

**PLEC DE PRESCRIPCIONS TÈCNIQUES
PARTICULARS QUE HA DE REGIR EL
CONTRACTE DE SERVEIS DE
MANTENIMENT DE L'APLICACIÓ RAS (RISK
ALERT SYSTEM)**



1. ANTECEDENTS	3
2. OBJECTE I REQUERIMENTS	4
3. DESCRIPCIÓ DE L'ENTORN ACTUAL.....	6
4. REQUERIMENTS FUNCIONALS.....	7
4.1 Gestió i creació de rols d'usuari (supervisor/operador) intercomunicació o incidències.....	7
4.2 Mòdul notificació de riscos en instal·lacions (iBeacons).....	8
4.3 Sistema de Xat	9
4.4 Mòdul d'incidències.....	9
4.5 Mòdul d'ubicacions.....	11
4.6 Mòdul permisos de treball.....	12
5. ALLOTJAMENT DE LA PLATAFORMA.....	15
6. REQUERIMENTS TECNOLÒGICS	15
6.1 Relació de tecnologies a utilitzar:	15
6.2 Descripció de l'entorn d'ús tecnològic:	16
6.3 Requeriments mínims dels Ibeacons:.....	17
7. MANTENIMENT	17
8. INTERLOCUCIÓ AMB EMATSA	19
9. MITJANS HUMANS I MATERIALS.....	19
10. GARANTÍA, SERVEI DE SUPORT I DE MANTENIMENT.....	20
11. SEGURETAT	21
12. GESTIÓ DE DADES DE CARACTER PERSONAL	24

1. ANTECEDENTS

EMATSA per a les seves tasques ordinàries i extraordinàries de manteniment i millora de les xarxes del servei d'abastament d'aigua potable i sanejament i depuració de les aigües residuals, requereix de la execució de tasques de diferents perfils multidisciplinaris a on, moltes d'elles, comporten riscos específics i associats per als treballadors/es; fet que implica la rigorosa implementació de sistemes i metodologies en matèria de prevenció de riscos associats a cada activitat i acord amb els requisits legals vigents.

Per aquest motiu amb la finalitat d'augmentar la vigilància i prevenció requerides per a les tasques realitzades, l'any 2019 es va desenvolupar l'aplicació mòbil per a ús intern del personal de la companyia, Risk Alert System, eina utilitzada pels treballadors/es per tal d'implementar millores en els procediments, alertes e incidències associades a les metodologies de treball i instal·lacions del servei. Dotant l'activitat d'una major vigilància, prevenció i traçabilitat de les actuacions incrementant les mesures de protecció per al personal.

Es tracta de una aplicació mòbil, de distribució únicament interna al personal d'EMATSA, amb les següents funcionalitats i definides amb major detall en capítols posteriors del present plec:

- Notificacions (avisos de incidència o presència de perills per detecció d'iBeacons)
- Mòdul d'Incidències (notificació i gestió d'incidències)
- Mòdul Xat intern
- Mòdul d'Ubicacions (per definir ubicació i accés a instal·lacions fora de l'àmbit urbà i de complicada localització)
- Mòdul de permisos de treball (per a la creació, complimentació, tancament, aprovació i corresponent registre de permisos de treball associats a tasques amb riscos específics)

L'Aplicació, com es definirà més endavant, disposa d'un backoffice per tal de gestionar els usuaris, assignar rols, així com visualitzar i gestionar els diferents serveis, com són:

- Gestió d'usuaris, departaments i rols
- Gestió i alimentació de perills associats a instal·lacions (ibeacons)
- Gestió d'incidències (resolució, assignació, filtratge,...)
- Gestió de permisos de treball (creació, consulta, filtratge assignació,...)

Tenint en compte que és una aplicació per implementar les mesures de protecció i seguretat de les instal·lacions d'Ematsa així com les tasques que desenvolupa el mateix personal intern com l'extern, amb la única finalitat de vetllar per la protecció i seguretat d'aquests, es fa imprescindible la robustesa i continuïtat de l'aplicació Risc Alert System (RAS) mitjançant un rigorós manteniment i adequació a cada necessitat amb immediates capacitats de resposta davant possibles incidències del sistema així com una important disponibilitat continuada.

2. OBJECTE I REQUERIMENTS

L'objecte del present contracte es el manteniment de l'actual aplicació mòbil programari nadiu Android i del servidor/backOffice web, amb totes les seves funcionalitats ja desenvolupades i implantades a través del RAS. Així com la constant actualització, millora puntual i adequació de les aplicabilitats del RAS existents a noves necessitats.

L'APP funciona contra un sistema WebService que es gestionarà des de l'empresa adjudicatària mentre duri el contracte. A la finalització del contracte l'empresa adjudicatària resta obligada a entregar tant els executables de l'aplicació com els codis font d'aquesta.

S'haurà de garantir un servidor dedicat per tal de no presentar limitacions d'usuaris ni de continguts (notícies, incidències, rols, fotografies, documents, enquestes, iBeacons, xats, etc.).

La comunicació és mitjançant un protocol segur SSL contra un WebService REST. Tanmateix, ateses les limitacions de connectivitat d'algunes localitzacions, l'app ha de permetre treballar on i off line en tot moment, fent-se la sincronització de la informació quan torni a disposar de cobertura.

L'app permet interactuar amb els iBeacons situats en els diferents centres de treball, amb l'objectiu d'informar els treballadors i/o persones que hagin d'accedir o a l'apropar-se als recintes de les mesures de seguretat de les que cal disposar.

El sistema actual està desenvolupat amb Laravel i l'aplicació amb Java per a Android. Caldrà actualitzar l'aplicació segons sigui necessari i així ho requereixi pel sistema operatiu. També està disponible l'aplicació en iOS i per a Windows programada amb Xamarin.

Les funcionalitats de detecció d'iBeacons així com la introducció de noves localitzacions es gestionen amb el BackOffice web actual.

Així mateix, el sistema permet la recollida de dades per al seu ús estadístic i disposa d'un mecanisme automàtic per detectar possibles problemes de funcionament en l'aplicació.

El disseny i la navegabilitat de les apps segueix la imatge corporativa de l'empresa i s'ajusta a la navegabilitat de cada dispositiu i sistema operatiu.

3. DESCRIPCIÓ DE L'ENTORN ACTUAL

L'empresa adjudicatària haurà de donar el servei tant d'actualització d'aplicacions (dispositius mòbils i smartwatches) com de manteniment del sistema de backOffice i del servidor.

L'actual estructura està formada per:

- Framework de desenvolupament de backOffice i WebService basat en Laravel.
- Oauth2 per a validar usuaris a una API REST.
- Accés a dades mitjançant webService.
- Entorn de gestió basat en HTML5, Vue, Awesome, CSS3, Less & Sass, i plantilles blade amb totes les seves extensions.
- Api inside Main System per a realitzar peticions asíncrones.
- Sistema de passive and active module systems.
- Sistema de cues per a peticions.
- Sistema d'encriptació de dades.
- Integració amb Api de Google Charts.
- Sistema propi de control d'errors i logs.
- Apps desenvolupades amb Xamarin per a la versió Windows, Swift iOS i Java i Kotlin per Android.
- Funcionament tant on com Off Line.
- Tecnologia Bluetooth 5.0 Beacon - BLE iBeacon

Les característiques mínimes del servidor requerit hauran de ser les següents:

- Servidor dedicat amb els recursos necessaris que garanteixi el correcte funcionament per als actuals i futurs usuaris en tot moment.
- 4GB RAM
- 2 Vcpus

- 60 GB d'espai SSD
- Tràfic il·limitat
- Php 7.0 o superior
- Mysql 5.3 o superior
- Firewall WAF
- Còpies de seguretat diàries, setmanals i mensuals, tant al servidor com externes al núvol
- Monitorització de servei 24 h x 7 dies a la setmana

4. REQUERIMENTS FUNCIONALS

El Manteniment ha de garantir el correcte funcionament de tots els apartats descrits a continuació, tant per als dispositius mòbils (telèfons, tabletas i smartwatches) com de WebServices i BackOffice. Les següents apartats estan ja desenvolupats i implants, per tant s'ha de garantir el manteniment dels mateixos i les millores-adequacions que puguin sorgir sobre aquestes.

4.1 Gestió i creació de rols d'usuari (supervisor/operador) intercomunicació o incidències

Des de la part de gestió a l'entorn web backoffice, es poder crear diferents perfils d'usuari i departaments. En funció del rol d'aquests usuaris tindran uns privilegis diferents.

Des de un super administrador assigna codi d'usuaris i password a cada nou usuari el qual pot gestionar el seu password desde l'aplicació web.

Es poden crear departaments, i cada departament té un supervisor per tal d'agilitzar el procés. Es designa (configurable) un supervisor per defecte, que en el cas de no triar-ne un de diferent, s'assignarà aquest.

Un superadministrador (pot fer tot) pot crear tant supervisor com operador. Un supervisor pot crear operadors, i un operador només podrà fer les accions que tingui privilegis per a fer.

Tots els usuaris pertanyen a un o diversos departaments.

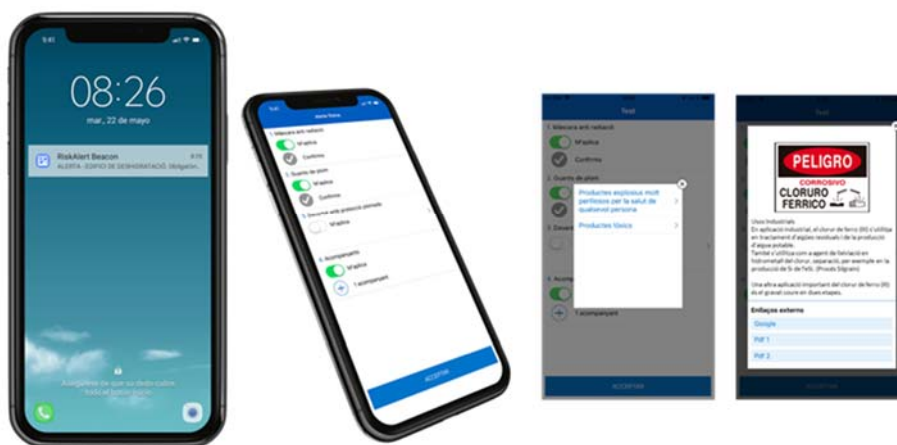
Un superadministrador, pot assignar incidències tant a operadors com a supervisors, i un supervisor pot assignar incidències a operadors.

Les normes i regles de configuració de l'aplicació descrites en el present poden ser modificades acord a les necessitats, a on forma part de l'objecte del present esmentades modificacions.

4.2 Mòdul notificació de riscos en instal·lacions (iBeacons)

l'APP permet interactuar amb els iBeacons situats en els diferents centres de treball, amb l'objectiu d'informar els treballadors i/o persones que hagin d'accedir, o en apropar-se als mateixos, de les mesures de seguretat de les que cal disposar.

Les funcionalitats de detecció d'iBeacons així com la introducció de noves localitzacions i riscos associats es poden gestionar des del BackOffice web actual mitjançant l'identificador MINOR i MAJOR. A on s'introdueixen totes les fitxes de seguretat, procediments de treball i indicacions requerides per a cada espai de treball.



4.3 Sistema de Xat

Es tracta d'un xat intern on es podran realitzar les següents operacions:

- Creació de grups d'usuaris amb els privilegis corresponents.
- Poder triar des de la part administradora, qui pot escriure o qui només pot llegir.
- Realitzar converses 1 to 1 (persona amb persona).
- Des del Back-Office es podrà tenir tot l'historial de converses realitzades per grups i usuaris.
- Es podran donar d'alta, crear grups i donar privilegis tant des de la part administradora com des de la mateixa App.

4.4 Mòdul d'incidències

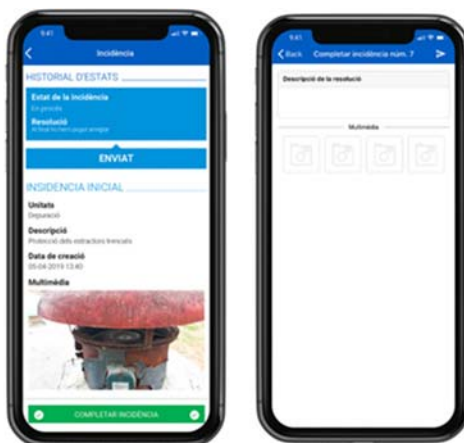
Amb aquesta funcionalitat, els empleats i tècnics que tenen a la seva mà la possibilitat de reportar qualsevol incidència que puguin trobar en el seu dia a dia. Donat que l'empresa disposa de múltiples instal·lacions en localitzacions diverses, és necessari disposar d'una eina que optimitzi i ajudi a poder realitzar un manteniment preventiu efectiu i amb la màxima agilitat possible.

Els usuaris tenen la possibilitat de categoritzar la incidència, geolocalitzar-la, realitzar fins a 4 fotografies i/o vídeos, i indicar una descripció. El sistema, en rebre la incidència, enviarà un correu a la persona encarregada. Segons la categoria de la incidència, es pot fer que es notifiqui al departament que li pertochi.

Les incidències s'emmagatzemen al backend d'administració de l'aplicació, podent canviar l'estat de la incidència i posar un comentari. Quan es canvia d'estat és notificar mitjançant notificació Push a l'operari que l'ha enviat del seu nou estat.

A l'apartat de backOffice, es poden realitzar cerques (data, categoria, estat de la incidència, etc.). També es pot visualitzar en format de llista i en format de mapa per a tindre una visió general d'on es localitzen les incidències.

En finalitzar la incidència, es podrà reportar fins a 4 imatges des del backend per tal d'informar de l'estat en què s'ha resolt la incidència.

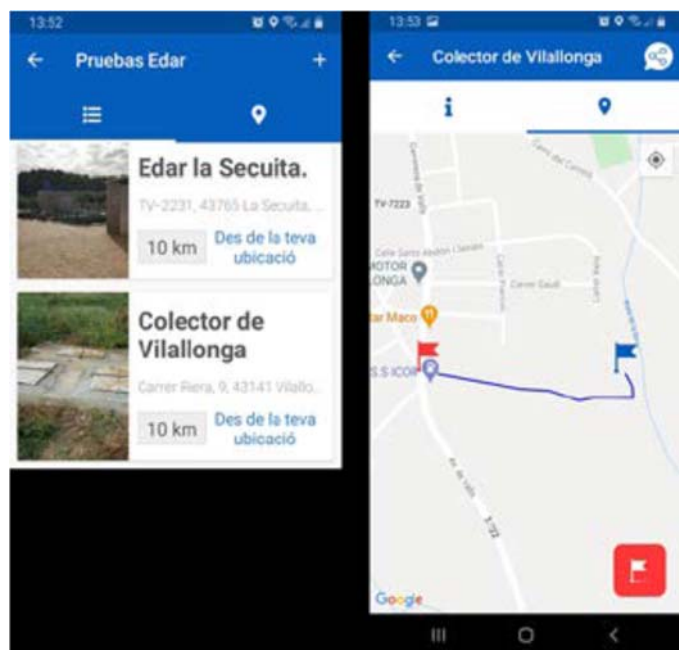


4.5 Mòdul d'ubicacions

Aquest mòdul permet determinar el camí d'accés per a una instal·lació de difícil localització.

En aquest apartat els administradors poden definir uns llocs categoritzats i geolocalitzats així com definir unes rutes pròpies més enllà del que Google Maps o altres eines de lliure difusió permeten.

Es poden afegir imatges del lloc, una petita descripció i un PDF adjunt que es visualitzarà al mòbil.



Les categories es poden gestionar des del backoffice.

4.6 Mòdul permisos de treball

En la realització d'activitats d'especial perillositat existeix un risc potencial de generació d'accidents greus. Per prevenir aquests accidents és necessari disposar de sistemes de treball segurs que incloguin permisos de treball per a la realització d'aquestes activitats. No es tracta simplement d'una autorització per dur a terme una activitat potencialment perillosa, sinó més aviat d'una part essencial del sistema de treball que determina com aquesta activitat ha de dur-se a terme de forma segura. L'autorització d'un permís de treball implica que s'han adoptat les mesures adequades per planificar l'execució d'una activitat i s'han tingut en compte els riscos associats a la mateixa. L'autorització pot referir-se a la realització d'un determinat tipus de treball (treball en alçades, treball en calent,...), i/o a l'accés a certes àrees o locals d'especial risc (espais confinats, ATEX,...) per a la realització de qualsevol tipus de treball.

Les tipologies de permisos de treball desenvolupades a l'app son les següents:

- Permís de treball en espais confinats i en alçades
- Permís de treball per a treballs en calent
- Permís de treball per a treballs en calent
- Permís de treball en bastides PEM i escales

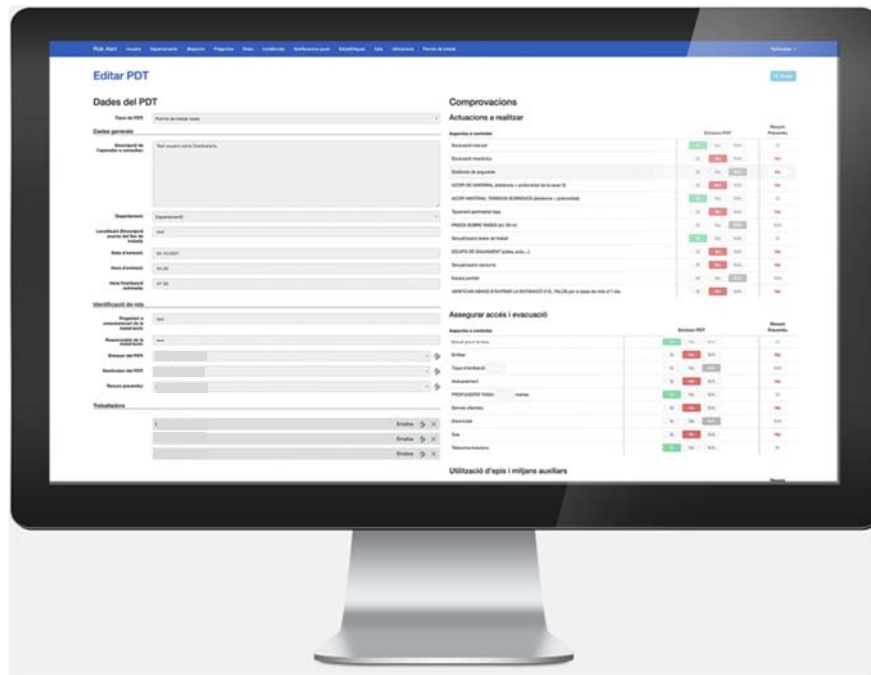
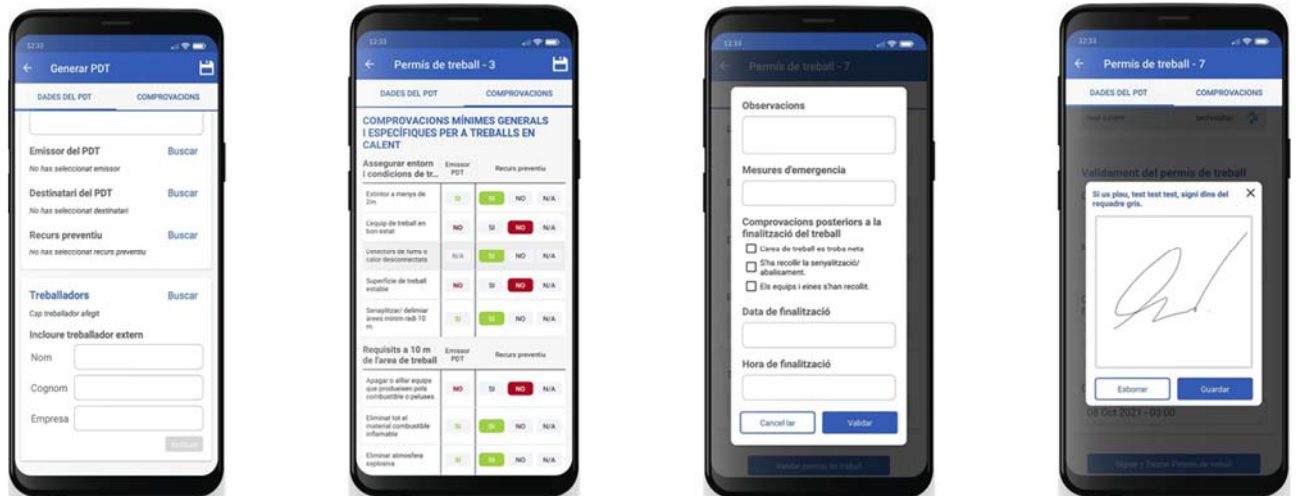
El present mòdul del sistema permet gestionar els permisos de treball per a tasques amb riscos específics. Aquests es poden crear tant de l'aplicatiu mòbil com des del backoffice web. Cada tipologia de permís de treball, té una sèrie de preguntes opcionals i obligatòries a contestar per cadascun dels participants de l'ordre de treball,

Un emissor, pot crear una nova ordre en el qual ha de triar el tipus i emplenar unes certes preguntes obligatòries, ha de definir qui és el destinatari, recurs preventiu i treballadors que formaran part. Des del backoffice ens permet guardar

una ordre de treball en esborrany. El recurs preventiu ha de respondre les preguntes obligatòries abans de poder tancar el comunicat mitjançant la seva signatura en el propi dispositiu mòbil la qual quedarà recollida digitalment. Els treballadors poden ser interns (d'Ematsa) o externs, on s'ha d'indicar les seves dades, empresa i si és recurs preventiu extern.

Tant d'emissor, destinatari, recurs preventiu i treballadors han de signar manualment al dispositiu mòbil conforme la seva part està revisada i correcta, d'aquesta manera es recullen digitalment totes les signatures dels diferents rols implicats per reflectir-les en el document de registre final, es a dir el permís de treball complimentat i tancat, exportable a Microsoft Word. Des de l'apartat de backoffice es pot generar el document final una vegada el comunicat ha estat finalitzat, així com veure les signatures de cadascun dels participants. Cada ordre de treball disposa d'un circuit de validació on, finalment, es tanca indicant una sèrie de dades o fins i tot, adjuntant imatges per a que quedi annexades a l'ordre de treball.

També hi ha el mòdul d'estadístiques on permet fer anàlisi de les dades de les ordres de treball i permet mostrar la quantitat d'hores per usuari i segons el perfil d'usuari (emissor, receptor, recurs preventiu i treballador) donat dues dates. També hi ha possibilitat de filtrar per tipus d'ordre de treball, persona, departament.



5. ALLOTJAMENT DE LA PLATAFORMA

Forma part de l'abast del contracte, la disposició i cost, els quals aniran a càrrec de l'adjudicatari, del servidor anual, segons les característiques anteriorment descrites, així com totes les llicències que calgui disposar per tal de garantir el correcte funcionament del projecte.

6. REQUERIMENTS TECNOLÒGICS

Les necessitats tecnològiques que requereix el manteniment de l'aplicatiu són:

6.1 Relació de tecnologies a utilitzar:

- Framework Laravel.
- PHP 7.x.
- API REST.
- JSON.
- Llenguatge SQL
- Css3, Html5, Vue.
- Ajax.
- GIT.
- Google Charts.
- JQuery .
- Laravel Eloquent.
- Microsoft Xamarin.
- Swift i Swift UI
- Java
- Kotlin
- Android Wear OS
- iBeacon (IPS indoor positioning system).
- Comunicació amb Bluetooth 5.0 BLE.

- OAuth2.

6.2 Descripció de l'entorn d'ús tecnològic:

L'entorn de desenvolupament ha de ser l'última versió del Framework Laravel.

El llenguatge de desenvolupament ha de ser PHP a l'última versió tant per a la part de gestió com per al Webservice, el protocol de comunicació entre les App's i el sistema és JSON, l'app d'iOs està desenvolupada amb Swift la de Windows amb Xamarin i la d'Android amb Java i Kotlin.

Les apps consumeixen serveis REST, que retornen una estructura de dades JSON, la qual, per velocitat, es guarda en cache tant a nivell de servidor com a nivell de base de dades dels dispositius.

La part de gestió està adaptada per a tot tipus de dispositius. s'han usat llenguatges tals com CSS4, HTML5, Bootstrap, Vue, etc.

Es requereix l'ús d'un software de control de versions (GIT) per al desenvolupament de les dues app's així com per l'entorn de gestió.

Per garantir la seguretat del sistema, aquest ha de complir els estàndards de seguretat necessaris (https, encriptació de dades amb SHA256), definits en l'apartat de seguretat.

L'arquitectura compleix els actuals estàndards de programació.

El sistema de gestió és compatible i es visualitza correctament amb els exploradors actuals més comuns, com Microsoft Edge, Mozilla Firefox, Chrome, Safari i Opera.

Les aplicacions són compatibles amb iOS 14 o superior i adaptada a pantalles així com Android 6 o superior.

El sistema incorpora un mecanisme de traçabilitat d'operacions (log) per a poder depurar qualsevol acció que realitzi la plataforma.

Ha de quedar inclòs al manteniment possibles adaptacions de la solució a noves versions dels entorns o de llenguatges de desenvolupament que puguin sorgir en la duració del contracte.

6.3 Requeriments mínims dels Ibeacons:

- Ibeacon bluetooth 5
- 300 m de radi
- Antena omnidireccional
- IP67
- Funcionament entre 1 Hz - 10 Hz
- Transmissió +4dBm als -30 dBm

7. MANTENIMENT

En aquest capítol es detallen les tasques comunes a realitzar en el manteniment de les apps, de la part de gestió i de l'apartat d'Ibeacons. Les accions que s'han de fer són:

- Fer test i reparar possibles errades de l'app abans que surtin noves versions de sistemes operatius (fer test a beta).
- Renovació i cost del certificat SSL per a la connexió xifrada amb el servidor.

- Renovació dels certificats PUSH.
- Adaptar les apps a noves pantalles o resolucions en el seu moment.
- Adaptar l'apartat de gestió per la seva correcta visualització a noves versions dels exploradors.
- Actualitzar el programari, tant d'apps com del sistema.
- Fer-se càrrec de les còpies de seguretat.
- Disponibilitat del servidor 24x7.
- Establir totes les mesures de seguretat necessàries per a garantir la seguretat de la informació i dels sistemes.
- Servidor sense límit de tràfic ni espai.
- Ajustos i canvis en el codi per a funcionalitats que hagin quedat en desús o hagin deixat de disposar de suport del proveïdor de les APIs. Això garanteix disposar sempre de les últimes funcionalitats i compatibilitat amb les últimes versions de sistema operatiu.
- Actualització de noves versions de llibreries o SDKs de tercers.
- Fer-se càrrec de qualsevol cost afegit (Google, Apple, Amazon, etc.).
- Actualització i extracció de dades per a estadístiques.
- Resolució d'incidències o consultes sobre ibeacons.
- Resoldre dubtes i consultes que pugui tenir Ematsa referent al funcionament del programari (backoffice o apps).
- Correccions, modificacions i adequacions dels serveis implantats acord a les necessitats que puguin sorgir com afegir o treure camps, adaptar les recerques i històrics, etc.

Totes les accions definides han de permetre el correcte i continuat funcionament dels serveis desenvolupats en l'aplicació així com petites millores i adequacions sobre les mateixes

8. INTERLOCUCIÓ AMB EMATSA

L'empresa adjudicatària ha de garantir que disposa del suficient personal tècnic i amb els coneixements necessaris per tal de poder donar solució a qualsevol incidència que hi pugui haver.

L'adjudicatari designarà una persona de la seva organització amb responsabilitat i capacitat de decisió sobre el servei. Aquesta persona serà la interlocutora amb els serveis tècnics i de comunicació d'Ematsa. Serà la responsable de la correcta organització dels treballs a realitzar i del compliment del contracte.

9. MITJANS HUMANS I MATERIALS

L'adjudicatari adscriurà al servei un equip tècnic mínim següent amb les corresponents experiències mínimes:

- Director/a de projectes: mínim 10 anys d'experiència
- Programador/desenvolupador/a mòbil: mínim 5 anys d'experiència
- Programador/desenvolupador/a web amb PHP / Laravel: mínim 5 anys d'experiència

La experiència vàlida serà tota aquella igual o similar a la naturalesa del contracte per tant, la relacionada amb el desenvolupament, implantació, i manteniment de programaris per a aplicacions en entorns, locals, web i/o mòbil

Caldrà aportar el CV del personal adscrit a la present contractació. L'adjudicatari haurà de garantir la continuïtat de l'equip de treball durant tot el termini de prestació del servei.

Qualsevol canvi en els integrants de l'equip que presti el servei de manteniment haurà de ser comunicat i autoritzat prèviament per Ematsa.

Durant el període de vacances o festius, l'adjudicatari coordinarà les absències de les persones del seu equip i aportarà les solucions adequades amb objecte de garantir el manteniment i la bona execució del manteniment de les aplicacions relacionades amb el contracte.

L'empresa adjudicatària haurà de disposar de tot el software i hardware necessari per a l'execució del servei de manteniment i en cap cas podrà demorar els terminis d'entrega de tasques parcials o totals degudes a manca de material o programari informàtic.

10. GARANTÍA, SERVEI DE SUPORT I DE MANTENIMENT

Tractant-se d'una aplicació necessària per a la vigilància, control i minimització dels riscos dels treballs, tant ordinaris com extraordinaris que implica la gestió i manteniment de les instal·lacions del servei. Es fa necessari la disponibilitat de resolució d'incidències de l'APP en el menor temps possible, a fi de poder registrar, gairebé a temps real, o inclòs poder verificar i controlar prèviament les mesures de seguretat associades a una tasca.

Per això es requereix un SLA mínim per tal de prestar el servei de manteniment de l'aplicatiu. Es pot requerir que el servei de manteniment calgui fer-ho in situ, per a donar suport o resoldre incidències presencials o en dispositius mòbils dels treballadors en un període de temps curt. Caldrà disposar d'un entorn de proves així com un altre de producció. El desplegament de l'aplicació mòbil als treballadors d'Ematsa es farà mitjançant l'MDM corporatiu.

Es classifiquen les incidències de la següent manera:

- Molt crítica: Quan els errors de software impedeixin el funcionament de la solució de manera que el servei quedi interromput.
- Crítica: Quan els errors impedeixin operar amb el servei de forma parcial.

- Mitja: Errors parcials del servei que limitin la funcionalitat o el rendiment.
- Lleu: Errors detectats que han de ser resolts, però que no impedeixen el funcionament de la solució.

Els temps de mínima resposta i de solució han de ser els següents:

- Molt crítica: Resposta en 4 hores. Resolució en 8 hores.
- Crítica: Resposta en 8 hores. Resolució en 16 hores.
- Mitja: Resposta en 24 hores. Resolució en 48 hores.
- Lleu: Resposta en 48 hores. Resolució en 72 hores.

11. SEGURETAT

Allotjament de la plataforma i seguretat de la informació

Es requereix un servei d'allotjament extern en un servidor dedicat administrat. El proveïdor haurà de comptar amb unes infraestructures que compleixin els requeriments de l'Esquema Nacional de Seguretat de nivell bàsic, tal com fixa el Real Decret 311/2022, de 3 de maig, pel que es regula el Esquema Nacional de Seguretat.

Al considerar-se la informació continguda en la base de dades que dona accés a la plataforma com a informació Restringida segons la RGPD al constar dades personals que permeten identificació dels interessats, l'adjudicatari haurà d'assumir l'acompliment de les següents mesures de seguretat en el servei prestat:

- Tallafores d'aplicació (WAF)
- Sistema d'identificació i autenticació d'usuaris
- Sistema de gestió de privilegis d'accés
- Límit d'intents reiterats d'accés no autoritzat
- Sistema de control d'accés al sistema d'informació
- Registre d'accessos al sistema d'informació (vgr. Log d'accessos)

- Certificat SSL a la pàgina web (protocol HTTPS)
- Procediment de gestió d'incidents i emergències
- Procediment de comunicació i notificació de forats de seguretat
- Contracte de confidencialitat (amb el proveïdor i amb totes les persones que puguin tenir accés a la informació)
- Control d'accés físic a les instal·lacions
- Aplicació de criteris i mètodes d'organització documental (classificació i ordenació)
- Control d'accés a la documentació (vgr. tancament amb clau, identificació biomètrica, tarjeta intel·ligent, codi personal d'accés, etc.)
- Formació del personal implicat en seguretat de la informació i continuïtat (inclòs RGPD)
- Identificació dels riscos i tractament per aquells no tolerables
- Establiment de comitè de crisi
- Sistema d'anàlisi i gestió de vulnerabilitats tècniques
- Sistema de protecció contra codi maliciós i descarregable (vgr antivirus)
- Política de gestió d'actius d'informació
- Inventari d'actius i actius d'informació
- Registre d'accés a la documentació
- Segregació de les xarxes. (Entorns DEV, PRE i PRO segregats. Només exposat l'entorn de Producció)
- Política de taules netes
- Normes d'ús de les impressores de documentació
- Destrucció segura i confidencial de documentació -- Ha de complir una de les dues opcions
 - Màquines destructores de documentació.
 - Contracte de serveis amb empresa externa de destrucció documental certificada.

- Document de política de protecció de dades personal (RGPD i Llei Orgànica 3/2018 de Protecció de dades personals i garanties de drets digitals)
- Funcions i obligacions dels usuaris i normes d'ús dels recursos TIC
- Mesures tècniques i organitzatives de pseudonimització
- Tallafocs (firewall)
- Servidor on resideix l'aplicació -- Ha de complir una de les següents opcions:
 - Servidor propi
 - Servidor virtual privat (VPS) (EEE / Nivel equivalent)
 - Servidor Cloud (EEE / Nivel equivalent)
 - Ubicació: Espai Econòmic Europeu
- Control d'accés físic a l'entrada del Centre de Procés de Dades (CPD) / Sala del servidor
- Sistema d'identificació, registre i gestió d'incidències.
- Sistema de gestió de còpies de seguretat i recuperació de dades
- Sistema d'alimentació ininterrompuda (SAI) / Grup electrògen
- Auditoria automàtica de la o les aplicacions web afectades.
- Auditoria de seguretat dels sistemes implicats en el proveïdor
- Auditoria de seguretat de les xarxes

Per part d'EMATSA i en el cas de que en l'aplicació hi hagi evolutius dins del període del contracte, EMATSA haurà de fer una auditoria de seguretat de l'aplicació abans de la implantació d'aquests evolutius.

12. GESTIÓ DE DADES DE CARACTER PERSONAL

En quant en aquest plataforma s'emmagatzemen dades personals que permeten identificació de l'interessat, tan de treballadors d'EMATSA com personal extern que presta serveis en les instal·lacions de EMATSA.

Les dades que podrà accedir son les que consten en la plataforma, i que son les que s'enumeren: dades identificatives de contacte professional, rol dels usuaris, lloc de feina o càrrec, signatura hològrafa, rol d'usuari en aquesta aplicació i dades d'informació respecte a requisits de cursos-aptituds des de la vessant de prevenció de riscos laborals i així com aquelles dades que es puguin incorporar per donar compliment a les obligacions d'EMATSA.

Per aquest motiu, l'empresa adjudicatària del servei haurà de donar compliment a la normativa de protecció de dades personal en quant accedirà a aquestes dades realitzant tractaments vers aquestes dades allotjades responsabilitat d' EMATSA.

Aquesta comunicació de dades implicarà que l'empresa ostentarà la condició d'encarregat de tractament. Per tant caldrà que signi el corresponent acord regulador de la seva condició d'encarregat de tractament on assumirà totes les obligacions i assumpció de la realització de les mesures organitzatives i tècniques necessàries per tal de garantir que la prestació dels serveis s'adeqüi a la normativa de protecció de dades. I degut a que EMATSA es tracta d'una empresa pública caldrà que s'acompanyi de la perceptiva declaració responsable de la ubicació dels servidors i d'on es prestarà els serveis, que haurà de ser en l'Espai Econòmic Europeu

Tarragona a la data de la signatura electrònica