

---

This is the **published version** of the bachelor thesis:

Gascón Rodríguez, Nil. *Disseny i implementació d'un sistema NAS domèstic per a còpies de seguretat automàtiques en dispositius Android*. Treball de Final de Grau (Universitat Autònoma de Barcelona), 2026 (Enginyeria Informàtica)

---

This version is available at <https://ddd.uab.cat/record/334363>

under the terms of the  license.

# Disseny i implementació d'un sistema NAS domèstic per a còpies de seguretat automàtiques en dispositius Android

Nil Gascón

**Resum** — Aquest treball presenta el desenvolupament d'una aplicació mòbil a Android i la construcció d'un NAS domèstic de baix cost com a alternativa als serveis d'emmagatzematge al núvol comercial. L'objectiu és oferir una solució privada, econòmica i fàcil d'utilitzar als usuaris, permetent així que tinguin el control de les seves dades en tot moment i no es puguin utilitzar en cap punt per entrenar models d'intel·ligència artificial. El resultat d'aquest sistema és proporcionar una alternativa real i de codi lliure als sistemes actuals, per permetre l'accés a qualsevol tipus d'usuari.

**Paraules claus** — NAS, Còpies de seguretat, ZFS, RAID, API REST, Núvol privat, VPN Mesh, Tailscale.

**Abstract** — This project presents the development of a mobile application for Android and the construction of a low-cost domestic NAS as an alternative to the commercial version. The objective is to offer a private, economical and easy-to-use solution for users, allowing them to maintain control of their data at all times and cannot be used at any point to train artificial intelligence models. The result of this system is to provide a real and reliable alternative to current systems, allowing access to any type of user.

**Index Terms** — NAS, Backups, ZFS, RAID, REST API, Private Cloud, VPN Mesh, Tailscale.

## 1 INTRODUCCIÓ - CONTEXT DEL TREBALL

El mòbil s'ha convertit, en poc més d'una dècada, en el dispositiu on s'acumula bona part de la nostra vida digital: fotografies, vídeos, documents importants, contactes... Tot centralitzat en un únic dispositiu. Però, paradoxalment, la facilitat amb la qual es genera tota aquesta informació contrasta amb la dificultat que suposa conservar-la de manera fiable a llarg termini.

Quan la memòria del dispositiu s'omple, la resposta del mercat és clara: puja-ho al núvol. Google, Apple, Microsoft, Amazon, entre d'altres, ofereixen serveis d'emmagatzematge que funcionen de manera pràcticament invisible per a l'usuari: la sincronització és automàtica, l'accés és des de qualsevol dispositiu i el procés no requereix cap coneixement tècnic. El problema és que, darrere d'aquesta comoditat, hi ha un model de negoci molt concret: el *freemium*[1]. Es comença gratis amb una capacitat limitada i, en el moment que la necessitat creix (i creix inevitablement), cal pagar una quota mensual o anual que, amb el temps, s'acumula en un cost notable.

Però el cost econòmic no és l'únic factor a considerar. Quan es delega l'emmagatzematge de dades personals a una plataforma de tercers, s'accepten condicions d'ús i polítiques de privacitat que, com s'ha vist en diverses ocasions, poden canviar de manera unilateral. Les preguntes sobre on s'emmagatzemen realment les dades, qui hi pot accedir o si es poden usar per entrenar models d'intel·ligèn-

cia artificial no sempre tenen una resposta clara o satisfactòria per a l'usuari.

És en aquest context on ha guanyat terreny la idea de disposar d'una infraestructura pròpia. Un NAS[2] domèstic permet centralitzar arxius, automatitzar còpies de seguretat i accedir als continguts des de fora de la xarxa local, tot reproduint l'experiència d'un servei de núvol però sobre maquinari i programari sota el control directe de l'usuari.

Ara bé, la disponibilitat de tecnologia no és suficient. Hi ha un perfil d'usuari molt concret (persones que fan ús quotidià del mòbil però que no tenen coneixements tècnics per gestionar còpies de seguretat manuals) per al qual totes aquestes eines resulten inaccessibles. Configurar un NAS, establir una política de backup[3] o verificar la integritat d'un arxiu no és quelcom que qualsevol persona estigui disposada o que sigui capaç de fer. Per a aquest tipus d'usuari, el sistema ha de ser transparent: ha de funcionar sol, sense intervencions, i ha de ser igual de senzill que qualsevol servei comercial.

Partint d'aquesta necessitat concreta, aquest treball proposa el disseny i la implementació d'un NAS domèstic orientat a la còpia de seguretat automàtica des de dispositius Android. La idea no és simplement replicar el que ja fa un Google Drive o un iCloud, sinó construir una solució real, de baix cost, que combini automatització, redundància física, xifratge de dades i accés remot segur, sense renunciar a la facilitat d'ús. En essència: que l'usuari mai no hagi de pensar en fer còpies de seguretat perquè el

---

- E-mail de contacte: [nil.gascon@autonoma.cat](mailto:nil.gascon@autonoma.cat)
- Menció realitzada: *Tecnologies de la Informació*
- Treball tutoritzat per: Bernat Gaston (DEIC)
- Curs 2025/26

sistema ja les hagi fet per a ell.

## 1.1 Objectius

Per al desenvolupament de totes aquestes idees ha estat necessari marcar-se uns objectius clars, consistents i realistes. Aquests han estat els següents:

### O1. Construir un servidor NAS domèstic de baix cost.

Dissenyar i muntar físicament un servidor NAS amb maquinari assequible (pressupost màxim de 400 €) capaç d'allotjar un sistema operatiu basat en Linux i gestionar volums d'emmagatzematge amb redundància i les còpies de seguretat de tots els arxius adjuntats[4].

### O2. Programar un model híbrid de còpies de seguretat.

Desenvolupar el motor de sincronització dins de l'aplicació mòbil que permeti programar i executar la transferència automàtica o manual de dades (fotografies, documents i contactes) cap al servidor NAS.

### O3. Garantir la integritat de les dades amb xifratge.

Configurar l'arquitectura del servidor per tal que el sistema compleixi amb els paràmetres de redundància física i estigui protegit davant d'una fallada i, alhora, també tingui la informació xifrada. Finalment, que existeixi la possibilitat de recuperar informació mitjançant Snapshot automàtic, de forma periòdica i aplicant una política de retenció.

### O4. Integrar la gestió d'arxius i l'accés remot segur a l'aplicació mòbil.

Implementar una interfície d'usuari, dins de la mateixa aplicació Android, que permeti explorar, gestionar i restaurar els arxius centralitzats al NAS, establint connexions xifrades d'extrem a extrem mitjançant una MeshVPN[5] (Tailscale[6]/WireGuard[7]), garantint un túnel segur independent de la xarxa física, i preparant l'arquitectura per a una futura integració de mTLS o protocols P2P.

### O5. Realitzar la documentació i manteniment

Descriure el procés de desenvolupament i les principals característiques del sistema, així com crear eines de suport que en facilitin el manteniment i permetin possibles ampliacions en un futur proper.

## 2 ESTAT DE L'ART

Per entendre l'aportació d'aquest projecte cal situar-lo dins del panorama actual de solucions per a l'emmagatzematge i còpia de seguretat de dades personals. En termes generals, les alternatives disponibles es poden agrupar en tres blocs: serveis de núvol públic, plataformes NAS comercials i alternatives self-hosted basades en programari lliure. Cadascun d'aquests blocs respon a necessitats i perfils d'usuari diferenciats, i tots tres presenten avantatges i limitacions que justifiquen la necessitat d'una solució intermèdia, com la que es proposa en aquest treball.

### 2.1 Serveis de núvol públic

Els grans serveis d'emmagatzematge al núvol (Google Drive[8], iCloud[9], Microsoft OneDrive[10] i Dropbox[11]) s'han consolidat com la solució predominant per a

l'usuari de consum. La seva adopció massiva respon a factors molt clars: instal·lació immediata, sincronització automàtica i accés des de qualsevol dispositiu sense necessitat de configuració tècnica ni vinculació a un sistema operatiu concret.

Tanmateix, des d'un punt de vista econòmic, totes aquestes plataformes comparteixen el mateix model de negoci: una capa gratuïta amb capacitat limitada i subscripcions de pagament per accedir a més espai o funcions avançades. A tall d'exemple, Google Drive i OneDrive ofereixen 15 GB de manera gratuïta, mentre que Dropbox en limita la capa lliure a 2 GB; per ampliar-la, cal pagar quotes mensuals que oscil·len entre 1 € i més de 17 € al mes, depenent del pla i la plataforma. A llarg termini, el cost acumulat és notable, especialment per a famílies o usuaris que generen grans volums de fotografies i vídeos en alta resolució.

Més enllà del cost, cal tenir en compte que l'ús d'aquests serveis implica cedir la custòdia de les dades a un tercer[12]. Les condicions d'ús poden variar, i l'usuari no té control sobre on s'emmagatzemen físicament les dades ni sobre les polítiques de privacitat aplicades. En alguns casos, les dades poden ser processades per sistemes d'intel·ligència artificial del proveïdor, la qual cosa és especialment rellevant en un context on la sobirania digital ha guanyat importància[13].

### 2.2 Plataformes NAS comercials

Davant les polítiques invasives del núvol públic, el mercat del NAS domèstic ha crescut com una alternativa orientada a centralitzar dades localment. En aquest segment, Synology i QNAP són els dos fabricants que dominen el mercat de consum i pimes, cadascun amb propostes de programari i maquinari ben diferenciades.

Synology s'ha posicionat com l'opció orientada a la simplicitat i la fiabilitat. El seu sistema operatiu, DSM (DiskStation Manager)[14], ofereix una interfície accessible i un ecosistema d'aplicacions pròpies que inclou Synology Drive (per a sincronització d'arxius) i Synology Photos (per a còpia i gestió de fotografies des del mòbil), reproduint d'alguna manera l'experiència d'un Google Photos privat. En matèria d'emmagatzematge, Synology treballa sobre un sistema de fitxers Btrfs, amb suport per a Hybrid RAID (SHR) i snapshots natius[15]. El principal inconvenient de la seva proposta és la dependència creixent de discs durs certificats pel fabricant, una decisió comercial que ha generat controvèrsia des del 2025, perquè limita les opcions de l'usuari i incrementa el cost del sistema[16].

QNAP, per la seva banda, aposta per maquinari més potent i flexible. Ofereix suport per a ZFS[17] a través del seu sistema QTS Hero[18], funcionalitats avançades d'emmagatzematge per nivells (tiering) i una gamma de dispositius amb connectivitat 10GbE, ranures PCIe i fins i tot suport per a targetes gràfiques. Aquesta flexibilitat el fa atractiu per a usuaris tècnics, però el perfil de complexitat és notablement superior al de Synology, i la seva trajectòria

en matèria de seguretat ha estat marcada per diverses vulnerabilitats rellevants.

## 2.3 Alternatives self-hosted

En paral·lel a les solucions comercials, existeix un ecosistema actiu de programari de codi obert orientat a oferir una experiència de núvol privat sense costos de plataforma ni dependències de fabricant. Les dues propostes més consolidades per a la gestió de fotografies i còpia des del mòbil són Nextcloud[19] i Immich[20].

Nextcloud és una plataforma de col·laboració i emmagatzematge de fitxers que inclou mòdul de fotos i integració, amb l'aplicació mòbil pròpia per a còpies de seguretat automàtiques. És molt versàtil i pot instal·lar-se sobre qualsevol servidor Linux, però el seu pes en recursos i la seva complexitat de manteniment el fan menys idoni com a solució exclusiva de backup de mòbil[19].

Immich ha guanyat molta popularitat precisament per cobrir el buit que deixa Nextcloud en la gestió de fotografia. Dissenyat específicament com a alternativa self-hosted a Google Photos, ofereix una aplicació Android i iOS amb còpia de seguretat automàtica, visualització per línia de temps, reconeixement facial i suport per a còpia selectiva per a àlbum. La seva integració amb Docker el fa fàcilment desplegable sobre qualsevol servidor Linux[20].

Ambdues eines, però, assumeixen que l'usuari és capaç de desplegar i mantenir un servidor, gestionar actualitzacions i diagnosticar problemes tècnics. No disposen de maquinari integrat ni d'una proposta d'instal·lació transparent per a usuaris no especialitzats.

## 2.4 Oportunitat del projecte

Les solucions analitzades cobreixen de manera eficient els segments d'usuaris especialitzats o disposats a assumir una certa complexitat de configuració. En canvi, cap d'elles ofereix una proposta que combini, de manera integrada i accessible per a usuaris no tècnics, maquinari de baix cost construït des de zero, automatització transparent des d'Android, xifratge, redundància i accés remot segur. Aquest buit és precisament l'espai que ocupa el present projecte.

## 3 METODOLOGIA

El projecte s'ha planificat i executat seguint un model de desenvolupament seqüencial per fases, comunament conegut com a model en cascada o waterfall[21]. En aquest enfocament, cada fase té un inici i un final definits, i el pas a la fase següent queda condicionat a l'assoliment dels objectius de l'anterior.

Aquesta estructura s'ha escollit perquè la naturalesa del projecte presenta dependències tècniques clares i ordenades: no té sentit construir el maquinari físic fins que existeixi un prototip virtual funcional, ni integrar l'aplicació mòbil fins que el servidor sigui operatiu. A diferència dels models iteratius, pensats per a equips que treballen en paral·lel sobre diferents mòduls, el model seqüencial s'adapta millor a un projecte individual on cada bloc depèn directa-

ment del que el precedeix.

A més, aquest enfocament encaixa de manera natural amb el marc d'avaluació contínua del treball: cada fase culmina amb un producte parcial verificable que coincideix amb els lliuraments intermedis establerts com a milestones acadèmics. Això permet fer un seguiment real del progrés sense necessitat d'esperar al lliurament final per detectar possibles desviacions o problemes tècnics.

El projecte s'organitza en cinc fases consecutives que cobreixen des de l'anàlisi inicial i el prototipatge virtual fins a la construcció del maquinari, la integració de tots els components, les proves de validació i la documentació final. La planificació detallada amb el diagrama de Gantt associat es pot consultar a l'Apèndix A.

### 3.1 Planificació

Partint de la definició metodològica exposada, a continuació es desglossa l'organització temporal establerta per assegurar l'acompliment del projecte dins de l'assignatura. L'horitzó de temps previst és de dinou setmanes.

L'execució del treball ha estat assumit íntegrament per un únic desenvolupador i s'estructura a partir d'un conjunt de tasques clau. Tal com queda patent en la Taula 1, cadascuna d'aquestes activitats pretén cobrir un o diversos dels objectius generals detallats prèviament.

TAULA 1  
PLANIFICACIÓ DEL PROJECTE

| ID Objectiu | ID Tasca | Tasca                                        |
|-------------|----------|----------------------------------------------|
| O1 - O4     | T1       | Recerca i definició de requisits             |
| O1          | T2       | Desplegament NAS virtual (Prototip)          |
| O4          | T3       | Disseny UI/UX i lògica base                  |
| O2          | T4       | Sincronització, programari i traspàs fitxers |
| O1          | T5       | Adquisició i muntatge de peces               |
| O1 i O3     | T6       | Instal·lació i configuració                  |
| O1          | T7       | Migració de l'entorn virtual al físic        |
| O2 - O4     | T8       | Proves d'estrès i accés remot                |
| O1 - O4     | T9       | Possibles millores físiques i de software    |
| O5          | T10      | Crear eines de manteniment                   |
| O5          | T11      | Elaborar la documentació final               |

## 4 DESENVOLUPAMENT

Una vegada definida la metodologia de treball, aquest bloc s'endinsa en la materialització del projecte. Al llarg de les següents seccions s'exposen les decisions tecnològiques adoptades i el procés de configuració de l'entorn, que abasta des de la preparació del servidor base fins a la integració dels serveis de xarxa i l'arquitectura de l'aplicació. Per tal de facilitar la comprensió global de la solució abans d'entrar en el detall tècnic, a l'apèndix B es presenta un diagrama simplificat de l'arquitectura del sistema.

## 4.1 Preparació i configuració del servidor NAS

### 4.1.1 Sistema operatiu base

El servidor NAS s'ha desplegat sobre Debian en la seva variant mínima (minimal install), sense entorn gràfic ni serveis innecessaris. Aquesta elecció respon a criteris de lleugeresa, estabilitat i control: Debian és una de les distribucions Linux més consolidades en entorns de servidor, amb un cicle de publicació conservador que prioritza la fiabilitat per sobre de la novetat. La instal·lació mínima garanteix que els recursos del sistema (CPU, RAM i I/O de disc) es dediquin exclusivament als serveis del NAS, sense processos de fons que consumeixin capacitat de manera innecessària.

Durant la fase de prototipatge virtual, el servidor s'ha desplegat en una màquina virtual amb dos discos de dades i un disc de paritat, reproduint l'estructura que tindrà el sistema físic definitiu. Aquesta aproximació ha permès validar tota la configuració de programari (sistema de fitxers, redundància, API i serveis de xarxa) abans de fer cap inversió en maquinari real.

### 4.1.2 Sistema d'emmagatzematge: ZFS vs MergerFS

L'arquitectura d'emmagatzematge del NAS es basa en ZFS amb configuració RAIDZ2 [22], una solució integrada que combina la gestió de volums, redundància, verificació d'integritat i snapshots nadius en una única capa robusta. Abans d'optar per aquest sistema, es va considerar la combinació MergerFS + SnapRAID[23], una alternativa molt estesa en entorns domèstics de baix cost per la seva simplicitat i compatibilitat amb discs heterogenis. A la Taula 2 es presenta una comparativa resumida d'ambdues arquitectures.

TAULA 2  
ZFS vs MERGERFS

| Característica                                       | MergerFS + SnapRAID                             | ZFS + RAIDZ2                                         |
|------------------------------------------------------|-------------------------------------------------|------------------------------------------------------|
| Càlcul de paritat                                    | Diferit i periòdic (cron)                       | En temps real, a cada escriptura                     |
| Protecció entre sincronitzacions de paritat          | No garantida                                    | Sempre activa                                        |
| Viable amb discs de diferent tecnologia i capacitat? | Excel·lent, està dissenyat amb aquest objectiu. | No, rendiment baix i no s'aprofita tota la capacitat |
| Snapshots nadius                                     | No                                              | Sí, quasi instantanis                                |
| Complexitat de configuració                          | Baixa - Mitjana                                 | Mitjana - Alta                                       |
| Rendiment en I/O simultània                          | Bo                                              | Excel·lent gràcies al caché ARC integrat             |

La decisió final d'escollir ZFS amb RAIDZ2 es fonamenta en les limitacions de seguretat de MergerFS + SnapRAID. En aquesta darrera combinació, el càlcul diferit de la paritat deixa les dades desprotegides entre sincronitzacions i la falta de coordinació en operacions I/O simultànies pot generar inconsistències.

En canvi, ZFS garanteix la consistència de les dades gràcies al mecanisme de copy-on-write (on mai se sobreescrueixen dades existents fins que les noves estan consolidades)

i al càlcul de paritat en temps real amb verificació per checksum. A més, el nivell RAIDZ2 (equivalent a RAID 6) tolera la fallada simultània de fins a dos discos, mentre que els snapshots nadius permeten recuperar el sistema davant d'esborrats o atacs de ransomware de manera gairebé instantània [24]. Durant la fase de prototipatge virtual, aquesta configuració ha permès simular amb precisió el comportament de l'entorn definitiu, validant correctament l'API i l'aplicació mòbil abans de fer la migració al maquinari físic.

RAIDZ2, equivalent al RAID 6, aplica doble paritat distribuïda i permet tolerar la fallada simultània de fins a dos discos sense pèrdua de dades. Els snapshots nadius permeten recuperar contingut eliminat o xifrat per ransomware de manera quasi instantània[24].

Durant el prototipatge virtual s'ha emprat RAIDZ2 precisament per simular el comportament del sistema definitiu, permetent validar l'API i l'aplicació mòbil abans de la migració al maquinari físic.

### 4.1.3 API REST i servei de sistema

Un cop establerta la capa d'emmagatzematge, el pas següent va ser desplegar l'API REST[25] que exposa les funcionalitats del NAS a l'aplicació mòbil. L'API s'executa dins d'un entorn virtual Python aïllat, una pràctica estàndard que evita conflictes entre les dependències del projecte i les llibreries del sistema operatiu. El servidor d'aplicacions utilitzat és Uvicorn, un servidor ASGI d'alt rendiment dissenyat específicament per a aplicacions asíncrones com FastAPI.

Per garantir que l'API s'iniciï automàticament en arrencar el servidor i es reiniciï en cas d'error, s'ha creat un servei gestionat per systemd, el sistema d'inicialització de Debian. Això significa que el servei de l'API té el mateix comportament que qualsevol altre servei del sistema operatiu: arrenca sol, es pot aturar o reiniciar amb una sola comanda i deixa registres al sistema de logs. Aquesta configuració és essencial per garantir l'autonomia del NAS: si el servidor es reinicia per un tall de llum o una actualització, tots els serveis es recuperen sols sense cap intervenció manual.

### 4.1.4 Accés remot: Tailscale

L'accés al NAS des de fora de la xarxa local es gestiona a través de Tailscale, una solució de VPN mesh basada en el protocol WireGuard. A diferència d'una VPN tradicional que requereix un servidor central, Tailscale estableix connexions directes xifrades entre els dispositius registrats, i assigna a cadascun una adreça IP privada fixa dins de la xarxa virtual.

Des d'un punt de vista pràctic, això significa que l'aplicació mòbil pot accedir al NAS utilitzant sempre la mateixa adreça IP, independentment de si el dispositiu es troba a la mateixa xarxa local o connectat a través de dades mòbils. La connexió és transparent per a l'usuari i no requereix cap configuració al router ni obertura de ports, la qual cosa elimina una de les principals barreres tècniques per accedir a recursos domèstics de manera remota.

Tailscale s'ha configurat com a servei de sistema, de manera que s'inicia automàticament amb el servidor i manté el túnel actiu en tot moment. Combinat amb el servei de l'API, el resultat és un sistema completament autònom: un cop configurat, el NAS és accessible des de qualsevol lloc sense necessitat de cap intervenció tècnica.

## 4.2 Aplicació Android i API REST

### 4.2.1 Arquitectura de l'aplicació

L'aplicació ha estat desenvolupada en Kotlin per a Android, seguint el patró d'arquitectura MVVM (Model-View-ViewModel)[26]. Aquesta elecció no és arbitrària: en un projecte on la interfície ha de reflectir en tot moment l'estat real d'un servidor extern, separar la lògica de la capa de presentació és imprescindible per tenir el codi mantenible i coherent.

L'arquitectura s'organitza en tres capes ben diferenciades. La capa de model defineix les estructures de dades que circulen per l'aplicació: respostes de l'API, estats de la interfície i entitats del domini, com arxius, còpies de seguretat o mètriques del sistema. La capa de ViewModel centralitza tota la lògica i la comunicació amb l'API; és l'únic component que coneix l'estat de l'aplicació i el que decideix com evoluciona en resposta a les accions de l'usuari o als canvis del servidor. Finalment, la capa de vista, construïda íntegrament amb Jetpack Compose, és purament reactiva: no conté lògica pròpia, sinó que s'actualitza automàticament cada vegada que el ViewModel publica un nou estat.

Aquesta separació té implicacions pràctiques importants. Significa, per exemple, que si es vol modificar com es mostra la informació de CPU a la pantalla d'estat del sistema, el canvi és aïllat a la capa de vista i no afecta res més. I a la inversa: si es canvia la font de dades (per exemple, substituir una crida HTTP per un WebSocket) la vista no necessita cap modificació. En un projecte amb un sol desenvolupador i un temps limitat, aquesta predictibilitat és especialment valuosa.

La navegació entre pantalles es gestiona de manera centralitzada, de forma que l'estat d'autenticació determina en tot moment quina part de l'aplicació és accessible. Si el token JWT[27] caduca o no és vàlid, l'usuari és redirigit automàticament a la pantalla de login sense necessitat d'intervenir manualment.

### 4.2.2 Comunicació amb l'API: Retrofit i autenticació JWT

Tota la comunicació entre l'aplicació i el servidor NAS es realitza a través d'una API REST, dissenyada específicament per a aquest projecte amb FastAPI[28] (Python). La interfície de comunicació a l'aplicació s'implementa amb Retrofit2, una llibreria HTTP àmpliament estesa a l'ecosistema Android que permet definir els endpoints com a funcions Kotlin suspensibles i gestionar automàticament la serialització JSON, en fer que el codi resultant sigui llegible i fàcil d'estendre.

El client es connecta al servidor a través de Tailscale. La comunicació es realitza via HTTP dins del túnel xifrat, permetent l'accés al NAS des de qualsevol ubicació sense exposar serveis a Internet. La implementació de mTLS queda prevista com a millora futura.

El mecanisme d'autenticació segueix l'estàndard OAuth2 amb credencials de formulari[29]. En introduir les seves dades, l'aplicació les envia a l'endpoint de login, que verifica les credencials al servidor i retorna un token JWT (JSON Web Token) amb un temps de vida d'una hora. A partir d'aquell moment, totes les peticions inclouen el token a la capçalera HTTP d'autorització. Si el servidor detecta que el token ha caducat o és invàlid, retorna un codi d'error 401 que l'aplicació gestiona de manera transparent per a l'usuari.

Des del punt de vista de la seguretat a l'API, totes les operacions sobre el sistema de fitxers passen per una funció de validació que resol la ruta relativa rebuda del client i verifica que el resultat sigui sempre un subdirectori de l'arrel d'emmagatzematge del NAS. Això preveu qualsevol intent d'accés a zones del sistema de fitxers fora de l'àmbit permès, un patró d'atac conegut com path traversal[30].

### 4.2.3 Actualització en temps real

Un dels requisits de disseny de l'aplicació era que la informació mostrada reflectís en tot moment l'estat real del servidor, sense que l'usuari hagués de refrescar manualment cap pantalla. Per aconseguir-ho, s'ha implementat un mecanisme de polling concurrent basat en corutines de Kotlin.

El funcionament és el següent: cada secció de l'aplicació que necessita dades en temps real gestiona el seu propi bucle asíncron independent, que consulta l'API cada segon i actualitza l'estat publicat pel ViewModel. Quan l'usuari navega cap a una secció, el bucle s'inicia; quan en surt, s'atura. Aquesta gestió explícita del cicle de vida de les consultes és important per evitar peticions innecessàries al servidor quan la informació no és visible, i per garantir que no hi hagi fuites de memòria associades a corutines actives en segon pla.

Gràcies a aquest mecanisme, les mètriques de CPU, RAM, temperatura i emmagatzematge s'actualitzen contínuament, i qualsevol canvi al sistema de fitxers del NAS (per exemple, un arxiu creat per un altre dispositiu) es reflecteix automàticament a la pantalla del gestor d'arxius sense cap acció per part de l'usuari.

### 4.2.4 Pantalles i funcionalitats

L'aplicació s'estructura en vuit pantalles connectades per la navegació central, amb un sistema de control d'accés basat en rols que adapta la interfície segons si l'usuari és administrador o estàndard. Al·l'apèndix D es podran trobar una varietat de captures de pantalla de l'aplicatiu:

Pantalla de configuració inicial (Setup). Es mostra automàticament la primera vegada que s'instal·la el sistema o

quan no hi ha cap administrador definit. Permet establir les credencials del primer usuari administrador real, elimina l'accés per defecte insegur i a més assegura que el NAS neixi protegit des del primer minut.

Pantalla de login. És el punt d'entrada de l'aplicació i la primera barrera de seguretat. Presenta un formulari d'autenticació que suporta contrasenyes de qualsevol longitud, gràcies a un sistema de pre-hash SHA-256 combinat amb l'algorisme Bcrypt. En cas d'error, informa l'usuari i permet reintentar-ho.

Dashboard. Actua com a centre de control. Presenta un resum de l'estat del NAS en temps real i dona accés a les seccions principals. Inclou un botó de tancament de sessió accessible per a tots els usuaris. Si l'usuari no és administrador, la interfície es simplifica automàticament, ocultant les mètriques de rendiment i les seccions tècniques per mostrar només les funcionalitats de còpia de seguretat.

Estat del sistema. Amplia la informació del dashboard amb un nivell de detall tècnic molt superior: ús de CPU global i per nucli, freqüència actual del processador, estat de la memòria RAM i de la memòria d'intercanvi, temperatures llegides des dels sensors de maquinari i velocitat de rotació dels ventiladors. Tota aquesta informació és llegida en temps real pel servidor a través de la llibreria psutil de Python, que ofereix una interfície unificada als recursos del sistema operatiu independentment de la distribució Linux instal·lada.

Gestor d'arxius. Permet navegar i gestionar tot el contingut del NAS, de manera similar a un explorador d'arxius convencional. L'usuari pot moure's per l'estructura de directoris, crear carpetes noves, pujar fitxers des del dispositiu, descarregar arxius individuals o carpetes completes en format ZIP, canviar el nom d'elements i eliminar-los. Tot el contingut es mostra ordenat (primer carpetes, després arxius, per ordre alfabètic) i s'actualitza en temps real. Queda fora de l'abast d'aquesta versió la previsualització de contingut, com ara documents PDF o fitxers de text, el que es considera una millora futura. Aquesta és la part tècnicament més exigent de l'aplicació, ja que requereix sincronitzar de manera coherent operacions que afectaven simultàniament el dispositiu mòbil i el servidor.

Còpies de seguretat i automatització. Permet realitzar còpies manuals o programar tasques automàtiques per preservar fotos, vídeos, contactes o SMS. Mostra el progrés detallat en temps real i s'executa en segon pla per no interrompre l'ús del dispositiu.

Administració d'usuaris. Secció exclusiva per a administradors, la qual permet la gestió completa del parc d'usuaris. Inclou la capacitat de crear nous perfils, eliminar-los o editar-ne les dades existents (nom, contrasenya i nivell de permisos).

Registres de l'App (Logs). Pantalla de diagnòstic on es poden consultar els esdeveniments del sistema per verifi-

car que totes les operacions (càrregues, descàrregues i accessos) s'han realitzat correctament.

#### 4.2.5 Motor de còpia de seguretat

El motor de còpia de seguretat és la funcionalitat central del projecte i una de les parts amb més profunditat d'implementació. S'executa en un fil de treball dedicat a no bloquejar en cap moment la interfície d'usuari, i segueix un procés organitzat en quatre etapes consecutives.

La primera etapa és l'escaneig del dispositiu. Depenent dels tipus de contingut seleccionats per l'usuari, el motor consulta les APIs del sistema operatiu Android per obtenir les llistes d'arxius corresponents. Les imatges, vídeos i àudios s'obtenen a través de MediaStore, el proveïdor de contingut del sistema que indexa tot el multimèdia del dispositiu. Els documents (PDF, Word, Excel, fitxers de text, arxius comprimits i altres formats compatibles) s'obtenen a través de DocumentFile, en què permet accedir a l'emmagatzematge extern de manera segura. Els contactes s'extreuen via ContactsContract i els SMS via proveïdor de missatgeria del sistema, ambdós serialitzats en format JSON.

La segona etapa és la preparació de l'estructura de carpetes al NAS. Abans de pujar cap arxiu, el motor crea una jerarquia de directoris organitzada de la forma `backups/mobil/{fabricant_model}/{data_hora}/`, amb subcarpetes per a cada tipus de contingut. Aquesta estructura permet identificar amb precisió el dispositiu d'origen, la data de cada còpia i el tipus de contingut que conté, per facilitar enormement la gestió i la recuperació posterior.

La tercera etapa consisteix en la pujada seqüencial del contingut. Cada arxiu multimèdia s'envia al servidor i es desa al NAS conservant directament les metadades originals del fitxer, de manera que la informació necessària per a una restauració posterior es manté associada al recurs original. D'aquesta manera, atributs com la data de captura, la mida original o l'URI d'origen s'hi preserven durant tot el procés. Paral·lelament, la interfície actualitza de manera contínua l'estat del procés i mostra una estimació del temps restant basada en la velocitat de pujada observada.

Finalment, un cop completat tot el procés, la interfície confirma a l'usuari que la còpia s'ha realitzat correctament i indica la carpeta de destinació al NAS. Si es produeix un error en qualsevol punt, el motor el captura i informa sense interrompre bruscament l'aplicació.

#### 4.2.6 Permisos de l'aplicació

L'accés a les dades personals del dispositiu requereix la declaració explícita de permisos al manifest de l'aplicació i, en molts casos, la seva acceptació activa per part de l'usuari en temps d'execució. Android ha endurit progressivament el model de permisos, en les darreres versions, per protegir la privacitat dels usuaris, i l'aplicació s'adapta a aquest model[31].

Per a contingut multimèdia, Android 13 i versions posteriors introdueixen permisos granulars separats per tipus: imatges, vídeo i àudio es gestionen de manera independent. L'accés a documents generals i a l'emmagatzematge extern requereix un permís de gestió ampliada que l'usuari ha de concedir explícitament des de la configuració del sistema. L'accés a contactes i a SMS es gestiona amb permisos específics per a cadascun. L'aplicació proporciona el conjunt mínim de permisos necessaris per a les funcionalitats implementades, sense sol·licitar accessos superflus.

### 4.3 Hardware

El muntatge del servidor NAS físic s'ha plantejat amb una estratègia híbrida, combinant components reutilitzats, peces noves i material adquirit de segona mà. Aquesta decisió respon principalment a criteris d'optimització de costos, ja que ha permès construir una plataforma funcional i suficientment robusta sense haver de partir íntegrament de maquinari nou.

A continuació, es detalla la selecció i procedència de cadascun dels elements mecànics i electrònics utilitzats, així com l'anàlisi de l'impacte financer global d'aquesta tria en el pressupost del projecte.

#### 4.3.1 Components de maquinari i estudi de costos

Per a la infraestructura de còmput s'ha optat per una solució de contenció econòmica dividida en tres tipologies de recursos. En primer lloc, s'aprofiten components clau ja disponibles de l'arquitectura base (processador, placa, RAM i unitats d'emmagatzematge inicials), fet que redueix el cost d'aquesta partida a zero. En segon lloc, s'adquireixen elements estructurals totalment nous indispensables per garantir l'eficiència i seguretat elèctrica del conjunt (caixa, font d'alimentació i cablejat expansor). Finalment, es complementa el pool de dades mitjançant la compra d'unitats de disc addicionals de segona mà, assolint així la capacitat de disseny requerida a un preu reduït.

L'avaluació financera d'aquesta combinació demostra la viabilitat real de la solució en un entorn domèstic. Per tal d'evitar la duplictat de dades i agilitzar la lectura d'aquest bloc, s'ha extret el llistat numèric complet de la memòria principal. El desglossament detallat de cadascun dels components i les seves despeses d'enviament es poden veure a l'Apèndix C. El projecte presenta un cost total general de 295,54 €, assolint folgadamente l'objectiu de mantenir-se per sota dels 400 € proposats inicialment i registrant un estalvi net de 104,46 €.

#### 4.3.4 Arquitectura d'emmagatzematge

La configuració final dels discs s'ha estructurat en dos nivells diferenciats. D'una banda, el sistema principal de dades s'ha muntat sobre sis discs HDD d'1 TB, agrupats en un pool ZFS amb RAIDZ2, una solució que ofereix redundància davant la fallada de dos disc i aprofita les funcionalitats natives de ZFS: integritat per checksum, gestió avançada del sistema de fitxers i suport futur per a snapshots. D'altra banda, els dos SSD de 240 GB s'han configurat en RAID1 (mirror) per allotjar el sistema operatiu, garantint-ne la disponibilitat en cas de fallada d'un dels dos.

La partició del sistema s'ha organitzat de la manera següent:

- Partició d'arrel (~130 GB): allotja Debian Minimal i tots els serveis del servidor.
- Partició d'intercanvi / swap (~8 GB en RAID): permet externalitzar dades de la RAM durant operacions de compressió o de càrrega intensiva, evitant pèrdues per desbordament.
- Pool de dades ZFS (RAIDZ2): sis HDD d'1 TB, destinats exclusivament a l'emmagatzematge d'arxius i còpies de seguretat.

Cal destacar que, durant la instal·lació de Debian, es va descartar l'aplicació de xifrat sobre els volums RAID del sistema operatiu, a causa de la complexitat tècnica que suposa combinar aquesta configuració amb les particions d'arrencada. Malgrat que el sistema incorpora dades sensibles, aquestes no corresponen principalment a contingut funcional d'usuari, sinó, sobretot, a elements de configuració i accés interns, l'exposició dels quals queda vinculada principalment a un escenari d'accés físic no autoritzat al maquinari. Atès que el xifrat de disc complet protegeix sobretot davant de pèrdua, robatori o accés físic al dispositiu, es va valorar que, en aquest cas, el guany de seguretat no compensava la complexitat afegida per la implementació.

#### 4.3.5 Muntatge físic i gestió de cables

Un dels principals reptes del muntatge ha estat la integració de la safata portadiscs dins d'una caixa, no dissenyada específicament, per a ús NAS. En una primera aproximació, el suport es va intentar fixar a la part superior del xassís, però aquesta solució dificultava el tancament correcte de la caixa, no proporcionava una subjecció estable i comprometia la ventilació dels discs. Davant d'aquesta situació, es va optar per reubicar el conjunt a la base del xassís i fixar-lo amb cintes de subjecció, el que va permetre resoldre alhora l'estabilitat, la circulació d'aire i la coherència de la disposició interna.

L'organització del cablejat ha representat una dificultat afegida, per tractar-se d'una font de cablejat fix (no modular) que obliga a gestionar un nombre superior de cables dins del xassís. Malgrat aquest inconvenient, s'ha aconseguit una distribució interna ordenada i funcionalment acceptable. Pel que fa al comportament acústic, el nivell de soroll percebut, un cop instal·lat el sistema, és relativament baix per al tipus i la quantitat de maquinari emprat; sense ser un sistema silenciós, el resultat és compatible amb un ús domèstic continuat.

## 5 OPTIMITZACIÓ I REFINAMENT DEL SISTEMA

Una vegada completat el bloc anterior, el projecte avança cap a la preparació de l'entorn de programari i la integració del sistema. En el marc d'un desenvolupament seqüencial, abans de sotmetre la infraestructura física a càrregues de treball, és indispensable aplicar un conjunt d'ajustos estructurals i optimitzacions prèvies que assegurin una experiència superior a l'usuari final.

Aquest capítol es concentra, de manera exclusiva, en detallar aquestes millores i refinaments de configuració. L'objectiu és consolidar una base operativa totalment estable i eficient, deixant el servidor NAS i l'aplicació mòbil completament preparats per a l'etapa posterior, la qual es dedicarà íntegrament a les proves d'estrès, validació del rendiment i corroboració global de tot el sistema.

### 5.1. Gestió de connexions i xarxa VPN

Un dels canvis més rellevants ha consistit a condicionar l'inici de sessió a l'estat de la xarxa virtual. Ara, quan s'obre l'aplicació, el sistema comprova de fons si la VPN de Tailscale està activa. Si tot és correcte, permet procedir amb l'autenticació estàndard. En cas contrari, es bloqueja l'accés i es convida l'usuari a connectar-se, tot oferint una redirecció directa cap a l'aplicació oficial (o cap a la Play Store si encara no la té instal·lada). Aquesta decisió de disseny suprimeix gran part dels errors freqüents de connexió. Paral·lelament, s'ha introduït un mòdul per gestionar múltiples servidors NAS. Això resulta molt pràctic si es vol alternar entre un equip domèstic i un de remot, ja que permet emmagatzemar direccions IP i ports sota noms personalitzats per agilitzar accessos futurs.

### 5.2. Panell de control i diagnòstic

El dashboard principal ha canviat força respecte als primers esborranys, per prioritzar-ne la claredat visual. S'han suprimit dades tècniques que podien resultar aclaparadores, deixant únicament la informació crítica: temperatura global, càrrega del processador i ús de la memòria. Addicionalment, s'ha integrat una eina de diagnòstic pròpia (Speed Test). D'aquesta manera, i sense necessitat de sortir de l'aplicació, l'usuari pot analitzar la qualitat de l'enllaç al servidor en visualitzar la latència (ping), el jitter i les velocitats reals de pujada i descàrrega a través del túnel xifrat.

### 5.3. Navegació i càrrega de fitxers

Moure's per l'arbre de directoris ara és una tasca molt més àgil. Aquest sistema permet l'opció de retrocedir diverses carpetes de cop, sense haver de prémer constantment el botó d'anar enrere. Pel que fa al backend, l'optimització de les pujades representa un salt qualitatiu important. L'aplicació ja no es limita a transferir fitxers solts o múltiples arxius individuals; la nova actualització permet carregar carpetes senceres. Així, el sistema replica automàticament tota la jerarquia original del dispositiu mòbil al servidor.

### 5.4. Automatització de les còpies de seguretat

Aquesta era sens dubte una de les funcionalitats més esperades i, amb aquesta darrera versió, s'ha integrat per complet. La secció de backups incorpora actualment un programador intuïtiu. Des d'aquí, l'usuari pot establir cada quantes hores s'ha de forçar la sincronització i especificar exactament quin tipus de contingut vol salvaguardar (fotografies, documents, missatges, etc.). Per tal de mantenir un control visual ràpid, la pantalla sempre mostra la data exacta i el resultat de l'última còpia executada.

### 5.5. Monitoratge mitjançant registres (Logs)

Amb l'objectiu de facilitar les tasques d'auditoria i el manteniment, s'hi ha habilitat un visor de registres. Aquest mòdul es divideix en dues pestanyes diferenciades: per una banda, els esdeveniments locals que succeeixen al telèfon mòbil; per l'altra, els registres centralitzats al servidor NAS. L'eina incorpora filtres per classificar els avisos segons el seu grau de severitat (informació, depuració, error o emergència), i així simplificar notablement la detecció de qualsevol anomalia.

### 5.6. Seguretat i rols d'usuari

El compte predeterminat que s'utilitzava per fer proves s'hi ha eliminat definitivament. Al seu lloc, hi trobem un sistema d'administració d'usuaris madur. La figura de l'administrador pot donar d'alta nous perfils, alterar-ne les credencials o suprimir-los. El detall més destacat d'aquest apartat, però, és la implementació de rols. Ara és perfectament viable crear un compte d'usuari estàndard que només disposi de permisos per fer còpies de seguretat. Amb aquesta restricció, un usuari secundari pot protegir les seves dades al NAS sense tenir cap mena d'accés a l'explorador de fitxers globals, i garantir així la privacitat entre les diferents persones que utilitzin el mateix maquinari.

## 6 VALIDACIÓ DEL RENDIMENT I PROVES D'ESTRÈS

Per tenir la certesa que aquestes modificacions de programari fossin robustes, es va dissenyar una prova d'estrès. Aquesta prova va consistir a forçar la pujada ininterrompuda d'un arxiu de grans dimensions des d'una xarxa externa directament cap al NAS.

Les mètriques extretes durant el procés van evidenciar un comportament excel·lent de la màquina. Ni el processador ni la memòria RAM van patir desbordaments o saturacions excessives, fins i tot assumint el cost computacional de xifrar i desxifrar constantment el trànsit VPN. D'aquests resultats es conclou que l'arquitectura del codi és ferma, i que qualsevol coll d'ampolla a l'hora de transferir fitxers estarà condicionat, gairebé exclusivament, per l'ample de banda que proporcioni l'operadora de telefonia i/o la VPN. A l'apèndix E s'hi pot trobar una captura del test.

## 7 PRESENTACIÓ DE RESULTATS I CONCLUSIONS

El desenvolupament d'aquest projecte ha cristal·litzat en una solució tangible que demostra com és possible eludir la dependència dels grans serveis del núvol comercial. El sistema NAS dissenyat s'ha revelat com una alternativa plenament funcional, real i assequible, la qual cosa permet donar per validats la gran majoria dels objectius que es van plantejar a l'inici d'aquest document.

A continuació, es condensa l'avaluació global del projecte, integrant tant l'anàlisi dels resultats tècnics com les valoracions finals sobre el conjunt de la feina desenvolupada.

### 7.1. Fites assolides: Maquinari i viabilitat

## econòmica

Des de la perspectiva del maquinari, s'ha aconseguit aixecar una infraestructura física robusta amb una despesa final de 295,54 €. Aquesta xifra se situa per sota del topall de 400 € fixat al pressupost inicial, un èxit que respon directament a l'estratègia de combinar components reciclats (placa base, un processador Intel Core i3-7100, RAM DDR4 i unitats SSD) amb l'adquisició de cinc discs durs mecànics d'1 TB, al mercat de segona mà, per només 85 €.

Si posem aquest cost en perspectiva amb els models de subscripció a plataformes com Google Drive o Dropbox (on les quotes ballen entre 1 € i més de 17 € al mes), queda clar que construir un entorn privat amb redundància és una opció molt competitiva a llarg termini. Tota aquesta informació s'emmagatzema sota una arquitectura ZFS configurada en RAIDZ2 sobre un conjunt de sis discs durs. Aquest sistema d'emmagatzematge garanteix la supervivència de les dades davant la fallada crítica de dos dels discs, i n'assegura la integritat constant mitjançant la comprovació automàtica per checksum.

## 7.2. Fites assolides: Programari i ecosistema mòbil

El veritable eix vertebrador d'aquest treball ha estat la capa de programari. S'ha programat una aplicació nativa per a Android fent ús del llenguatge Kotlin, orquestrada sota l'arquitectura MVVM i dissenyada visualment amb Jetpack Compose. Aquest client mòbil no té res a envejar a eines consolidades com Synology Photos o Immich, amb el gran avantatge de ser codi de propietat que no depèn de cap fabricant ni depara costos ocults de llicència.

Durant la recta final del projecte, el programari ha madurat substancialment. La implementació d'un motor de còpia de seguretat totalment automatitzat, (capaç de discernir entre fotografies, vídeos, documents i contactes), tanca la premissa fonamental del treball: oferir un servei desatès a l'usuari. Així mateix, l'autenticació gestionada mitjançant el protocol OAuth2 amb tokens JWT, combinada amb la recent introducció de rols d'administració, blinden l'accés a les dades.

La interacció amb el NAS des de l'exterior, s'ha resolt integrant Tailscale (una solució basada en el protocol WireGuard) com a VPN de tipus mesh. Aquesta elecció tècnica esquivava la feixuga necessitat d'obrir ports a l'encaminador domèstic i xifra la informació de punta a punta, un plantejament que s'alinea a la perfecció amb els estàndards actuals de connexió remota sense configuració, (l'anomenat zero-config remote access), que avui dia s'apliquen en entorns empresarials.

## 7.3. Eines de manteniment i diagnòstic integrades

Mantenir l'operativitat contínua del servidor exigeix rutines de supervisió proactives, de les quals se n'han consolidat tres de fonamentals en la versió definitiva.

En primer lloc, la integritat de les dades es garanteix mitjançant l'escombrat natiu (scrub) de ZFS. Aquesta utilitat s'ha programat directament a Linux, com una tasca au-

tomatitzada d'execució diària, que verifica els checksums en segon pla per localitzar i reparar qualsevol indici de corrupció silenciosa. En segon lloc, s'ha implementat un mòdul de registres (logs) centralitzat que unifica els esdeveniments del client Android i del backend del NAS. Aquest historial conjunt simplifica enormement l'auditoria, per atorgar traçabilitat absoluta sobre connexions de xarxa, transferències i alertes.

Aquestes utilitats de fons es complementen amb el pànel de monitoratge en temps real de l'aplicació, el qual permet avaluar visualment l'estrès de la CPU, l'ús de la RAM, l'estat tèrmic i la ventilació. Amb els blocs crítics coberts, queden com a línies de continuació naturals l'automatització dels snapshots de ZFS amb polítiques de retenció i l'anàlisi SMART[32] profund dels discs mecànics.

## 7.4. Justificació tecnològica i metodologia

Fent balanç de les tecnologies utilitzades per assolir aquests resultats, (Debian Linux, FastAPI, Retrofit2, Kotlin, Tailscale i ZFS), podem afirmar que la construcció d'aquest ecosistema s'ha mantingut completament dins de l'abast dels recursos estàndard de programari lliure. Totes elles disposen d'un ampli suport de la comunitat.

Un encert metodològic clau va ser l'aixecament d'un prototip en una màquina virtual abans de comprar cap peça. Aquest pas previ ha evitat malbaratar diners i ha disminuït dràsticament el risc tècnic a l'hora de traslladar el programari al maquinari físic. El seguiment del projecte, mitjançant un model seqüencial o en cascada (waterfall), s'ha demostrat idoni per a una feina unipersonal amb dependències tecnològiques tan paleses, per tal de facilitar el control i la correcció d'errades fase per fase.

## 7.5. Línies de continuació i treball futur

Tot projecte de programari és susceptible a millores constants. Malgrat que les capacitats prioritàries s'han assolit, s'hi han detectat diversos camins per continuar evolucionant el sistema en futures iteracions:

- Reforç de la capa de seguretat: Tot i que actualment s'utilitza un hash robust combinant SHA-256 i Bcrypt, una evolució natural seria la implementació d'autenticació multifactor (2FA) o l'ús de claus biomètriques mitjançant l'estàndard WebAuthn/Passkeys, per eliminar totalment la dependència de les contrasenyes tradicionals.
- Refactorització del codi font: A mesura que el projecte ha crescut, els ViewModels han acumulat massa responsabilitats. Una pròxima passa lògica seria extreure la gestió de xarxa cap a classes Repository independents, i guanyar així en escalabilitat i manteniment.
- Experiència al gestor de fitxers: S'ha d'incorporar la capacitat de previsualitzar el contingut incrustat de determinats documents, com per exemple els arxius de text o PDF, sense obligar l'usuari a descarregar-los prèviament al mòbil.

## 8. US DE LA IA GENERATIVA

Al llarg del projecte s'han fet servir eines d'intel·ligència artificial generativa com a recurs de suport en moments concrets. El seu rol ha estat similar al d'un interlocutor tècnic: ajudar a desencallar dubtes puntuals, contrastar possibles solucions, revisar fragments de codi i polir algunes parts del text per millorar-ne la llegibilitat.

Tant l'arquitectura del sistema com les eleccions tecnològiques, la implementació i les conclusions d'aquest treball responen a un procés de reflexió i aprenentatge propi. El material generat per aquestes eines sempre ha estat revisat, contrastat i adaptat abans d'incorporar-s'hi qualsevol element, sense substituir en cap cas el criteri ni la comprensió tècnica.

## 9. AGRAÏMENTS

Vull expressar el meu agraïment al tutor del treball pel seguiment realitzat al llarg de tot el projecte, per l'orientació aportada en els moments clau i per ajudar a enfocar correctament tant la part tècnica com la part escrita de la memòria.

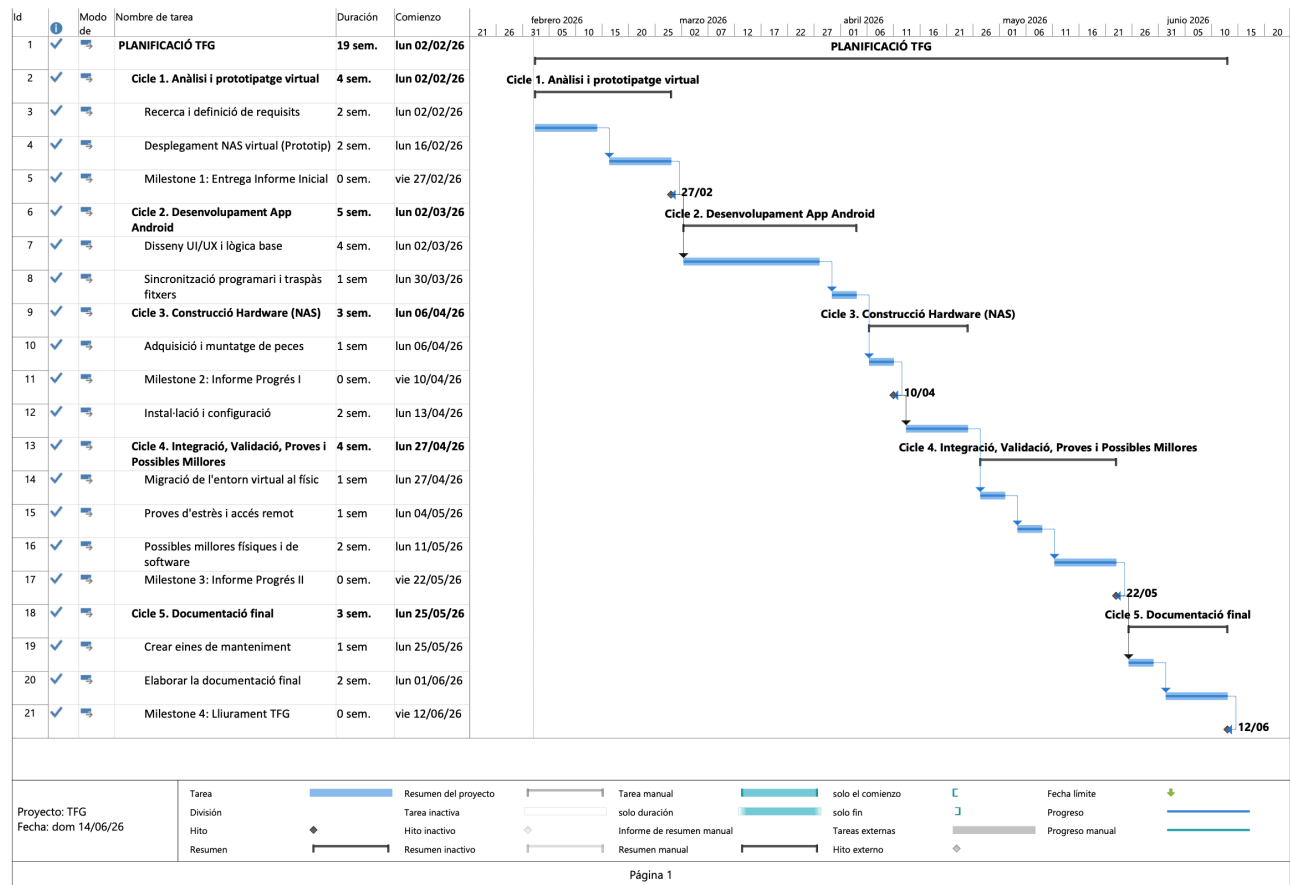
I també vull agrair el suport constant de la meua família i de la meua parella, tant en l'àmbit personal com en el moral, durant tot el desenvolupament del treball. L'ur paciència i recolzament han estat fonamentals per mantenir la constància necessària fins arribar a aquest punt.

## BIBLIOGRAFIA

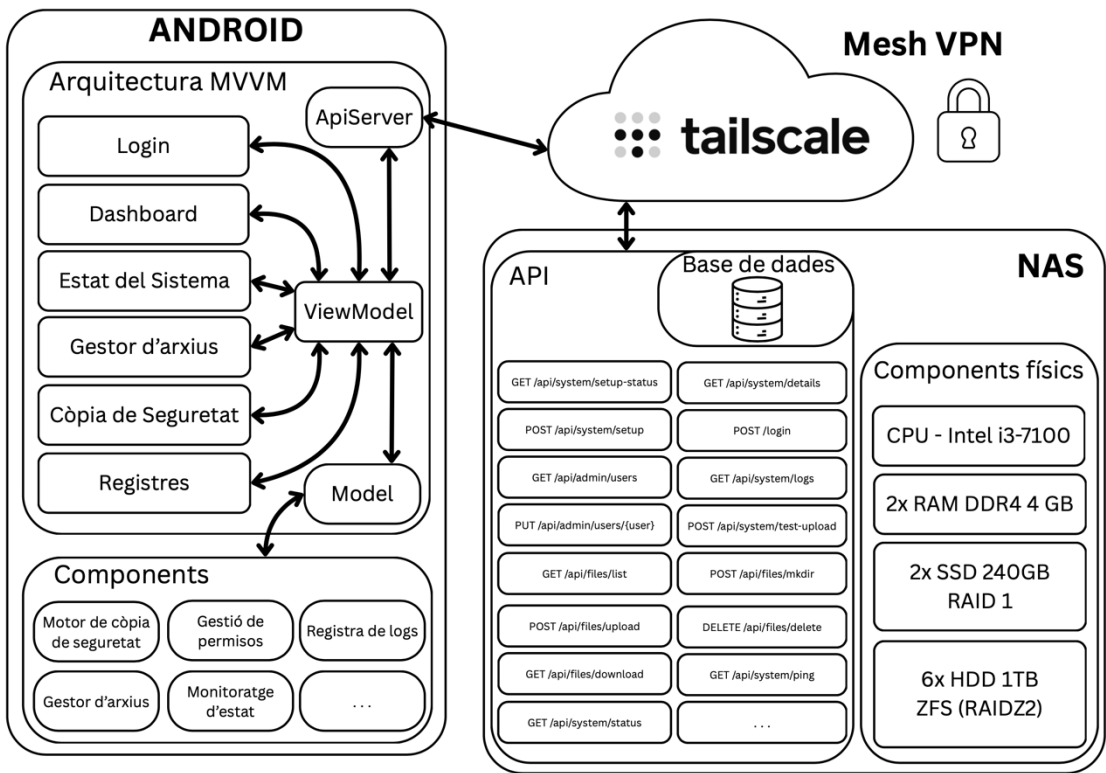
- [1] V. Kumar, "Making 'Freemium' Work," Harvard Business Review, vol. 92, no. 5, pp. 27–29, May 2014.
- [2] G. A. Gibson and R. Van Meter, "Network Attached Storage Architecture," Communications of the ACM, vol. 43, no. 11, pp. 37–45, Nov. 2000. doi: 10.1145/353360.353362
- [3] VEEAM, "La regla de backup 3-2-1," VEEAM Blog. [En línia]. Disponible a: <https://www.veeam.com/blog/es/321-backup-rule.html> [Accedit: març de 2026].
- [4] IBM, "RAID (Redundant Array of Independent Disks)," IBM Documentation. [En línia]. Disponible a: <https://www.ibm.com/docs/en/ds8900/9.3.0?topic=config-ration-raid-implementation> [Accedit: abril de 2026].
- [5] M. Castaneda, "VPN vs Mesh: Microsegmentación," Marcelo Castaneda. [En línia]. Disponible a: <https://marcelocastaneda.com/vpn-vs-mesh-microsegmentacion/> [Accedit: juny de 2026].
- [6] Tailscale, "How Tailscale works," Tailscale Docs, 2020. [En línia]. Disponible a: <https://tailscale.com/blog/how-tailscale-works> [Accedit: juny de 2026].
- [7] WireGuard Project, "WireGuard: conceptual overview," WireGuard, 2023. [En línia]. Disponible a: <https://www.wireguard.com> [Accedit: juny de 2026].
- [8] Google LLC, "Google Drive Storage Plans," Google Support. [En línia]. Disponible a: <https://support.google.com/drive/answer/2375123> [Accedit: abril de 2026].
- [9] Apple Inc., "iCloud+ plans and pricing," Apple Support. [En línia]. Disponible a: <https://support.apple.com/en-us/108047> [Accedit: abril de 2026].
- [10] Microsoft, "Microsoft OneDrive Plans," Microsoft Support. [En línia]. Disponible a: <https://www.microsoft.com/en-us/microsoft-365/onedrive/compare-onedrive-plans> [Accedit: abril de 2026].
- [11] Dropbox, "Dropbox Plans and Pricing," [En línia]. Disponible a: <https://www.dropbox.com/plans> [Accedit: abril de 2026].
- [12] E. Mollakuqe, E. Hamdiu, N. Santuri Fishekqiu, S. Jakupi i J. Qarkaxhija, "Comparison of cloud storage in terms of privacy and personal data - Sync, pCloud, IceDrive and Egnyte," Open Research Europe, vol. 4, no. 128, juny 2024. [En línia]. Disponible a: <https://open-research-europe.ec.europa.eu/articles/4-128> [Accedit: juny de 2026].
- [13] European Commission, "Strengthening Europe's Tech Sovereignty," Shaping Europe's Digital Future. [En línia]. Disponible a: <https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty> [Accedit: abril de 2026].
- [14] Synology Inc., "DiskStation Manager (DSM) Overview," Synology Knowledge Center. [En línia]. Disponible a: <https://www.synology.com/en-global/dsm> [Accedit: abril de 2026].
- [15] Synology Inc., "What is Synology Hybrid RAID (SHR)?," Synology Knowledge Center. [En línia]. Disponible a: [https://kb.synology.com/en-global/DSM/tutorial/What is Synology Hybrid RAID SHR](https://kb.synology.com/en-global/DSM/tutorial/What%20is%20Synology%20Hybrid%20RAID%20SHR) [Accedit: abril de 2026].
- [16] Synology Inc., "Hard Drive Compatibility List," Synology Support. [En línia]. Disponible a: <https://www.synology.com/en-global/compatibility> [Accedit: abril de 2026].
- [17] iXsystems, "Hardware Recommendations for TrueNAS/ZFS," TrueNAS Documentation Hub [En línia]. Disponible a: <https://www.truenas.com/docs/core/gettingstarted/core-hardwareguide> [Accedit: abril de 2026].
- [18] QNAP Systems, Inc., "QuTS hero Operating System," QNAP. [En línia]. Disponible a: <https://www.qnap.com/en/operating-system/qu-ts-hero> [Accedit: juny de 2026].
- [19] Nextcloud GmbH, "Nextcloud - The On-Premises Content Collaboration Platform." [En línia]. Disponible a: <https://nextcloud.com/> [Accedit: abril de 2026].
- [20] Immich Contributors, "Immich - Self-hosted photo and video backup solution," GitHub. [En línia]. Disponible a: <https://github.com/immich-app/immich> [Accedit: abril de 2026].
- [21] W. W. Royce, "Managing the Development of Large Software Systems," in Proc. IEEE WESCON, Los Angeles, CA, USA, Aug. 1970, vol. 26, pp. 1–9.
- [22] OpenZFS Documentation, "ZFS Pool Concepts: RAIDZ," OpenZFS Project. [En línia]. Disponible a: <https://openzfs.github.io/openzfs-docs/man/master/7/zpool-concepts.7.html> [Accedit: 29-jun-2026].
- [23] A. Pompei, "SnapRAID - Backup for Disk Arrays," SnapRAID Documentation. [En línia]. Disponible a: <https://www.snapraid.it> [Accedit: abril de 2026].
- [24] ENISA, "ENISA Threat Landscape 2023 – Ransomware," European Union Agency for Cybersecurity, 2023. [En línia]. Disponible a: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023> [Accedit: abril de 2026].
- [25] R. T. Fielding, "Architectural Styles and the Design of Network-based Software Architectures," Ph.D. dissertation, Univ. of California, Irvine, 2000. [En línia]. Disponible a: <https://ics.uci.edu/~fielding/pubs/dissertation/top.htm> [Accedit: abril de 2026].
- [26] A. Syromiatnikov and D. Weyns, "A Journey through the Land of Model-View-Design Patterns," in Proc. IEEE Int. Conf. Software Architecture Workshops (ICSAW), Sydney, Australia, 2014, pp. 21–28. doi: 10.1109/ICSAW.2014.13
- [27] M. Jones, J. Bradley and N. Sakimura, "JSON Web Token (JWT)," IETF, RFC 7519, May 2015. [En línia]. Disponible a: <https://datatracker.ietf.org/doc/html/rfc7519> [Accedit: abril de 2026].
- [28] S. Ramírez, "FastAPI," Tiangolo. [En línia]. Disponible a: <https://fastapi.tiangolo.com/> [Accedit: juny de 2026].
- [29] D. Hardt, Ed., "The OAuth 2.0 Authorization Framework," IETF, RFC 6749, Oct. 2012. [En línia]. Disponible a: <https://datatracker.ietf.org/doc/html/rfc6749> [Accedit: abril de 2026].
- [30] OWASP Foundation, "Path Traversal," OWASP Top 10 – A01:2021 Broken Access Control. [En línia]. Disponible a: [https://owasp.org/www-community/attacks/Path\\_Traversal](https://owasp.org/www-community/attacks/Path_Traversal) [Accedit: març de 2026].
- [31] A. P. Felt, E. Chin, S. Hanna, D. Song and D. Wagner, "Android Permissions Demystified," in Proc. 18th ACM Conf. Computer Commun. Security (CCS '11), Chicago, IL, USA, 2011, pp. 627–638. doi: 10.1145/2046707.2046779
- [32] A. Klein, "What S.M.A.R.T. Stats Tell Us About Hard Drives," Backblaze Blog, Oct. 2016. [En línia]. Disponible a: <https://www.backblaze.com/blog/what-smart-stats-indicate-hard-drive-failures> [Accedit: abril de 2026].

APÈNDIX

A. DIAGRAMA DE GANTT



B. Diagrama de l'arquitectura del sistema



C. PRESSUPOST DETALLAT

RESUM ECONÒMIC

Desglossament del pressupost dels components físics del TFG

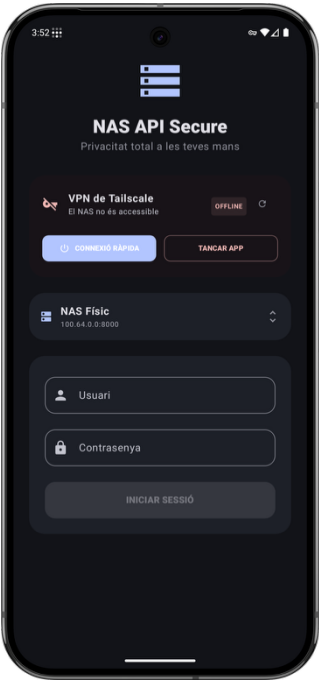
| Component                        | Tipus       | Preu unitari | Quantitat | Total   |
|----------------------------------|-------------|--------------|-----------|---------|
| Caixa Aerocool Visor ATX RGB     | NOU         | 86,74 €      | 1         | 86,74 € |
| Font Tacens Radix Eco X 750 W    | NOU         | 43,21 €      | 1         | 43,21 € |
| Safata / bracket de discs 5,25"  | NOU         | 27,59 €      | 1         | 27,59 € |
| Adaptador / connector SATA       | NOU         | 4,37 €       | 1         | 4,37 €  |
| Targeta expansora PCIe SATA      | NOU         | 18,99 €      | 1         | 18,99 € |
| Cintes de subjecció i cablejat   | NOU         | 7,99 €       | 2         | 15,98 € |
| HDD 1 TB                         | 2a mà       | 17,00 €      | 5         | 85,00 € |
| Placa base Gigabyte GA-H110M-DS2 | Reutilitzat | 0,00 €       | 1         | 0,00 €  |
| 4 GB RAM DDR4                    | Reutilitzat | 0,00 €       | 2         | 0,00 €  |
| HDD 1 TB                         | Reutilitzat | 0,00 €       | 1         | 0,00 €  |
| SSD 240 GB                       | Reutilitzat | 0,00 €       | 2         | 0,00 €  |
| Processador Intel Core i3-7100   | Reutilitzat | 0,00 €       | 1         | 0,00 €  |
| HDD 1 TB                         | Reutilitzat | 0,00 €       | 1         | 0,00 €  |

| RESUM FINANCER             |          |
|----------------------------|----------|
| Subtotal Components        | 281,88 € |
| Enviament (Productes Nous) | 5,98 €   |
| Enviament (Segona Mà)      | 7,68 €   |
| COST TOTAL GENERAL         | 295,54 € |

| CONTROL DE PRESSUPOST ASSIGNAT  |          |
|---------------------------------|----------|
| Pressupost Inicial Assignat     | 400,00 € |
| (-) Despeses Totals Realitzades | 295,54 € |
| ESTALVI NET ACONSEGUIT          | 104,46 € |

D. CAPTURES DE PANTALLA DE L'APLICACIÓ

C1. LOGIN



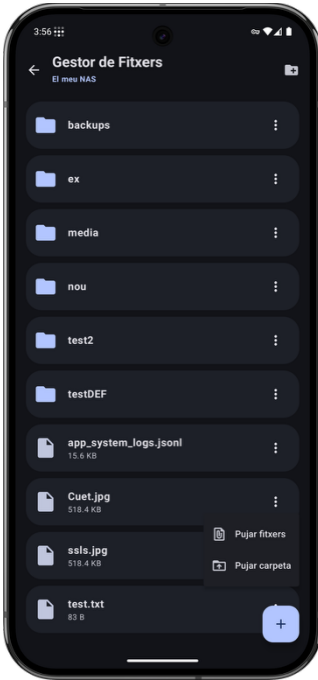
C2. DASHBOARD



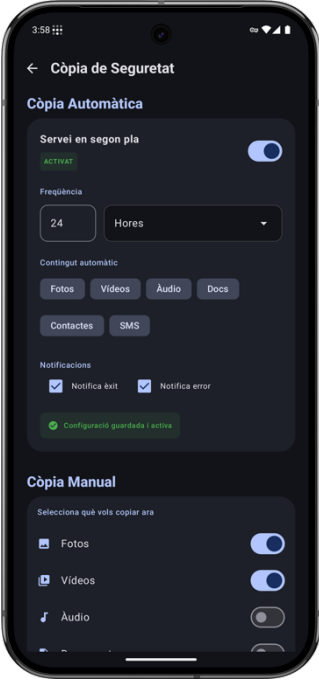
C3. DETALLS DEL SISTEMA



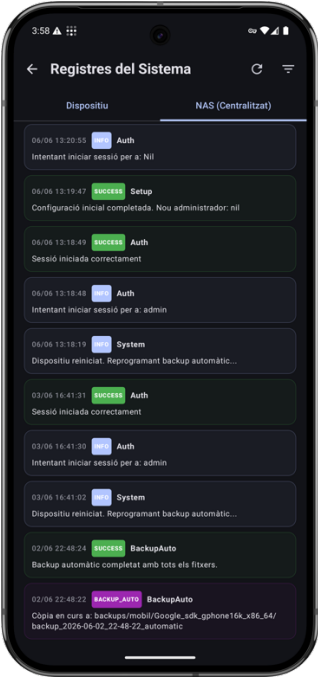
C4. GESTOR DE FITXERS



C5. GESTOR CÒPIES



C6. LOGS SISTEMA



C7. GESTIÓ D'USUARIS

