
Servei de suport per a la gestió i actualització de l'entorn NAC de FGC.

Especificació tècnica

Àrea de Ciberseguretat
Tecnologies de la Informació i les Comunicacions

Índex

1. Introducció	3
2. Objecte	3
3. Abast i descripció del servei.....	3
4. Infraestructura de seguretat	6

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 establert un software de control d'accés a les seves xarxes (NAC). Amb l'objectiu mantenir al dia aquest sistema, aquest plec pretén la contractació de serveis per al manteniment, les actualitzacions i ajut a la gestió.

2. Objecte

FGC pretén ampliar el control dels dispositius que accedeixen a la seva xarxa i és per aquest motiu que té com a objectiu actualitzar, revisar i millorar totes les capacitats que ofereix el sistema de control de xarxa que té establert.

L'objecte d'aquesta licitació, és la contractació d'un suport que permeti realitzar el manteniment, actualització i doni suport a la gestió de tots els dispositius que accedeixen a xarxa i que s'estan controlant mitjançant l'eina de NAC de FGC.

3. Abast i descripció del servei

L'abast del servei, és la contractació d'un servei que permeti millorar el manteniment, la evolució i la gestió de l'eina de NAC implantada a FGC.

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

Servei de suport

- Suport de nivell 2. Les activitats mínimes que han d'estar cobertes:

Revisió de logs interns en CLI i la seva interpretació i anàlisi.

Modificació de paràmetres de la configuració per l'adaptació a les necessitats donades o resoldre problemes puntuals.

Incidències associades a certificats dels components de la solució.

Verificació de fluxos de connectivitat que puguin afectar al funcionament general.

Manteniment, operació de polítiques, perfils seguretat i regles de la solució.

Modificació/adaptació de polítiques per resoldre incidències o sol·licitades per FGC.

Manteniment i operació de dispositius de xarxa, xarxes, VLANs, etc. dintre de la CMDB de la solució.

Modificació i adequació de paràmetres pel correcte funcionament.

Suport en la resolució d'incidents interpretant logs de dispositius client.

Suport i diagnostic de perfilat i creació de regles, segons calgui.

Revisió i modificació de plugins de la solució segons calgui.

Resolució de incidències tècniques associades a Autenticació i Autorització.

Troubleshooting avançat de polítiques i modificacions o adaptació segons calgui.

Revisió i anàlisi de logs de radius i proxy radius para seguiment i resolució d'incidents.

- Suport nivell 3. Les activitats mínimes que han d'estar cobertes:

Diagnòstic de situacions que requereixin configuració de scripting y anàlisis forense.

Incidències associades a mal funcionament dels components (bugs) o que afectin a la continuïtat del servei en producció.

Informació per realització d'actualitzacions, noves funcionalitats i correcció de bugs

Escalat d'incidències de N2.

Partida a l'alça a justificar . Les activitats mínimes que han d'estar cobertes:

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)

Servei de migració a nova versió, configuració i posada en servei

Es necessari que el licitador gestioni i executi tècnicament la actualització de la solució NAC de FGC a la última versió recomanada pel fabricant.

Cal que s'analitzi l'impacte que pot tenir aquest Update. Cal que es realitzi un pla d'acció detallat de tot el procés, proves i roll back en cas necessari.

Cal que es desplegui i es configuri la nova infraestructura necessària.

Cal que es realitzi la migració tota la configuració de sistemes, polítiques desplegades i objectes de les BBDD.

Cal que es realitzin les configuracions adients en tots els components de la solució NAC tenint en compte les premisses en producció.

Cal realitzar anàlisi i bateries de proves per garantir l'èxit del procés de migració.

Servei de monitorització proactiva

El servei ha d'oferir una monitorització que garantitzi el bon funcionament de la infraestructura on esta desplegada la solució de NAC, així com la disponibilitat dels serveis.

Com a mínim es necessari:

- Gestió centralitzada de totes les alertes de sistema NAC

- Revisió i resolució de totes les alertes generades per la solució

- Realització d'informes periòdics de l'estat de la infraestructura,

4. Infraestructura de seguretat

La infraestructura de seguretat, quedarà determinada en els criteris de solvència tècnica i el proveïdor haurà de certificar que pot mantenir i administrar la infraestructura de control d'accés de xarxa segons els criteris establerts en aquest document. El detall de la infraestructura es donarà sota un acord de confidencialitat (NDA).