Plataforma Transversal de Dades

Directrius de seguretat

Juliol 2024

Finançat per la Unió Europea NextGenerationEU
GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Next Generation Catalunya
Generalitat de Catalunya

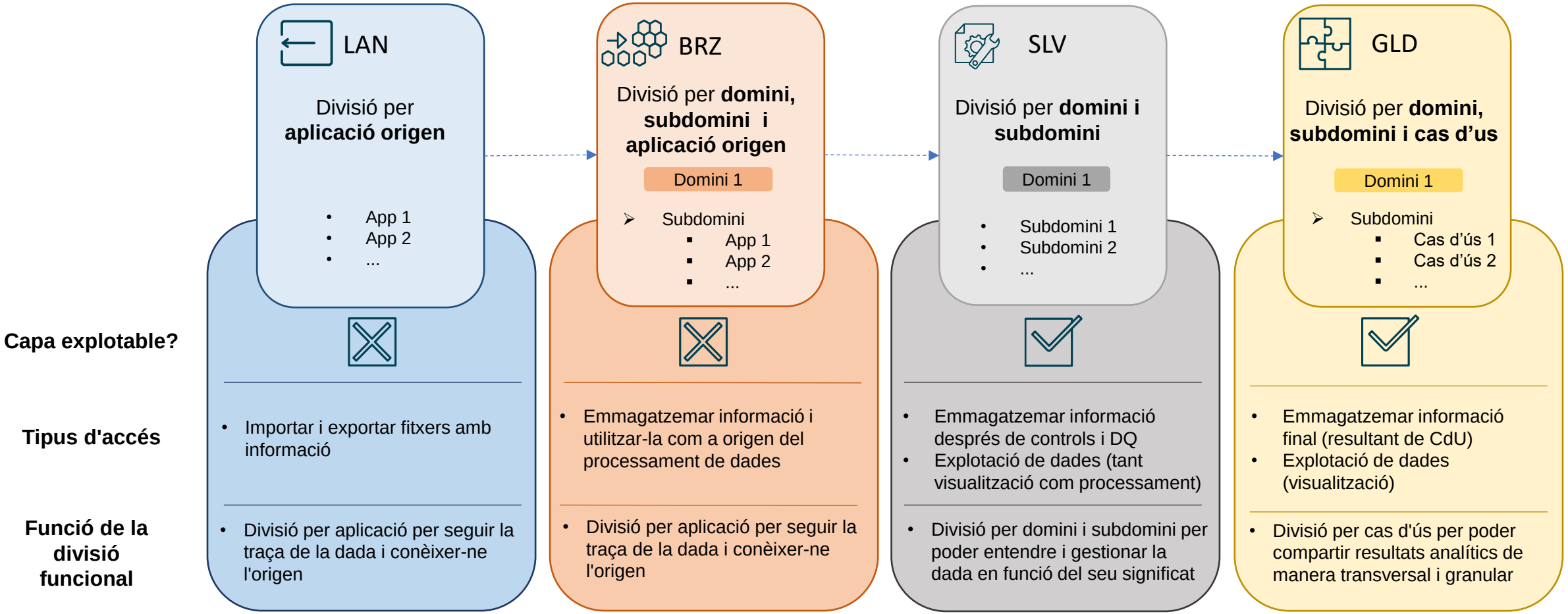
1

Seguretat

Seguretat

Accés a les capes en funció de la finalitat

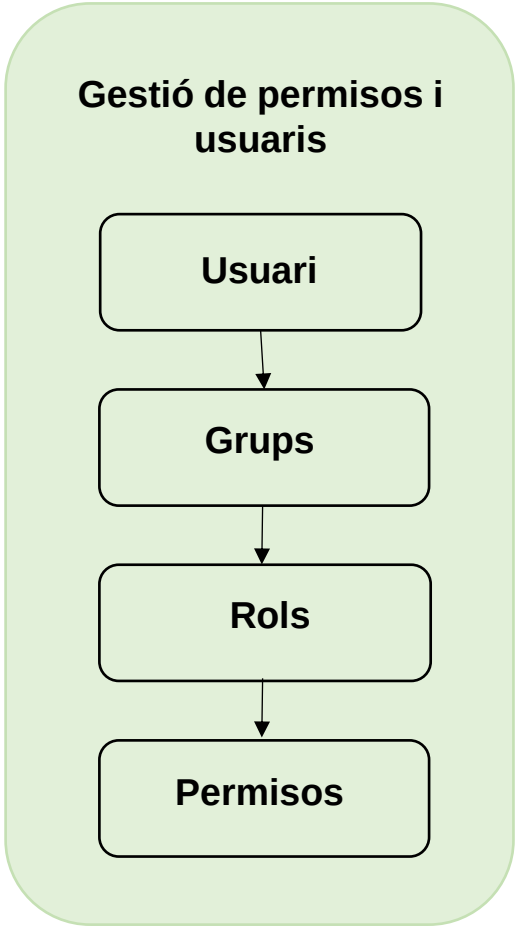
Cada capa tindrà una política d'accés depenent de la finalitat amb què ha estat definida i les subdivisions funcionals permetran la gestió granular:



Seguretat

Usuaris, funcions i permisos dins de la plataforma

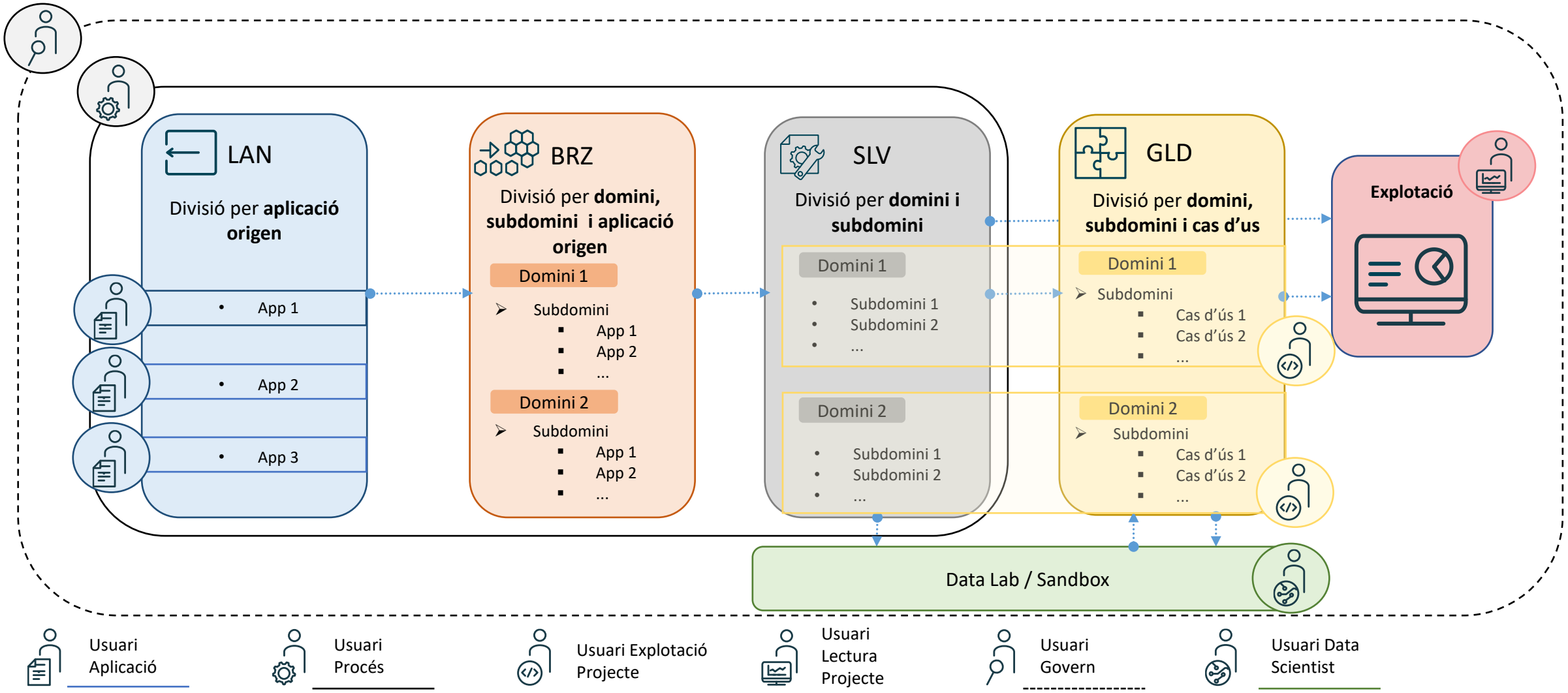
La creació d'usuaris i concessió de **permisos es realitzarà mitjançant grups i rols** per facilitar-ne la gestió de manera àgil:



Tipus d'usuari	Funció	Capes i permisos	Divisió de permisos
Aplicació	Importació de fitxers a la capa Landing.	• Landing (read & write)	Aplicació origen
Procés	Gestió de càrrega des de Landing fins a Silver.	• Landing (read & write) • Bronze (read & write) • Silver (read & write)	Nivell plataforma
Explotació projecte	Explotació i transformació/ processament de dades entre Silver i Gold.	• Silver (read) • Gold (read & write)	Subdomini (SLV) Cas d'us (GLD)
Lectura projecte	Visualització de dades de Silver i Gold. Particularitzable en funció cas d'ús.	• Silver (read) • Gold (read)	Subdomini (SLV) Cas d'us (GLD)
Govern	Control de la metadata i compliment de polítiques.	• Landing (read metadata) • Bronze (read metadata) • Silver (read metadata) • Gold (read metadata)	Nivell plataforma
Data Scientist	Creació i gestió de models d'analítica avançada.	• Silver (read) • Gold (read)	Subdomini (SLV) Cas d'us (GLD)

Seguretat

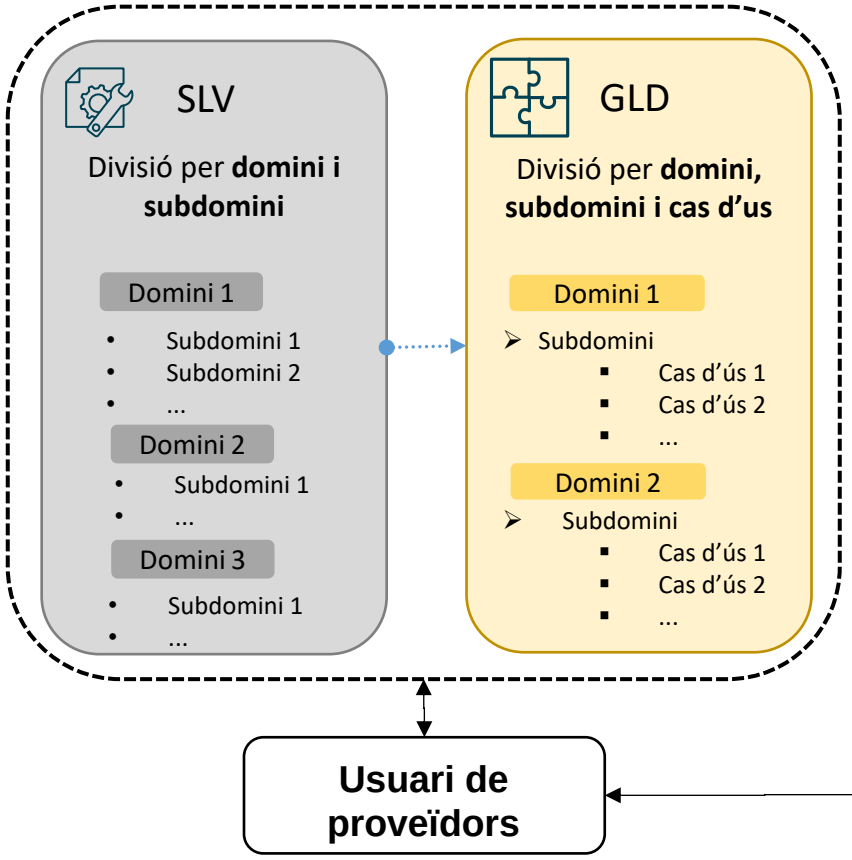
Esquema de permisos d'usuaris al llarg de la plataforma



Seguretat

Sistema de permisos d'usuaris multiproveïdor gestionat per subdominis

La distribució funcional de la plataforma **permet gestionar de manera granular l'accessibilitat** de diferents usuaris i proveïdors de serveis:



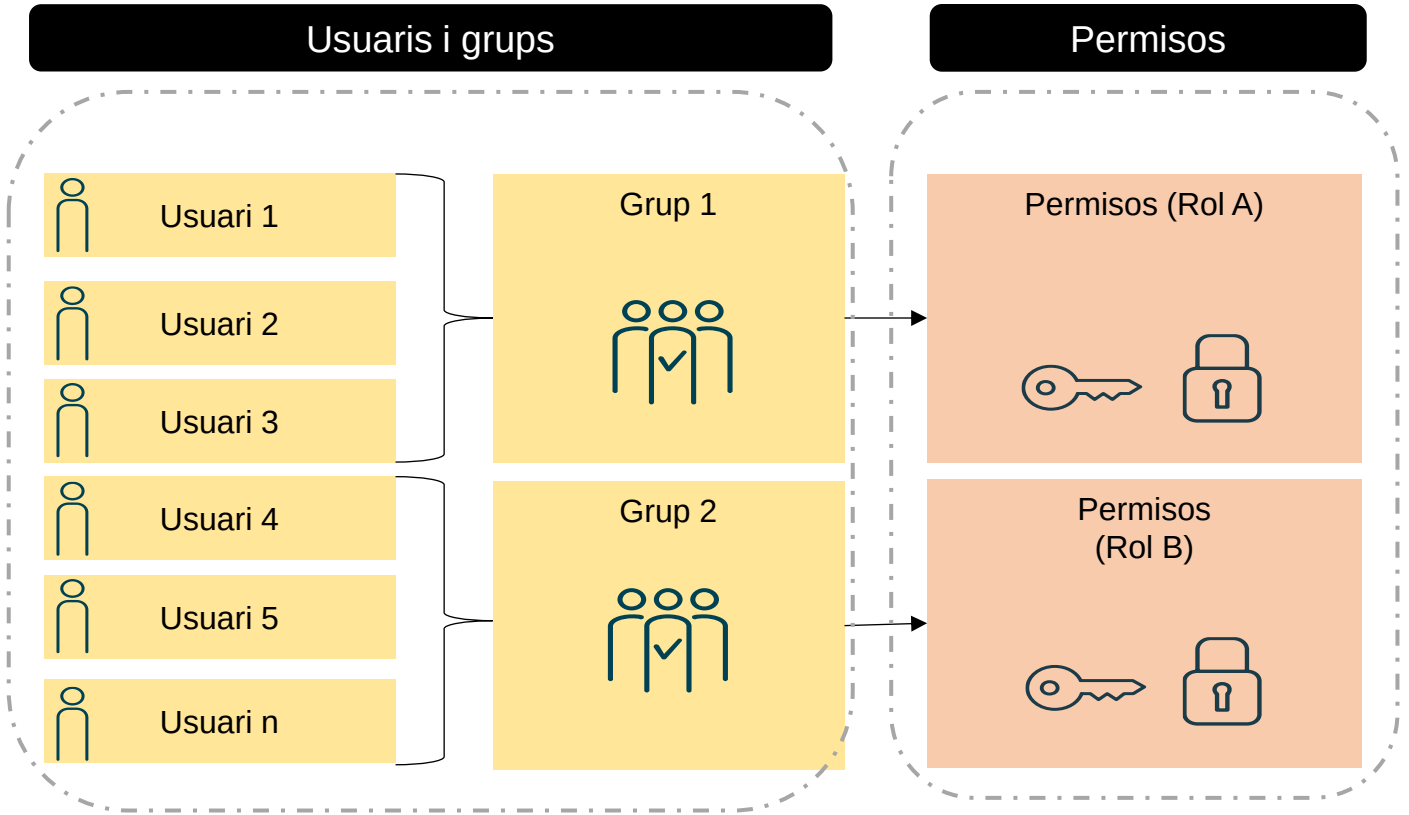
- A la capa Silver, la informació està dividida en **dominis i subdominis**, la qual cosa permet donar **permisos de forma granular** als usuaris de proveïdors, dotant la plataforma de la capacitat d'aïllar i separar les dades visibles a cada perfil (els permisos seran només de lectura),
- A la capa Gold els usuaris proveïdors tindran **permisos de lectura** (usuari lectura projecte) o de **lectura i escriptura** (usuari explotació projecte). Aquests permisos es podran **gestionar a nivell de cas d'ús**, permetent controlar de forma granular la informació a què té accés cada proveïdor i la potestat de poder editar-la o només consultar-la.
- Els rols permeten agrupar les **combinacions de permisos** de Subdominis i casos d'ús necessàries perquè cada perfil pugui exercir les funcions. Per exemple, un usuari de lectura projecte podrà tenir accés de lectura simultàniament a diversos subdominis de dominis diferents i a diversos casos d'ús.

Tipus d'usuari	Funció	Capes i permisos	Divisió de permisos
Explotació Projecte	Explotació i transformació/ processament de dades entre Silver i Gold iched	• Silver (read) • Gold (read & write)	Subdomini (SLV) Cas d'us (GLD)
Lectura Projecte	Visualització de dades de Silver i Gold	• Silver (read) • Gold (read)	Subdomini (SLV) Cas d'us (GLD)

Seguretat

Gestió de la seguretat

Es crearan grups d'usuaris als quals se'ls assignaran rols específics, atorgant-los així determinats permisos:



- Els usuaris* són agregats en grups d'usuaris i des de la plataforma es concediran rols aquests grups, considerant un rol com un conjunt de permisos.
- Aquest sistema permet separar la gestió d'usuaris de la de permisos, quan es creï un usuari i s'assigni a un grup, aquest ja comptarà amb els permisos necessaris per operar.

*A excepció d'usuaris màquina

2

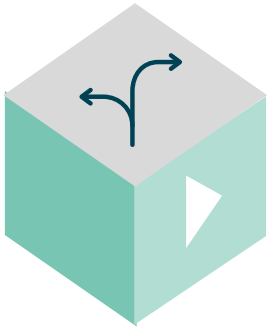
Privacitat

Privacitat

Gestió de la privacitat basada en 4 accions

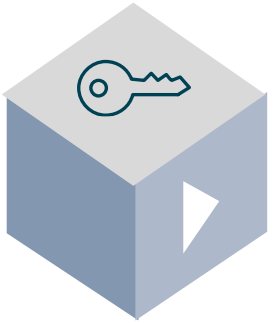
1 **Minimització**

Es minimitzarà la informació personal ingestada a la plataforma fent una anàlisi previ dels camps o entitats que puguin estar subjectes a polítiques o regulacions i el seu ús potencial. En altres paraules, **s'evitarà carregar informació personal si aquesta no és necessària.**



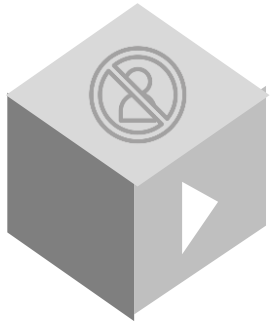
2 **Criptografia**

La informació personal que sigui ingestada però no s'exploti directament (dades per creuar taules, futurs casos d'ús...) **s'emmagatzemaran utilitzant funcions criptogràfiques**.



3 **Agrupació estadística**

L'agrupació estadística de dades **implica la supressió d'elements identificatius entre les dades i els individus específics, així les dades no estan associades directament amb les persones.**



4 **Control d'accés**

Es gestionarà **de forma dinàmica i mitjançant permisos qui pot visualitzar cada informació** utilitzant el control d'accés.

Privacitat

Etapa del cicle de la dada s'apliquen les accions

Minimització

Es sol·licitarà a l'usuari que no ingesti dades crítiques si no és necessari.

Criptografia

Hi ha **3 nivells d'encriptació:**

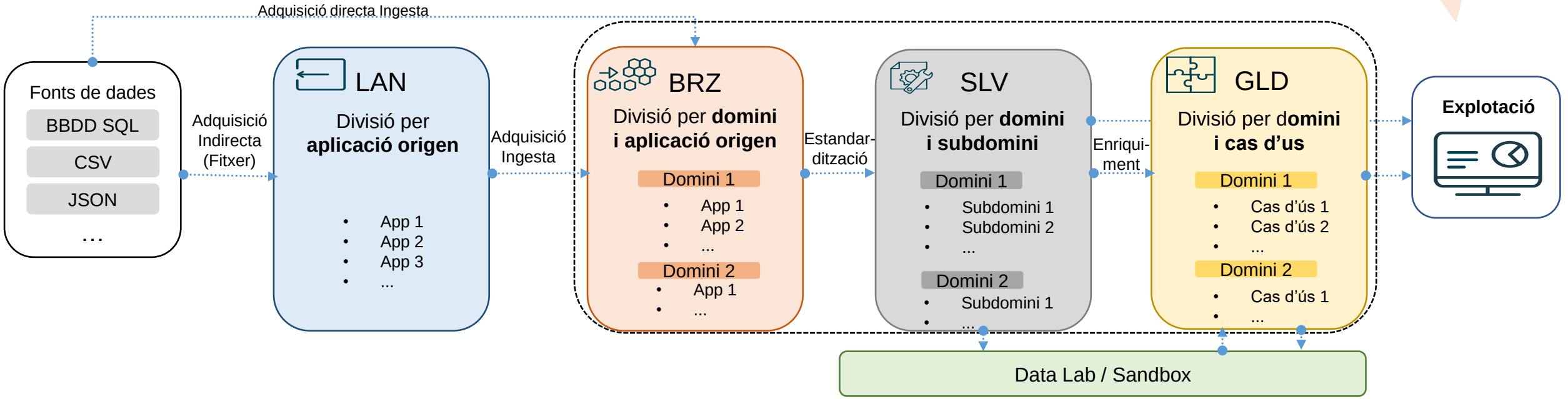
- Físicament al disc.
- L'encriptació d'Azure.
- De forma personalitzada en els camps sensibles a l'aplicació.

Agrupació estadística

Les dades a la capa Gold es desvincularan de les persones amb el fi de suprimir tota relació. (*Aquesta acció es farà en funció de la necessitat del cas d'ús.)

Control d'accés

Mitjançant permisos d'accés es controlarà quins usuaris poden visualitzar la informació sensible.



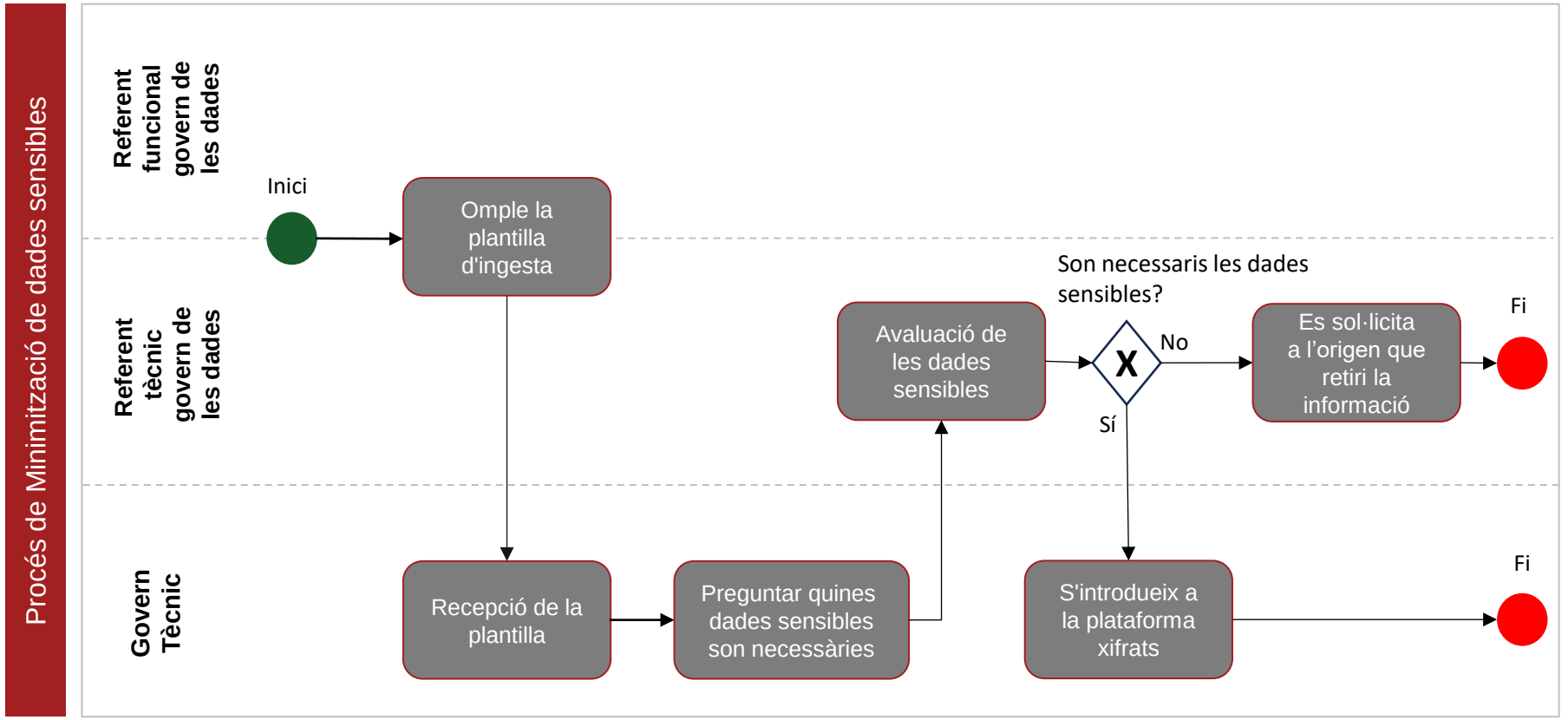
Privacitat

Minimització

La minimització es basa en ingestar a la plataforma únicament aquelles dades sensibles que calgui:

Quines problemàtiques volem evitar?

La presència de dades sensibles implica riscos addicionals, que poden posar en perill la seguretat de l'organització.



Privacitat

Criptografia

La criptografia és la codificació de la informació de forma que es converteix intel·ligible per mantenint-la segura i privada a la vista de persones que no tenen els permisos per visualitzar-la:

Quines problemàtiques volem evitar?

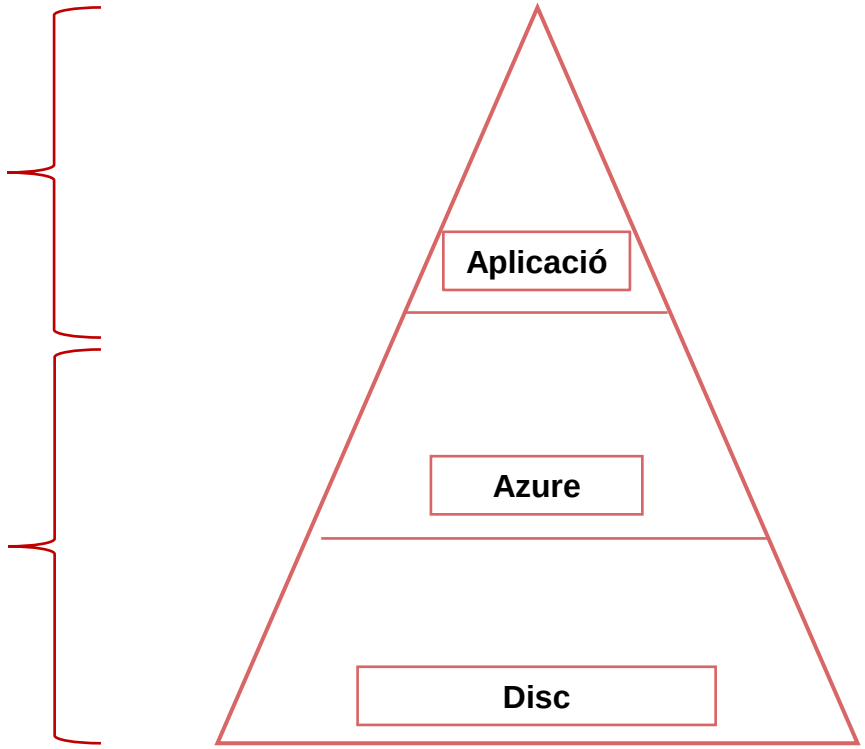
La manca d'encriptació deixaria les dades **exposades i vulnerables** a accessos no autoritzats.

A l'aplicació **la informació sensible es xifrarà abans de ser emmagatzemada**, adaptant-se segons les necessitats del negoci.

De forma **automàtica Azure encripta sempre tota la informació.**

A més a més, **també s'encripta automàticament la informació que s'emmagatzema al hardware**, es a dir, el disc.

3 nivells d'encriptació



Privacitat

Agrupació estadística

La agrupació estadística és una estratègia de desvinculació de dades sensibles relacionades amb persones físiques, per visualitzar les dades de forma d'agrupació Els usuaris autoritzats poden accedir i utilitzar aquestes dades a la capa Gold, on es mostraran agregades:

Quines problemàtiques volem evitar?

No fer una agrupació estadística pot conduir a la divulgació d'informació personal i sensible, **vulnerant la privacitat dels individus.**

Exemple il·lustratiu

Nom	Salari
Ramón Garcia Guardiola	40 000
Judith Carrasco Huertas	35 000
Pilar Muñoz Fernández	20 000
Francisco Pérez Domenech	14 000

Nombre de persones	Interval salarial
2	30 000 – 40 000
2	10 000 – 20 000

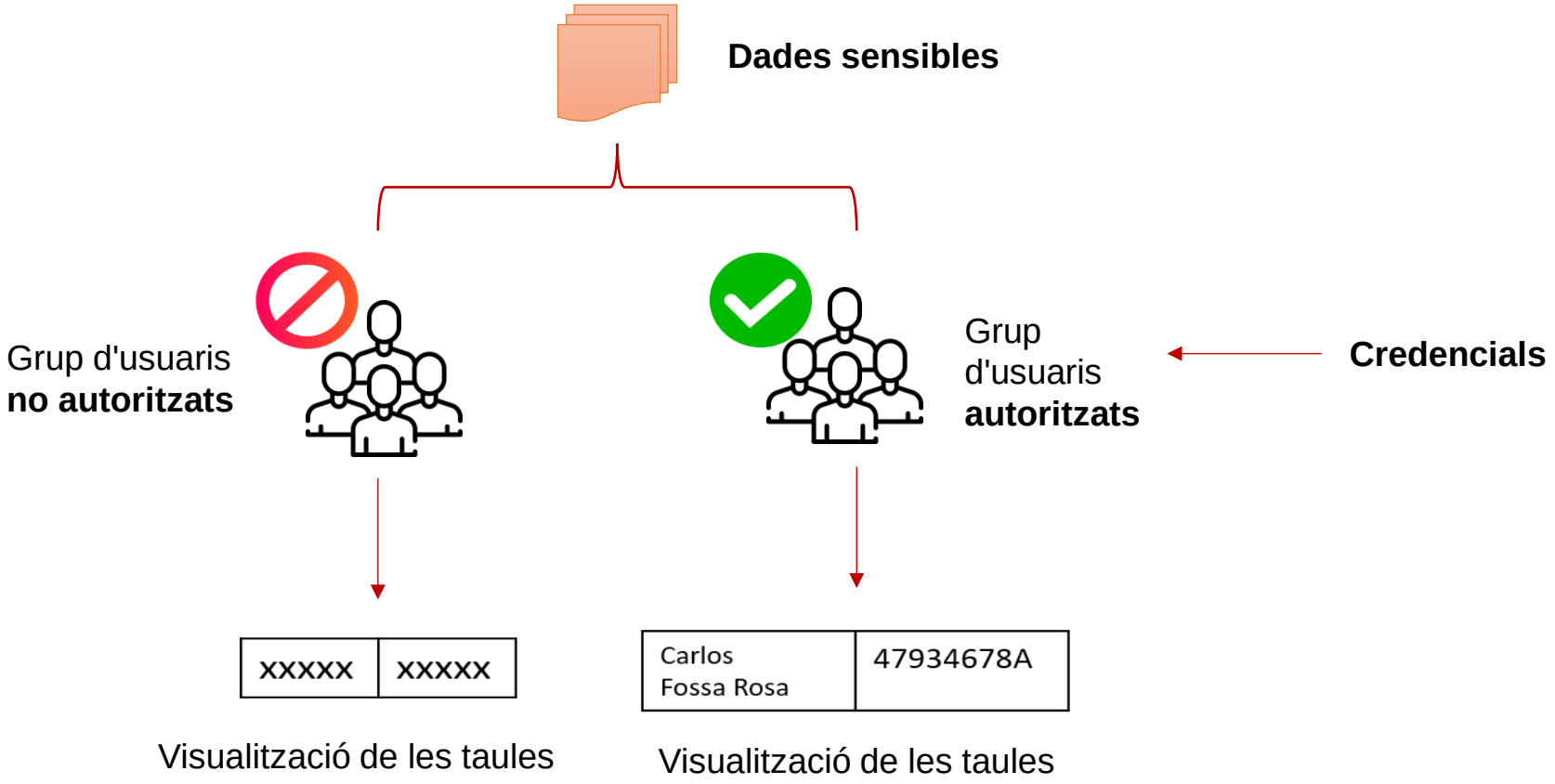
Privacitat

Control d’accés

La agrupació estadística és una estratègia de desvinculació de dades sensibles relacionades amb persones físiques, per visualitzar les dades de forma d'agrupació Els usuaris autoritzats poden accedir i utilitzar aquestes dades a la capa Gold, on es mostraran agregades:

Quines problemàtiques volem evitar?

El control d'accés ajuda a prevenir que **persones no autoritzades obtinguin accés.**



Generalitat de Catalunya

Centre de Telecomunicacions i Tecnologies de la Informació (CTTI)

www.gencat.cat

ptd.ctti@gencat.cat