FGC
Ferrocarrils
de la Generalitat
de Catalunya

Servei de plataforma de Data Secure Posture Management per FGC

Especificació tècnica

Àrea de Ciberseguretat

2026

Índex

Introducció 2
Objecte 3
Requeriments generals 4
Requisits de seguretat de la solució 4
Requisits funcionals 5
Detecció, gestió del risc, amenaces i monitoreig 7
Requeriments de posada en servei 8
Requeriments de suport i manteniment 11

Introducció

Ferrocarrils de la Generalitat de Catalunya (FGC) gestiona un volum creixent d'informació digital crítica associada a l'operació ferroviària, la gestió d'infraestructures, la prestació de serveis públics, la relació amb la ciutadania, així com dades de caràcter personal, econòmic, estratègic i tècnic. Aquest conjunt de dades constitueix un actiu essencial per a l'organització i, alhora, un vector de risc elevat si no es governa, protegeix i controla adequadament .

L'adopció progressiva de solucions d'Intel·ligència Artificial generativa i assistents digitals corporatius (com Copilot per a Microsoft 365 o entorns d'IA empresarial) introdueix nous riscos específics relacionats amb la confidencialitat, la traçabilitat i l'ús indegut de la informació.

En aquest context, amb la complexitat dels entorns híbrids, la proliferació de repositoris col·laboratius, l'increment del teletreball i l'ús intensiu de plataformes com Microsoft 365 i assistents de IA generativa, fan imprescindible disposar d'una visió transversal, contínua i contextualitzada del risc associat a les dades. Els enfocaments tradicionals de seguretat, centrats exclusivament en el perímetre o en l'endpoint, resulten insuficients per garantir la protecció efectiva de la informació en escenaris actuals .

La implantació d'una eina de Data Security Posture Management (DSPM) permet a FGC avançar cap a un model madur de Govern de la Dada, alineat amb els principis de seguretat per disseny, mínim privilegi i confiança zero. Aquest tipus de solució proporciona capacitats clau com ara:

- Coneixement precís de quines dades existeixen, on es troben i quin nivell de sensibilitat tenen.
- Identificació de sobreexposicions, permisos excessius i dades obsoletes.
- Correlació entre sensibilitat de la informació, permisos efectius i activitat real.
- Priorització del risc en funció de l'impacte potencial sobre els serveis essencials.

Objecte

FGC gestiona informació essencial per a la prestació de serveis públics, l'operació ferroviària, la gestió d'infraestructures i la relació amb la ciutadania. Aquest entorn exigeix un model avançat de govern de la dada, que permeti passar d'una protecció reactiva a un enfocament proactiu, continu i basat en risc.

La contractació d'una plataforma DSPM constitueix una peça clau dins l'estratègia corporativa de seguretat de la informació, govern de la dada i compliment normatiu, especialment en entorns híbrids i col·laboratius.

L'objecte del present plec és la contractació d'una plataforma de Data Security Posture Management (DSPM) en modalitat SaaS, destinada a garantir la protecció, govern, control i supervisió contínua de tota la informació gestionada per Ferrocarrils de la Generalitat de Catalunya (FGC), classificada com a categoria ALTA segons l'Esquema Nacional de Seguretat (ENS).

La solució haurà de permetre identificar, analitzar i reduir de manera contínua els riscos associats a les dades, assegurant la confidencialitat, integritat, disponibilitat i traçabilitat de la informació crítica i sensible.

Requeriments generals

La plataforma proposada ha de ser SaaS.

Ha de ser capaç de detectar ciberamenaces d'actors interns i externs a través de l'anàlisi de les dades, l'activitat dels comptes dels usuaris i el seu comportament en el context organitzatiu; prevenir i limitar les catàstrofes associades a incidents de fuga de dades, exfiltració o el ransomware, protegint totes les dades; i mantenir eficaçment un estat segur mitjançant la correcció automatitzada dels riscos associats a les dades i als usuaris.

La plataforma necessària ha de proporcionar casos d'ús addicionals que incloguin protecció de dades, privacitat i governança a través d'un enfocament de confiança zero, compliment normatiu, classificació i detecció i resposta a amenaces.

L'eina proposada i la tota la solució ha de permetre el compliment de l'Esquema Nacional de Seguretat en nivell alt (ENS nivell alt) a FGC.

El contracte objecte d'aquesta licitació, ha d'incloure la solució, la posada en servei i el manteniment, i haurà de garantir com a mínim:

- Gestió i control de dades estructurades i no estructurades.
- Gestió i control de repositoris On-Premisses i Microsoft 365.
- Gestió i control de les dades i les interaccions amb agents de IA (mínim Copilot i ChatGPT).
- Gestió i control de les identitats d'usuari, comptes privilegiades i comptes de servei.
- Gestió i control de l'activitat sobre dades, permisos i configuracions. Ha de permetre accions de resposta automàtica sobre l'activitat detectada sobre les dades.
- Generació d'evidències per a auditories ENS categoria ALTA i RGPD.

El contracte inclourà totes llicències necessàries per garantir totes les funcionalitats demanades, el manteniment de la solució, el suport, les actualitzacions, serveis professionals i formació durant tota la vigència del contracte.

Requisits de seguretat de la solució

La solució implantada haurà de fonamentar-se en un model de seguretat de confiança zero (Zero Trust), en què cap accés sigui considerat fiable per defecte. Haurà d'aplicar el principi de mínim privilegi dinàmic, ajustant els permisos en funció de l'ús real i del context de risc. La seguretat haurà d'estar integrada per disseny i per defecte en tots els components de la solució. S'haurà de garantir una separació clara de funcions i rols, evitant conflictes i accessos indeguts. La

plataforma haurà d'oferir monitorització contínua de l'estat de seguretat i capacitats de resposta automatitzada davant incidents. Així mateix, haurà de proporcionar una visió contextual i unificada del risc, combinant la sensibilitat de la dada, els permisos efectius, el grau de compliment normatiu (ENS i RGPD, com a mínim) i l'activitat real dels usuaris i sistemes, permetent una gestió proactiva i basada en risc.

Requisits funcionals

La solució haurà de disposar de capacitats de descobriment automàtic i continu de dades sensibles i crítiques en tots els repositoris corporatius, tant On-Premises com en entorns al núvol. Haurà de permetre la classificació de la informació segons criteris de sensibilitat, criticitat i impacte, alineats amb el model de govern de la dada de FGC. La plataforma identificarà i visualitzarà concentracions de dades d'alt impacte, facilitant la priorització del risc. Haurà d'incloure regles predefinides per a la detecció de PII, dades sotmeses a GDPR, PCI, propietat intel·lectual, secrets i credencials. Igualment, haurà de permetre la definició de regles personalitzades adaptades a les necessitats específiques de FGC. La classificació haurà de garantir una alta precisió, minimitzant el nombre de falsos positius, i generar evidències auditables per al compliment normatiu i l'ENS.

La solució haurà de garantir una classificació incremental i contínua de les dades en temps real, de manera que qualsevol creació o modificació d'informació sigui analitzada automàticament sense necessitat d'execucions completes periòdiques. Haurà de disposar de capacitats d'etiquetatge automàtic, així com de mecanismes per detectar i corregir etiquetes incorrectes o absents, assegurant la coherència amb el model de govern de la dada de FGC. La plataforma haurà de permetre la realització d'anàlisis puntuals (ad-hoc) sota un estricte control de rols i permisos, limitant l'accés únicament als perfils autoritzats. Totes les accions de classificació, reclassificació, etiquetatge i consulta hauran de quedar registrades de manera íntegra i traçable, constituint evidències auditables per al compliment de l'Esquema Nacional de Seguretat en categoria ALTA.

La plataforma haurà de disposar de capacitats avançades per a la detecció automàtica de secrets i credencials exposats en repositoris corporatius, tant en entorns On-Premises com al núvol. Haurà d'identificar contrasenyes, claus criptogràfiques, certificats digitals i tokens d'accés emmagatzemats en text pla o en ubicacions no autoritzades. La solució haurà de detectar secrets emmagatzemats de manera insegura o que no compleixin les polítiques corporatives de seguretat de FGC. Així mateix, haurà de permetre la detecció d'accessos indeguts a secrets per part d'usuaris o serveis no autoritzats, correlacionant permisos i activitat real. La plataforma haurà d'identificar i prioritzar els riscos associats a comptes de servei, especialment aquells amb

privilegis elevats o credencials compartides. Totes aquestes deteccions hauran de generar alertes, registres traçables i evidències auditables.

S'haurà de proporcionar una visibilitat completa, unificada i en temps real sobre les dades corporatives de FGC, independentment de la seva ubicació o tecnologia subjacent. Haurà de ser plenament compatible amb els sistemes On-Premises corporatius, garantint el control dels accessos, permisos i activitat associada a la informació crítica. Igualment, haurà d'integrar-se de manera nativa amb Microsoft 365, incloent SharePoint, OneDrive, Exchange i Teams, permetent la descoberta, classificació i auditoria de dades sensibles en entorns col·laboratius. La plataforma haurà de donar suport als entorns d'Intel·ligència Artificial corporativa, com Copilot per a Microsoft 365 o solucions d'IA empresarial (mínim ChatGPT), assegurant una traçabilitat completa de l'accés, ús i exposició de dades sensibles. Aquesta visibilitat híbrida haurà de facilitar el compliment normatiu, el govern de la dada i la generació d'evidències auditables.

La solució haurà de disposar de capacitats avançades de gestió d'accessos i privilegis sobre les dades corporatives, permetent l'anàlisi detallada dels permisos efectius i heretats en tots els repositoris. Haurà d'identificar de manera automàtica permisos excessius, inconsistents o no justificats, especialment en dades sensibles o crítiques. La solució haurà de permetre la correcció automàtica o assistida d'aquests permisos, d'acord amb les polítiques corporatives. S'hauran d'aplicar polítiques de mínim privilegi basades en l'ús real de les dades, ajustant els accessos en funció del comportament observat. Igualment, la solució haurà de gestionar dades i accessos obsolets, detectant informació no utilitzada i comptes inactius. Totes les accions de remediació, modificació de permisos i revocació d'accessos hauran de quedar registrades de forma completa, traçable i auditables.

La solució ha de protegir totes les bases de dades de l'empresa. Ha de ser capaç de detectar accessos no autoritzats, comportaments anòmals i possibles exfiltracions (basades en l'anàlisi també del comportament dels usuaris). Ha de ser capaç de donar informació i traçabilitat de qui accedeix a quines dades, quan i com. Haurà de permetre monitoritzar l'activitat en temps real, capturar de consultes i activitat amb detall forense, i capacitat de detectar i bloquejar consultes sospitoses o exfiltració en temps real. Haurà de permetre, com en els altres àmbits, el descobriment i la classificació automàtica de dades sensibles mitjançant així com l'etiquetat automàtic i mapejats amb diferents marcs de compliment.

La protecció de les bases de dades haurà de ser el mínim intrusiu i sense haver d'instal·lar clients ni agents pesats als servidor. S'hauran de protegir mínim els següents tipus: SQL Server, Oracle, MySQL, PostgreSQL; i com a mínim 12 servidors bases de dades dels tipus esmentats.

Detecció, gestió del risc, amenaces i monitoreig

La solució haurà de proporcionar funcionalitats de millora contínua de la postura de seguretat orientades a la protecció de dades:

- Capacitats d'avaluació contínua del risc, combinant nivell de sensibilitat de la informació, accessos i activitat detectada.
- Identificació i gestió de configuracions errònies en entorns SaaS i cloud.
- Control i monitoratge del risc associat a terceres aplicacions connectades.
- Disponibilitat de panells (dashboards) per a la visualització global de l'estat de seguretat de les dades, accessos i exposició al risc.

La solució haurà d'incloure capacitats específiques per a la gestió i monitoratge del risc associat a identitats:

- Descobriment automàtic d'identitats de risc en entorns híbrids i multi-cloud.
- Monitoratge específic de comptes privilegiats amb generació d'alertes davant comportaments anòmals.
- Identificació i eliminació d'identitats obsoletes o inactives.
- Detecció d'usuaris sense mecanismes d'autenticació robusta (ex. sense SSO o MFA).
- Correlació d'identitats entre múltiples entorns per tenir una visió unificada del risc.

La solució haurà de proporcionar capacitats avançades de monitoratge continu, detecció d'amenaces i resposta automatitzada, garantint la integració amb els serveis de monitorització del SOC de FGC (Centre d'operacions de Ciberseguretat) mitjançant el seu SIEM:

- La plataforma haurà de permetre l'establiment de línies base de comportament per usuari, identitat i dispositiu, amb capacitat de detecció de desviacions mitjançant tècniques UEBA (User and Entity Behavior Analytics).
- Haurà d'integrar-se amb el SIEM corporatiu mitjançant mecanismes estàndard de recollida, normalització i correlació de logs, assegurant l'enviament d'esdeveniments en temps real per a la seva explotació al SOC de FGC.
- El sistema haurà de suportar la monitorització contínua 24x7 d'esdeveniments i alertes de seguretat, permetent la detecció primerenca d'incidents i amenaces.

- La solució haurà de proporcionar capacitats de detecció d'anomalies i generació d'alertes contextualitzades, amb classificació i priorització segons risc.
- Haurà de disposar de mecanismes de resposta automatitzada que permetin contenir o mitigar amenaces en temps real.
- Haurà de garantir la traçabilitat completa de l'activitat sobre les dades, incloent registres detallats per a anàlisi forense i compliment normatiu.
- La plataforma haurà d'oferir capacitats de correlació amb intel·ligència d'amenaces (CTI) i models actualitzats basats en amenaces reals.
- Es requerirà la integració amb els processos del SOC de FGC per a la gestió d'incidents, investigació i escalat, incloent la generació de casos d'ús i playbooks associats.

Totes les deteccions hauran de generar alertes, registres traçables i evidències auditables conforme al compliment de l'ENS categoria ALTA.

Requeriments de posada en servei

La solució proposada haurà de se claus en mà. S'haurà de posar en servei de manera coordinada amb el equip de Ciberseguetat de FGC, pero no s'acceptarà el pas a producció fins a la valoració positiva del projecte per part de FGC.

El proveïdor haurà de:

▪ Incloure totes les llicencies per complir els requeriment definits al llarg d'aquest document, així com el suport del fabricant pel període de durada del contracte.

▪ S'haurà de realitzar una auditoria de la situació actual per dimensionar i avaluar la planificació del projecte que serà presentada i aprovada per FGC.

Aquesta haurà d'incloure:

- Estat actual (seguretat, polítiques, etc.)
- Pla d'actuació per implantar i protegir tots els repositoris de dades
- Pla d'activitats a realitzar, ordenades i prioritzades
- Pla de possibles millores de postura de seguretat de les dades

▪ El licitador haurà de garantir el correcte funcionament de tots els repositoris i totes les dades en producció de FGC durant el desplegament de la solució.

Serveis requerits de posada en servei

El licitador haurà de gestionar tot el cicle de vida del projecte d'implantació, configuració i posada en servei, així com la detecció de riscos, mitigacions i millores (*fine tunning).*

El projecte haurà de contemplar com a mínim les següents fases:

1.- Preparació i governança del projecte

El licitador haurà de definir l'abast, actors, responsabilitats, planificació, dependències, riscos i mecanismes de decisió i seguiment. Serà necessari, com a mínim, acta de definició i constitució del projecte, acta de kick-off, pla de projecte i matriu de responsabilitats.

2.- Descobriment i inventari de dades

El licitador haurà de recollir tots els repositoris i les ubicacions de dades (on-prem i/o cloud), així com creació d'un catàleg únic de totes les fonts de dades existents i que s'integraran a la solució per a tenir un definició de seguretat única per a totes les dades de FGC.

3.- Arquitectura i integració tècnica

El licitador haurà de realitzar un pla de desplegament de la solució per tal de desplegar la solució de DSPM i connectar-la a identitats, fonts de dades, SIEM i/o altres eines de seguretat existents i que s'hagi identificat durant la preparació del projecte que aportarà valor a la millora de la seguretat de les dades.

El contractista haurà de desplegar la solució DSPM SaaS i configurar connectors/agents necessaris per a l'escaneig, garantint el principi de mínims privilegis i la màxima seguretat.

La solució haurà d'integrar-se com a mínim amb IAM/Directori corporatiu (EntraID/AD), amb SIEM (Splunk) i el nostre sistema de ticketing (Jira), per a la gestió d'alertes i correlació.

4.- Classificació de dades i model de risc

En aquesta fase, s'haurà d'identificar totes les dades sensibles, assignar etiquetes/classificacions automàtiques i generar un informe del risc al que estan exposades les dades.

La solució haurà de disposar de mecanismes de classificació automàtica (per patrons, diccionaris, tipus de dades) i classificació assistida, amb suport per a categories com PII i dades sensibles.

El licitador haurà de definir i parametritzar un model de risc de les dades basat en criteris recomanats i acordats: sensibilitat, exposició, configuracions, permisos i criticitat del repositori.

Finalment en aquesta fase s'ha de presentar un informe del nivell de risc actual i una proposta de mitigació del risc a assolir al llarg de la implantació i posada en servei de la solució i durant la durada del contracte.

5.- Detecció d'exposicions i bretxes de postura

En aquesta fase cal localitzar dades mal protegides (públiques, compartides, sense xifrar, permisos excessius) i "shadow data".

La solució haurà de detectar i reportar exposicions (comparticions externes, dades públiques, permisos excessius, dades sense control) i males configuracions relacionades amb protecció de dades.

El licitador haurà de preparar i lliurar un registre de tot el que s'ha trobat prioritzat (risc alt/mitjà/baix) amb descripció, evidència, impacte.

6.- Remediació i implantació de controls

El licitador haurà d'executar accions correctores (mínim privilegi, tancament d'exposicions, enfortiment de configuracions, etc.) i establir controls preventius.

El licitador haurà de proposar i executar (quan s'autoritzi) accions de remediació, incloent revisió d'accessos, retirada de comparticions inadequades, aplicació de xifrat/configuració segura i hardening relacionat amb dades.

S'hauran de definir playbooks de remediació (manuals o automatitzats) i criteris de validació post-correcció.

El licitador haurà de preparar el pla de remediació, amb evidència de canvi (abans/després), informe de reducció de risc i planificació per dur a terme.

7.- Monitoratge continu, alertes i reporting

En aquest punt cal passar de descobriment estàtic ("foto fixa") a vigilància contínua. Cal que el licitador prepara una bateria d'alertes automàtiques per a qualsevol detecció de risc, noves dades sensibles, canvis de permisos, noves exposicions, etc.

La solució haurà d'oferir i quedar configurada en monitoratge continu (o escanejos programats) i generació d'alertes davant canvis rellevants: noves dades sensibles, ampliació de permisos, comparticions externes, moviments de dades.

El licitador haurà de configurar l'eina per tal de mostrar i visualitzar l'estat, mitjançant dashboards executius i operatius, i informes periòdics orientats a: risc, compliment i tendències.

8.- Compliment normatiu i evidències d'auditoria

Cal que queri clar i referenciat l'enllaç de l'eina de DSPM amb el compliment normatiu que li és d'aplicació a FGC, RGPD/ENS/NIS2.

El licitador haurà de donar evidencies entre les capacitats de detecció de la solució i els requeriments de compliment normatiu de RGPD/ENS/NIS2. Cal

referenciar tot el compliment normatius amb les capacitats de la solució de DSPM, definir totes les evidencies i com avaluar-les. Es necessària una matriu de correspondència entre capacitats DSPM i requisits de compliment definits, així com definir quines evidències es generen automàticament.

La solució haurà de permetre exportar evidències (informes, logs, inventari, traçabilitat d'accessos quan apliqui) per a auditories i control intern.

9.- Operació, transferència i millora contínua

El licitador ha de preparar un document final amb tota la documentació i el detall del projecte així com el model operatiu de la solució, la transferència de coneixement, el pla de millora i el manual operatius.

El projecte serà traspassat a FGC un cop s'hagi revisat i aprovat tota la documentació i s'hagi fet sessió formativa complerta a l'equip de FGC.

Serveis requerits d'acompanyament tècnic

El licitador haurà d'incloure durant la durada del contracte, un acompanyament tècnic especialitzat i continu per garantir l'ús òptim de la solució i la millora progressiva de la postura de seguretat de les dades de FGC.

Aquest servei haurà d'incloure una interacció recurrent per analitzar el seguiment i la evolució del servei per tal de donar suport en la identificació i planificació de millores i iniciatives relacionades amb la millora de seguretat global de les dades. Haurà de contemplar com a mínim:

- Seguiment continu del servei i suport tècnic especialitzat.
- Coordinació amb l'equip de Ciberseguretat de FGC per a la gestió, evolució i millora de la solució.
- Revisió periòdica de l'estat de la seguretat i del nivell de risc.
- Recomanacions de millora i optimització de la configuració i ús de la plataforma.

Requeriments de suport i manteniment

L'adjudicatari, donarà un suport especialitzat que contemplarà coma mínim les següents tasques durant tota la durada del contracte:

Resoldre consultes o incidents relacionats amb l'operació i administració dels dispositius de seguretat subministrats que puguin sorgir. S'haurà d'ajudar a resoldre dubtes d'administració sobre les funcionalitat dels equips objecte d'aquest contracte, així com donar suport necessari en cas d'incidència que requereixi coneixement expert sobre la tecnologia i/o el fabricant.

Donar suport, resoldre dubtes i aconsellar en les tasques de manteniment i actualitzacions a realitzar als equips.

Donar formació i actualització a l'equip de Ciberseguretat de FGC segons novetats d'ús i administració de la plataforma, així com optimització continua de seguretat.

Monitoreig i resposta a incidents, s'haurà de fer monitoratge, investigació i remediació/resposta de qualsevol incident detectat. S'haurà de donar cobertura continuada 24x7 i s'haurà de coordinar i integrar amb el SOC de FGC. Els mínims que s'hauran de cobrir son:

- Determinar si un incident constitueix una bretxa real de dades.
- Disposar de visibilitat completa sobre l'accés i ús de la informació.
- Respondre de manera eficaç davant amenaces internes i externes que evadeixen controls tradicionals.
- Monitorització contínua de l'activitat sobre dades.
- Detecció de comportaments anòmals i generació d'alertes.
- Investigació i resposta a incidents per part d'un equip expert.
- Suport forense, incloent recollida d'evidències, anàlisi i elaboració d'informes.
- Execució d'accions de mitigació i resolució d'incidents.

Per tal de poder requerir suport especialitzat a l'adjudicatari, aquest haurà de proporcionar una eina de tiquets, portal web o procediment per tal de garantir la correcta gestió i resposta sobre els incidents o consultes realitzades. Periòdicament l'empresa adjudicatària enviarà un informe del número d'incidents, peticions i consultes gestionades, en quin estat es troben i agrupades per severitat/criticitat durant el període d'enviament definit.

S'ha de complir un SLA de servei:

Detecció d'incident, investigació i notificació (FGC i SOC FGC):

Nivell de Severitat	Resposta
CRÍTIC	30 min
NO CRÍTIC	120 min

Catalogació:

Nivell de Severitat	Definició
CRÍTIC	Qualsevol esdeveniment que impliqui o pugui implicar l'exposició, l'accés no autoritzat o la manipulació de dades sensibles, amb un impacte immediat en la seguretat, el negoci o el compliment normatiu.

NO CRÍTIC	Resta d'incidents relacionats amb la seguretat de les dades.