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

Antúnez González, Arnau. *Proof of Concept d'un model híbrid de gestió d'identitat corporativa amb dades sintètiques*. Treball de Final de Grau (Universitat Autònoma de Barcelona), 2025 (Enginyeria Informàtica)

This version is available at <https://ddd.uab.cat/record/334361>

under the terms of the  license.

Proof of Concept d'un model híbrid de gestió d'identitat corporativa amb dades sintètiques

Arnau Antúnez González

Resum— Els sistemes de gestió d'identitats estan evolucionant d'infraestructures on-premise cap a entorns distribuïts i serveis al núvol. Davant la retirada del suport de Microsoft Identity Manager el 2029, aquest treball presenta, en col·laboració amb Grupo Catalana Occidente, una Proof of Concept d'un motor híbrid de gestió d'identitats corporatives com a alternativa a les solucions comercials. La proposta replica funcionalitats clau dels sistemes IAM, com la font d'autoritat única, el provisionament automàtic i la reconciliació autoritativa, mitjançant scripts PowerShell sobre una arquitectura híbrida d'Active Directory i Microsoft Entra ID. El sistema, desplegat en un entorn de laboratori amb dades sintètiques, gestiona el cicle de vida complet de la identitat a partir d'una base de dades de Recursos Humans. Els resultats obtinguts mostren que el model és tècnicament viable, tot identificant-ne les limitacions.

Paraules clau— Gestió d'identitats i accessos (IAM), Active Directory, Microsoft Entra ID, model híbrid, PowerShell, reconciliació autoritativa, cicle de vida de la identitat, dades sintètiques.

Abstract— Identity management systems are evolving from on-premise infrastructures towards distributed environments and cloud services. In view of the withdrawal of support for Microsoft Identity Manager in 2029, this work presents, in collaboration with Grupo Catalana Occidente, a Proof of Concept of a hybrid engine for corporate identity management as an alternative to commercial solutions. The proposal replicates key functionalities of IAM systems, such as the single source of authority, automatic provisioning and authoritative reconciliation, through PowerShell scripts on a hybrid architecture based on Active Directory and Microsoft Entra ID. The system, deployed in a laboratory environment with synthetic data, manages the complete identity lifecycle from a Human Resources database. The results obtained show that the model is technically viable, while also identifying its limitations.

Keywords— Identity and Access Management (IAM), Active Directory, Microsoft Entra ID, hybrid model, PowerShell, authoritative reconciliation, identity lifecycle, synthetic data.

1 INTRODUCCIÓ - CONTEXT DEL TREBALL

AVUI en dia, la gestió de la identitat i de l'accés, també coneguda com IAM (Identity and Access Management), és un element indispensable per garantir la seguretat i el correcte funcionament del sistema en grans organitzacions independentment del seu àmbit d'activitat[1]. Tradicionalment, la gran majoria d'organitzacions han basat la seva infraestructura d'identitat en so-

lucions totalment on-premise, com per exemple Active Directory, ja que proporcionen un control directe sobre l'emmagatzematge i l'ús de les dades, d'un menor cost a llarg termini i més control sobre la seguretat per complir requisits interns i normatius [2]. Tanmateix, aquest model també presenta limitacions en entorns distribuïts, dificultats d'escalabilitat i més complexitat d'integració amb serveis cloud [3].

L'evolució cap a entorns distribuïts i l'adopció constant de serveis al núvol, ha impulsat un canvi de paradigma en l'arquitectura dels sistemes d'identitat [2]. Alguns dels principals proveïdors tecnològics, com Microsoft, orienten la seva estratègia cap a models híbrids o *Cloud-first* [4], reduint progressivament la rellevància de les solucions on-premise, com és el cas de Microsoft Identity Manager (MIM), el qual deixa de tenir suport l'any 2029 [5]. Aquest

• E-mail de contacte: arnau.antunez@autonoma.cat
 • Menció: Tecnologies de la Informació
 • Treball tutoritzat per: David Alegre Alarza (Àrea de Ciències de la Computació i Intel·ligència Artificial)
 • Curs 2025/26

procés no només planteja reptes tècnics, ja que la coexistència de múltiples dominis, la heterogeneïtat dels models de confiança (dominis tradicionals, federació, tokens signats) i les dependències entre plataformes amb enfocaments diferents afegeixen una complexitat arquitectònica considerable. En aquest context, definir i validar un model híbrid que asseguri la interoperabilitat, l'escalabilitat i la seguretat, tot mantenint el control sobre les identitats corporatives, resulta imprescindible [6].

El present Treball de Final de Grau es desenvolupa en col·laboració amb Grupo Catalana Occidente (GCO), empresa que actualment basa la seva arquitectura d'identitat en Microsoft Identity Manager (MIM), juntament amb una integració parcial amb Microsoft Entra ID mitjançant els components Microsoft Cloud Sync i Entra Connect. Aquest enfocament planteja un model híbrid on el motor de la identitat resideix a la infraestructura local de l'empresa. Davant la retirada progressiva del suport de MIM i la tendència del mercat cap a models *Cloud-first*, resulta necessari analitzar la infraestructura de la identitat actual i explorar alternatives que permetin avaluar la viabilitat tècnica i funcional per dur a terme una transició cap a un model híbrid més alineat amb les arquitectures modernes. Aquesta transició no només implica un canvi tecnològic, sinó també la validació dels fluxos d'aprovisionament, desprovisionament i sincronització entre entorns on-premise i cloud.

Amb aquesta finalitat, aquest treball defineix una Proof of Concept (PoC) en un entorn aïllat de laboratori dins la infraestructura de l'empresa. L'escenari proposat reproduïx un model híbrid de gestió d'identitats en què una base de dades de Recursos Humans, alimentada amb dades sintètiques, actua com a font acreditada de la identitat, permetent validar els mecanismes d'integració, sincronització i govern de les identitats entre els diferents components de la solució.

2 OBJECTIUS

El treball té com a objectiu principal dissenyar i implementar una Proof of Concept (PoC) que permeti simular un model de gestió d'identitat híbrid en un entorn controlat amb la finalitat d'analitzar-ne el comportament operatiu, identificar avantatges i limitacions i extreure conclusions tècniques que puguin orientar futures decisions estratègiques relatives a la modernització de la infraestructura d'identitat corporativa. Per assolir aquest objectiu es plantegen els objectius específics següents:

- Dissenyar una arquitectura IAM híbrida basada en *Active Directory* i Microsoft Entra ID.
- Implementar un entorn de laboratori amb una base de dades de Recursos Humans, un servidor d'execució dels scripts PowerShell i una OU dedicada a la gestió d'identitats.
- Avaluar els processos d'alta, modificació, baixa, reactivació i reconciliació d'identitats.
- Analitzar el comportament, la viabilitat, els avantatges i les limitacions del motor desenvolupat en un entorn corporatiu híbrid.

Recalcar que el projecte no contempla la migració completa d'un entorn productiu, ni la implementació en alta disponibilitat o amb garanties de nivell empresarial, sinó el desenvolupament d'una prova de concepte en un entorn controlat. Les consideracions de seguretat s'analitzaran des d'un punt de vista conceptual i d'avaluació de riscos, però no s'implementaran mecanismes avançats de protecció ni configuracions pròpies d'un entorn productiu.

3 ESTAT DE L'ART

Actualment, el mercat de la gestió d'identitat i accés (IAM) està dominat per diverses plataformes empresarials que integren funcionalitats d'autenticació, federació i governança del cicle de vida de les identitats [7]. Dins d'aquest àmbit, es poden distingir dos grans enfocaments: les solucions d'*Access Management*, orientades principalment al control d'accés i l'autenticació, i les plataformes d'*Identity Governance and Administration* (IGA), enfocades a la supervisió i gestió dels permisos al llarg del temps [8].

Entre les plataformes més utilitzades a escala corporativa destaquen Microsoft Entra ID [9], SailPoint [10], Okta [11] i One Identity [12] [13]. Microsoft Entra ID i Okta estan orientades principalment a l'*Access Management*, proporcionant serveis com autenticació, federació d'identitats, *Single Sign-On* (SSO), autenticació multifactor (MFA) i control d'accés condicional. Aquestes plataformes destaquen especialment per la seva orientació cap a entorns cloud i multi-cloud, així com per la seva capacitat d'integració amb aplicacions SaaS [14].

En canvi, SailPoint i One Identity s'emmarquen dins l'àmbit de l'IGA, ja que ofereixen funcionalitats orientades a la gestió integral del cicle de vida de les identitats, incloent mecanismes d'aprovisionament i desaprovisionament automatitzats, certificacions periòdiques d'accés i eines enfocades al compliment normatiu. Tot i que la seva implementació acostuma a ser més complexa, proporcionen un major nivell de control i traçabilitat sobre els accessos corporatius [15], [16].

4 METODOLOGIA

La construcció del sistema s'ha dut a terme mitjançant una metodologia iterativa basada en components, implementant i validant progressivament cadascun dels scripts abans de passar al següent. Aquesta aproximació és especialment adequada per a sistemes fortament interconnectats, on un error de disseny primerenc pot tenir efectes en cadena sobre el conjunt. A més, ha permès detectar errades introduïdes per components nous que afectaven funcionalitats ja implementades i validades, de manera que cada iteració no només aportava noves capacitats al motor sinó que també consolidava i refinava les existents. El projecte s'ha estructurat en quatre fases seqüencials.

La primera fase, d'anàlisi i investigació, ha comprès l'estudi de l'estat de l'art de la gestió d'identitats híbrides, la identificació de requisits i l'avaluació de solucions existents al mercat. La segona fase, de disseny, ha inclòs la definició de l'arquitectura híbrida, el disseny de les principals taules SQL i els seus atributs, el disseny de l'estructura de l'OU per al treball i l'estructura i fluxos del motor personalitzat.

A la fase de desenvolupament i validació, s'ha cobert la configuració de l'entorn de laboratori, la generació d'una base de dades de recursos humans sintètica, la implementació de la integració entre Active Directory i cloud mitjançant Microsoft Cloud Sync, la implementació dels scripts del motor, la integració i orquestració de tots els components, i l'execució de proves funcionals, de casos límit i de tolerància a errors. Finalment, la quarta fase ha comprès l'anàlisi dels resultats, la valoració del grau d'assoliment dels objectius i la identificació de limitacions i línies futures de treball.

5 DISSENY DEL SISTEMA

5.1 Principis de disseny

El desenvolupament de la PoC es guia per un conjunt de principis tècnics que s'han definit amb l'ajuda del tutor de l'empresa. Aquests orienten totes les decisions de disseny preses. El primer, i més important, és el principi de font d'autoritat única. Aquest estableix que la font d'autoritat és sempre HR_EMPLOYEES. Qualsevol divergència entre la base de dades i l'Active Directory es resol sempre a favor de la base de dades, mai al revés. Tota la metodologia de desenvolupament s'ha dissenyat per preservar i garantir aquest principi en cada component del sistema.

El segon principi és la separació de responsabilitats. Cada script té una funció molt concreta: *Get-Data.ps1* s'encarrega de llegir les dades, *Compare-Snapshots.ps1* detecta els canvis, els scripts de provisioning actuen sobre l'AD i l'*Orchestrator.ps1* coordina tot el flux. Aquesta separació no només fa que el sistema sigui més ordenat, sinó que també facilita reutilitzar components i poder provar cada part de manera independent. A més, ajuda a evitar que un error en un punt concret acabi afectant la resta del sistema.

El tercer principi és la idempotència, entesa com la capacitat d'un script d'executar-se repetidament sense provocar efectes no desitjats o esperats. Per exemple, si un compte ja existeix a l'AD, l'script d'altres ha de ser capaç de detectar-ho i, simplement, informar que aquell usuari ja existeix i que, per tant, no és necessari proveir-lo novament. Aquesta propietat és clau per garantir que el sistema es pot recuperar fàcilment davant d'errors parcials, sense haver de fer intervencions manuals de manera recurrent.

El quart principi és l'externalització de la configuració. Els valors configurables, com el domini, el mapa d'OUS, els "paths" de fitxers o les credencials, no es defineixen directament dins dels scripts, sinó que es centralitzen en un únic fitxer anomenat *config.json*. D'aquesta manera, si cal adaptar el sistema a un altre entorn, només cal modificar aquest fitxer, sense haver de tocar tots els scripts.

El cinquè principi és la traçabilitat, que estableix que totes les operacions executades pel sistema han de quedar registrades en un fitxer de log, estructurat en carpetes per dia. Cada fitxer *.log* inclou el seu timestamp, el nom de l'script que l'ha generat, el nivell de gravetat dels missatges que conté i el detall necessari per entendre què ha passat i, si cal, poder reproduir o auditar l'acció. En el cas concret de les modificacions d'atributs, el log registra tant el valor anterior, com el nou valor de cada camp modificat, facilitant el seguiment dels canvis produïts.

5.2 Estructura del sistema

Des d'un punt de vista estructural, el sistema es desplega sobre dos servidors amb responsabilitats clarament diferenciades: el servidor *narya*, que allotja la base de dades SQL Server i constitueix la font d'autoritat de les identitats, i el servidor *evileye*, que actua com a motor IAM i executa tots els scripts PowerShell. Les tasques s'han organitzat en dos blocs principals, on els resultats de cada tasca, en molts casos, són els prerequisits de la següent.

A continuació, la Figura 1 representa el disseny a nivell general de la PoC, amb els servidors SQL *narya* i *evileye*.

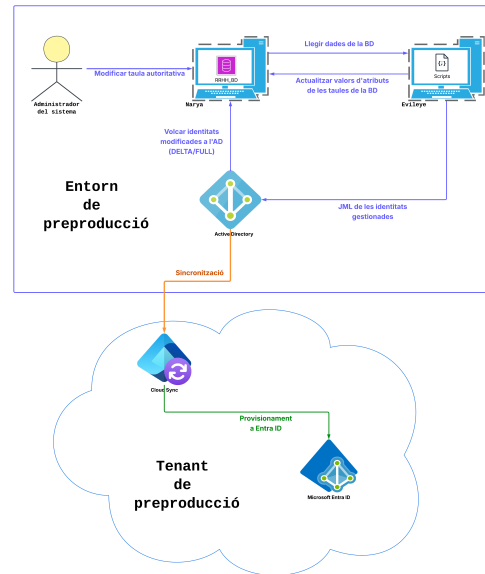


Fig. 1: Diagrama del disseny general de la PoC.

5.2.1 Narya

El primer bloc comprèn totes les tasques que afecten el servidor *narya*. Aquestes tasques defineixen l'estructura de dades sobre la qual descansa tot el sistema i han de ser completades i validades abans de passar al bloc de scripts.

Creació de taules: En aquesta primera tasca, es defineixen i creen totes les taules necessàries. Cada taula té una funció específica dins de l'arquitectura del sistema i la seva estructura reflecteix la separació de responsabilitats entre la capa de RRHH i la del motor IAM.

La taula HR_EMPLOYEES és la taula principal del sistema i actua com a font d'autoritat de totes les identitats corporatives. Conté els atributs que provenen del sistema simulat de recursos humans, com ara dades personals, organitzatives, de contacte i de localització, així com els camps que el motor IAM construeix i manté durant el cicle de provisioning, com el *displayName*, el *mail* o el *userPrincipalName*. El camp *Status* implementa una màquina d'estats que l'*Orchestrator.ps1* consulta en cada execució per determinar quina acció ha d'aplicar sobre cada identitat. El valor *Pending* és per a les altes pendents de crear a l'AD, *Active* per a l'estat nominal d'un compte actiu, *PendingUpdate* per a les modificacions detectades per *Compare-Snapshots.ps1*, *PendingSync* per a les divergències detectades per *Invoke-Reconciliation.ps1*,

PendingDeprovisioning per a les baixes sol·licitades però encara no executades, i Disabled per a les baixes confirmades, a més dels estats d'error que activen el reintent automàtic en el proper cicle.

HR_EMPLOYEES_SNAPSHOT és una còpia idèntica de HR_EMPLOYEES que preserva l'estat de la taula principal al final de cada iteració. La comparació entre les dues taules és el mecanisme central de detecció de canvis del sistema. Qualsevol diferència entre l'estat actual i l'estat anterior es tradueix en una acció de provisioning concreta.

AD_EMPLOYEES actua com a mirall SQL de l'estat actual de l'Active Directory. El seu contingut s'actualitza periòdicament a través del procés d'importació de deltes, o full quan s'especifica, i és la taula que utilitza la capa de reconciliació per comparar l'estat real del directori amb la font d'autoritat. AD_IMPORT_CONTROL emmagatzema el "watermark" de l'última importació de l'AD, és a dir, l'últim "timestamp" que indica quan s'han processat canvis al directori. Aquesta taula permet al procés d'importació determinar quin filtre aplicar en cada execució, recuperant únicament els objectes modificats des de l'última consulta.

SQL Server Agent Job: La segona tasca d'aquest bloc és la configuració del SQL Server Agent mitjançant una tasca que s'encarrega d'actualitzar diàriament la taula HR_EMPLOYEES_SNAPSHOT amb el contingut del dia anterior de la taula HR_EMPLOYEES. És necessari per a la detecció de canvis.

5.2.2 Evileye

El segon bloc comprèn totes les tasques que afecten el servidor *evileye*, on resideix el motor IAM. Les tasques d'aquest bloc s'organitzen en quatre paquets funcionals: la capa de mòduls comuns, la capa de lectura i detecció de canvis, la capa de provisioning JML, i la capa de reconciliació autoritativa.

Mòduls comuns: El primer paquet estableix la infraestructura compartida que utilitzen tots els scripts del sistema, importada per dot-sourcing en cada component.

Logging.ps1 proporciona la funció Write-ProvLog, que escriu entrades al log amb timestamp, mòdul d'origen i nivell de gravetat. El sistema de logging s'organitza en carpetes per dia i fitxers per mòdul, facilitant el diagnòstic per data i per component.

Database.ps1 conté les funcions Set-HRStatus i Update-HREmployee, que gestionen totes les escriptures de tornada a la taula HR_EMPLOYEES.

Directory.ps1 conté Get-OUTarget, que deriva l'OU de destinació d'un compte a partir de la combinació de company i department consultant el mapa ADOUs del *config.json*, i ShouldUpdate, que normalitza i compara valors entre la base de dades i l'AD per determinar si un atribut requereix actualització.

Utils.ps1 conté ConvertTo-ASCIIName, que normalitza cadenes de text eliminant accents i caràcters especials per construir els atributs de compte com el *mail*.

Lectura i detecció de canvis: El segon paquet constitueix el punt d'entrada del flux diari de provisioning. **Get-Data.ps1** llegeix HR_EMPLOYEES o

HR_EMPLOYEES_SNAPSHOT i retorna un array de PSCustomObjects normalitzats, incorporant una validació que atura el procés si la consulta retorna zero registres. **Compare-Snapshots.ps1** compara l'estat actual amb l'snapshot anterior per detectar altes i modificacions, actualitzant el camp *Status* de cada usuari afectat a HR_EMPLOYEES perquè l'orquestrador determini quina acció executar.

Provisionament JML: El tercer paquet implementa el cicle de vida de les identitats mitjançant scripts independents per a cada operació. **ADProvisioning.ps1** gestiona la creació de comptes a l'AD a partir de registres amb Pending. **ADUpdater.ps1** gestiona l'actualització d'atributs i canvis d'OU a partir de registres amb PendingUpdate o PendingSync, incloent la reactivació de comptes prèviament deshabilitats. **ADDeprovisioning.ps1** gestiona les baixes desactivant el compte i movent-lo a l'OU de Deshabilitats a partir de registres amb PendingDeprovisioning. Per últim, **Orchestrator.ps1** coordina l'execució seqüencial de tots els components, gestionant els reintents automàtics per als estats d'error.

Reconciliació autoritativa: Finalment, el quart paquet garanteix la consistència entre la font d'autoritat i l'AD. **DeltaImportAD.ps1** manté actualitzada la taula AD_EMPLOYEES com a mirall SQL de l'AD mitjançant un mecanisme de "watermark" que processa únicament els canvis des de l'última execució. **Invoke-Reconciliation.ps1** detecta divergències d'atributs, CN i OU entre HR_EMPLOYEES i AD_EMPLOYEES, marcant els usuaris afectats amb PendingSync perquè l'orquestrador apliqui la correcció en el cicle següent.

5.3 Decisions de disseny

Al llarg del desenvolupament s'han pres diverses decisions de disseny que mereixen ser explicades a causa de la seva rellevància. La primera és l'ús de PSCustomObject en lloc del DataTable que retorna el driver SQL. A diferència del DataTable, el PSCustomObject permet accedir als camps amb la sintaxi habitual de PowerShell, normalitza automàticament els valors nuls i és totalment compatible amb els operadors de filtratge del pipeline.

La segona és la validació de taula buida a la lectura de dades. Si la consulta retornés zero registres, **Compare-Snapshots.ps1** interpretaria que tots els empleats han estat donats de baixa, iniciant un desproveïment massiu. La validació atura el procés immediatament si es detecten zero registres, protegint el sistema contra aquest escenari catastròfic.

La tercera és la normalització defensiva en la comparació d'atributs. La comparació directa de strings pot generar falsos positius si un valor és null i l'altre és una cadena buida, o si hi ha espais addicionals. Convertint els nuls a cadena buida i aplicant `.Trim()`, el sistema detecta únicament els canvis reals.

La quarta és l'adopció del model "soft-delete" per a les baixes. En lloc de detectar-les per absència de registre, el camp *Status* s'estableix a PendingDeprovisioning, indicant que la baixa ha estat sol·licitada però no executada. Això conserva l'historial complet de l'empleat a la base de

dades i permet revertir una baixa errònia simplement modificant el camp *Status* a la font d'autoritat.

Finalment, s'ha optat per utilitzar Microsoft Cloud Sync per a la sincronització d'identitats al núvol, a causa de les limitacions de connectivitat de l'entorn i de la disponibilitat d'un tenant de reproducció alineat amb l'entorn corporatiu.

6 PREPARACIÓ DE L'ENTORN

6.1 Desplegament de màquines virtuals

L'entorn de treball de la PoC es basa en dues màquines virtuals allotjades a la infraestructura de producció de GCO, i copiades a l'entorn de reproducció aïllat, evitant així qualsevol afectació a l'empresa. Un cop ubicades, es van configurar com a estàtiques, desvinculant-les dels processos d'actualització automàtics de la infraestructura. Aquesta decisió garanteix la reproductibilitat de les proves i assegura que totes les modificacions realitzades durant el projecte, com ara la creació de taules, scripts o comptes d'usuari a l'AD, es mantenen estables entre sessions de treball.

La primera, *narya*, actua com a servidor de base de dades executant Microsoft SQL Server. És on resideix la base de dades RRHH_BD amb les taules necessàries, les dades sintètiques i el SQL Server Agent Job. La segona, *evileye*, actua com a motor IAM i punt d'execució centralitzat de tots els scripts PowerShell, disposant del mòdul ActiveDirectory. Tots dos servidors pertanyen al domini grupocatalanaoccidente.com.

6.2 Estructura d'OUS a l'Active Directory

Un dels primers passos de la preparació de l'entorn ha estat definir l'estructura d'Unitats Organitzatives (OUS) de l'Active Directory necessàries per al projecte. Les OUS constitueixen els contenidors lògics on es crearan els comptes d'usuari, i la seva estructura determina l'aplicació de polítiques de grup (GPOs) i facilita la gestió administrativa dels comptes.

Per evitar interferències amb l'estructura d'OUS existent a l'empresa, s'ha creat una OU arrel exclusiva per al projecte, anomenada "*TFG_PE2614*", que actua com a contenidor de tot el treball. Sota aquesta OU s'han creat 3 sub-OUS, que representen tres empreses sintètiques d'un grup corporatiu: Empresa SA (amb Data, IT i RRHH), Empresa SB (amb IT i RRHH) i Empresa SC (amb IT i Logística). Addicionalment, s'ha creat una OU de Deshabilitats, destinada als comptes dels empleats donats de baixa seguint la pràctica corporativa estàndard de desactivar i moure els comptes en lloc d'eliminar-los. Tota la lògica de derivació de l'OU de destinació d'un usuari a partir dels seus atributs *company* i *department*, es gestiona dinàmicament a través del fitxer *config.json*.

6.3 Configuració centralitzada de l'entorn

Amb l'objectiu d'evitar dependències entre els scripts i l'entorn específic on s'executen, s'ha dissenyat un fitxer de configuració centralitzat en format JSON que recull tots els paràmetres variables del sistema, com el nom del servidor

SQL i la base de dades, la ruta dels logs, el domini d'Active Directory i el mapa complet de les OU. Gràcies a aquest disseny, per adaptar el sistema a un altre entorn, per exemple modificant l'estructura d'OUS, únicament cal modificar aquest fitxer.

Pel que fa a les credencials, les d'accés al servidor SQL es gestionen mitjançant el mecanisme Export-Clixml de PowerShell, que les xifra usant Windows Data Protection API (DPAPI). Aquest mecanisme vincula el fitxer resultant a l'usuari i a la màquina on ha estat creat, garantint que no pugui ser desxifrat en cap altre context.

6.4 Arquitectura i fluxos

L'arquitectura segueix el patró d'identitat híbrida de Microsoft, on l'Active Directory on-premise actua com a directori primari i font d'autoritat, mentre que Microsoft Entra ID actua com a rèplica al núvol sincronitzada.

El flux comença amb la taula HR_EMPLOYEES al servidor *narya*. Diàriament, un SQL Server Agent Job en preserva l'estat a HR_EMPLOYEES_SNAPSHOT, permetent fer la comparació per a la detecció de canvis. Després, el servidor *evileye* llegeix ambdues taules i AD_EMPLOYEES, i identifica les diferències respecte la font d'autoritat. A continuació, actualitza el camp *Status* amb el valor corresponent i executa les accions JML que pertorquen, segons el valor de *Status*, sobre l'AD. Finalment, Microsoft Cloud Sync sincronitza les identitats de l'Active Directory on-premise cap al tenant de reproducció d'Entra ID, completant el cicle de vida d'una identitat híbrida.

7 DESENVOLUPAMENT DE LA POC

En aquest apartat s'exposen els components del sistema implementats al llarg del treball. En primer lloc, es descriuen les taules SQL i, a continuació, els scripts que conformen el motor IAM.

7.1 HR_Employees

És la taula principal del sistema, la qual actua com a font d'autoritat i conté l'estat complet de cada identitat corporativa. HR_EMPLOYEES ha de contenir les dades que provenen del sistema de recursos humans. A més a més, també conté els atributs tècnics que el motor construeix durant el provisioning, com el *displayName* o el *mail*, que es creen automàticament a partir d'atributs existents, i mai han de ser introduïts manualment per RRHH.

Els camps s'organitzen en grups funcionals. El grup d'identificadors conté el camp *uid*, que actua com a clau primària de la taula i és alhora el sAMAccountName dels comptes a l'AD, i el camp *employeeID*, que conté l'identificador intern del sistema de RRHH de l'empresa. La decisió de fer el *uid* igual a sAMAccountName és una simplificació conscient que elimina un nivell de mapping que en el sistema de producció real, basat en MIM, sí que existeix. El grup de dades personals conté el nom (*givenName*) i els cognoms (*sn*), tots dos NOT NULL perquè són necessaris per construir els atributs derivats. El grup de dades organitzatives inclou el títol, el departament, l'empresa i l'identificador del responsable directe, emmagatzemat com a *uid* per poder-lo resoldre dinàmicament a l'AD. Els grups de

contacte i localització contenen els telèfons, la ubicació de l'oficina, el codi postal i la província.

El grup d'atributs de compte conté *displayName*, *mail* i *userPrincipalName*, tots tres inicialitzats a NULL i construïts pel motor durant el primer provisioning. El *displayName* segueix el format corporatiu “Cognom1 Cognom2, Nom”, el *mail* el format *nom.cognom@domini* i el *userPrincipalName* el format *uid@domini*. El *mail* s'emmagatzema a la base de dades un cop calculat perquè, en cas de col·lisió, el motor genera un *mail* alternatiu afegint-hi un número al final.

Finalment, el grup de cicle de vida conté el camp *accountExpires*, el qual no s'ha acabat utilitzant. També hi ha quatre camps gestionats exclusivament pel motor: *Status*, *forcePassChange*, *provisionedAD* i *provisionedEntraID*. Tots quatre tenen valors per defecte (DEFAULT) a la definició de la taula, impedit que RRHH els pugui establir inadvertidament. *Status* s'inicialitza a Pending, *provisionedAD* i *provisionedEntraID* a 0, i *forcePassChange* a 1, obligant al nou empleat a canviar la contrasenya en el primer accés.

7.1.1 Màquina d'estats del camp Status

El camp *Status* implementa una màquina d'estats que permet a l'orquestrador determinar automàticament quina acció ha d'executar per a cada usuari en cada execució. A més, és el mecanisme que fa possible el reintent automàtic davant errors.

Pending és el punt de partida de tot usuari nou, indica que el registre existeix a HR_EMPLOYEES però que el compte encara no s'ha creat a l'AD. Si el provisioning té èxit passa a Active i si falla passa a ErrorProvisioning. PendingUpdate indica una modificació detectada per *Compare-Snapshots.ps1* pendent d'aplicar a l'AD, i és també l'estat que s'ha de forçar per reactivar un usuari Disabled. PendingSync indica una divergència detectada per *Invoke-Reconciliation.ps1* pendent de corregir. PendingDeprovisioning indica que una baixa ha estat sol·licitada però encara no executada, implementant el model soft-delete. Active és l'estat nominal d'un empleat en actiu i Disabled és l'estat terminal d'una baixa confirmada i executada. Els estats ErrorProvisioning, ErrorUpdating i ErrorDeprovisioning indiquen que l'última operació ha fallat per un problema potencialment transitori i l'orquestrador la reintentarà en el proper cicle. Error indica un problema greu que requereix intervenció manual, com una OU de destinació no definida al *config.json*. Finalment, Other agrupa qualsevol valor de *Status* no reconegut pel motor, actuant com a escut davant d'estats inesperats.

7.2 HR_Employees_Snapshot

La taula HR_EMPLOYEES_SNAPSHOT té exactament la mateixa estructura que HR_EMPLOYEES, amb l'addició d'un camp *SnapshotDate* que registra quan es va fer l'snapshot. La seva funció és preservar l'estat de la taula d'autoritat al final de cada jornada, de manera que l'endemà el sistema pugui comparar l'estat actual amb l'estat anterior i detectar qualsevol canvi produït.

L'actualització de la taula de l'snapshot es realitza diàriament a les 07:00 hores mitjançant un SQL Server

Agent Job que executa una operació de buidatge i recàrrega. Si el Job falla o és interromput, aquest mostra un missatge d'error, garantint que l'snapshot mai es troba en un estat parcial, ja que això generaria deteccions de canvis erronis.

A diferència de la taula principal, la taula de l'snapshot no té restriccions CHECK sobre el valor de *Status* ni restriccions UNIQUE sobre *mail* i *userPrincipalName*, perquè aquesta és una còpia de lectura que no rep insercions directes.

7.3 AD_Employees i la capa de reconciliació

La taula AD_EMPLOYEES actua com a mirall SQL de l'estat actual de l'Active Directory i constitueix la base de la capa de reconciliació autoritativa. A diferència de HR_EMPLOYEES, és una taula de lectura que el motor manté actualitzada periòdicament mitjançant *DeltaImportAD.ps1*, que pot executar-se en mode delta, processant únicament els objectes modificats des de l'última execució, o en mode full, que reimporta tot des de zero. El mecanisme de watermark, implementat a través de la taula AD_Import_Control, permet al mode delta filtrar els canvis aplicant el filtre *whenChanged* sobre els objectes de l'AD.

A més dels atributs de compte compartits amb HR_EMPLOYEES, la taula afegeix dos camps específics del directori: *distinguishedName*, que emmagatzema el DN complet de l'objecte, i *ADOU*, que conté la Unitat Organitzativa pare. Aquests dos camps són els que permeten a *Invoke-Reconciliation.ps1* detectar divergències estructurals, és a dir, casos en què el CN o l'OU d'un objecte AD no coincideixen amb els que es derivarien a partir dels camps de HR_EMPLOYEES.

Un cop descrites les taules que conformen la base de dades del sistema, a continuació s'exposen els scripts que implementen la lògica del motor IAM. La Figura 2 mostra l'arquitectura general del motor i les interrelacions entre els components abans d'entrar en el detall de cadascun.

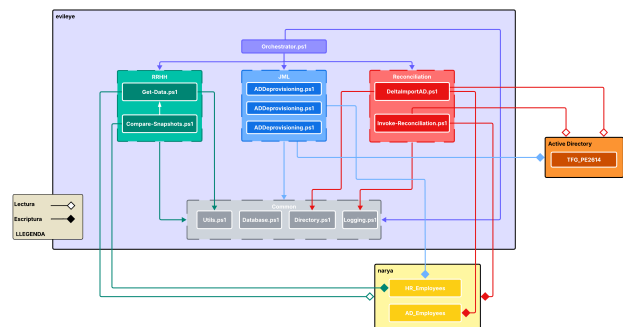


Fig. 2: Diagrama de les interrelacions dels scripts del motor.

7.4 Mòduls comuns

Els mòduls comuns proporcionen diverses funcions reutilitzables, que s'importen per dot-sourcing en cada component que les necessita.

Logging.ps1 és essencial per a la traçabilitat i el diagnòstic d'errors. És utilitzat per tots els scripts i proporciona la funció Write-ProvLog, que accepta el nom del mòdul

que genera el missatge, el nivell de gravetat i el text del missatge. El format de sortida és consistent al llarg de totes les execucions, tal com s'observa a les imatges de l'apèndix A.2. Destacar que els caràcters del missatge s'expressen en ASCII per evitar problemes de codificació, detectats en iteracions anteriors, del fitxer de log.

Database.ps1 encapsula totes les escriptures de tornada a `HR.EMPLOYEES`. `Set-HRStatus` actualitza el camp `Status` d'un usuari, `Update-HREmployee` escriu els flags i els atributs construïts durant el provisioning, i per últim, `Update-NomResp` propaga el canvi de nom d'un responsable a tots els seus subordinats.

Directory.ps1 conté quatre funcions que interactuen amb l'estructura de l'AD. `Get-OUTarget` deriva l'OU de destinació d'un compte a partir de la combinació de `company` i `department` consultant el mapa d'OUS del `config.json`, retornant `NULL` si la combinació no està definida. `Get-ManagedOus` retorna la llista d'OUS gestionades pel motor, delimitant l'abast de la reconciliació i la importació de l'AD. `Get-EscapedCN` construeix noms d'objecte AD vàlids tractant els caràcters especials del CN, com la coma, que al DN van precedits d'una barra invertida. Finalment, `Resolve-ADManager` reconcilia el camp `responsable` d'un objecte AD comparant el DN actual del responsable amb el que indica `HR.EMPLOYEES` i l'actualitza si divergeixen. Si el mànager encara no existeix a l'AD, no retorna error i es completarà la reconciliació a la pròxima iteració.

Utils.ps1 conté quatre funcions auxiliars reutilitzables. `ConvertTo-ASCIIName` normalitza cadenes de text per construir atributs de compte com el `mail`. `Normalize-Value` converteix valors `NULL`, `DBNull` i cadenes amb espais a cadena buida, garantint la consistència dels valors provinents de SQL. `ShouldUpdate` normalitza i compara el valor de `HR.EMPLOYEES` amb el de l'AD, retornant `true` únicament si HR té un valor vàlid i diferent. Finalment, `Compare-HRvsAD` compara un registre de `HR.EMPLOYEES` amb el seu homòleg a `AD.EMPLOYEES` i retorna un diccionari amb les divergències detectades, indicant per a cada camp el valor de HR i el valor real de l'AD.

7.5 Get-Data.ps1

Get-Data.ps1 conté dues funcions de lectura de dades del SQL Server que retornen els resultats com un array de `PS-CustomObjects`.

La funció `Get-Data` llegeix `HR.EMPLOYEES` o `HR.EMPLOYEES.SNAPSHOT` en funció del paràmetre `Snapshot`, de manera que la mateixa funció serveix per als dos casos d'ús de **Compare-Snapshots.ps1**. La funció `Get-ADEmployees` llegeix la taula `AD.EMPLOYEES` i és necessària per **Invoke-Reconciliation.ps1** per tal d'obtenir el mirall SQL de l'AD.

Totes dues funcions llegeixen les credencials des del fitxer xifrat `sql_reader.clixml`, construeixen el `connection string` a partir dels paràmetres del `config.json` i gestionen els errors amb un bloc `try-catch-finally`, garantint que la connexió es tanca sempre, evitant connexions penjades al servidor. A més, `Get-Data` incorpora una validació que atura el procés si la consulta retorna zero registres. Sense aquesta protecció, **Compare-Snapshots.ps1** interpretaria que tots els empleats han estat donats de baixa i iniciaria un desproveïment massiu.

Finalment, cada fila del `DataTable` es converteix en un `PSCustomObject`, millorant la llegibilitat del codi, normalitzant automàticament els valors `DBNull` a `Null` de PowerShell i facilitant la compatibilitat amb les operacions de filtratge del llenguatge [17].

7.6 Compare-Snapshots.ps1

És el cor de la lògica de detecció de canvis del sistema. Crida **Get-Data.ps1** dues vegades per obtenir l'estat actual de `HR.EMPLOYEES` i `HR.EMPLOYEES.SNAPSHOT`, comparant els dos conjunts per identificar altes i modificacions.

Les altes s'identifiquen com els registres presents a la taula d'autoritat però absents a l'snapshot. Representen nous empleats per als quals cal crear un compte a l'AD. D'altra banda, la detecció de modificacions comprova setze atributs agrupats en dades personals, de compte, organitzatives, de contacte, de localització i de cicle de vida. S'exclouen conscientment `uid` i `employeeID`, perquè mai haurien de canviar, `Status` i els indicadors de provisioning, perquè són gestionats pel motor, i `forcePassChange`, ja que només és rellevant en el moment de l'alta. A més, la comparació de cada atribut inclou la normalització defensiva descrita a la secció de decisions de disseny, que evita falsos positius per valors nuls o espais addicionals.

Per a cada modificació, la funció construeix un diccionari amb el valor anterior i el nou de cada camp, que es registra al log i es transmet a l'**Orchestrator.ps1**.

La funció també incorpora una protecció que evita modificar el camp `Status` d'usuaris que ja es troben en estats especials, com ara `PendingDeprovisioning`, `Disabled` o qualsevol estat d'error, per no interferir amb processos que ja estan en curs. De la mateixa manera, si un administrador marca manualment un usuari `Disabled` amb `Status=PendingUpdate` per indicar-ne la reactivació, l'script respecta aquest estat i no el sobreescriu.

Per acabar, la funció retorna un `PSCustomObject` amb dos arrays: `Joins` i `Moves`. Les baixes no es detecten per absència, sinó que es gestionen a través de `PendingDeprovisioning`.

7.7 ADProvisioning.ps1

Gestiona la creació d'un nou compte d'usuari a l'AD a partir d'un registre amb `Status=Pending` a `HR.EMPLOYEES`. La funció principal `Invoke-NewADUser` és cridada per l'**Orchestrator.ps1** per a cada element de l'array `Joins`.

Abans de crear el compte, l'script construeix els atributs derivats que no provenen directament de RRHH, com el `displayName`, el `mail` i el `userPrincipalName`. En cas que el `mail` derivat ja existeixi a l'AD, l'script en genera un d'alternatiu afegint un número al final fins a trobar un valor disponible. Paral·lelament, determina l'OU de destinació a partir de la combinació de `company` i `department`.

La creació del compte es realitza amb el cmdlet `New-ADUser`. Els atributs obligatoris s'afegeixen sempre, mentre que els opcionals s'afegeixen únicament si contenen un valor, evitant que l'AD emmagatzemi camps sense contingut on no hauria d'existir cap valor. Pel que fa al responsable, l'script resol el `uid` del responsable al seu DN de l'AD i l'assigna directament. Si el responsable encara

no existeix a l'AD en el moment del provisioning, s'usa el camp *nomResp* com a descripció provisional del compte, i l'assignació definitiva es completarà en un cicle posterior a través de *Resolve-ADManager*. El compte es crea amb una contrasenya inicial xifrada amb DPAPI i amb el flag *ChangePasswordAtLogon* activat, obligant l'empleat a canviar-la en el primer accés.

Si la creació té èxit, s'actualitza *HR_EMPLOYEES* amb els atributs construïts i *Status=Active*. Si es produeix qualsevol error, *Status* passa a *ErrorProvisioning* perquè l'orquestrador reintenti l'operació en el proper cicle.

7.8 ADDeprovisioning.ps1

S'executa quan l'orquestrador detecta un usuari amb *PendingDeprovisioning*. La seva funció és desactivar el compte de l'Active Directory i moure'l cap a l'OU de Deshabilitats, seguint la pràctica corporativa estàndard que preserva l'historial i permet recuperar la identitat si la baixa ha estat un error.

L'script cerca el compte a l'AD a partir de l'*uid*, que coincideix amb el *sAMAccountName*. Un cop localitzat, desactiva el compte amb *Disable-ADAccount* i n'actualitza la descripció amb la data de baixa, facilitant l'auditoria posterior. Abans de moure el compte, comprova si té activat el flag *ProtectedFromAccidentalDeletion* i el desactiva si cal, ja que sense aquest pas *Move-ADObject* fallaria. Finalment, mou l'objecte cap a l'OU de Deshabilitats.

Si totes les operacions finalitzen correctament, *Status* passa a *Disabled*, que és l'únic estat que indica una baixa confirmada i executada. Si qualsevol pas falla, *Status* passa a *ErrorDeprovisioning* per activar el reintent automàtic en el proper cicle.

7.9 ADUpdater.ps1

L'script gestiona l'actualització d'un compte existent a l'AD a partir d'un registre *PendingUpdate* o *PendingSync*, i és invocat per l'*Orchestrator.ps1* per a cada element en aquests dos estats.

L'script llegeix l'objecte d'AD un únic cop al principi i calcula el DN resultant després de cada operació estructural, sense tornar a llegir l'objecte entre operacions. Això resol un problema identificat durant les proves de validació, que quan s'executaven operacions encadenades com un canvi de nom seguit d'un moviment d'OU, PowerShell retornava resultats obsolets en la consulta immediatament posterior, causant errors del tipus "Directory object not found".

El flux s'organitza en quatre fases seqüencials. A la primera, de càlcul, l'script determina tots els valors objectiu: el nou CN si ha canviat el nom, el nou *mail* i l'OU de destí. Si l'OU no existeix al *config.json*, la funció surt immediatament, actualitzant l'estat a *Error* i sense fer cap escriptura. A la segona fase s'executen les operacions estructurals en ordre, habilitar si és una reactivació, reanomenar si ha canviat el nom i moure si ha canviat l'OU, actualitzant el DN després de cada operació. Abans de moure l'objecte, l'script comprova si té activat el flag *ProtectedFromAccidentalDeletion* i el desactiva si cal. A la tercera fase s'executa un únic *Set-ADUser*

amb tots els atributs que han canviat, usant el *sAMAccountName* com a identificador, ja que sempre és estable independentment del DN. A la quarta fase es confirma l'operació a la base de dades.

Pel que fa a la reactivació, quan l'script detecta un compte deshabilitat amb l'estat *PendingUpdate*, habilita el compte, actualitza la descripció amb la data de reactivació, el mou a l'OU correcta i aplica tots els canvis acumulats durant el període de baixa, si hi ha, tot en el mateix cicle.

Per últim, quant a les divergències estructurals, entenent com a tals els casos en què el CN o l'OU d'un objecte d'AD no coincideix amb el que es derivaria a partir dels valors de *HR_EMPLOYEES*, dels usuaris *PendingSync*, compara ambdós valors i activa el *Rename* o el *Move* si divergeixen, permetent corregir canvis fets manualment a l'AD. Si es produeix qualsevol error, l'estat passa a *ErrorUpdating*, activant el reintent automàtic en el proper cicle.

7.10 DeltaImportAD.ps1

Aquest script importa l'estat de l'Active Directory a la taula *AD_EMPLOYEES*, construint el mirall SQL del directori que utilitza la capa de reconciliació per detectar divergències.

El mecanisme central és el *watermark*, on la taula *AD_Import_Control* emmagatzema el timestamp de l'última execució. En mode delta, l'script consulta l'AD amb el filtre *whenChanged* sobre els objectes de les OUs gestionades, processant únicament els que han canviat des de l'última execució. S'aplica un marge de seguretat de 10 segons per evitar que canvis produïts en l'instant exacte de l'última execució es perdin per superposició de timestamps. En mode full, la taula *AD_EMPLOYEES* es buida completament i es reimporta des de zero, útil per a la sincronització inicial o per resoldre inconsistències acumulades.

L'abast està limitat a les OUs gestionades declarades al *config.json* i, per a cada objecte trobat, comprova si existeix a *HR_EMPLOYEES*. Si no hi existeix, l'ignora i el registra com a compte no gestionat al log. Per als objectes gestionats, comprova si ja existeix a *AD_EMPLOYEES* i executa un *UPDATE* si ja hi és o un *INSERT* si no hi és, garantint que el mirall reflecteix sempre l'estat més recent de l'AD. Al final de cada execució s'actualitza el *watermark* a *AD_Import_Control*.

7.11 Invoke-Reconciliation.ps1

Compara *HR_EMPLOYEES* amb *AD_EMPLOYEES* i detecta divergències entre el que mana la font d'autoritat i l'estat real de l'Active Directory. Per a cada divergència detectada, marca l'usuari amb *PendingSync* a *HR_EMPLOYEES* perquè l'orquestrador cridi *ADUpdater.ps1* i apliqui la correcció pertinent en el proper cicle.

L'script detecta tres categories de divergències. La primera són les divergències d'atributs, on un o més camps del compte a l'AD no coincideixen amb el valor de *HR_EMPLOYEES*. La comparació inclou la mateixa normalització defensiva de *Compare-Snapshots.ps1* per evitar falsos positius per nuls o espais. La segona és el CN incorrecte, on el nom de l'objecte AD no coincideix amb el que es derivaria dels valors dels camps de *HR_EMPLOYEES*

seguint el format Cognom, Nom. La tercera és l'OU incorrecta, on la posició de l'objecte a l'AD no correspon a l'OU esperada per la combinació d'empresa i departament de `HR_EMPLOYEES`.

Per últim, també detecta comptes no gestionats, és a dir, objectes d'AD que existeixen dins les OUs gestionades, però no tenen registre a `HR_EMPLOYEES`.

7.12 Orchestrator.ps1

Actua com a coordinador principal del sistema i és l'únic script que s'executa directament des de la tasca programada. Coordina l'execució seqüencial de tots els components i gestiona els reintents automàtics per als estats d'error.

La fase 1 executa *DeltaImportAD.ps1* per actualitzar `AD_EMPLOYEES` amb els canvis de l'AD des de l'última execució. La fase 2 carrega `HR_EMPLOYEES` i mostra l'estat inicial dels usuaris en estats no estables. La fase 3 executa *Compare-Snapshots.ps1* (3a) i *Invoke-Reconciliation.ps1* (3b) per detectar canvis i divergències respectivament. La fase 4 itera sobre els usuaris de `HR_EMPLOYEES` i crida el script JML corresponent en funció del seu *Status*, gestionant també els reintents automàtics per als estats d'error.

Un cop completada la fase 4, l'orquestrador rellegeix `HR_EMPLOYEES` per obtenir l'estat actualitzat post-JML. Aquest pas és necessari perquè les fases posteriors treballin amb els estats finals correctes, ja que durant la fase 4 alguns usuaris poden haver canviat de *Status*. La fase 4.5 reconcilia el camp *Manager* de l'AD per a tots els usuaris *Active* que tenen el responsable informat, corregint els casos en què el responsable no existia encara a l'AD en el moment de l'aprovisionament inicial. Finalment, la fase 5 genera un resum final amb els comptadors per estat i la llista d'usuaris que requereixen atenció.

8 RESULTATS

Els resultats obtinguts demostren la viabilitat tècnica del sistema i la solidesa dels components implementats. El cicle de vida de les identitats ha estat validat mitjançant l'execució de casos d'ús preparats amb dades sintètiques, dissenyats per cobrir tant els escenaris habituals com els casos límit i els escenaris d'error.

El sistema detecta i crea correctament les altes de nous empleats. Gestiona les modificacions d'atributs i els canvis organitzatius, incloent els canvis d'OU i la recalculació del *mail* si cal. Processa les baixes desactivant el compte i movent-lo a l'OU de Deshabilitats, i permet reactivar identitats prèviament donades de baixa aplicant tots els canvis acumulats en el mateix cicle. A més, detecta i corregeix divergències entre l'AD i la font d'autoritat i gestiona els errors de configuració marcant els usuaris afectats per a revisió manual. Finalment, en situacions sense canvis, el sistema no genera cap acció innecessària, confirmant el comportament idempotent del motor.

El sistema de logs proporciona una traçabilitat completa de cada execució, registrant el detall de cada detecció amb el nom de l'empleat, el seu *uid* i, en el cas de les modificacions, el camp modificat amb els valors anteriors i posteriors, facilitant tant l'auditoria com el diagnòstic d'errors.

Al llarg de les proves s'han detectat i resolt diversos incidents tècnics que han contribuït a millorar la robustesa del sistema. El més rellevant ha estat la comparació directa de valors nuls amb l'operador de desigualtat de PowerShell, que generava falsos positius en la detecció de modificacions. Aquest problema s'ha resolt mitjançant la normalització defensiva de tots els valors abans de la comparació, tal com es descriu a la secció de decisions de disseny. Els logs complets obtinguts durant l'execució de les proves sobre el sistema sintètic d'usuaris es poden consultar a l'Apèndix A.2.

9 CONCLUSIONS

9.1 Viabilitat i punts forts del motor

La PoC demostra que els principis fonamentals de MIM, com la font d'autoritat única i la reconciliació autoritativa, són replicables utilitzant scripts PowerShell sense necessitat d'una plataforma IAM comercial. El motor implementa correctament la separació entre la font d'autoritat i els sistemes destí, garantint que qualsevol divergència es resolgui sempre a favor de `HR_EMPLOYEES`. La màquina d'estats permet gestionar el cicle de vida de manera determinista i auditable, i la capa de reconciliació autoritativa detecta i corregeix automàticament desviacions no autoritzades produïdes directament a l'AD. A més, el mecanisme de reintent automàtic garanteix que un error puntual no interromp el flux global i la idempotència de totes les operacions assegura la recuperació correcta davant errors parcials.

Això és rellevant en el context de la retirada del suport de MIM el 2029, ja que suggereix que organitzacions amb casos d'ús acotats podrien considerar un motor personalitzat com a alternativa viable, especialment si la complexitat de l'entorn no justifica la inversió en eines com SailPoint o One Identity. Per a un entorn de la complexitat de GCO, amb múltiples dominis i requisits normatius exigents, una solució comercial continua oferint avantatges significatius en termes d'escalabilitat, governança, auditoria i experiència d'usuari. La PoC, per tant, no pretén ser una proposta de substitució directa de MIM, sinó un instrument per comprendre millor els requisits i els límits d'un enfocament alternatiu.

9.2 Limitacions conegudes

El sistema presenta diverses limitacions. En primer lloc, el motor funciona amb un model basat en consultes periòdiques, comprovant els canvis de manera recurrent en lloc de reaccionar immediatament davant dels esdeveniments, com fan les eines IAM corporatives. Aquesta diferència implica que entre el moment en què es produeix un canvi a `HR_EMPLOYEES` i el moment en què s'aplica a l'Active Directory pot haver-hi una latència equivalent a un cicle d'execució complet.

Pel que fa a la integració amb el núvol, la sincronització amb Entra ID mitjançant Microsoft Cloud Sync presenta una limitació d'entorn, ja que l'eina només permet seleccionar OUs situades directament a l'arrel del domini, sense possibilitat de configurar sub-OU's personalitzades, limitant el control sobre quines identitats es repliquen al tenant d'Entra ID.

Finalment, no es disposa de proves automatitzades. La validació s'ha fet manualment cobrint els casos principals, sense cap mecanisme que garanteixi la no-regressió davant canvis futurs. Els mecanismes de seguretat avançats, com el xifrat de les comunicacions internes o l'auditoria centralitzada, queden igualment fora de l'abast d'aquesta PoC. Cap d'aquests elements invalida les conclusions tècniques del treball, però seria necessari abordar-los abans de plantejar qualsevol evolució cap a un entorn productiu real.

ÚS DE LA IA GENERATIVA

Durant aquest treball s'ha utilitzat intel·ligència artificial generativa de manera responsable. El seu ús s'ha limitat a aspectes de revisió estilística del text, el suport en el formatge en LaTeX i l'aclariment puntual de conceptes a partir de continguts prèviament contrastats amb les fonts especialitzades referenciades. Així mateix, s'ha fet servir per a l'obtenció d'assistència puntual en aspectes tècnics, com ara la identificació d'errors desconeguts.

En cap cas s'ha fet servir per a la generació de continguts substantius del treball, com el disseny del sistema, la definició de la metodologia o l'anàlisi dels resultats, els quals han estat elaborats de manera autònoma.

AGRAÏMENTS

Vull donar les gràcies al Manel i al Xavi, de GCO, per la seva ajuda en la resolució de dubtes tècnics i per la confiança dipositada en mi per dur a terme aquest projecte.

Al meu tutor David, pels seus consells i la seva paciència durant tot el treball.

A la meua parella, per aguantar totes les converses sobre el projecte, alegrar-se amb cada petit avenç i animar-me sempre que ho he necessitat.

I, sobretot, als meus pares, per tots els esforços i sacrificis que han fet al llarg de la vida per donar-me una bona educació i uns bons valors. Gràcies a ells, avui estic acabant aquesta enginyeria i sóc qui sóc.

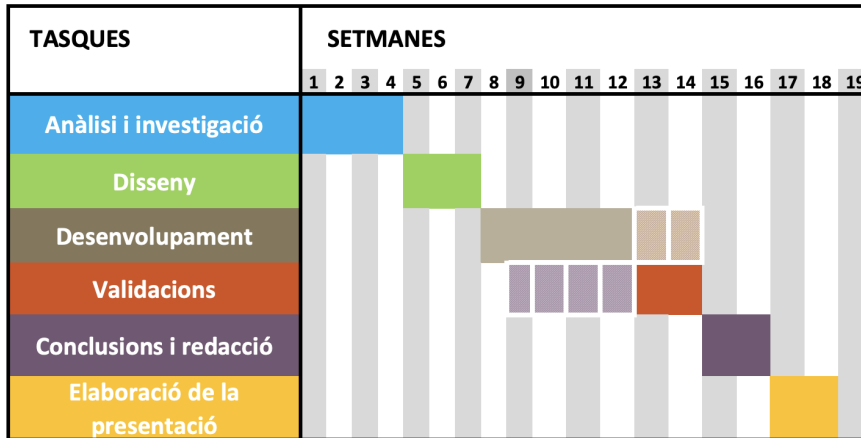
REFERÈNCIES

- [1] P. J. Windley, *Digital Identity: Unmasking Identity Management Architecture (IMA)*. Sebastopol, CA, USA: O'Reilly Media, 2010.
- [2] Cybersecurity and Infrastructure Security Agency (CISA), "Hybrid identity solutions guidance (hisg)," 2023, accessed: 02-Mar-2026. [Online]. Available: <https://www.cisa.gov/resources-tools/services/hybrid-identity-solutions-guidance-hisg>
- [3] SailPoint, "Cloud-based access control vs. on-premise," 2024, accessed: 24-Feb-2026. [Online]. Available: <https://www.sailpoint.com/identity-library/cloud-based-access-control-vs-on-premise>
- [4] Microsoft Learn, "Unified hybrid and multicloud operations – cloud adoption," 2026, accessed: 27-Feb-2026. [Online]. Available: <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/hybrid/strategy>
- [5] Microsoft, "Microsoft identity manager 2016," 2016, accessed: 27-Feb-2026. [Online]. Available: <https://learn.microsoft.com/en-us/microsoft-identity-manager/microsoft-identity-manager-2016>
- [6] V. Kodela, "Implementing identity and access management (iam) in hybrid cloud architectures: Challenges and solutions," *Journal of Informatics Education and Research*, vol. 2, no. 2, Jul. 2025.
- [7] MarketsandMarkets, "Identity and access management (iam) market worth \$42.61 billion by 2030," 2025, accessed: 02-Mar-2026. [Online]. Available: <https://www.marketsandmarkets.com/PressReleases/identity-access-management-iam.asp>
- [8] IBM, "¿qué es la gobernanza y administración de identidades (iga)?" 2024, accessed: 02-Mar-2026. [Online]. Available: <https://www.ibm.com/es-es/think/topics/identity-governance-and-administration>
- [9] Microsoft, "Microsoft entra id documentation," 2024, accessed: 03-Mar-2026. [Online]. Available: <https://learn.microsoft.com/en-us/entra/identity/>
- [10] SailPoint Technologies, "Identity security software — identityiq," 2024, accessed: 03-Mar-2026. [Online]. Available: <https://www.sailpoint.com/es/products/identity-security-software/identity-iq#features>
- [11] Okta, Inc., "Okta workforce identity product," 2024, accessed: 03-Mar-2026. [Online]. Available: <https://www.okta.com/products/workforce-identity/>
- [12] One Identity, "One identity manager product details," 2024, accessed: 03-Mar-2026. [Online]. Available: <https://www.oneidentity.com/products/identity-manager/>
- [13] Gartner, Inc., "Identity governance and administration reviews and ratings," 2024, accessed: 02-Mar-2026. [Online]. Available: <https://www.gartner.com/reviews/market/identity-governance-administration>
- [14] SIIT.io, "Microsoft entra id vs okta comparison," 2026, accessed: 02-Mar-2026. [Online]. Available: <https://www.siit.io/tools/comparison/microsoft-entra-id-vs-okta>
- [15] SailPoint Technologies, "What is identity governance and administration (iga)?" 2025, accessed: 02-Mar-2026. [Online]. Available: <https://www.sailpoint.com/identity-library/identity-governance>
- [16] One Identity, "What is identity governance and administration (iga)?" 2024, accessed: 02-Mar-2026. [Online]. Available: <https://www.oneidentity.com/what-is-iga/>
- [17] S. Roth, "Powershell – create "clean" custom objects from datatable object," 2018, accessed: 01-Apr-2026. [Online]. Available: <https://www.stefanroth.net/2018/04/11/powershell-create-clean-customobjects-from-datatable-object/>

APÈNDIX

A.1 Diagrama de Gantt del projecte

Planificació del TFG



■ Inici Real ■ Final Real

A.2 Log de l'Orchestrator.ps1 després d'una iteració

```

11-06-2026 13:31:40 [INFO] =====
11-06-2026 13:31:40 [INFO] INICI EXECUCIÓ ORQUESTADOR
11-06-2026 13:31:40 [INFO] Mode d'execució: FULL
11-06-2026 13:31:40 [INFO] =====
11-06-2026 13:31:40 [INFO] FASE 1: FULL Import AD --> AD_Employees
11-06-2026 13:31:40 [INFO] FASE 2: Estat inicial HR_Employees
11-06-2026 13:31:40 [INFO] Usuaris totals: 5
11-06-2026 13:31:40 [INFO] Usuaris amb estat diferent a 'Active' o 'Disabled' abans de la detecció de canvis: 1
11-06-2026 13:31:40 [INFO] uid = u00003 | Lopez Lopez, Maria | Status = PendingDeprovisioning
11-06-2026 13:31:40 [INFO] FASE 3: detecció de canvis
11-06-2026 13:31:40 [INFO] [3a] Compare-Snapshots OK.
11-06-2026 13:31:40 [INFO] [3a] Compare-Snapshots OK. Més info a Compare.log
11-06-2026 13:31:40 [INFO] [3b] Invoke-Reconciliation...
11-06-2026 13:31:40 [INFO] [3b] Reconciliation OK. Més info a Reconciliation.log
11-06-2026 13:31:40 [INFO] FASE 3.5: Canvis de Status detectats
11-06-2026 13:31:41 [INFO] Valors de l'atribut Status DESPRÉS de la detecció de canvis
11-06-2026 13:31:41 [INFO] - uid = u00001 | Status = PendingUpdate
11-06-2026 13:31:41 [INFO] - uid = u00002 | Status = PendingSync
11-06-2026 13:31:41 [INFO] - uid = u00003 | Status = PendingDeprovisioning
11-06-2026 13:31:41 [INFO] - uid = u00004 | Status = PendingUpdate
11-06-2026 13:31:41 [INFO] - uid = u00005 | Status = Active
11-06-2026 13:31:41 [INFO] FASE 4: Provisioning JML
11-06-2026 13:31:41 [INFO] [MOVER] Actualitzant usuari amb uid = u00001... Més info a Updater.log
11-06-2026 13:31:41 [INFO] [SYNC] Reconciliació de l'usuari amb uid = u00002... Forçant valors HR --> AD
11-06-2026 13:31:41 [INFO] [LEAVER] Deshabilitant usuari amb uid = u00003... Més info a Leaver.log
11-06-2026 13:31:41 [INFO] [MOVER] Actualitzant usuari amb uid = u00004... Més info a Updater.log
11-06-2026 13:31:42 [INFO] 1 usuaris sense cap acció necessària. 1 Active i 0 Disabled
11-06-2026 13:31:42 [INFO] FASE 4.5: Reconciliació de managers
11-06-2026 13:31:42 [INFO] Reconciliació de managers finalitzada. No s'han aplicat canvis.
11-06-2026 13:31:42 [INFO] FASE 5: Resum final
11-06-2026 13:31:42 [INFO] Estat del sistema: OK
11-06-2026 13:31:42 [INFO] Estat de les identitats |
11-06-2026 13:31:42 [INFO] -----
11-06-2026 13:31:42 [INFO] Active 4
11-06-2026 13:31:42 [INFO] Disabled 1
11-06-2026 13:31:42 [INFO] Pending (altes) 0
11-06-2026 13:31:42 [INFO] PendingUpdate 0
11-06-2026 13:31:42 [INFO] PendingSync 0
11-06-2026 13:31:42 [INFO] PendingDeprovisioning 0
11-06-2026 13:31:42 [INFO] ErrorProvisioning 0
11-06-2026 13:31:42 [INFO] ErrorUpdating 0
11-06-2026 13:31:42 [INFO] ErrorDeprovisioning 0
11-06-2026 13:31:42 [INFO] Error 0
11-06-2026 13:31:42 [INFO] -----
11-06-2026 13:31:42 [INFO] Cap usuari requereix accions addicionals. Estat correcte!
11-06-2026 13:31:42 [INFO] =====
11-06-2026 13:31:42 [INFO] FI ORQUESTADOR
11-06-2026 13:31:42 [INFO] Temps total: 00:00:02
11-06-2026 13:31:42 [INFO] =====

```

A.3 Gestió del cycle de vida de les identitats del sistema

Alta d'usuaris al sistema

```
10-06-2026 04:14:01 [INFO] =====
10-06-2026 04:14:01 [INFO] Donant d'alta l'usuari amb uid = u00001 | Joan Director Segura
10-06-2026 04:14:01 [INFO] =====
10-06-2026 04:14:01 [INFO] --- Atributs construïts ---
10-06-2026 04:14:01 [INFO] displayName : Director Segura, Joan
10-06-2026 04:14:01 [INFO] mail: joan.director@grupocatalanaoccidente.com
10-06-2026 04:14:01 [INFO] UPN: u00001@grupocatalanaoccidente.com
10-06-2026 04:14:01 [INFO] OU destí: OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
10-06-2026 04:14:01 [INFO] [OK] Compte creat: sAMAccountName = u00001 | OU =OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
10-06-2026 04:14:01 [INFO] -----
10-06-2026 04:14:01 [INFO] Alta de l'usuari amb uid = u00001 finalitzada
```

Baixa d'usuari al sistema

```
11-06-2026 13:31:41 [INFO] =====
11-06-2026 13:31:41 [INFO] Donant de baixa l'usuari amb uid = u00003 | Maria Lopez Lopez
11-06-2026 13:31:41 [INFO] =====
11-06-2026 13:31:41 [INFO] OU 'Deshabilitats' trobada: OU=Deshabilitats,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:41 [INFO] Usuari trobat a l'AD: DN = CN=Lopez Lopez, Maria,OU=Data,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:41 [INFO] 1) Deshabilitant usuari amb uid = u00003
11-06-2026 13:31:41 [INFO] 2) Actualitzant descripció amb la data de desactivació'Deshabilitat el 11-06-2026'
11-06-2026 13:31:41 [INFO] 3) ProtectedFromAccidentalDeletion està activat? False
11-06-2026 13:31:41 [INFO] 4) Movent usuari a OU=Deshabilitats,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:41 [INFO] Confirmit baixa a la BD... Status = 'Disabled'
11-06-2026 13:31:41 [INFO] -----
11-06-2026 13:31:41 [INFO] Usuari amb uid = u00003 mogut correctament a OU Deshabilitats
11-06-2026 13:31:41 [INFO] Baixa de l'usuari amb uid = u00003 finalitzada
```

Modificació d'usuari al sistema

```
11-06-2026 13:31:41 [INFO] =====
11-06-2026 13:31:41 [INFO] Actualitzant usuari amb uid = u00001 | Xavier Director Segural
11-06-2026 13:31:41 [INFO] =====
11-06-2026 13:31:41 [INFO] DN inicial : CN=Director Segural, Josep,OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:41 [INFO] Usuari habilitat : True
11-06-2026 13:31:41 [INFO] [DIVERGÈNCIA] DN incorrecte.
11-06-2026 13:31:41 [INFO] AD = 'CN=Director Segural, Josep,OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com'
11-06-2026 13:31:41 [INFO] Esperat='CN=Director Segural, Xavier,OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com'
11-06-2026 13:31:41 [INFO] Mail calculat: xavier.director@grupocatalanaoccidente.com
11-06-2026 13:31:41 [INFO] Rename CN: 'Director Segural' --> 'Director Segural, Xavier'
11-06-2026 13:31:41 [INFO] [OK] Rename completat. DN calculat: CN=Director Segural, Xavier,OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:41 [INFO] OU actual : OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:41 [INFO] OU destí : OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:41 [INFO] [OK] L'usuari ja és a la OU correcta
11-06-2026 13:31:41 [INFO] Actualitzant atributs: GivenName, DisplayName, EmailAddress
11-06-2026 13:31:41 [INFO] [OK] Set-ADUser completat
11-06-2026 13:31:41 [INFO] -----
11-06-2026 13:31:41 [INFO] Modificació de l'usuari amb uid = u00001 finalitzada correctament
11-06-2026 13:31:41 [INFO] =====
```

Reactivació d'usuari deshabilitat

```
11-06-2026 13:34:44 [INFO] =====
11-06-2026 13:34:44 [INFO] Actualitzant usuari amb uid = u00003 | Pepita Lopez Lopez
11-06-2026 13:34:44 [INFO] =====
11-06-2026 13:34:44 [INFO] DN inicial : CN=Lopez Lopez, Maria,OU=Deshabilitats,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:34:44 [INFO] Usuari habilitat : False
11-06-2026 13:34:44 [INFO] [DIVERGÈNCIA] DN incorrecte.
11-06-2026 13:34:44 [INFO] AD = 'CN=Lopez Lopez, Maria,OU=Deshabilitats,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com'
11-06-2026 13:34:44 [INFO] Esperat='CN=Lopez Lopez, Pepita,OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com'
11-06-2026 13:34:44 [INFO] Mail calculat: pepita.lopez@grupocatalanaoccidente.com
11-06-2026 13:34:44 [INFO] Reactivació detectada. Habilitant compte...
11-06-2026 13:34:44 [INFO] [OK] Compte habilitat. Descripció: 'Reactivat el 11-06-2026'
11-06-2026 13:34:44 [INFO] Rename CN: 'Lopez Lopez' --> 'Lopez Lopez, Pepita'
11-06-2026 13:34:44 [INFO] [OK] Rename completat. DN calculat: CN=Lopez Lopez, Pepita,OU=Deshabilitats,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:34:44 [INFO] OU actual : OU=Deshabilitats,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:34:44 [INFO] OU destí : OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:34:44 [INFO] Movent usuari a OU: OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:34:45 [INFO] [OK] Usuari mogut. DN calculat: CN=Lopez Lopez, Pepita,OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:34:45 [INFO] Actualitzant atributs: GivenName, DisplayName, EmailAddress, Department
11-06-2026 13:34:45 [INFO] [OK] Set-ADUser completat
11-06-2026 13:34:45 [INFO] -----
11-06-2026 13:34:45 [INFO] Modificació de l'usuari amb uid = u00003 finalitzada correctament
11-06-2026 13:34:45 [INFO] =====
```

A.4 Detecció de canvis i reconciliació a l'Active Directory

Detecció de canvis no autoritzats a l'AD

```

11-06-2026 13:31:40 [INFO] ===== INICI DELTA IMPORT AD I MODE: FULL =====
11-06-2026 13:31:40 [INFO] --- Watermark ---
11-06-2026 13:31:40 [INFO] Última execució: 01/01/2000 00:00:00
11-06-2026 13:31:40 [INFO] Watermark aplicat: 12/31/1999 23:59:50 (marge -10s)
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] [FULL] Esborrant snapshot AD_Employees
11-06-2026 13:31:40 [INFO] Escaneig d'OUs
11-06-2026 13:31:40 [INFO] - OU=Data,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Canvis detectats
11-06-2026 13:31:40 [INFO] -----
11-06-2026 13:31:40 [INFO] L'usuari amb uid = u00003 s'ha modificat el 06/11/2026 13:23:33
11-06-2026 13:31:40 [INFO] [INSERT] Afegint nou registre: u00003
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] - OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Canvis detectats
11-06-2026 13:31:40 [INFO] -----
11-06-2026 13:31:40 [INFO] L'usuari amb uid = u00001 s'ha modificat el 06/11/2026 13:27:22
11-06-2026 13:31:40 [INFO] [INSERT] Afegint nou registre: u00001
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] L'usuari amb uid = u00002 s'ha modificat el 06/11/2026 13:27:16
11-06-2026 13:31:40 [INFO] [INSERT] Afegint nou registre: u00002
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] L'usuari amb uid = u00005 s'ha modificat el 06/11/2026 13:29:41
11-06-2026 13:31:40 [INFO] [INSERT] Afegint nou registre: u00005

11-06-2026 13:31:40 [INFO] - OU=RRHH,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Cap canvi detectat a aquesta OU.
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] - OU=IT,OU=Empresa SB,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Canvis detectats
11-06-2026 13:31:40 [INFO] -----
11-06-2026 13:31:40 [INFO] L'usuari amb uid = u00004 s'ha modificat el 06/11/2026 13:18:22
11-06-2026 13:31:40 [INFO] [INSERT] Afegint nou registre: u00004
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] - OU=RRHH,OU=Empresa SB,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Cap canvi detectat a aquesta OU.
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] - OU=IT,OU=Empresa SC,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Cap canvi detectat a aquesta OU.
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] - OU=Logistica,OU=Empresa SC,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Cap canvi detectat a aquesta OU.
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] - OU=Deshabilitats,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Cap canvi detectat a aquesta OU.
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] ===== FI DELTA IMPORT AD =====

```

Reconciliació de valors de la font d'autoritat a l'AD

```

11-06-2026 13:31:40 [INFO] ===== INICI RECONCILIATION =====
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] --- Càrrega de dades ---
11-06-2026 13:31:40 [INFO] HR_Employees: 5 registres
11-06-2026 13:31:40 [INFO] AD_Employees: 5 registres
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] --- RH vs AD ---
11-06-2026 13:31:40 [WARNING] Divergència detectada a l'usuari amb uid = u00002 I Divergència: locinfo : AD='Terrassa' --> HR='Barcelona'
11-06-2026 13:31:40 [INFO] Usuari amb uid = u00002 marcat com a PendingSync. L'orquestrador aplicarà la correcció pertinent.
11-06-2026 13:31:40 [INFO]
11-06-2026 13:31:40 [INFO] --- Comptes no gestionats pel motor IAM ---
11-06-2026 13:31:40 [INFO] Analitzant OU=Data,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Analitzant OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Analitzant OU=RRHH,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Analitzant OU=IT,OU=Empresa SB,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Analitzant OU=RRHH,OU=Empresa SB,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Analitzant OU=IT,OU=Empresa SC,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Analitzant OU=Logistica,OU=Empresa SC,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:31:40 [INFO] Analitzant OU=Deshabilitats,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com

11-06-2026 13:31:40 [INFO] I Resum Reconciliació      I
11-06-2026 13:31:40 [INFO] -----
11-06-2026 13:31:40 [INFO] Revisats (Active):      2
11-06-2026 13:31:40 [INFO] Omesos (no Active):     3
11-06-2026 13:31:40 [INFO] Sense registre AD:      0
11-06-2026 13:31:40 [INFO] Divergències:           1
11-06-2026 13:31:40 [INFO] No gestionats:          0
11-06-2026 13:31:40 [INFO] -----
11-06-2026 13:31:40 [INFO] ===== FI RECONCILIATION =====

```

A.5 Detecció i tractament d'errors

Error detectat i tractat pel sistema

```

11-06-2026 13:38:22 [INFO] =====
11-06-2026 13:38:22 [INFO] INICI EXECUCIÓ ORQUESTADOR
11-06-2026 13:38:22 [INFO] Mode d'execució: FULL
11-06-2026 13:38:22 [INFO] =====
11-06-2026 13:38:22 [INFO] FASE 1: FULL Import AD --> AD_Employees
11-06-2026 13:38:22 [INFO]
11-06-2026 13:38:22 [INFO] FASE 2: Estat inicial HR_Employees
11-06-2026 13:38:22 [INFO] Usuaris totals: 5
11-06-2026 13:38:22 [INFO] Tots els usuaris estan en estat estable (Active/Disabled).
11-06-2026 13:38:22 [INFO]
11-06-2026 13:38:22 [INFO] FASE 3: detecció de canvis
11-06-2026 13:38:22 [INFO] [3a] Compare-Snapshots...
11-06-2026 13:38:22 [INFO] [3a] Compare-Snapshots OK. Més info a Compare.log
11-06-2026 13:38:22 [INFO] [3b] Invoke-Reconciliation...
11-06-2026 13:38:22 [INFO] [3b] Reconciliation OK. Més info a Reconciliation.log
11-06-2026 13:38:22 [INFO]
11-06-2026 13:38:22 [INFO] FASE 3.5: Canvis de Status detectats
11-06-2026 13:38:22 [INFO] Valors de l'atribut Status DESPRÉS de la detecció de canvis
11-06-2026 13:38:22 [INFO] - uid = u00001 | Status = PendingUpdate
11-06-2026 13:38:22 [INFO] - uid = u00002 | Status = PendingSync
11-06-2026 13:38:22 [INFO] - uid = u00003 | Status = PendingUpdate
11-06-2026 13:38:22 [INFO] - uid = u00004 | Status = PendingUpdate
11-06-2026 13:38:22 [INFO] - uid = u00005 | Status = Active
11-06-2026 13:38:22 [INFO]
11-06-2026 13:38:22 [INFO] FASE 4: Provisioning JML
11-06-2026 13:38:22 [INFO] [MOVER] Actualitzant usuari amb uid = u00001... Més info a Updater.log
11-06-2026 13:38:22 [INFO] [SYNC] Reconciliació de l'usuari amb uid = u00002... Forçant valors HR --> AD
11-06-2026 13:38:22 [INFO] [MOVER] Actualitzant usuari amb uid = u00003... Més info a Updater.log
11-06-2026 13:38:22 [INFO] [MOVER] Actualitzant usuari amb uid = u00004... Més info a Updater.log
11-06-2026 13:38:22 [INFO] 1 usuaris sense cap acció necessària. 1 Active i 0 Disabled
11-06-2026 13:38:22 [INFO]
11-06-2026 13:38:23 [INFO] FASE 4.5: Reconciliació de managers
11-06-2026 13:38:23 [INFO] Reconciliació de managers finalitzada. No s'han aplicat canvis.
11-06-2026 13:38:23 [INFO]
11-06-2026 13:38:23 [INFO] FASE 5: Resum final
11-06-2026 13:38:23 [INFO] Estat del sistema: AMB ERRORS
11-06-2026 13:38:23 [INFO]
11-06-2026 13:38:23 [INFO] Estat de les identitats      |
11-06-2026 13:38:23 [INFO] -----
11-06-2026 13:38:23 [INFO] Active                        4
11-06-2026 13:38:23 [INFO] Disabled                     0
11-06-2026 13:38:23 [INFO]
11-06-2026 13:38:23 [INFO] Pending (altes)              0
11-06-2026 13:38:23 [INFO] PendingUpdate                0
11-06-2026 13:38:23 [INFO] PendingSync                  0
11-06-2026 13:38:23 [INFO] PendingDeprovisioning        0
11-06-2026 13:38:23 [INFO]
11-06-2026 13:38:23 [INFO] ErrorProvisioning            0
11-06-2026 13:38:23 [INFO] ErrorUpdating                0
11-06-2026 13:38:23 [INFO] ErrorDeprovisioning          0
11-06-2026 13:38:23 [INFO] Error                        1
11-06-2026 13:38:23 [INFO] -----
11-06-2026 13:38:23 [INFO]
11-06-2026 13:38:23 [INFO] Cap usuari requereix accions addicionals. Estat correcte!
11-06-2026 13:38:23 [INFO]
11-06-2026 13:38:23 [INFO] =====
11-06-2026 13:38:23 [INFO] FI ORQUESTADOR
11-06-2026 13:38:23 [INFO] Temps total: 00:00:01
11-06-2026 13:38:23 [INFO] =====

11-06-2026 13:38:22 [INFO] =====
11-06-2026 13:38:22 [INFO] Actualitzant usuari amb uid = u00003 | Pepita Lopez Lopez
11-06-2026 13:38:22 [INFO] =====
11-06-2026 13:38:22 [INFO] DN inicial: CN=Lopez Lopez\, Pepita,OU=IT,OU=Empresa SA,OU=TFG_PE2614,DC=grupocatalanaoccidente,DC=com
11-06-2026 13:38:22 [INFO] Usuari habilitat: True
11-06-2026 13:38:22 [ERROR] OU no vàlida: company= 'Empresa SA' dept= 'Ventas'

```