FGC
Ferrocarrils
de la Generalitat
de Catalunya

Allotjament, manteniment i suport de la infraestructura web de FGC a AWS

Especificació tècnica

Àrea de Tecnologia Informàtica
Tecnologies de la Informació i les Comunicacions
Rev. 1.0 – Maig 2023

Ferrocarrils de la Generalitat de Catalunya, c/ Vergós 44, 08017, Barcelona

ÍNDEX

1. Introducció

Ferrocarrils de la Generalitat de Catalunya (d'aquí en endavant FGC) es una entitat empresarial pública depenent del Departament de Territori i sostenibilitat (TES) que té com a principal finalitat l'administració d'infraestructures i l'explotació de serveis ferroviaris, així com la gestió de ferrocarrils turístics i d'estacions de muntanya.

Per això, FGC es una empresa productora de serveis que, tot i ser de titularitat pública, la seva gestió, el tracte amb els seus clients i proveïdors, i les seves relacions laborals, són més similars als d'una empresa privada.

L'activitat desenvolupada per FGC segueix la següent classificació:

- Transport de viatgers:
  - Línia Barcelona – Vallés.
  - Línia Llobregat – Anoia.
  - Línia Lleida – La Pobla de Segur.
- Transport de mercaderies:
  - Línia Llobregat – Anoia.
- Explotació de muntanya:
  - La Molina.
  - Espot.
  - Port Ainé.
  - Vallter.
  - Vall de Nuria (inclou el tren cremallera).
  - Montserrat (inclou el tren cremallera).
  - Boí
  - Centre d'Observació de l'Univers
- Altres activitats comercials:
  - Operador de telecomunicacions:
  - Lloguer de fibra òptica pròpia als operadors de telefonia i dades.
  - Lloguer de canalitzacions per al pas de fibres òptiques de tercers.
  - Comercialitzador d'espais publicitaris en trens i estacions.

En definitiva, FGC es una empresa al servei de la Generalitat de Catalunya per garantir la mobilitat a Catalunya i per a contribuir al dinamisme econòmic i social de les regions de muntanya.

2. Objecte

FGC està immersa en una contínua evolució tecnològica dels seus serveis digitals per integrar nous sistemes de mobilitat, gestió d'horaris, venta online i informació dels seus serveis.

Aquesta licitació sorgeix de la necessitat d'unificar tota la plataforma de servidors de FGC al Cloud d'Amazon. Per a això, es requereixen serveis de suport per a la migració en cas que sigui necessari, serveis de hosting de la plataforma de servidors i el manteniment i monitorització de tota la infraestructura. A més, es requereixen serveis d'assessorament, suport i atenció tècnica 24x7 per a FGC i les empreses desenvolupadores que col·laboren amb ella.

Tot això en compliment d'uns requeriments específics de seguretat i d'acords de nivell de servei tal i com s'especifiquen mes endavant en aquest plec de condicions.

3. Context

Actualment FGC disposa de la següent infraestructura de servidors a AWS allotjats a la regió Europe (Irlanda):

	Nom	Tipus	Cores	Memòria (G)	Disc (G)	Sistema	Observacions
1	chronos	t3.2xlarge	8	32	100	Linux	Disc SSD tipus gp2
2	fgccat-dev	t3.large	2	8	160	Linux	Disc SSD tipus gp2
3	fgccat-prod	t3.2xlarge	8	32	160	Linux	Disc SSD tipus gp2
4	lapobla	t3a.xlarge	4	16	40	Linux	Disc SSD tipus gp2
5	leaks	t3.medium	2	4	80	Linux	Disc SSD tipus gp2
6	m1	a1.xlarge	4	8	60	Linux	Disc SSD tipus gp2
7	pam	t3a.large	2	8	20	Linux	Disc SSD tipus gp2
8	piezometres	t3a.large	2	8	80	Windows	Disc SSD tipus gp2. Llicència inclosa.
9	smtp	t3.medium	2	4	20	Linux	Disc SSD tipus gp2
10	timvol	t3.xlarge	4	16	100	Linux	Disc SSD tipus gp2

11	timweb	c5a.4xlarge	16	32	200	Linux	Disc SSD tipus gp2
12	transparencia	t3a.large	2	8	60	Linux	Disc SSD tipus gp2
13	volturisme	t3.xlarge	4	16	60	Windows	Disc SSD tipus gp2. Llicència inclosa.
14	vpn	a1.large	2	4	20	Linux	Disc SSD tipus gp2
15	RDS Mysql	db.m4.large	2	8	20	RDS	Disc SSD tipus gp2, implementació Multi A-Z amb proxy
16	Workspace 1	Value	1	2	10	Windows	Llicència inclosa. Paquet d'aplicacions Office inclòs.
17	Workspace 2	Value	1	2	10	Windows	Llicència inclosa. Paquet d'aplicacions Office inclòs.
18	Workspace 3	Value	1	2	10	Windows	Llicència inclosa. Paquet d'aplicacions Office inclòs.
19	Workspace 4	Standard	2	4	50	Windows	Llicència inclosa. Paquet d'aplicacions Office inclòs.
20	Workspace 5	Performance	2	8	100	Windows	Llicència inclosa. Paquet d'aplicacions Office inclòs.
21	RDS Oracle	db.m5.large	2	8	1024	RDS	Disc SSD tipus gp2, implementació Multi A-Z amb proxy. Llicència d'Oracle inclosa.

Les instàncies d'AWS poden requerir ampliacions en una mitjana del 15% de les hores mensuals.

La transferència de dades cap a Internet dels **21** servidors virtuals allotjats actualment al Cloud d'Amazon és d'una mitjana mensual de **29 TB/mes**. Cal tenir en compte i previst un possible increment d'un 15% en la transferència mitjana mensual.

També haurà de contemplar-se un increment acumulat d'un 5% mensual dels requeriments d'espai en disc SSD.

4. Requeriments

S'ha d'incloure a la proposta els imports a pagar per tots els serveis d'AWS i de proveïdors externs a FGC que hauran de ser assumits per la empresa adjudicatària.

4.1. Serveis de hosting i administració dels servidors

- Manteniment i actualització de les instàncies EC2 i RDS de AWS i de les seves possibles ampliacions (mitjana del 15% de les hores mensuals).
- Administració del emmagatzematge SSD de EBS Europe (Ireland) dels servidors, amb un increment mensual d'un 5% dels requeriments d'espai actual en disc SSD
- Les instantànies de EBS (snapshots): es fan 2 cops al dia amb una variació mitjana de la informació diària d'un 20%.
- Ample de banda i transferència de dades de AWS de sortida a internet fins a 33 TB/mes
- Manteniment de la xarxa CDN (Content Delivery Network), utilitzada per emmagatzemar els continguts estàtics de les webs d'FGC i millorar la velocitat d'entrega de tràfic. La CDN estarà disponible per a un màxim de 100 dominis de FGC i haurà de suportar un ample de banda màxim de 100 TB i/o de 100 milions de peticions.
- VPNs Site-to-site per garantir la connectivitat amb protocols de seguretat des de la pròpia xarxa de FGC i des de les xarxes dels diferents desenvolupadors de les webs que col·laboren amb FGC fins a un màxim de 10 empreses amb uns 20 usuaris connectats amb els seus servidors de treball en qualsevol horari. Aquestes empreses col·laboradores poden canviar depenent dels projectes.
- Backup incremental diari del contingut complet de cada servidor amb un temps de retenció de 365 dies i una variació mitjana de la informació diària d'un 20%. Les còpies s'emmagatzemen en servidors d'un centre de dades que d'una regió de la UE diferent de la del centre de dades de AWS dels servidors de FGC (UE Irlanda). Màxim de 100 TB de espai de copies de seguretat.
- Serveis de DNS externs: es prestarà servei de DNS per als diferents dominis, protocols i serveis utilitzant un servidor de DNS extern a la infraestructura de AWS. S'inclourà la gestió (creació, modificació i eliminació) de registres DNS segons necessitats de FGC. Es requerirà l'establiment de regles de tallafocs que filtrin el tràfic de DNS sortint segons aquestes regles.

4.2. Administració, manteniment i monitorització de la infraestructura de FGC

El proveïdor es responsabilitzarà de les següents tasques d'administració, manteniment i monitorització:

- Manteniment (predictiu i correctiu) de la infraestructura de FGC a AWS.
- Gestió i monitoratge permanent dels recursos i les aplicacions de tota la infraestructura de FGC amb suport 24/7. L'objectiu principal d'aquest servei és proporcionar una gestió predictiva a través del monitoratge dels elements i entorns que componen la plataforma i les auditories periòdiques que permetran detectar les situacions de risc reals o potencials i iniciar les accions necessàries, de forma proactiva, per a la seva gestió i resolució en el menor temps possible, garantint la màxima disponibilitat de l'activitat. FGC disposarà d'accés per a visualitzar les mètriques de tots els serveis utilitzats i podrà indicar la incorporació de noves monitoritzacions i/o d'alarmes sobre les seves aplicacions o serveis.
- Actualització periòdica dels sistemes, instal·lant les actualitzacions necessàries per al correcte funcionament i realitzant aquelles configuracions que FGC pugui necessitar.
- S'inclouran les ampliacions de recursos de les instàncies dels servidors que es faran quan sigui necessari com a resultat de la monitorització o per indicació expressa de FGC. S'hauran de monitoritzar i detectar aquelles situacions que puguin suposar una ampliació temporal de recursos.
- Administració de les bases de dades dels servidors virtuals incloent xifrat i la seguretat d'accessos.
- Subministrament, instal·lació i gestió del software necessari pel desenvolupament de l'entorn. Instal·lació del programari addicional que es pugui necessitar
- Manteniment del servei de SMTP que permet l'enviament massiu de correus des dels servidors.
- Resolució de problemes o fallades que afectin el correcte funcionament dels servidors i/o dels serveis instal·lats.
- Configuració de serveis, plugins i/o accessoris necessaris per al funcionament de les aplicacions i/o serveis web
- Instal·lació i configuració de certificats de seguretat
- Gestió i eliminació d'entrades en llistes negres.
- Programació i verificació de Backups i d'instantànies (snapshots)
- S'inclourà la restauració de Backups (complets o a nivell de fitxers i/o de bases de dades) i la restauració de snapshots en resposta a un requeriment de FGC o dels seus desenvolupadors.
- Les tasques de manteniment que puguin afectar al funcionament dels diferents servidors es realitzaran en horari nocturn o de baixa incidència de visites i amb prèvia comunicació i acceptació de FGC en cas de necessitar reiniciar els serveis i sempre sota la seva aprovació
- Monitorització de serveis TCP estàndard i també de serveis d'aplicació i programari (URL concretes, login a serveis FTP, LDAP o correu, consultes a BBDD). En cas de detectar qualsevol incidència en el monitoratge, el proveïdor notificarà a FGC immediatament (per correu electrònic i per telèfon) i, en coordinació amb FGC, haurà de dur a terme determinades accions per solucionar el problema, com ara l'ampliació de recursos del servei, el reinici del servidor afectat i/o l'arrencada o parada d'un determinat servei

- Serveis d'auditoria i anàlisi forense per esbrinar les causes davant qualsevol incidència que afecti als sistemes, com caigudes de rendiment, problemes de funcionament o amb la sospita, detectada o reportada, de qualsevol intrusió o infecció en els sistemes i webs de FGC.
- Neteja i desinfecció de webs i/o bases de dades infectades, en producció o en pre-producció. Caldrà a més esbrinar les causes i implementar les accions requerides per evitar noves infeccions i solucionar les vulnerabilitats de seguretat.
- Manteniments programats (mínim d'un cop al mes). A banda de les actuacions sota demanda i/o per problemes tècnics, mensualment es realitzarà un manteniment per assegurar que tots els servidors tenen els pegats de seguretat actualitzats i que disposen de la ultima versió estable del sistema operatiu instal·lada i de les llibreries i programes en execució: PHP, MySQL, SQL Server, Oracle, etc. També s'haurà de revisar el rendiment i consum del servidor per ajustar els recursos. En cas de que fos necessari el reinici del servidor per instal·lar pegats de sistema i/o noves versions de llibreries o programes, es programarà en la finestra de temps aprovada per FGC.
- L'empresa adjudicatària lliurarà un informe mensual de les actuacions realitzades que inclogui, a més de la relació d'incidències i el seu estat de resolució (sistema de tiquets), una llista de comprovacions (check list) fetes a cadascun dels servidors: versions de sistema, consum mig de CPU i memòria RAM, espai lliure en disc, mitjana de l'ample de banda consumit, nombre de connexions (en el cas dels RDS), estat dels Backups, etc. Aquest informe inclourà, per cadascun dels dominis: el nombre d'atacs bloquejats pel WAF, una estadística detallada del nombre de sol·licituds, ample de banda, visitants únics, ús de la memòria cau, sol·licituds per país, etc.

4.3. Atenció tècnica, suport i assessorament a FGC i als seus desenvolupadors

- FGC requereix un servei tècnic i d'assessorament amb un telèfon d'emergències (atès per tècnics) 24x7
- Atenció tècnica en 24x7 per a FGC i als seus desenvolupadors amb un temps de resposta garantit en funció del tipus de incidència
- S'inclourà un sistema de tiquets per enregistrar, a més de les incidències, totes aquelles sol·licituds d'assessorament i d'atenció tècnica. FGC haurà de tenir accés al sistema de tiquets per veure l'historial o crear un nou tiquet.
- L'empresa adjudicatària lliurarà un informe 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.

- **PLA DE SUPORT REQUERIT**
  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. S'inclou:

- Actuacions davant de qualsevol atac a qualsevol dels equips o dispositius de la infraestructura de FGC
- Actuar amb un servidor o servei per solucionar problemes de saturació o rendiment.
- Resolució de problemes o fallades que afectin el correcte funcionament dels servidors i/o dels serveis instal·lats
- Ajustar els recursos dels servidors en producció en cas necessari (com a resultat del monitoratge o en resposta a una alarma) o per sol·licitud d'FGC o dels seus desenvolupadors.
- Desactivar els accessos a una web o servidor mitjançant filtres i regles en cas de sospita d'intrusió a bases de dades o informació protegida
- Configuració de serveis, plugins i/o accessoris necessaris per al funcionament de les aplicacions i/o serveis web
- Gestió i eliminació d'entrades en llistes negres
- Restauració de Backups (complets o a nivell de fitxers i/o de bases de dades) i la restauració de snapshots en resposta a un requeriment de FGC o dels seus desenvolupadors
- Serveis d'auditoria i anàlisi forense per esbrinar les causes davant qualsevol incidència que afecti als sistemes, com caigudes de rendiment, problemes de funcionament o amb la sospita, detectada o reportada, de qualsevol intrusió o infecció en els sistemes i webs de FGC
- Neteja i desinfecció de webs i/o bases de dades infectades.
- Incidències que afectin a la integritat, confidencialitat i disponibilitat de la informació.

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. S'inclou:

- Creació i configuració de nous servidors instal·lant el sistema operatiu i el programari addicional que es pugui necessitar.
- Ajustar els recursos dels servidors en pre-producció en cas necessari (com a resultat del monitoratge o en resposta a una alarma) o per sol·licitud d'FGC o dels seus desenvolupadors.
- Sol·licituds de canvis o incorporacions de registres al DNS
- Sol·licitud de canvis o incorporacions a la CDN.

- Sol·licituds de canvi en les regles de filtrat del Firewall i/o del WAF
- Creació, eliminació d'usuaris. Assignació i/o canvi dels permisos dels usuaris
- Sol·licituds de gestió de VPNs: afegir nous usuaris, creació de noves VPNs
- Requeriments d'informació o verificació sobre el funcionament de qualsevol dispositiu de la infraestructura de FGC
- Instal·lació, configuració i renovació de certificats de seguretat.
- Sol·licituds de creació de noves mètriques o d'alarmes de monitorització
- Informes d'incidències en el funcionament d'un determinat servei de l'entorn de FGC.

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. S'inclou:

- Assessorament general a FGC i/o als seus desenvolupadors
- Projectes de implantació de servidors i nous serveis
- Realització d'informes especials requerits per FGC
- Instal·lació de pegats de sistema i/o noves versions de llibreries o programes en la finestra de temps aprovada prèviament per FGC.

Temps de resposta: 2h (120 minuts)
Temps màxim de resolució: 2 dies laborables

4.4. Requeriments específics de seguretat

L'empresa adjudicatària haurà de realitzar una auditoria de seguretat en compliment d'aquest requeriments un cop s'hagi fet càrrec de la infraestructura de FGC.

Caldrà que l'empresa licitadora elabori documentació específica sobre el seu procediment de gestió de contingències que contempli les mesures a adoptar per solucionar el funcionament incorrecte de l'entorn.

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

Accés als servidors

FGC haurà de disposar d'accés exclusiu i il·limitat als seus servidors, per això podrà emprar protocols d'accés remot (Secure Shell SSH o VPN).

Els desenvolupadors d'FGC hauran de tenir accés exclusivament a la seva àrea de desenvolupament dins de cada servidor.

L'empresa adjudicatària haurà de garantir que tots els accessos a la infraestructura de FGC es realitzaran exclusivament a través de la VPN corresponent.

Gestió de VPNs

Gestió i configuració de connexions VPN Site-to-site entre les xarxes de les empreses desenvolupadores i els servidors corresponents de AWS.

Es configuraran VPNs Site-to-site per garantir la connectivitat amb protocols de seguretat des de la pròpia xarxa de FGC i des de les xarxes dels diferents desenvolupadors de les webs que col·laboren amb FGC fins a un màxim de 10 empreses amb uns 20 usuaris connectats amb els seus servidors de treball en qualsevol horari. Aquestes empreses col·laboradores poden canviar depenent dels projectes.

Gestió d'usuaris i permisos

El proveïdor haurà de ocupar-se de la gestió d'usuaris garantint el compliment de totes les mesures de seguretat, afegint aquells que es sol·liciten per a l'accés a través d'una determinada VPN i gestionant els seus permisos d'accés a la seva àrea de desenvolupament del servidor concret.

Pel que fa a la política de contrasenyes es treballarà amb claus d'un mínim de 8 caràcters que continguin números i símbols. S'haurà de sol·licitar als usuaris un canvi de contrasenyes amb una periodicitat màxima de 12 mesos.

Content Delivery Network (CDN)

L'empresa adjudicatària haurà de absorbir els sobre costos del trànsit generat pels atacs de DoS que pogués rebre la infraestructura de FGC.

En cas de caiguda del servidor principal d'una web, la CDN haurà d'oferir una còpia el més exacta possible de cada web. A més, la CDN haurà de permetre ocultar a l'exterior la IP real dels servidors.

La CDN comptarà amb un sistema de protecció anti atacs de DoS configurat per a un màxim de 100 dominis de FGC que permetrà que tot el trànsit d'atac que arribi a la infraestructura de servidors d'FGC s'enviï automàticament als servidors dels centres de dades destinats a discriminar el tràfic legítim de l'il·legítim. Aquest sistema haurà de permetre absorbir les inundacions de trànsit il·legítim a l'extrem de la xarxa.

La CDN permetrà gestionar un mínim de 5 regles WAF (tallafocs d'aplicacions) a tots els dominis de FGC. A més, en els dominis principals (fgc.cat, lamolina.cat, valldenuria.cat, vallter2000.cat, portaine.cat, espotesqui.cat, turismefgc.cat, boitaull.cat, parcastronomic.cat) la CDN permetrà:

- Gestionar un mínim de 10 regles WAF
- Bloqueig d'agents
- Anàlisi avançat de registres de DNS
- Mètriques operatives
- Registres d'auditoria

Per evitar que els hackers ataquin directament els servidors web saltant-se la seguretat proporcionada per la CDN caldrà a més esborrar qualsevol entrada de subdomini o informació històrica que pugui servir als hackers per esbrinar la IP real dels servidors web de FGC.

Integració d'un tallafocs d'aplicacions web (WAF)

La integració d'aquests tallafocs s'ha de fer contra la CDN i contra el servidor web principal de cada web (configurant les funcionalitats de ModSecurity) i hauran de permetre, a més de frenar les vulnerabilitats pròpies dels servidors web, frenar els atacs DDoS de nivell d'aplicació (capa 7). Al WAF (Web Application Firewall) hi haurà d'haver activades les regles OWASP (Open Web Application Security Project):

- Common exceptions
- Generic attacks
- SQL Injection
- Cross-Site Scripting
- Bad robots
- HTTP policy
- Protocol violations and anomalies
- Request limits
- LFI attacks

El WAF també haurà de tenir activades les regles bàsiques de protecció contra atacs cap a les plataformes CMS de FGC:

- PHP
- Wordpress
- Drupal
- Joomla
- Magento
- Prestashop
- WHMCS (Web Hosting Automation)
- PhpBB

Tallafocs exclusiu per a cada servidor

Aquest servei de seguretat haurà de permetre configurar per a cada servidor qui accedeix i a quins

ports, establint i personalitzant les regles d'entrada i sortida basant-se en adreces IP origen, adreces IP destí i protocols, ports o serveis.

A més, el tallafocs haurà de garantir la protecció enfront dels següents atacs i vulnerabilitats dels sistemes:

- Intents de localització i inspecció de servidors i serveis oberts:
  - Escombrats de ports TCP
  - Escombrats mitjançant ICMP
- Atacs de denegació de servei (Denial Of Service, DoS) per enviament massiu de peticions:
  - SYN Flooding
  - ICMP Flooding
  - UDP Flooding
- Atacs de denegació de servei (Denial Of Service - DoS) per vulnerabilitats del sistema operatiu:
  - Death ping
  - Atac Tear Drop
  - Atac WinNuke
  - Atac Land
- Enviament de paquets IP incorrectes:
  - "Filter IP Source Route Option."
  - "Spoofing" d'IP
  - Paquets IP amb opció/flags incorrectes
  - Paquets IP amb opció/flags insegures
- Nombre de connexions excessives des d'un origen:
  - Límit de sessions TCP, UDP i ICMP
- Atacs a vulnerabilitats de serveis:
  - Bloqueig de URLs malicioses
  - Atacs de "buffer-overflow" a SMTP, FTP i POP3
  - Bloqueig del tràfic de xarxa corresponent a protocols Windows (per exemple: NetBIOS sobre TCP/IP)

Còpies de seguretat

Serveis de Backup de fitxers, bases de dades i generació d'instantànies (snapshots) completes de cada servidor, així com la gestió de les possibles restauracions. Tot en compliment del Reglament general de protecció de dades europeu (UE) 2016/679 del Parlament Europeu de 27 d'abril de 2016 (RGPD)

Les còpies de seguretat de fitxers i bases de dades hauran de complir els requeriments següents:

- Full Backup diari del contingut complet de tots els servidors amb un temps de retenció mínim de 365 dies i una variació diària de la informació d'un 20%.
- Les còpies estaran comprimides i es realitzaran xifrades per garantir la seva seguretat

- Possibilitat de restauració completa o a nivell de fitxer de la situació exacta del servidor en un dia determinat dels últims 365 dies
- Per garantir el compliment del Reglament (UE) 2016/679 del Parlament Europeu de 27 d'abril de 2016 (RGPD), les còpies s'emmagatzemaran en servidors d'un centre de dades que estigui en una regió de la UE diferent de la del centre de dades de AWS dels servidors de FGC (UE Irlanda). En aquests servidors les còpies es realitzaran xifrades i la informació s'haurà d'enviar a través d'internet garantint la seguretat de la transmissió (SSL/HTTPs), utilitzant per a això protocols d'encriptació d'última generació (de fins a 448 bits)
- La empresa licitadora haurà de encarregar-se de les possibles restauracions i del tràfic generat.
- Les restauracions de les còpies de seguretat podran realitzar-se des de qualsevol lloc i podran ser completes (de tot el contingut de servidor) o a nivell de fitxer

Snapshots

Es crearan i emmagatzemaran dues instantànies diàries (snapshot) de cada un dels servidors de FGC amb una variació mitjana de la informació diària d'un 20%

La empresa licitadora haurà de encarregar-se de les possibles restauracions i del tràfic generat.

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.

5. 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 de spam, DoS o DDoS, virus, etc
- Sistema de tiquets de servei on quedin enregistrades les sol·licituds i incidències reportades per FGC o els seus col·laboradors o detectades directament per l'empresa adjudicatària pels sistemes de monitorització. Per a les incidències tècniques s'hauran d'incloure en el sistema la causa, la solució, les accions realitzades per a la seva resolució i el què es farà o s'ha fet per evitar que es repeteixi. Tota aquesta informació haurà d'aparèixer en l'informe mensual que

es lliurarà a FGC.

- Informe mensual de les actuacions realitzades que inclogui, a més de la relació d'incidències i el seu estat de resolució (sistema de tiquets), una llista de comprovacions (check list) fetes a cadascun dels servidors: versions de sistema, consum mig de CPU i memòria RAM, espai lliure en disc, mitjana de l'ample de banda consumit, nombre de connexions (en el cas dels RDS), estat dels Backups, etc. Aquest informe inclourà, per cadascun dels dominis: el nombre d'atacs bloquejats pel WAF, una estadística detallada del nombre de sol·licituds, ample de banda, visitants únics, ús de la memòria cau, sol·licituds per país, etc.
- 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.