
Pla Director de Seguretat: Adequació a l'Esquema Nacional de Seguretat.

Especificació tècnica

Àrea de Ciberseguretat
Tecnologies de la Informació i les Comunicacions

Agost 2024

Índex

1.	Introducció	3
2.	Objecte	3
3.	Context i situació actual	3
4.	Abast.....	4
5.	Requeriments i consideracions generals	4
6.	Descripció dels treballs a realitzar	5
6.1	Anàlisi i categorització dels serveis de negoci	5
6.2	Anàlisi dels Sistemes d'Informació que suporten els serveis de negoci i Declaració d'Aplicabilitat	6
6.3	Avaluació de compliment	7
6.4	Pla d'adequació	8
6.5	Actualització del Sistema de Gestió de la Seguretat de la Informació	8
7.	Gestió del servei	9
7.1	Metodologia de treball	9
7.2	Equip de treball	9
7.3	Govern del servei	10
7.4	Entregables del servei.....	11
7.5	Planificació i durada	11

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 complir amb la regulació vigent, es planteja millorar les seva visió estratègica en matèria de Ciberseguretat.

2. Objecte

La seguretat, tant de la informació, com dels sistemes i infraestructures que els donen suport és cabdal per al correcte funcionament de FGC i, per tant, és prioritari implantar mesures de seguretat adequades i eficients que garanteixin la continuïtat de les operacions de l'entitat davant qualsevol eventualitat que pugui afectar-los.

Aquesta licitació té per objecte la contractació de serveis de consultoria de seguretat que permetin dissenyar i donar suport a FGC en la definició d'un Pla Director de Seguretat que, addicionalment, contempli l'adequació al compliment de les mesures de seguretat recollides en el RD 311/2022, de 5 de maig, que regula l'Esquema Nacional de Seguretat.

FGC requereix de serveis de consultoria per, a partir de l'anàlisi de l'estat actual de la seguretat, identificar les necessitats del (utilitzant com a marc el Reial decret 311/2022) i dissenyar un pla d'acció que permeti implantar les mesures de seguretat necessàries.

3. Context i situació actual

FGC ha vingut implantant multitud de mesures de seguretat per protegir els seus actius amb un enfocament centrat principalment en els sistemes i infraestructures que donen suport als serveis de negoci.

La publicació del RD 3/2010, de 8 de gener, que regulava l'Esquema Nacional de Seguretat i les seves successives modificacions, l'última el RD 311/2022, de 5 de maig, han fet plantejar a FGC un canvi en l'estratègia de la seguretat, abordant la funció d'una forma transversal en tota l'organització i que els temes de seguretat siguin tinguts en compte en tots els àmbits de la seva activitat.

El grau d'implantació i nivell de maduresa actual de les mesures de seguretat és força heterogeni. Algunes estan implantades des de fa força temps, i per tant tenen un nivell de maduresa alt, però, d'altres, o estan en una fase incipient d'implantació, o directament no s'han abordat.

És desig de FGC contractar serveis de seguretat que permetin dissenyar i executar un pla específic d'adequació per implantar les mesures operacionals i de protecció necessàries per donar compliment a l'Esquema Nacional de Seguretat i implantar en tots els àmbits de l'organització una cultura de seguretat.

Per escometre els treballs es vol utilitzar un enfocament metodològic PDCA que permeti la millora contínua de tot el sistema de gestió de la seguretat mitjançant els corresponents cicles de revisió.

4. Abast

L'abast del present contracte és l'adequació al compliment de l'Esquema Nacional de Seguretat de tots els serveis de negoci de FGC, tant en l'àrea de mobilitat com en la de turisme:

- Mobilitat:
 - Línies metropolitanes
 - Línia Lleida-La Plobla de Segur
 - Xarxa ADIF
- Turisme:
 - Explotació de Montserrat
 - Funicular de Gelida
 - Ferrocarril Turístic de l'Alt Llobregat
 - Tren del Llacs
 - Vall de Núria
 - La Molina
 - Espot i Port Ainé
 - Vallter
 - Boí Taüll
 - Parc Astronòmic Montsec

Adicionalment, des del punt de vista tecnològic, l'abast del present contracte contempla tota la infraestructura de FGC que engloba sistemes IT, OT i IoT.

5. Requeriments i consideracions generals

Els requisits funcionals i tècnics del servei seran els necessaris per complir les especificacions d'aquest plec.

L'adjudicatari serà el responsable de complir amb els requeriments necessaris per cobrir les necessitats del servei, assignant tant els recursos humans com els tècnics necessaris per garantir la satisfacció de FGC i el compliment dels serveis contractats.

L'adjudicatari assumirà el lideratge del projecte, des d'un enfocament proactiu, i anticipant-se a les necessitats que puguin anar sorgint durant la prestació del servei, garantint la disponibilitat durant tot el servei dels recursos necessaris.

El servei ofert no haurà de tenir costos ocults que suposin l'adquisició de maquinari o programari per part de FGC. En el cas que es posessin de manifest durant l'execució del contracte, aquests costos correran per compte de l'adjudicatari.

Les ofertes dels licitadors hauran de proporcionar el detall complet de cadascun dels treballs a realitzar.

Tots els serveis recollits en el present Plec de Prescripcions Tècniques hauran d'executar-se per personal qualificat i d'acreditada experiència en els treballs a realitzar. El licitador ha de proporcionar una relació de les diferents qualificacions i experiència del personal integrant de l'equip que es farà càrrec del disseny i execució de les activitats incloses en el pla del projecte.

6. Descripció dels treballs a realitzar

Els treballs a realitzar durant l'execució del contracte, derivats del present Plec, s'han agrupat en les següents fases:

1. Anàlisi i categorització de tots els serveis de negoci.
2. Anàlisi dels Sistemes d'Informació que suporten els serveis de negoci i Declaració d'Aplicabilitat.
3. Avaluació de compliment.
4. Pla d'adequació (ordenat i prioritzat).
5. Actualització del Sistema de Gestió de la Seguretat de la Informació (definició i revisió).

6.1 Anàlisi i categorització dels serveis de negoci

En aquesta Fase, s'inclouran les activitats necessàries per determinar l'àmbit i abast del Sistema d'Informació de FGC, així com la seva categorització, que permetrà concretar les mesures de seguretat a aplicar, en base a l'impacte que un possible incident de seguretat podria afectar en el compliment dels objectius del negoci de FGC.

Activitats a realitzar

S'identificaran i documentaran els serveis de negoci de tot FGC, juntament amb el detall de la informació que gestionen (tipologia de dades que es tracten, etc.) i els seus responsables, tant de la informació com dels serveis.

A partir d'aquests serveis i informació s'elaborarà un catàleg d'actius essencials que els donen suport, i s'analitzaran les dimensions de seguretat DICAT (Disponibilitat, Integritat, Confidencialitat, Autenticitat i Traçabilitat) de cadascun d'ells.

Si en la prestació del servei estan implicades, totalment o parcialment, terceres parts a FGC (per exemple, serveis al núvol proporcionats per proveïdors externs), s'hauran d'identificar i documentar per incloure-les en l'anàlisi posterior.

Finalment es categoritzarà cada servei de negoci en base a l'anàlisi d'impacte que un possible incident de seguretat podria tenir en cadascun dels serveis atenent les dimensions Legal, Reputacional, Operativa i Econòmica.

Per a la realització d'aquesta activitat s'aplicarà la metodologia recollida a la [Guia del CCN-STIC 803: Valoració dels Sistemes](#).

Per recaptar tota la informació necessària per a l'anàlisi dels serveis de negoci, l'adjudicatari es reunirà amb els diferents responsables de les unitats de negoci de FGC.

Entregables mínims

- Relació definitiva de serveis de negoci que cal incloure en l'abast de l'ENS, juntament amb la informació associada a cadascun d'ells.
- Inventari d'actius essencials de suport als serveis de negoci i la valoració dels nivells de seguretat (DICAT) per a cadascun d'ells.
- Categorització dels serveis de negoci i dels actius essencials de suport als mateixos.

6.2 Anàlisi dels Sistemes d'Informació que suporten els serveis de negoci i Declaració d'Aplicabilitat

En aquesta fase es realitzarà un inventari dels actius tecnològics que suporten cadascun dels serveis de negoci i es definirà la corresponent Declaració d'Aplicabilitat (SoA) per a les mesures obligatòries corresponents a la categoria de cada sistema.

Activitats a realitzar

L'adjudicatari realitzarà inventari detallat actius tecnològics dels Sistemes d'Informació que suporten cadascun dels serveis de negoci, contemplat, al menys, els següents elements:

- Actius tecnològics del Sistema d' Informació. Es classificaran els actius essencials a nivell d'ubicació i instal·lacions, personal involucrat en cadascuna d'elles, equipament, xarxes i comunicacions, maquinari i programari, informació (dades de negoci, configuració i personals), així com els serveis inclosos en el Sistema (interns, externs, cloud i proveïdors).
- Dependències entre els actius.
- Fonts d' informació.
- Dominis de seguretat (un per cada actiu o agrupant-los per categoria).
- Responsables dels actius.

S'elaborarà el document de Declaració d'Aplicabilitat (SOA) per a les mesures obligatòries corresponents a la categoria de cada sistema ([Annex II de l'ENS](#)) juntament amb els reforços apropiats.

Si alguna mesura de l'ENS no pot ser implementada en la seva totalitat per FGC, l'adjudicatari elaborarà la corresponent justificació, juntament amb les mesures compensatòries a implantar, indicant, almenys, la següent informació:

- Àmbit d' aplicació.
- Limitacions o restriccions al compliment de la mesura.
- Objectiu de la mesura compensatòria.
- Definició de la mesura compensatòria.
- Risc identificat després de la implantació de la mesura compensatòria.
- Validació de la mesura compensatòria.

Per a cadascuna de les mesures, s'identificarà la Unitat i/o responsable d'implementar-la.

Per recaptar tota la informació necessària per a l'anàlisi dels serveis de negoci, l'adjudicatari es reunirà amb els diferents responsables de Tecnologia de FGC.

Entregables mínims

- Inventari d'actius tecnològics.
- Declaració d'Aplicabilitat (SOA) i, si cal, justificació de la/s mesura/s compensatòria/s.

6.3 Avaluació de compliment

En aquesta Fase s'identificarà i determinarà el nivell de compliment de les mesures de l'ENS per a la categoria establerta, la valoració del nivell de seguretat en cadascuna de les seves dimensions, així com el seu nivell de maduresa. La informació obtinguda durant aquesta activitat servirà per incorporar al pla d'adequació les accions que permetran complir amb cadascuna d'elles.

Activitats a realitzar

El grau d' implantació de les mesures serà avaluat per l'adjudicatari, amb el suport dels diferents responsables de Tecnologia de FGC, prenent com a base l'anàlisi inicial realitzat.

Per determinar el nivell de maduresa en la implantació de cada mesura se seguirà el criteri proposat pel Centre Criptològic Nacional:

- L0 – Inexistent: la mesura no s'està aplicant.
- L1 – Inicial / Ad hoc: es fan coses, de tant en tant.
- L2 – Reproduïble però intuïtiu: es fa però no està sistematitzat ni documentat.
- L3 – Procés definit: es realitza sistemàticament i els procediments estan documentats.
- L4 – Gestionat i mesurable: es fa un seguiment del seu exercici.
- L5 – Optimitzat: s'aplica un procés de millora continua.
- N/A – No aplica.

Per a cada mesura, l'adjudicatari recopilarà, les evidències que avalin el seu compliment, si és possible en format electrònic, i elaborarà un repositori amb totes elles. Aquestes evidències podran ser de qualsevol tipus: document normatiu, logs, captures de pantalla, diagrames, esquemes, registres en alguna eina/sistema, etc.

Si l'aplicació d'una mesura és responsabilitat d'una entitat o proveïdor extern a FGC, serà aquest qui reculli la informació necessària per verificar el seu compliment i la proporcionarà a l'adjudicatari per a la seva avaluació.

Aquelles mesures el nivell de compliment de les quals sigui L0, L1 o L2 es consideraran com a no implantades a efectes de l'anàlisi de compliment de l'ENS. És a dir, el compliment amb l'ENS es determinarà avaluant totes les mesures del SoA, que han d' estar en un nivell de compliment igual o superior a L3.

Per realitzar aquesta activitat s' atindrà al que disposen les Guies: [Guia CCN-CERT 808 Verificació de Compliment de l'ENS](#), [Guia CCN-CERT 802 Guia d'Auditoria per a l'ENS](#) i a la [Guia CCN-CERT 804 ENS. Guia d'Implantació](#).

Entregables mínims

- Informe de compliment de l'ENS que reculli el nivell de maduresa en la implantació de cada mesura recollida en la Declaració d'Aplicabilitat.
- Repositori amb les evidències recopilades per a cadascuna de les mesures.

6.4 Pla d'adequació

El pla d'adequació a l'ENS permetrà identificar totes les activitats o projectes que cal executar per assolir el compliment de l'ENS en la categoria establerta.

Aquesta planificació inclourà, a més de la identificació dels projectes a realitzar, la seva relació, planificació temporal, durada, els responsable/s de la seva execució, les fites i quick-wins dels projectes i les activitats de seguiment del pla.

Activitats a realitzar

L' adjudicatari elaborarà una planificació amb les activitats i projectes a realitzar per a l'adequació de FGC a l'ENS.

Les activitats incloses en el pla d'adequació, atenent a l'abast i esforç que sigui necessari realitzar, seran de dos tipus:

1. **Activitats**, inclou aquelles la durada de les quals està acotada a curt/mitjà termini.
2. **Projectes**, que engloba grups d'accions amb una entitat major, que serien executades en terminis mitjans/alts.

A més, atenent l'àmbit d' aplicació, aquestes activitats es poden classificar en:

1. **Verticals**, l'àmbit d'aplicació dels quals està focalitzat en una part de l'organització (per exemple, l'aplicació d'una determinada mesura de seguretat).
2. **Transversals**, que apliquen de forma horitzontal a tota l'organització (per exemple, gestió del canvi en la cultura de seguretat del personal de FGC).

El pla d'adequació contindrà diferents seccions per a cadascun dels blocs d'accions i permetrà veure l'efecte d'una determinada activitat o projecte sobre el nivell de compliment de l'ENS.

Entregables mínims

- Pla detallat d'adequació a l'ENS.

6.5 Actualització del Sistema de Gestió de la Seguretat de la Informació

De cara a poder mantenir en el futur el nivell de compliment del l'ENS, es fa necessari disposar d'un Sistema de Gestió de la Seguretat de la Informació.

Activitats a realitzar

L' adjudicatari actualitzarà i adequarà l'actual Sistema de Gestió de la Seguretat de la Informació de FGC en base a tota la informació recavada a les fases anteriors. Si escau en proposarà un de nou.

Entregables mínims

- Sistema de Gestió de la Seguretat de la Informació nou o actualitzat.

7. Gestió del servei

7.1 Metodologia de treball

S'aplicaran les bones pràctiques d'una metodologia “Agile” que permeti flexibilitzar i avançar de forma iterativa en els treballs identificats en el present plec de prescripcions, establint-se metes parcials per verificar que el treball realitzat s'ajusta als requeriments definits i, en el cas de desviacions, reconduir la situació en fases primerenques del servei.

L'adjudicatari presentarà i mantindrà actualitzat durant tota la vida del projecte un Pla General d'Activitats i Fites Principals del mateix, que haurà de ser aprovat a inici dels treballs.

7.2 Equip de treball

L'adjudicatari conformarà un equip de projecte amb els següents perfils mínims:

- Director Executiu del Projecte:
 - Serà l'únic interlocutor de l'adjudicatari amb la Direcció Executiva del servei de FGC en l'alineament estratègic del servei.
 - La seva dedicació serà la necessària per garantir el màxim nivell de qualitat del servei, i el seu cost quedarà inclòs en l' oferta presentada pel licitador, no suposant cap cost extra per a FGC al llarg de la prestació del servei.
- Responsable del servei:
 - Serà l'únic interlocutor de l'adjudicatari amb la Direcció del servei de FGC en la coordinació i seguiment del servei.
 - La seva dedicació serà la necessària per garantir el bon funcionament del servei, i el seu cost quedarà inclòs en l' oferta presentada pel licitador, no suposant cap cost extra per a FGC al llarg de la prestació del projecte.
- Consultor de Seguretat IT:
 - Encarregat de executar els treballs contemplats en el plec de prescripcions amb focus en l'àmbit IT.
 - La seva dedicació serà total al projecte.
- Consultor de Seguretat OT
 - Encarregat de encarregats de executar els treballs contemplats en el plec de prescripcions amb focus en l'àmbit IT.
 - La seva dedicació serà total al projecte.

L'adjudicatari proposarà i dimensionarà l'equip de treball que consideri necessari per realitzar, amb totals garanties, els treballs recollits en el present plec de prescripcions.

L'adjudicatari descriurà l'equip de treball proposat per a la prestació del servei. No és objectiu de FGC la contractació d'un equip de persones sinó el disposar d'un servei que doni resposta als treballs descrits.

L' adjudicatari aportarà tots els recursos humans, suficientment capacitats, especialitzats i formats per a la prestació del servei en les condicions requerides. Haurà d'especificar les qualificacions i certificacions de l'equip, així com l'experiència i funcions exercides en projectes similars.

No està permesa la subcontractació del servei per part de l'adjudicatari, havent de ser el personal dedicat al projecte de FGC personal propi de l'empresa adjudicatària.

7.3 Govern del servei

FGC estableix la següent estructura per nivells per a la governança del servei:

- El **nivell estratègic** és l'encarregat de vetllar perquè l'estratègia i objectius del servei estan alineats amb els corporatius, i de controlar i garantir que totes les decisions i operacions s'ajusten a aquesta estratègia.
- El **nivell tàctic** s'encarrega de transformar les decisions estratègiques en plans d'operació i acció, i de coordinar dirigir i controlar els esforços necessaris per a la seva execució.
- El **nivell operatiu** es responsabilitza de la gestió, execució, supervisió tècnica i control diari dels serveis, així com de gestionar les incidències.

En línia amb l'esmentat anteriorment existirà:

- Un **Comitè de Direcció** en el qual participarà FGC i l'adjudicatari assignant cadascun un Director Executiu, capaços d'assegurar el nivell de decisió i compromís que requereixen les disposicions estratègiques requerides a aquest nivell del model. Algunes de les responsabilitats d'aquest Comitè són:
 - Revisar l'estat dels plans d'acció en curs. Revisió d'objectius a mitjà i llarg termini.
 - Prendre decisió en cas necessari per al desbloqueig o priorització de determinades accions.
 - Altres accions a proposar per l'oferent.

El Comitè de Direcció es reunirà de forma recomanada mensualment, o amb la freqüència que raonablement es consideri necessària, o dins dels 10 dies laborables següents a una petició per escrit de qualsevol de les parts.

- Un **Comitè de Seguiment i Control**. En un nivell tàctic, tant FGC com l'adjudicatari designaran un Responsable de Projecte per establir aquest comitè encarregat de dirigir, monitoritzar i controlar l'execució de tots els serveis corresponents. Algunes de les responsabilitats d'aquest comitè són:
 - Supervisar la marxa dels treballs i els entregables.
 - Analitzar i aprovar les modificacions del servei, millores i la seva reestructuració per aconseguir que el funcionament del servei aconsegueixi assolir els objectius en un moment determinat.
 - Decidir la solució més adequada en cas de conflicte o problemes d'interpretació.
 - Mobilitzar els recursos que siguin necessaris per respondre a possibles situacions crítiques.
 - Revisió d'objectius a curt termini.
 - Altres accions a proposar per l'oferent.

Es reunirà quinzenalment, o amb la freqüència que raonablement es consideri necessària, i dins dels 3 dies laborables següents a una petició per escrit de qualsevol de les parts.

- Un **Comitè Operatiu** que analitzarà i avaluarà de manera contínua les activitats amb una freqüència setmanal, i que serà designat entre el Responsable de Projecte de l'empresa adjudicatària i el Responsable de Projecte de FGC.

Algunes de les responsabilitats d' aquest comitè són:

- Identificació i seguiment de plans d'acció.
- Identificació de problemes que requereixin escalat a nivells superiors.
- Revisar i prioritzar les peticions rebudes.
- Coordinar els grups i les persones assignades.
- Discutir nous requeriments o canvis.
- Assegurar que el personal assignat per a l'execució dels serveis per l'adjudicatari està disponible i disposen de l'equip, formació i suport necessaris per a la correcta execució de les seves tasques.
- Servir com a punt únic de contacte entre les organitzacions de FGC i de l'adjudicatari per a tots els assumptes del dia a dia relacionats amb el servei.
- Revisar i facilitar al Comitè de Seguiment i Control qualsevol informació que li sigui demanada.
- Executar qualsevol altra activitat relacionada amb assumptes de qualsevol naturalesa que pugui sorgir durant l' execució dels treballs.

Totes les reunions hauran de quedar documentades en actes de reunió realitzades per l'adjudicatari, que seran trameses a FGC per a la seva aprovació i posterior signatura per ambdues parts.

Independentment del model organitzatiu general plantejat, el Responsable del Contracte establirà els comitès i la periodicitat amb què es reuneixin en la reunió de llançament.

7.4 Entregables del servei

L'adjudicatari emetrà, amb periodicitat mensual, un informe de seguiment que proporcioni una visió general del servei i que mostri, entre d' altres, tota la informació necessària sobre l'avanç dels treballs, possibles desviacions sobre la planificació, així com en ambdós casos la seva evolució i tendències. Per tant, haurà d' incloure almenys:

- Informe de seguiment quinzenal i presentació executiva per al Comitè de Seguiment i Control.
- Informe de seguiment i presentació executiva setmanal per al Comitè Operatiu.

L'adjudicatari, durant l'execució dels treballs, presentarà els entregables especificats en cadascuna de les activitats del contracte i els mantindrà actualitzats (mantenint les versions dels mateixos) durant la prestació del servei. Aquests hauran de ser aprovats pel responsable del projecte designat per FGC.

7.5 Planificació i durada

L'adjudicatari realitzarà una proposta de planificació del projecte amb totes les activitats a realitzar desglossant-les en tasques i subtasques, segons els requeriments establerts en aquest plec, contemplant una durada màxima del servei de DOTZE MESOS.

