del RAID.

En resum, mentre que el SAI proporciona energia elèctrica de reserva per a la continuïtat dels dispositius connectats, el RAID ofereix diverses opcions de configuració per als discos durs, inclosa la redundància de dades per assegurar la integritat de les dades.

#### j) Fes una breu descripció dels riscos que es pot patir amb els CPD’s i quines són les prevencions pertinents.

Els Centres de Processament de Dades (CPD) són llocs crítics en què les empreses i les organitzacions allotgen les seves dades i sistemes informàtics. Hi ha diversos riscos que es poden patir en un CPD i, per tant, és important prendre mesures preventives per minimitzar-los. A continuació es presenten alguns dels riscos més comuns i les mesures preventives adequades:

* Pèrdua de dades: Una fallada del disc dur, un error humà o un desastre natural poden provocar la pèrdua de dades crítiques. Per prevenir aquest risc, és important fer còpies de seguretat regulars i verificar que aquestes còpies es puguin restaurar correctament.
* Interrupcions del servei: Una fallada dels sistemes, un atac cibernètic o una interrupció en el subministrament elèctric poden provocar interrupcions del servei. Per minimitzar aquest risc, és important tenir un pla de contingència i de recuperació davant d'aquestes situacions.
* Robatoris i vandalisme: Els robatoris i vandalisme poden afectar la seguretat física del CPD i dels seus equipaments. Per prevenir aquests riscos, és important instal·lar sistemes de seguretat física, com ara càmeres de vigilància, alarmes i accés restringit.
* Atacs cibernètics: Els atacs cibernètics poden afectar la seguretat de les dades i els sistemes del CPD. Per prevenir aquest risc, és important implementar mesures de seguretat informàtica, com ara antivirus, firewalls i altres solucions de seguretat de xarxes i aplicacions.
* Desastres naturals: Incendis, inundacions i altres desastres naturals poden afectar el CPD i els seus equipaments. Per prevenir aquests riscos, és important instal·lar sistemes de detecció d'incendis, protecció contra inundacions i altres mesures preventives adequades.

En resum, per garantir la seguretat i la continuïtat dels serveis del CPD, és important implementar mesures preventives adequades per a cada risc identificat. Això inclou mesures de seguretat física, informàtica i de contingència davant d'incidents.