Salut/ Institut Català de la Salut

PLEC DE PRESCRIPCIONS TÈCNIQUES

SERVEI INTEGRAL DE SUPORT I MONITORATGE DE LA PLATAFORMA DE L'ENTORN DE MOBILITAT DE L'ICS

CSE/CC00/1101428292/25 /PO

Salut/ Institut Català de la Salut

INDEX

1 Objecte de la contractació

1.1 Descripció

L'ICS requereix un servei de manteniment 24x7 de la infraestructura de l'Entorn de Mobilitat que disposa actualment i que es detalla en l'Annex 1. El sistema cobreix un total aproximat de 60 aplicacions que donen servei tant a l'ICS com a CatSalut.

L'Entorn de Mobilitat dona suport a una sèrie d'aplicacions corporatives de l'ICS que publiquen serveis web per HTTPS, orquestrades mitjançant Kubernetes sobre contenidors Docker i gestionades amb Git, Jenkins i Nexus.

Consta de dos clústers de contenidors, un dels clústers està dedicat a pre-producció per al desenvolupament de les aplicacions i l'altre a producció, que publica aplicacions tant a xarxa interna com a Internet.

A més, l'entorn inclou una arquitectura de seguretat basada en reverse proxies NGINX, sistemes de control d'accés i una xarxa interna segmentada, juntament amb sistemes de monitorització basats en Grafana, ElasticSearch i Filebeat.

En base a l'experiència de la licitació actual es requereix un nombre de 500h anuals en tasques d'administració, incloent gestió de contenidors, manteniment del clúster Kubernetes i administració de la infraestructura de seguretat.

La distribució prevista actual orientativa per al licitant requerida (Basada en informació de l'any 2024) és de :

Rol	% d'hores dedicades
Arquitecte de Sistemes	4%
Arquitecte d'aplicacions	1%
Administrador de sistemes	69%
Gestor de base de dades (DBA)	3%
Administrador Ciberseguretat	1%
DevOps	22%

2 Els serveis requerits son

L'adjudicatari ha de proporcionar serveis 24x7 que cobreixin els serveis detallats a continuació. Aquests perfils poden estar coberts per una o varies persones.

2.1 Arquitecte de sistemes

Definició:

Dissenya, planifica i supervisa una infraestructura tecnològica basada en contenidors Kubernetes, servidors Linux i arquitectura de xarxa segura.
Aquest rol implica proposar i portar a terme iniciatives crítiques sobre com han de funcionar els components del sistema per satisfer les necessitats actuals i futures del negoci, incloent optimització del rendiment dels clústers, gestió del trànsit mitjançant reverse proxies, gestió de seguretat perimetral, i planificant l'escalabilitat del l'entorn.
Administra i coordina l'ús eficient dels servidors, emmagatzematge, xarxes i sistemes d'informació, garantint la integració contínua de les aplicacions desplegades mitjançant Jenkins, Gitea i Nexus.

També s'encarrega de la gestió de la infraestructura ubicada al CPD de l'Hospital Trias i Pujol, que dona suport als serveis i eines corporatives desplegades per tot el territori de l'ICS.

Requeriments:

- Experiència i coneixements avançats d'entorns de publicació WEB amb contenidors, entorns de bases de dades, treball en xarxa i seguretat informàtica.
- Coneixements de Rocky Linux per a la seva aplicació en servidors crítics.

Tasques a realitzar:

- Realitzar tasques de disseny i assessorament en la presa de decisions sobre com ha de ser l'arquitectura de l'Entorn de Mobilitat cap a on cal evolucionar-la per conservar i/o augmentar el rendiment i disponibilitat.
- Proposar solucions per adaptar-la a noves especificacions de servei.
- Fer el seguiment dels treballs derivats de les propostes a implementar.
- Donar suport per a entorns de virtualització.
- Portar a terme la documentació de l'entorn.
- Administració de servidors Rocky Linux, gestionant-ne la configuració, manteniment i optimització per garantir-ne l'estabilitat en entorns productius.
- Gestionar la infraestructura del CPD ubicat a l'Hospital Trias i Pujol, assegurant que el seu funcionament doni suport als serveis corporatius de l'ICS.

2.2 Arquitecte d'aplicacions

Definició:

Dissenya l'estructura i l'arquitectura de les aplicacions de programari dins d'una organització, enfocant-se en l'optimització de l'eficiència i escalabilitat de les solucions. Treballa per assegurar-se que les aplicacions compleixin amb els requisits del negoci i s'integrin adequadament amb els propis sistemes de l'entorn. Sovint coordina i/o dona suport els equips de desenvolupadors i implementa millores tecnològiques. És responsable de prendre decisions tècniques sobre les eines, tecnologies i patrons de desenvolupament a utilitzar.

També és responsable de la gestió de plataformes CMS com Liferay, utilitzat per a la gestió de planes webs, així com del manteniment d'aplicacions de tercers dins del territori de l'ICS.

Requeriments:

- Experiència i coneixements avançats d'arquitectura d'aplicacions, programari i desenvolupament d'aplicacions, metodologies de backup i restauració.
- Coneixement en la instal·lació, manteniment i actualització del CMS Liferay.
- Experiència en suport i manteniment d'aplicacions de tercers en funcionament en diferents zones del territori.
- Coneixement en desenvolupament i manteniment d'aplicacions amb PHP i diverses versions de Java.

Tasques a realitzar:

- Realitzar tasques de disseny dels microserveis amb els que s'han de publicar les aplicacions.
- Definir i dissenyar el sistema de còpies de seguretat general, els seus processos, i decidir el programari a utilitzar.
- Definir i dissenyar el sistema de còpies de seguretat de les imatges dels contenidors, els seus processos i decidir el programari a utilitzar.
- Fer el seguiment dels treballs derivats de les propostes a implementar.
- Instal·lació, actualització i manteniment del CMS Liferay, garantint la seguretat i el bon rendiment de la plataforma web.
- Manteniment d'aplicacions de tercers en diferents zones del territori, incloent la resolució d'incidències i la implementació d'actualitzacions i millores.
- Suport en el desenvolupament i manteniment d'aplicacions amb PHP i diferents versions de Java, assegurant la seva correcta integració en l'entorn de l'ICS.

2.3 Administrador de Sistemes

Definició:

Gestiona la configuració, manteniment i suport de sistemes informàtics i servidors. Responsable de garantir que els sistemes informàtics i de xarxes estiguin operatius i funcionin sense problemes, solucionant qualsevol problema que pugui sorgir. Instal·la programari, gestiona usuaris, actualitza els sistemes i monitoritza el rendiment del sistema. A més, s'encarrega de les còpies de seguretat i de la seguretat general de la infraestructura de TI.

També s'encarrega de l'administració i manteniment de servidors basats en Rocky Linux, així com del manteniment i operació de la infraestructura del CPD de l'Hospital Trias i Pujol. Això inclou la configuració, monitorització i manteniment dels sistemes que donen servei a aplicacions i serveis crítics.

Requeriments:

Son necessaris experiència i coneixements avançats a nivell d'instal·lació i manteniment de:

- Sistemes operatius: **Debian, RedHat (amb HA Addon), Rocky Linux**
- Contenidors i orquestració: **Kubernetes**
- Servidors web i proxy: **Nginx, Apache, Tomcat**
- Aplicacions de comunicació i desenvolupament: **Jitsi-Meet, Jenkins, Git, Gitea, Nexus, Sonarqube**
- Sistemes de monitoratge i registre: **Kibana, ElasticSearch, Filebeat**
- Certificació i seguretat: **Certificats SSL, SMTP**
- Administració d'entorns web i aplicacions: **Liferay**
- Coneixements en administració de xarxes i infraestructura de CPD.

Tasques a realitzar:

- Instal·lació, manteniment de sistemes operatius i gestió d'usuaris.
- Realitza tasques d'administració dels sistemes que comprenen l'actualització, configuració, instal·lació de programes i ajustaments de rendiment dels sistemes i programari.
- Tractar les incidències que es puguin produir a nivell de sistema i processos.
- Implementar els canvis en el disseny de l'entorn.
- Implementar i gestionar les còpies de seguretat de sistemes.
- Administració del Reverse-proxy (nginx) corporatiu que dona servei aplicacions mòbils i WEB de tot Catalunya.
- Operació de Xarxes:
    - Monitoratge i manteniment de la infraestructura de xarxa.
    - Configuració de dispositius de xarxa i gestió de la connectivitat.
- Resolució d'incidents de xarxa i optimització del rendiment.
- Documentació de configuracions i processos tècnics.

2.4 Gestor de base de dades - DBA

Definició:

Responsable de la creació, gestió, manteniment i optimització de les bases de dades que contenen la informació crítica del programari d'una organització. A més de gestionar la seguretat de les dades, el DBA s'encarrega de garantir el bon funcionament de les bases de dades, incloent la creació de còpies de seguretat, la recuperació de dades, la millora del rendiment i la resolució de qualsevol problema relacionat amb l'accés o la integritat de les dades. Treballa per assegurar-se que la informació sigui fàcilment accessible pels sistemes que l'utilitzen, i que sigui escalable a mesura que creixen les necessitats de dades de l'empresa.

Requeriments:

Cal experiència i coneixements avançats en:

- Instal·lació, administració, actualització i optimització del rendiment de:
  - Clústers de **MySQL**.
  - Clústers de **MariaDB** (amb **Galera**).
  - Bases de dades **Oracle, MySQL i MariaDB (Galera).**
- Gestió d'incidències en l'entorn de bases de dades, incloent la seva anàlisi i resolució.
- Implementació de canvis de disseny en bases de dades per millorar-ne l'eficiència i escalabilitat.
- Aplicació de mesures de seguretat per protegir la integritat i confidencialitat de les dades.
- Gestió de còpies de seguretat i processos de recuperació de dades, assegurant la disponibilitat i fiabilitat dels sistemes.

Tasques a realizar:

- **Gestió de servidors de bases de dades**: Instal·lació, configuració i manteniment dels servidors de bases de dades, assegurant que funcionin de manera òptima i estan alineats amb les necessitats del negoci.
- **Optimització del rendiment de les bases de dades**: Monitorització constant per detectar i resoldre colls d'ampolla, aplicant millores de rendiment a les consultes, índexs, particions i altres elements estructurals.
- **Implementació de polítiques de seguretat**: Assegurar que les bases de dades estiguin protegides davant accessos no autoritzats mitjançant l'ús d'encriptació, gestió d'usuaris, i permisos adequats.
- **Realització de còpies de seguretat**: Programar i supervisar la realització periòdica de còpies de seguretat per garantir la recuperació de les dades en cas d'emergència.
- **Recuperació de dades**: Implementació de procediments de recuperació en cas de pèrdua de dades o desastres, garantint la mínima pèrdua de temps i informació.
- **Actualització i migració de bases de dades**: Planificar i executar actualitzacions de versions de bases de dades i migracions a nous sistemes, garantint la mínima interrupció del servei.

- **Suport a l'equip de desenvolupament**: Col·laborar amb els desenvolupadors per oferir suport en la creació i manteniment de consultes SQL eficients i en la millora del disseny de les bases de dades.
- **Auditories de seguretat i rendiment**: Realització d'auditories periòdiques per identificar possibles vulnerabilitats de seguretat i per detectar àrees de millora en el rendiment de les bases de dades.
- **Monitorització constant**: Supervisar l'estat de les bases de dades en temps real per identificar possibles problemes o anomalies abans que afectin els serveis productius.
- **Gestió de capacitat**: Preveure el creixement de les dades i planificar adequadament per evitar problemes de capacitat, assegurant que les bases de dades es mantinguin escalables.
- **Documentació**: Mantenir una documentació actualitzada sobre la configuració, canvis, incidents i millores de les bases de dades per assegurar un bon seguiment i traspàs de coneixement.

2.5 Administrador de Ciberseguretat

Definició:

El seu paper principal és protegir els sistemes, xarxes i dades de la organització contra possibles amenaces i atacs cibernètics. Desenvolupa i implementa mesures de seguretat com tallafocs, sistemes de detecció d'intrusions i protocols de xifrat de dades. A més, realitza auditories periòdiques per identificar vulnerabilitats, proposa solucions per reforçar la seguretat, coordina i/o dona resposta i suport davant incidents de seguretat. El seu objectiu és garantir de forma proactiva que les dades i sistemes crítics estiguin protegits en tot moment.

Requeriments:

Cal experiència i coneixement de:

- Administració de sistemes.
- Administració d'aplicacions.
- Aplicacions i processos de còpies de seguretat i restauració.
- Pentesting i valuació de seguretat informàtica.
- Polítiques de seguretat definides pel l'Agència de Ciberseguretat de Catalunya i l'Oficina de Seguretat de l'ICS.

Tasques a realitzar:

- Definir les directives de ciberseguretat de l'entorn.
- Definir les directives de ciberseguretat de les aplicacions.
- Vetllar per a que les directives de ciberseguretat s'apliquin.
- Executar avaluacions periòdiques de la ciberseguretat de l'entorn.
- Donar suport a l'Arquitecte d'Aplicacions alhora de definir el sistema de còpies de seguretat.

- Donar suport a l'Administrador de Sistemes en el restaurament de còpies de seguretat.
- Seguretat Informàtica:
    - Monitoratge i gestió de seguretat de la xarxa.
    - Implementació de mesures de seguretat en aplicacions i sistemes.
    - Resposta a incidents de seguretat i auditoria de sistemes.
- Auditories proactives de seguretat de sistemes, aplicacions i base de dades, abans dels desplegaments en producció.

2.6 DevOps

Definició:

S'encarrega d'automatitzar processos com el desplegament de codi, les proves de programari i la integració contínua mitjançant **Jenkins, Gitea i Docker.**
Això permet una entrega ràpida i eficient dels serveis digitals, minimitzant errors humans i augmentant la col·laboració entre els equips de desenvolupament i operacions.
A més, gestiona la configuració del clúster Kubernetes, el desplegament d'imatges Docker des de Nexus, i la integració dels logs de funcionament mitjançant Filebeat i ElasticSearch.

L'objectiu és garantir que les aplicacions es despleguin de manera segura i ràpida, i que siguin fàcils de mantenir i escalables. Aquest rol híbrid combina coneixements i tasques de desenvolupament de programari i operacions de TI per optimitzar els processos d'entrega de programari.

Requeriments:

Es necessari coneixement en la integració i automatització dels processos entre el desenvolupament de software i les operacions de TI. També cal tenir coneixements de programació.

Tasques a realitzar:

- Realitzar les tasques d'administració de l'entorn DevOps, programant els processos d'integració continua i vetllant per la correcta relació entre les aplicacions que formen l'entorn.
- Efectuar les altes, baixes i modificacions d'usuaris i aplicacions publicades.
- Assessorar i cooperar amb els equips de programadors i resoldre els dubtes que puguin tenir en la posada en marxa de les aplicacions.
- Crea les imatges dels contenidors i manté un dipòsit propi d'imatges base que s'usa per crear les de les aplicacions publicades a l'entorn.
- Desenvolupament i manteniment de pipelines d'Integració Contínua / Desplegament Continu.
- Gestió d'entorns de desenvolupament, pre-producció i producció.
- Automatització de desplegaments i gestió de contenidors.
- Suport en el desplegament de les aplicacions a l'equip de l'ICS

- Realització de petites correccions puntuals en els desenvolupaments, amb l'objectiu d'integrar-los a l'entorn.
- Administració, gestió i control del sistema de control de versions i dipòsits de codi.
- Suport a la Implementació de millores i noves funcionalitats en aplicacions existents.
- Preparació i instal·lació d'aplicacions prèviament ja existents en contenidors de tercers, a nous contenidors, així com la resolució d'incidències puntuals posteriors, com per exemple amb la configuració d'enviament SMPT, on mètodes d'encriptació que calgui de generar noves claus, i testeig.

3 Sistema de monitorització i gestió

L'objectiu d'aquest sistema ha de ser assegurar l'òptima operativitat dels actuals (9) i futurs servidors de l'espai de Mobilitat, incloent els clústers Kubernetes, la infraestructura de seguretat i el sistema de gestió d'aplicacions.

Es requereix la construcció d'un nou sistema de monitorització amb tecnologia similar a Grafana i/o ElasticSearch que permeti la identificació i prevenció d'aturades o mal funcionaments, seguiment en temps real dels logs de kubernetes, base de dades, tota la resta de serveis de la infraestructura, i detecció d'anomalies en el tràfic de la xarxa.

A més ha de permetre efectuar revisions regulars per confirmar l'estat dels servidors i aplicar les solucions necessàries en cas de trobar qualsevol tipus de incidència en els serveis, sistemes o bases de dades.

El sistema de monitorització i gestió, encara que durant el servei sigui utilitzat només per l'adjudicatari, **serà propietat de l'ICS**. Per aquest motiu, el sistema ha d'estar documentat i s'ha de poder empaquetar i lliurar a l'ICS per a fer la transferència del mateix a la finalització de la present licitació.

El servei de formació/informació de la plataforma de monitoratge de l'Entorn de Mobilitat de l'ICS i els posteriors adjudicataris del servei està inclosa dintre de la present adjudicació i no es pot generar cap despesa addicional en aquest sentit.

Mentrestant no hi hagi un de nou, es requereix continuar amb el sistema de monitoratge actual, desenvolupat amb codi propietari de l'actual empresa que presta els serveis.

La nova plataforma, ha d'incorporar :

- Servei de monitoratge sobre programari lliure (Nagios, Grafana) personalitzat a la infraestructura de Mobilitat.
- Informació online sobre l'estat de tota la infraestructura.
- Seguiment històric dels paràmetres de funcionament (CPU, memòria, latència de xarxa, rendiment de base de dades,..).
- Sistema de detecció d'atacs de ciberseguretat
- Emissió d'alertes via email de les incidències de funcionament detectades.
- Generació de gràfics amb informació de l'evolució del rendiment dels recursos.

Les activitats resultants han d'incloure:

- Revisió sistemàtica dels servidors per verificar la seva funcionalitat i desenvolupament.
- Identificació, detecció i prevenció de comportaments anòmals abans que puguin arribar a afectar al servei.
- Ajustaments i reparacions en els sistemes i bases de dades per resoldre incidències observades.
- Resposta i maneig de les incidències identificades.
- Reports mensuals sobre la condició de cada servidor.
- Suport i orientació per consultes via trucada telefònica o correu electrònic.

4 Servei 24x7

L'adjudicatari ha de garantir la prestació del servei de manteniment 24x7 per assegurar la continuïtat i disponibilitat de l'Entorn de Mobilitat de l'ICS. Això inclou la gestió de qualsevol incidència o emergència que pugui sorgir fora de l'horari laboral habitual.

4.1 Cobertura del servei

El servei 24x7 ha de cobrir els següents aspectes:

- Monitoratge en temps real de l'Entorn de Mobilitat, incloent servidors, bases de dades i serveis publicats.
- Resposta a incidències crítiques que puguin afectar la disponibilitat de les aplicacions i serveis corporatius de l'ICS.
- Atenció a emergències mitjançant mecanismes de comunicació predefinits.
- Execució de tasques preventives i correctives per garantir l'estabilitat i seguretat del sistema.

4.2 Protocol d'actuació en incidències

En cas de detectar una incidència fora de l'horari laboral, l'adjudicatari haurà de:

1. **Classificar la incidència** segons la seva criticitat:

- **Crítica (P1)**: Impacte alt en la disponibilitat del servei.
- **Alta (P2)**: Disminució del rendiment o afectació parcial de serveis.
- **Mitjana (P3)**: Problemes que no impedeixen el funcionament però requereixen atenció.
- **Baixa (P4)**: Consultes o millores que poden esperar al següent horari laboral.

2. **Activar el procediment de resposta**, seguint els següents temps màxims de resolució:

   - **P1 (Crítica)**: Resposta immediata i resolució en un màxim de 2 hores.
   - **P2 (Alta)**: Resposta en menys de 4 hores i resolució en 6 hores.
   - **P3 (Mitjana)**: Resposta en 8 hores i resolució en 24 hores.
   - **P4 (Baixa)**: Resolució en un termini màxim de 72 hores.

3. **Comunicació a l'ICS**: L'adjudicatari haurà d'informar immediatament de qualsevol incidència de nivell P1 o P2 mitjançant el sistema de comunicació acordat (correu electrònic, telèfon o plataforma d'incidències).

4. **Registre i documentació de la incidència**: Totes les incidències resoltes fora de l'horari laboral hauran de quedar documentades i identificades a l'informe periòdic que es lliurarà a l'ICS.

4.3 Equips i disponibilitat del servei

- L'adjudicatari haurà de comptar amb **personal tècnic qualificat** disponible en tot moment per atendre les incidències.
- Es facilitaran diversos sistemes de comunicació amb l'equip de suport, incloent-hi telèfon directe, correu electrònic i, si es disposa, accés a una plataforma de gestió d'incidències.
- Es realitzaran **simulacres periòdics** per verificar l'efectivitat del servei 24x7 i assegurar que els procediments d'actuació són òptims.

4.4 Auditoria i control del servei 24x7

- L'ICS podrà dur a terme auditories per comprovar el compliment dels compromisos adquirits en relació amb la disponibilitat i temps de resposta del servei.
- En cas d'incompliment dels terminis establerts, es podran aplicar penalitzacions conforme a l'apartat 8. Penalitzacions.

5 Requeriments de Seguretat

L'empresa adjudicatària es compromet a prendre totes les mesures tècniques i organitzatives al seu abast per garantir l'objectiu de seguretat de la informació, que es basa en els 5 principis següents:

- La **confidencialitat** de la informació, assegurant que només hi accedeixen les persones que han estat autoritzades a fer-ho.
- La **integritat** de la informació, assegurant que la informació i els mètodes que la processen són exactes i complets.
- La **disponibilitat** d'aquesta informació, assegurant que els usuaris autoritzats tenen accés a aquestes dades, mòduls i aplicacions quan ho necessitin.
- L'**autenticitat**, verificant la identitat dels usuaris i la validesa de les dades.
- La **traçabilitat**, perment rastrejar l'accés i ús de la informació, facilitant d'aquesta forma l'auditoria i seguiment d'activitats.

Igualment, es compromet a prendre les mesures que preveu la normativa en vigor en matèria de seguretat de la informació i protecció de dades de caràcter personal.

L'adjudicatari ha de complir els requisits establerts pel Reglament UE 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en allò que respecte al tractament de dades personals i a la lliure circulació d'aquestes dades (Reglament General de Protecció de Dades - RGPD), així com la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i de garantia dels drets digitals, i pel Reial Decret 1720/2007, de 21 de desembre, en tot allò que sigui d'aplicació, i tota altra norma relacionada que estigui vigent.

A més, l'adjudicatari haurà d'aplicar les mesures establertes per la norma ISO/IEC 27001 (Sistema de Gestió de la Seguretat de la Informació) i ISO/IEC 27002 (Codi de pràctiques per a la seguretat de la informació), així com les directrius de l'Esquema Nacional de Seguretat (ENS) d'Espanya, amb l'objectiu de garantir la protecció de la informació durant el desenvolupament i l'execució del contracte.

També s'haurà de complir amb la Directiva (UE) 2016/1148 relativa a mesures per garantir un alt nivell comú de seguretat de les xarxes i sistemes d'informació a la Unió Europea, en tot allò aplicable a la infraestructura de la solució proposada.

En cas que per la execució del contracte impliqui o requereixi de l'ús d'algun servei en el núvol, s'haurà de complir amb la norma ISO/IEC 27018, per garantir la protecció de dades personals en serveis de núvol, i aplicar les pràctiques de seguretat establertes pel NIST Cybersecurity Framework (CSF) en matèria de seguretat cibernètica.

L'adjudicatari haurà de garantir la seguretat de les dades en tot moment, incloent la seva protecció contra accessos no autoritzats, modificacions, divulgacions o destrucció accidental o il·legal.

6 Compromisos de confidencialitat, seguretat i protecció de dades

Accés a dades personals, o de caràcter reservat:

- L'empresa adjudicatària es compromet a no accedir innecessàriament a aquelles dades a les quals tingui accés per raó de la tasca que té encomanada.
- Sempre que calgui manipular dades, es treballarà amb dades de proves, simulades o fictícies. Un cop acabat el desenvolupament o prova, s'esborraran totes les dades manipulades, tant si són fictícies com reals.
- En cas que sigui necessari accedir a les dades reals, l'empresa i els seus treballadors es comprometen a mantenir la confidencialitat respecte a la informació coneguda, a no alterar-ne el contingut i a no revelar, comunicar, ni posar a disposició de tercers, per cap mitjà, escrit, electrònic, verbal o per qualsevol altre procediment, cap d'aquestes dades o part d'elles, o la informació que se n'hagi pogut extreure.

Aquesta obligació de confidencialitat s'haurà de mantenir de manera indefinida, fins i tot després de la finalització del contracte amb nosaltres, d'acord amb el mateix criteri que s'aplica a tots els professionals de l'ICS i a les empreses i entitats externes que ens presten serveis, inclosos contractistes, col·laboradors i proveïdors tecnològics.

- L'accés a aquestes dades reals haurà de ser autoritzat pel responsable del fitxer o pel responsable de seguretat de l'ICS.

Col·laboració en les auditories periòdiques

- L'empresa adjudicatària es compromet a facilitar tota la informació necessària per realitzar les auditories periòdiques que dugui a terme el centre, així com a aportar els coneixements i informacions que tingui a fi de millorar els aspectes relacionats amb la seguretat i la protecció de dades de caràcter personal.

Col·laboració en gestió de la ciberseguretat

- L'empresa adjudicatària es compromet aplicar els pegats necessaris per resoldre vulnerabilitats detectades per l'Agència de Ciberseguretat i Sistemes d'Informació de l'ICS, així com a emetre avisos en cas de detecció de vulnerabilitats en els seus productes i a col·laborar en el diagnòstic i resolució d'incidents de seguretat facilitant tota la informació necessària, així com a aportar els coneixements i informacions que tingui a fi de millorar els aspectes relacionats amb la seguretat i la protecció de dades de caràcter personal.

Mesures organitzatives:

- L'empresa adjudicatària informarà al Comitè de Seguiment de les mesures organitzatives i tècniques que ha pres per assegurar la confidencialitat, integritat i disponibilitat de la informació i les dades de caràcter personal propietat de l'Institut Català de la Salut.

7 Seguiment i supervisió

Per garantir un servei de manteniment eficient i alineat amb els requeriments de l'ICS, s'estableixen mecanismes de seguiment i supervisió que permetin monitoritzar i avaluar el rendiment del servei prestat per l'adjudicatari. Aquest seguiment es realitzarà a través d'informes **trimestrals** i reunions de seguiment que assegurin la correcta execució del contracte. La periodicitat dels informes podrà disminuir segons necessitats.

7.1 Informes periòdics

L'adjudicatari haurà de proporcionar informes periòdics detallats sobre l'estat del servei de manteniment. Els informes hauran de contenir, com a mínim, la següent informació:

- Resum de les activitats realitzades durant el període.
- Nombre d'hores dedicades per perfil i per tipus de tasca.
- Peticions pendents i resoltes, amb el seu temps de resolució.
- Incidències detectades i resoltes, amb el seu temps de resolució.
- Incidències pendents i el seu estat.
- Anàlisi de l'estat de la infraestructura i recomanacions de millora.
- Detall de les actuacions realitzades en matèria de seguretat i protecció de dades.
- Resum de les operacions relacionades amb la monitorització i manteniment dels servidors.
- Qualsevol altra informació rellevant per a la supervisió del servei.

Els informes es lliuraran amb una periodicitat mensual i seran revisats pel personal competent o comissió de seguiment corresponent de Sistemes d'Informació Corporatius l'ICS.

7.2 Reunions de seguiment

Per garantir una comunicació fluida i la correcta supervisió del servei, es realitzaran reunions de seguiment de manera periòdica entre l'ICS i l'adjudicatari. Aquestes reunions tindran els objectius següents:

- Revisar els informes periòdics i aclarir qualsevol dubte.
- Analitzar el compliment dels objectius i indicadors de qualitat del servei.
- Identificar possibles problemes i establir mesures correctores.
- Planificar millores i optimitzacions de l'entorn de mobilitat.
- Garantir el compliment dels requisits de seguretat i protecció de dades.

La periodicitat de les reunions serà mensual amb possibilitat de ser bimensuals per acord mutu, encara que podran convocar-se sessions extraordinàries en cas de necessitat. De cada reunió caldrà que quedi constància escrita dels acords presos i les accions a portar a terme, la qual serà compartida amb totes les parts implicades.

7.3 Indicadors de seguiment

Els indicadors clau de rendiment (KPIs) es basaran en la informació proporcionada als informes periòdics de l'adjudicatari i en l'anàlisi qualitativa del servei. No es realitzaran càlculs detallats tret que es detectin desviacions greus que requereixin una quantificació específica. Aquesta metodologia permet detectar i abordar problemes de manera àgil sense generar càrregues administratives innecessàries.

Indicador	Font d'informació	Criteris d'alerta
Temps mitjà de resolució d'incidències	Incidències detectades i resoltes, amb el seu temps de resolució	Si hi ha incidències crítiques obertes durant diversos informes consecutius
Disponibilitat dels sistemes i aplicacions	Anàlisi de l'estat de la infraestructura	Si hi ha problemes recurrents o temps d'inactivitat prolongat
Compliment del servei per perfil	Nombre d'hores dedicades per perfil i per tipus de tasca	Només es revisa si hi ha queixes o desviacions evidents
Resolució de peticions i incidències	Peticions pendents i resoltes, incidències detectades i resoltes	Si hi ha un nombre elevat de peticions acumulades sense resposta
Qualitat de la documentació i millores proposades	Detall de les actuacions en seguretat, protecció de dades i millores de la infraestructura	Si no s'aporten millores ni documentació en diversos informes seguits

7.4 Procediment de seguiment

A continuació, es detalla el procediment de seguiment a partir dels indicadors anteriors:

- Els indicadors es revisaran mensualment en base als informes periòdics proporcionats.
- La seva anàlisi es durà a terme durant les reunions de seguiment.
- Si es detecten anomalies recurrents, es podrà requerir un anàlisi més detallat.
- Els canvis i millores es documentaran per garantir la traçabilitat i evolució del servei.

7.5 Mecanismes de comunicació

L'adjudicatari haurà de posar a disposició de l'ICS diversos canals de comunicació per facilitar el seguiment i la supervisió del servei. Aquests inclouran:

- Un punt de contacte principal per a la gestió de la comunicació amb l'ICS.
- Correu electrònic per a la notificació d'incidències i sol·licituds.
- Telèfon d'atenció per a incidències urgents.
- Accés a una plataforma de gestió d'incidències i seguiment.

Aquestes mesures garantiran una supervisió eficaç i un servei de qualitat que respongui a les necessitats de l'ICS en l'Entorn de Mobilitat.