Subministrament i servei de desplegament, configuració i posada en servei del sistema corporatiu de control d'accés a la xarxa (NAC) amb la finalitat d'incorporar la filial FGC Mobilitat / línia R-Aeroport a la solució ja existent de Ferrocarrils de la Generalitat de Catalunya.

Especificació tècnica

Àrea de Ciberseguretat

Juliol 2026

Índex

1. Introducció

Ferrocarrils de la Generalitat de Catalunya, en endavant FGC, és una empresa que aposta per les tecnologies en tots els seus àmbits de negoci. La tecnologia té avui en dia un paper imprescindible en el funcionament i l'avanç de les organitzacions. La informació i el seu correcte tractament, s'ha convertit en un dels principals actius. FGC, conscient d'això, i de la importància de protegir els seus actius té establertes unes mesures de Ciberseguretat i uns sistemes de control d'accés a les seves xarxes.

Amb l'objectiu mantenir el nivell de Ciberseguretat, aquest plec pretén la contractació de serveis d'un centre d'operacions de seguretat i el software de protecció d'accés a la xarxa definit a FGC.

2. Objecte

FGC té com a objectiu incorporar la filial de la línia R-Aeroport. L'objecte del present plec tècnic inclou el desplegament i la posada en servei del sistema corporatiu de control d'accés a la xarxa (NAC), amb l'objectiu de garantir una gestió centralitzada, segura i eficient dels accessos a la infraestructura de xarxa de FGC i de la seva filial, tot assegurant el compliment de les polítiques de seguretat definides per l'organització.

Per abastir aquest subministrament, l'empresa ha de disposar de software necessari pel desplegament NAC sent partner certificat del fabricant, a fi de poder gestionar l'escalat directe amb el fabricant (Nivell 3) necessari per aquesta contractació. Així mateix, l'empresa haurà de presentar tècnics certificats pel fabricant del producte de NAC que es fa servir a FGC per la posada en servei d'acord s'estableix a continuació del plec.

3. Abast i descripció del servei

3.1 **Subministrament i posada en servei NAC corporatiu**

L'abast del servei, és el subministrament i posada en servei de la protecció d'accés a la xarxa ja implementada en FGC.

- Posada en servei 60 dies naturals

Els serveis principals que s'hauran de contemplar i que seran detallats al llarg d'aquest document seran:

Llicenciament, serveis de suport i posada en servei

Cal contemplar el llicenciament necessari per afegir la filial de FGC Mobilitat a l'eina existent de NAC.

La previsió d'elements a controlar en la xarxa es de 300 dispositius i cal tenir visibilitat de la xarxa i controlar l'accés dels dispositius.

Les activitats mínimes que han d'estar cobertes en el servei de suport especialitzat (N2-N3):

· Configuració i posada en servei de tota la infraestructura.

· Definició i perfilat de tots els dispositius de la seu.

· Definició i implementació de regles de seguretat.

· Tasques que requereixin un coneixement dels components de fabricant, no associades a una incidència o mal funcionament de la plataforma.

· Revisió de la plataforma i polítiques. Enginyer Certificat pel Fabricant de la solució garantirà revisions de configuració per assegurar que la instal·lació i les polítiques definides compleixen amb les millors pràctiques.

· Certificació de la instal·lació per garantir la implementació òptima de la solució i assegurar que oferirà un rendiment òptim en funció de l'arquitectura de xarxa i mòduls.

- Identificació del final de vida i suports dels components.

- Recomanació de polítiques addicionals segons calgui.

- Monitorització i utilització de la memòria i CPU.

- La configuració de xarxa interna de les interfícies de xarxa.

- Auditoria de connexions dels ports SPAN i configuracions.

- Informes i configuracions de Dashboards.

- Comprovar actualitzacions disponibles i informar sobre les millores de les versions actuals.

- Homologacions de dispositius de xarxa addicionals si cal (Switches, Controladores WIFI/AP o Firewalls).

· Resolució d'incidències tècniques associades Autenticació i Autorització.

· Recuperació primària de serveis que NO afectin la continuïtat del servei en producció.

· Incidències associades als certificats dels components de la solució.

· Manteniment i Operació de polítiques, perfils de seguretat i regles de la solució.

· Manteniment i Operació de dispositius de xarxa, xarxes, VLAN…dins de la CMDB de la solució.

· Consultes, configuració i troubleshooting sobre la instal·lació:

- Diagnòstic de perfilat i creació de regles per resoldre situacions puntuals.

- Monitorització i healtcheck dels serveis necessaris als diferents components.

- Verificació dels fluxos de connectivitat que puguin afectar el funcionament de l'eina.

- Modificació de paràmetres de la configuració per adaptar-los a les necessitats o resoldre problemes de manera puntual.

- Diagnòstic i troubleshooting de configuració sensor (port span) i polítiques.

· Probes d'alta disponibilitat (HA) de la infraestructura i serveis crítics així com el seu manteniment.

· Revisió i homologació de l'electrònica de xarxa.

· Creació de Dashboards i Bussiness Profiles personalitzats

· Re-certificació del entorno (components i performance operacional)

· Actualitzacions periòdiques de la infraestructura (de sistema i de seguretat)

· Escalat a Nivell 3 del Fabricant de NAC, si cal, gestionant l'obertura de tiquets amb el fabricant i la gestió i supervisió dels mateixos.

S'estableix un termini davant incidències critiques de 4 hores.