PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS

CONTR/2023/734

PER AL SERVEI DE MANTENIMENT DEL PORTAL DE TRANSPARÈNCIA DE FERROCARRILS DE LA GENERALTITAT DE CATALUNYA I LES ENTITATS DEL SEU GRUP

ÍNDEX

1. OBJECTE DEL PLEC

Ferrocarrils de la Generalitat de Catalunya es troba en la necessitat de contractar un servei de manteniment del portal de transparència d'FGC i les entitats del seu grup, el qual necessita un manteniment tècnic i d'actualització constant.

En tot allò què no s'especifica al present plec particular, l'adjudicatari haurà d'acomplir allò especificat en les normatives d'obligat compliment, en especial aquelles relatives a la Prevenció de riscos laborals i Reial Decret 1627/1997.

2. ABAST

Les tasques a desenvolupar per l'adjudicatari seran les següents (aquest llistat no és exhaustiu):

a) Resolució d'incidències

b) Actualització de continguts

c) Manteniment de seguretat

3. REQUERIMENTS ESPECÍFICS DEL CONTRACTE

Permetre disposar d'un equip amb coneixements suficients per poder resoldre possibles situacions d'incidències i actualització de continguts en un **termini no superior a 24 hores (per a resolució d'incidències i actualització de continguts de fins a 2 apartats) o de 72 hores (per a actualització de continguts de 3 apartats o més) (de dilluns a divendres)**, a requeriment de l'àrea de Bon Govern Corporatiu.

El desconeixement del contracte en qualsevol de les seves condicions i dels documents annexos que en formen part, o de les instruccions, plecs i normes de tota classe promulgades per FGC, que puguin tenir aplicació en l'execució d'allò pactat, no eximirà el contractista de l'obligació del seu compliment.

El contractista quedarà vinculat per l'oferta que hagi presentat, el compliment de la qual, en tots els seus termes, tindrà el caràcter d'obligació essencial del contracte.

4. EQUIP DE TREBALL, PROGRAMACIÓ I LLOC DE TREBALL

El licitador haurà d'adscriure a l'execució del contracte, un equip integrat, com a mínim per:

- 1 responsable tècnic, encarregat de la gestió del servei, amb una experiència mínima de 3 anys relacionat amb l'objecte del contracte.
- 2 tècnics, encarregats de la gestió del servei, amb una experiència mínima de 2 anys relacionats amb l'objecte del contracte.
- 1 responsable de seguretat encarregat de garantir les polítiques i mesures de seguretat adients, així com la interlocució única en temes de Ciberseguretat amb FGC.

L'equip haurà de treballar amb les característiques d'aquest sistema de programació:

- CMS Plone
- Desenvolupament en codi obert
- Llenguatge de programació Python

El lloc de treball habitual de l'equip de l'adjudicatari es durà a terme a les instal·lacions de l'empresa adjudicatària.

5. TERMINI D'EXECUCIÓ

La durada del servei serà de 3 anys prorrogable fins a 5.

L'inici de la seva execució serà el dia 9 de març de 2024, data en què s'hauria exhaurit l'actual servei de manteniment contractat.

6. ABONAMENT DEL SERVEI

FGC satisfarà l'import resultant del preu del contracte, trimestralment i per avançat.

7. REQUERIMENTS ESPECÍFICS DE SEGURETAT

La web de transparència està hostatjada a infraestructura de FGC i l'adjudicatari haurà de complir estrictament les mesures de seguretat establertes i que es sol·licitin per tal d'accedir i realitzar el manteniment.

Es requereix el manteniment dels següents serveis de seguretat en la infraestructura de FGC:

Auditories de seguretat periòdiques

Cada 6 mesos com a màxim, tant en l'àmbit tècnic com en l'organitzatiu, que incloguin test d'intrusió (OSSTMM, OWASP o PTES), anàlisi de vulnerabilitats i l'avaluació de la seguretat perimetral i interna de l'entorn de servidors d'FGC. Per cada auditoria de seguretat es lliurarà un informe amb l'avaluació de les mesures de protecció dels serveis exposats (webs, email, accessos remots, vpn, aplicacions, Backup, etc.) que inclogui un resum executiu, les proves realitzades, les vulnerabilitats detectades i les recomanacions per a la seva solució que hauran de ser implantades per l'empresa adjudicatària un cop analitzades per FGC.

L'adjudicatari haurà d'implementar totes les accions i millores identificades.

Manteniment d'aplicacions i actualitzacions

Tot el programari i aplicatius que intervinguin en el servei de la web de transparència, hauran de ser actualitzats de manera periòdica a les versions recomanades pel fabricant i lliures de vulnerabilitats.

En cas de detecció de vulnerabilitats noves o zero day, s'haurà d'actualitzar l'aplicatiu o sistema afectat immediatament.

L'àrea de Ciberseguretat FGC es reserva el dret de sol·licitar actualitzacions o actuacions en base a la seguretat, en qualsevol moment i que s'hauran de resoldre amb la major celeritat.

Tot desenvolupament fet a mida, cal que tingui un pla de manteniment i actualitzacions associat i cal que es faci una avaluació de riscos abans de la posada en producció.

Acords de Nivell de Servei

- Servei d'emergències amb telèfon 24x7 atès per personal tècnic
- Suport tècnic als usuaris i desenvolupadors de FGC en 24 x 7 amb els temps de resposta indicats en el Pla de suport
- Atenció tècnica immediata davant eventuals atacs o incidents de seguretat.
- Informes específics d'incidències. Independentment de l'informe mensual de manteniment, l'empresa adjudicatària lliurarà en un màxim de 24 hores un informe específic davant de qualsevol incidència que hagi provocat interrupcions o disfuncions en el servei. Aquest informe inclourà el motiu de la incidència, la seva afectació, el detall de les actuacions realitzades per solucionar-la, el registre horari de apertura i tancament de la incidència i les accions empreses perquè no

torni a repetir-se.

- Auditories de seguretat periòdiques (cada 6 mesos) tant en l'àmbit tècnic com en l'organitzatiu que incloguin test d'intrusió (OSSTMM, OWASP o PTES), anàlisi de vulnerabilitats i l'avaluació de la seguretat perimetral i interna de l'entorn de servidors d'FGC. Per cada auditoria de seguretat es lliurarà un informe amb l'avaluació de les mesures de protecció dels serveis exposats (webs, email, accessos remots, vpn, aplicacions, Backup, etc.) que inclogui un resum executiu, les proves realitzades, les vulnerabilitats detectades i les recomanacions per a la seva solució que hauran de ser implantades per l'empresa adjudicatària un cop analitzades per FGC.

- **Pla de suport**

  FGC i els seus desenvolupadors podran reportar incidències i sol·licituds en horari de 24x7 a través del telèfon, email, xat o directament des de la plataforma de tiquets. Aquestes incidències seran avaluades pel tècnic de suport que crearà el tiquet de servei corresponent amb un temps de resposta garantit en funció del tipus d'incidència, tal com es detalla a continuació:

  - **Incidències/tiquets de servei de tipus GREU:** Interrupcions o disfuncions en el funcionament dels serveis i/o processos en producció que donin lloc a una completa inoperativitat del sistema, d'un servidor, d'una web o d'un servei crític en particular.
    - Temps de resposta: 30min
    - Temps màxim de resolució: 3h

  - **Incidències/tiquets de servei de tipus MIG**: Interrupcions o disfuncions en el funcionament dels serveis i/o processos en producció que afectin lleugerament a la qualitat del servei. Incidències en els serveis en pre-producció. Sol·licituds de canvis de la configuració de la infraestructura. Suport tècnic en general.
    - Temps de resposta: 1h
    - Temps màxim de resolució: 1 dia laborable

  - **Incidències/tiquets de servei de tipus LLEU**: Disfuncions en el funcionament dels serveis i/o processos en producció que no afectin a la qualitat del servei. Sol·licituds de assessorament.
    - Temps de resposta: 2h (120 minuts)
    - Temps màxim de resolució: 2 dies laborables

- Pla de suport de AWS (pla de nivell Business com a mínim). Que permeti a FGC l'accés per telèfon, email i xat les 24 hores a el dia els 7 dies a la setmana al servei de suport i atenció al client, la documentació, els documents tècnics i els fòrums de suport de AWS.

Detecció, anàlisi i gestió de vulnerabilitats

L'objectiu és tenir un mecanisme per detectar i contrarestar les amenaces que puguin haver als sistemes i plataformes de FGC, així com poder fer un seguiment del cicle de vida de les vulnerabilitats detectades (detecció, correcció, verificació).

Pels actius interns aquest servei de manera general ha de cobrir:

Alerta i identificació de vulnerabilitats potencials i confirmades: acció repetida en el temps periòdicament, establerta com cicles d'auditoria sobre els actius identificats. La detecció de vulnerabilitats l'haurà de fer el proveïdor adjudicatari mitjançant eines especialitzades les quals han de tenir un nivell de falsos positius molt baix (menys del 10% de les deteccions).

Els modes en que es duguin a terme les auditories, anàlisis i pentest, podran ser en qualsevol modalitat (caixa negra o caixa negra, amb intrusió externa o interna), pero sempre previ avís i acord amb FGC. De la mateixa manera per verificar l'explotació de qualsevol vulnerabilitat també haurà de ser notificat i acordat amb FGC.

Per a la gestió de les vulnerabilitats detectades en el procés de detecció i identificació hauran de ser classificades i documentades d'acord als organismes especialitzats i bases de dades de coneixement com son CVE (Common Vulnerabilities and Exposures) i CWE (Common Weakness Enumeration) i fent servir el mètode de càlcul l'estàndard CVSS (Common Vulnerability Scoring System), del conegut organisme FIRST. S'haurà de facilitar la lectura i la comprensió de les debilitats trobades mitjançant aquest servei.