Revisió	Redactat per	Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	Sipan Robles, Juan Carlos	Franch Espuny, Gustau	Minsait		

NOTA: Al final del document es troben les signatures i comentaris a la revisió i aprovació

Registre de Canvis

Revisió	Apartat	Data Modificació	Motiu del canvi
1.0		21/06/24	Primera versió

RESPONSABLE DEL DOCUMENT:

ÍNDEX

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

1. INTRODUCCIÓ

Aquest document té com objectiu establir les directrius bàsiques que han de seguir totes les aplicacions per poder treballar amb la PTD de forma segura. La seguretat, des del principi, ha estat un element clau en la construcció de la plataforma i la integració del diferents projectes que l'utilitzen. El punt de partida i principal marc de controls, treballat amb l'Agència de Ciberseguretat de Catalunya (Agència), ha estat l'Esquema Nacional de Seguretat (ENS), juntament amb el marc normatiu de la Generalitat de Catalunya en matèria de seguretat de la informació.

De totes formes, a banda d'aquest document, és essencial mantenir **reunions** amb els equips de desenvolupament a l'inici de qualsevol projecte i **acompanyar**-los durant tota l'etapa de creació de les aplicacions sobre la PTD.

2. DIRECTRIUS DE SEGURETAT

De tots els controls que hi apliquen, s'han extret els necessaris (les directrius) que ha de seguir qualsevol desenvolupament nou per poder treballar amb la PTD. Aquests s'han dividit en:

- Desenvolupament segur.
- Gestió d'usuaris i control d'accés.
- Seguretat de la informació.
- Altres directrius.

2.1 Desenvolupament segur

Tot desenvolupament sobre la PTD ha de seguir el seu **marc de desenvolupament segur**, basat en OWASP SAMM. Principalment:

1. S'han de seguir els **estàndards i polítiques** de seguretat aplicables a nivell autonòmic, nacional i europeu. Els principals a tenir en compte són:

   ✓ Marc normatiu del CTTI.
   ✓ Esquema Nacional de Seguretat (ENS).
   ✓ RGPD/LOPDGDD.

2. És essencial seguir **guies de bones pràctiques**, principalment d'OWASP, segons les necessitats de desenvolupament. Algunes d'aquestes són:

   ✓ OWASP Top Ten.
   ✓ OWASP Application Security Verification Standard (ASVS).
   ✓ OWASP Top 10 API Security Risks.
   ✓ Java Oracle Secure Coding Guidelines.
   ✓ Angular Security Guide.
   ✓ Azure Databricks Security Best Practices.
   ✓ Guies Scala.

3. S'ha de mantenir un **catàleg de requisits** de seguretat, per garantir la implementació efectiva de mesures de seguretat, protegir actius i dades, i facilitar el compliment de la normativa.

4. En quant a la **implementació**:

   ✓ Totes les **eines de desenvolupament** (IDE principalment) han de:
   - Ser configurades de forma segura.

Finançat per
Unió Europea Fons Europeu Next Generation · Gobierno de España · Plan de Recuperación, Transformación y Resiliencia · Next Generation Catalunya · Generalitat de Catalunya

- Incloure els següents **plugins** de detecció de vulnerabilitats, problemes de qualitat i seguretat (o d'altres de similars):
  - SpotBugs.
  - SonarLint, connectat amb SonarQube.
  - Dependency Check, per poder analitzar dependències amb tercers.

✓ S'ha de mantenir el **control de versions** del software.

✓ Per al desenvolupament segur s'ha de tenir en compte:

- Els controls proactius d'OWASP, d'**obligat** compliment. Al següent Excel es detalla cadascun dels controls i permet fer un seguiment de la seva implementació, que ha de ser presentat a l'equip de seguretat de la plataforma abans de poder posar res en producció.

PTD - Checklist
Proactive Controls OV

- Guies de desenvolupament segur de:
  - Angular
  - Java
  - JavaScript
  - Spring Boot
  - Scala
  - Python

✓ Tots els secrets han d'estotjar-se a **Azure Key Vault**. Si es treballa amb Databricks, s'empraran els Secret Scopes associats als Azure Key Vault. La creació de secrets ha de ser **gestionada amb l'equip de seguretat encarregat**.

5. En quant a la **verificació** s'han de dur a terme, al menys, les següents proves de seguretat:

✓ **Tests unitaris** amb un cobriment mínim del 85% del codi.

✓ **Anàlisi estàtica de codi font (SAST)** amb SonarQube + FindBugs. Aquestes anàlisis es duran a terme dins els pipelines CI/CD. El codi que no passi les proves SAST no pujarà al repositori. Per tant, és recomanable que els desenvolupadors facin servir els plugins esmentats abans per detectar possibles vulnerabilitats.

✓ **Anàlisi de dependències de tercers (SCA)** amb Dependency Track dins el pipelines CI/CD. El codi que no passi les proves SCA no pujarà al repositori. Per tant, és recomanable que els desenvolupadors facin servir el plugin Dependency Check esmentat abans dins els seus IDE per detectar possibles problemes.

✓ **Anàlisi dinàmica d'aplicacions (DAST)**. Són proves dinàmiques que només es duran a terme a l'entorn de PRE amb l'eina OWASP ZAP. Aquesta només és utilitzada per l'equip de la Oficina de Seguretat de Minsait de CTTI (rspminsait@minsait.com) i per tant és qui gestiona les peticions de proves DAST, la seva realització i l'entrega de resultats a Gencat.

6. S'ha de dur a terme el **registre d'activitats dels usuaris i d'esdeveniment** dins l'aplicació. Aquestes traces escrites per l'aplicació seran recollides pels serveis de logs del proveïdor cloud, pel que serà necessari coordinar-se amb l'equip de seguretat per tal de realitzar la configuració adient. Per defecte, el **període de retenció de logs** serà de 6 mesos disponibles en tot moment i de 12 mesos disponibles sota demanda, el que implica un total de 18 mesos de retenció. Quan sigui possible, **s'ha d'enregistrar**:

✓ Falles en la validació d'entrada, per exemple, violacions del protocol, codificacions inacceptables, noms i valors de paràmetres invàlids.

Finançat per
Unió Europea Fons Europeu Next Generation · Gobierno de España · Plan de Recuperación, Transformación y Resiliencia · Next Generation Catalunya · Generalitat de Catalunya

- ✓ Falles de validació de sortida, per exemple, desajustaments del conjunt de registres de la base de dades, codificació de dades invàlida.
- ✓ Èxits i fracassos de l'autenticació. Important no enregistrar la contrasenya en els logs.
- ✓ Falles d'autorització (control d'accés).
- ✓ Falles en la gestió de la sessió, per exemple, modificació del valor d'identificació de la sessió de *cookies*.
- ✓ Errors d'aplicació i esdeveniments del sistema, per exemple, errors de sintaxis i de temps d'execució, problemes de connectivitat, problemes de rendiment, missatges d'error de servei de tercers, errors del sistema d'arxius, detecció de virus de càrrega d'arxius, canvis de configuració.
- ✓ Arrencades i tancaments d'aplicacions i sistemes relacionats, i inicialització del registre (inici, parada o pausa).
- ✓ Utilització de funcions de major risc, per exemple, connexions de xarxa, addició o eliminació d'usuaris, modificació de privilegis, assignació d'usuaris a fitxes, addició o eliminació de fitxes, utilització de privilegis d'administració de sistemes, accés d'administradors d'aplicacions, totes les accions d'usuaris amb privilegis administratius, accés a dades de titulars de targetes de pagament, utilització de claus de xifratge de dades, canvis de claus, creació i eliminació d'objectes a nivell de sistema, importació i exportació de dades, inclosos informes en pantalla, presentació de contingut generat pels usuaris, especialment càrregues d'arxius.
- ✓ Permisos legals i d'un altre tipus, per exemple, permisos per a la utilització de telèfons mòbils, condicions d'ús, termes i condicions, consentiment per a l'ús de dades personals, permís per a rebre comunicacions comercials.
- ✓ Fallada en la seqüenciació.
- ✓ Ús excessiu.
- ✓ Canvis de dades.
- ✓ Frau i altres activitats delictives.
- ✓ Comportament sospitós, inacceptable o inesperat.
- ✓ Modificacions de la configuració.
- ✓ Arxiu de codi d'aplicació i/o canvis en la memòria.

2.2 Gestió d'usuaris

Les directrius a seguir en quant a la gestió d'usuaris són les següents.

1. A la Plataforma de Dades del CTTI es defineixen les següents tipologies d'usuaris:

   - ✓ **Usuaris d'administració**, amb privilegis administratius sobre els diferents components de la plataforma de dades (Databricks, MongoDB Atlas, Microsoft Azure, etc.). Quan sigui possible, seran usuaris nominals del CTTI i sempre es farà servir MFA durant la seva autenticació.
   - ✓ **Usuaris nominals** associats a persones físiques. Aquests seran usuaris de la Generalitat i iniciaran sessió SSO a través de **GICAR** del CTTI. GICAR es sincronitza alhora amb Microsoft Entra ID de la plataforma, de manera automàtica. És competència de CTTI.
   - ✓ **Usuaris màquina**, que accediran a la plataforma a través de SSH, SFTP, JDBC, interfases no SSO, etc. Principalment, seran **usuaris genèrics** associats a altres sistemes que no formen part de la plataforma de dades (BI, portals i backoffices departamentals, sistemes de tercers, etc.) i aquells **usuaris automàtics** d'explotació i processament de les dades de la plataforma.

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

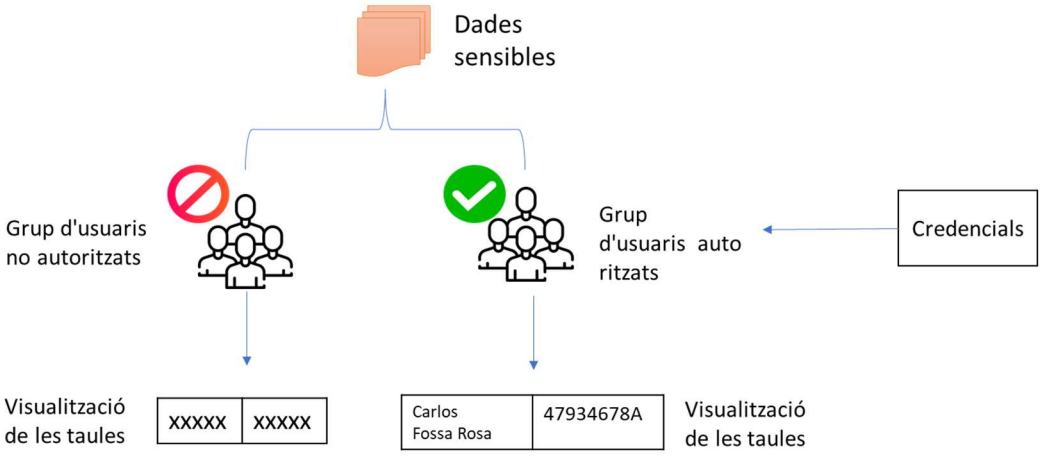
2. Els **usuaris màquina** s'han de crear des dels diferents components de la plataforma de dades. Aquests, per fer-los servir, han de tenir assignades les credencials corresponents, segons el component de la plataforma:

   - ✓ Databricks: *access token* associat al compte d'App d'Azure del Service Principal.
   - ✓ MongoDB: password.
   - ✓ Eventhub: certificat mTLS.
   - ✓ SFTP d'ingesta de dades: password o clau SSH.
   - ✓ Denodo: OAUTH o password.

3. Per poder treballar amb un **usuari**, s'ha de fer petició a l'equip d'administració d'usuaris, **justificar** necessitat i indicar els requisits d'accés als components de la plataforma (Databricks, MongoDB Atlas, etc.).

2.3 Control d'accés

El control d'accés ajuda a prevenir que persones no autoritzades obtinguin accés als diferents recursos de la PTD. Mitjançant els permisos d'accés a la plataforma, es podrà controlar de forma granular quins usuaris hi tenen accés.

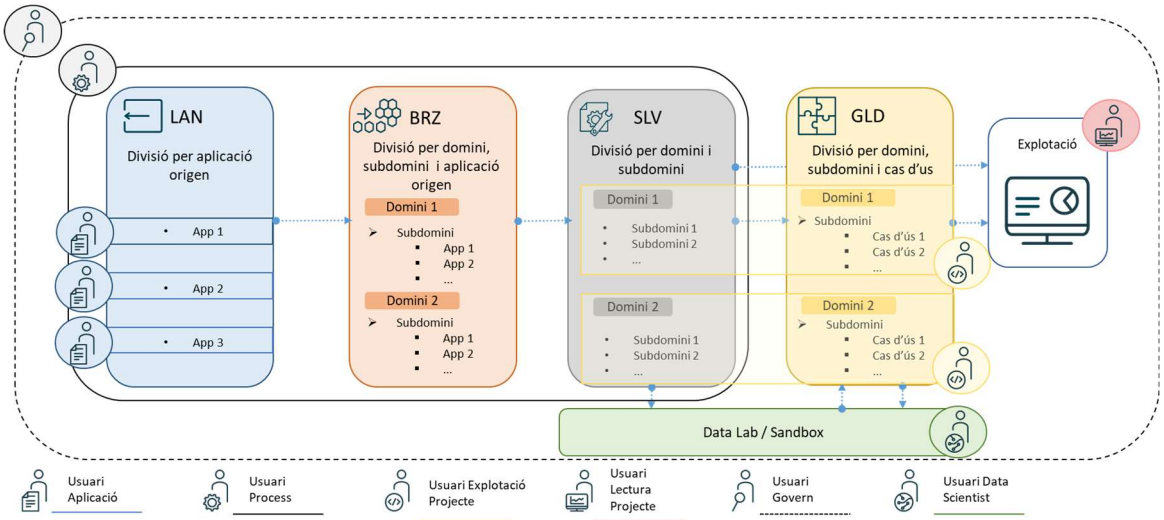


En quant a les directrius de **control d'accés** a les dades i altres recursos de la PTD:

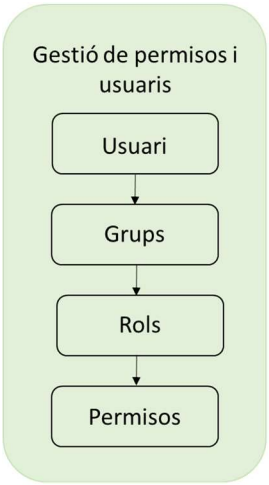
1. Els prestadors de serveis de manteniment i desenvolupament **no han de tenir accés a les dades de PRO**. La gestió d'usuari a PRO és **responsabilitat de negoci** (departament). No obstant això, els prestadors de serveis han de procurar que les mesures establertes i configurades de control d'accés siguin les adients (contrasenyes segures, que el sistema permeti crear rols, MFA, etc.).

2. Es faran servir els **rols i grups** definits per l'equip de seguretat. Qualsevol nova petició haurà de ser **avaluada i aprovada per aquest equip, actuant baix les directrius del CTTI**. Al següent esquema es mostra la definició dels perfils principals d'usuari existents i els seus accessos a cadascuna de les capes de dades d'un projecte a la PTD.

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



Al quadre següent es poden veure l'assignació dels diferents permisos per tipus d'usuari i capa de dades.



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'ús (GLD)
Lectura projecte	Visualització de dades de Silver i Gold. Particularitzable en funció cas d'ús.	• Silver (read) • Gold (read)	Subdomini (SLV) Cas d'ús (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'ús (GLD)

3. Els recursos i dades del sistema es protegiran de tal forma que **per defecte s'impedeix el seu ús**, excepte per als usuaris amb els drets d'accés suficients.

4. Els **drets d'accés** de cada recurs s'establiran segons les decisions de la **persona responsable del recurs**, que s'haurà d'atendre a les polítiques i normatives de seguretat de la PTD.

5. Es gestionaran els permisos i les autoritzacions d'accés amb incorporació dels principis de **menor privilegi i separació de funcions**.

6. Els **drets d'accés de cada usuari** es limitaran atenent els principis següents:

   - ✓ **Tot accés estarà prohibit**, excepte autorització expressa.
   - ✓ **Mínim privilegi**. Els privilegis de cada usuari es reduiran al mínim estrictament necessari per complir amb les seves obligacions.
   - ✓ **Necessitat de conèixer**. Els privilegis es limitaran de manera que els usuaris només accediran al coneixement d'aquella informació requerida per complir les seves obligacions.

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

- ✓ **Capacitat d'autoritzar**. Només i exclusivament el personal amb competència per fer-ho pot concedir, alterar o anul·lar l'autorització d'accés als recursos, d'acord amb els criteris establerts pels responsable.

Els **mecanismes d'autenticació**, que actualment es poden emprar a la PTD, són els de la taula següent, qualsevol altra necessitat s'ha de presentar, avaluar i ser aprovada pel CTTI i l'Agència:

Plataforma	Mecanismes/sistemes autenticació	Descripció
Databricks	Microsoft Entra ID/OAUTH	L'autenticació d'usuaris nominals es realitzarà mitjançant el Microsoft Entra ID del CTTI, que es sincronitza amb el GICAR (no federat) i no permetrà SSO.
	Service principal/OAUTH	Mecanisme de Databricks que representa un usuari màquina dintre del sistema, permetent l'automatització de tasques. Per a cada *service principal* a fer servir, s'ha d'enregistrar una aplicació dins Microsoft Entra ID.
MongoDB Atlas	GICAR CTTI/SAML	MongoDB Atlas permet gestionar l'autenticació d'usuaris nominals federant-se amb GICAR CTTI, emprant el protocol SAML 2.0. Els usuaris entraran amb les seves credencials de GICAR. S'emprarà principalment per l'accés a les consoles d'administració.
	SCRAM	Usuari i password per als usuaris de les bases de dades, és a dir, els usuaris màquina.
Eventhub	mTLS	Dins la Plataforma Eventhub els clients han d'emprar mTLS per autenticar-se contra els brokers de Kafka, ja sigui per produir com per consumir esdeveniments.
SFTP	Usuari/Password	Usuari i password de l'SFTP de la plataforma.
	PKI	Parell de claus pública-privada per connectar-se a l'SFTP de la plataforma sense necessitat d'utilitzar un usuari i contrasenya.
Denodo	GICAR CTTI/OIDC	Denodo permet gestionar l'autenticació d'usuaris nominals federant-se amb GICAR CTTI, emprant el protocol OIDC. Els usuaris entraran amb les seves credencials de GICAR amb MFA. S'emprarà principalment per l'accés a les consoles d'administració.
	Usuari/Password	Per als usuaris màquina, serà necessari emprar usuari i password.

2.4 Seguretat de la informació

En quant a les seguretat de les dades, s'han de seguir les següents directrius:

1. S'ha de complir amb els requisits del Marc de Ciberseguretat per a la Protecció de Dades (MCPD) - Mesures de seguretat de l'Agència, segons el nivell de protecció resultant de la qualificació de la informació.

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

2. S'ha d'omplir el formulari de qualificació de la informació exigida per l'Agència de Ciberseguretat i l'ENS. L'Agència farà arribar la seva qualificació i una llista de requisits a complir. Per al conjunt de la PTD s'han establert els nivells de protecció de la següent taula.

Nivell de Seguretat	Molt Crític	**Crític**	Sensible	Intern	Públic
Nivell de Privacitat	Alt		**Mitjà**		Baix
Nivell de Visibilitat	**Molt Alt**	Alt		Mitjà	Baix
Nivell de Disponibilitat	Essencial	**Estratègic**		Important	Bàsic

+ → -

La categorització anterior no eximeix del fet que els projectes nous hagin de qualificar la seva informació, abans d'aplicar les mesures de seguretat més adients per protegir les seves dades.

3. Queda **prohibit l'ús de dades personals reals en entorns no productius**. Queda prohibida l'exportació de dades personals de producció cap a entorns no productius sense haver rebut prèviament un **tractament d'anonimització** i l'aprovació del seu responsable.

4. **Les dades a preproducció i desenvolupament mai no podran ser reals**.

5. Tots els **accessos de dades de producció** han de ser aprovats pel seu responsable i justificat convenientment. S'ha d'indicar sobre quines dades s'actuarà, com s'hi accedirà i quant de temps serà necessari el seu accés.

6. Les **extraccions** de dades de **producció** cap a sistemes tercers seran aprovades pel seu responsable. Només s'extrauran les dades mínimes per cobrir els requisits dels casos d'ús i, sempre que es pugui **anonimitzades** o **pseudonimitzades**. Totes les dades viatjaran **xifrades**.

7. Totes les dades seran **xifrades en repòs i en trànsit**. Tot el material criptogràfic emprat al xifrat de dades s'ha d'emmagatzemar i gestionar dins Azure Key Vaults.

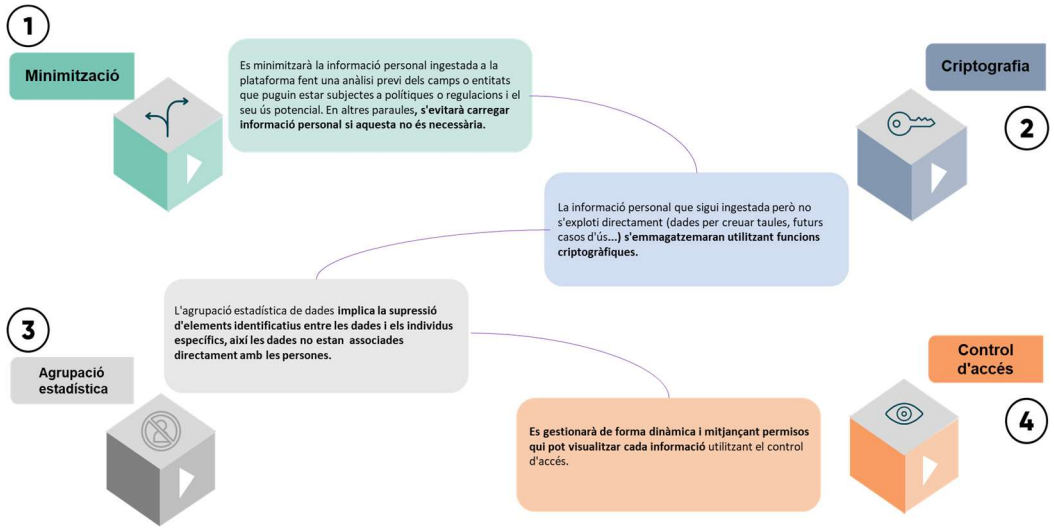
8. Es **minimitzarà** la informació personal i de negoci ingestada a la PTD. És a dir, només s'ingestaran les dades necessàries per a cada cas d'ús.

9. S'han **d'auditar els accessos a dades personals**.

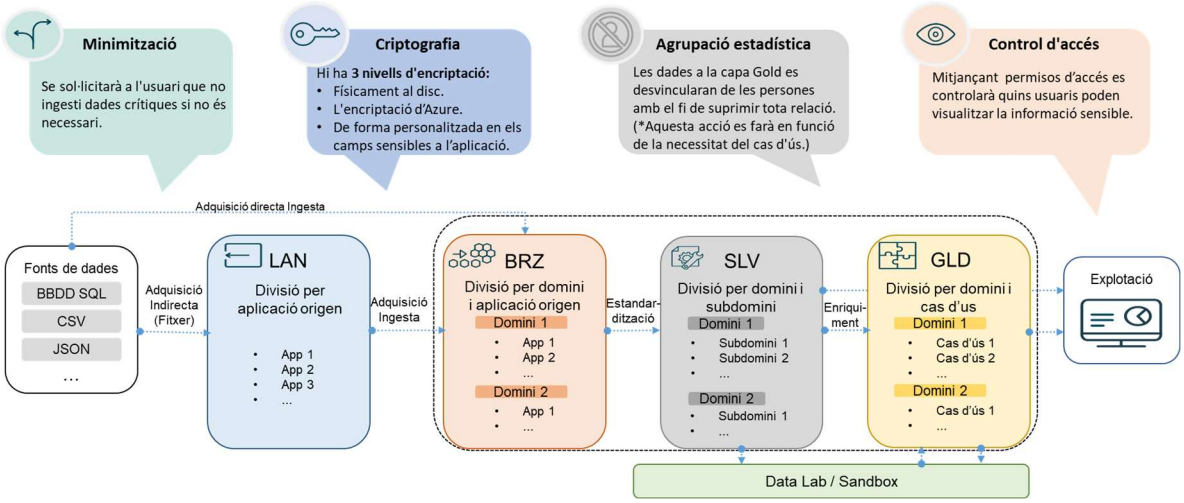
10. Es realitzaran **còpies de seguretat** de les dades. La **política** de compliment de còpies de seguretat per a la PTD és la següent: **estàndard**. És a dir, diària incremental amb 2 setmanes de retenció, setmanal completa amb 1 mes de retenció, mensual completa amb 3 mesos de retenció i anual completa amb 1 any de retenció (cobrint 1 any i 3 mesos de retenció de dades). Està alineada amb la guia del CTTI de còpies de seguretat.

A la següent imatge es poden veure algunes de les tècniques a fer servir per tal de garantir la protecció de les dades personals.

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



I a la següent imatge a on és convenient aplicar cadascuna de les tècniques esmentades dins el flux de les dades dins la PTD.



2.5 Altres directrius de seguretat

Retirar comptes i contrasenyes estàndard. No és faran servir en cap moment comptes ni contrasenyes estàndard. Els usuaris nominals entraran per GICAR o Entra ID; és en aquests sistemes on es gestionen les contrasenyes dels usuaris nominals.

Aplicació de la regla de mínima funcionalitat. Totes les aplicacions que es creen sobre la PTD només han de proporcionar les funcionalitats necessàries per al seu funcionament correcte.

Aplicació de la regla de seguretat per defecte. Totes les aplicacions que es creen sobre la PTD han d'incloure el control d'accés dels usuaris, el que implica que els usuaris només han de poder realitzar accions definides pel seu perfil. Només l'administrador pot reduir la seguretat de manera conscient. I encara que un usuari desconegui com treballar no podrà realitzar accions fora de les accions permeses dins del seu perfil.

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

Tots els **intercanvis d'informació i prestació de serveis amb altres sistemes** hauran de ser objecte d'una **autorització** prèvia. Tot flux d'informació estarà prohibit excepte autorització expressa. Per a cada **interconnexió** es documentarà explícitament: les característiques de la interfície, els requisits de seguretat i protecció de dades i la naturalesa de la informació intercanviada.

A la PTD existeix el xifrat de les dades en trànsit per tal d'evitar qualsevol tipus d'atac que puguin comprometre la integració de la informació. Només s'admeten els **protocols de comunicacions segures TLS v1.2 o superior i ssh**. Totes les comunicacions han de passar per la NET0 de CTTI, tant internes com externes.

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