PLEC DE PRESCRIPCIONS TÈCNIQUES

Serveis per a la migració a una nova plataforma de Prevenció de Riscos Laborals i Salut Laboral per a l'Hospital Clínic de Barcelona i subscripció al programari

Exp. 2024-143

Índex

1 ELEMENTS TÈCNICS DEL CONTRACTE ..... Error! No s'ha definit el marcador.
1.1 Objecte del contracte *3*
2 Requeriments ..... Error! No s'ha definit el marcador.
2.1 Requeriments de les llicencies ..... ***Error! No s'ha definit el marcador.***
2.2 Requeriments de manteniment *3*
2.3 Seguretat i confidencialitat *4*
2.3.1 Gestió i Seguretat de la identitat *4*
2.4 Seguretat *4*
2.4.1 Seguretat de les dades *4*
2.4.2 GDPR *4*
2.4.3 Encriptació End-to-End *5*
2.4.4 Backup de Bases de dades *5*
2.4.5 Auditories *5*
2.5 Idioma *5*
3 Estructura de la oferta tècnica **5**
3.1 Resum de gestió *5*
3.2 Descripció de la solució *6*
3.2.1 Gestió i Seguretat de la identitat *6*
3.2.2 Usuaris del programari *7*
3.2.3 Usuaris del programari (Azure AD) ..... ***Error! No s'ha definit el marcador.***
3.2.4 Seguretat de la xarxa *8*
3.2.5 Accessos privats *8*
3.2.6 Encriptació End-to-End *8*
3.2.7 Seguretat de les dades i GDPR *8*
3.2.8 Backup de Bases de dades *9*
3.2.9 GDPR *9*
3.2.10 Validadors de contrasenyes *9*
3.2.11 Custodia segura de claves, secrets i certificats *10*
3.2.12 Directives de Seguretat *10*
3.2.13 Monitorització de Seguretat *10*
3.3 Pla d'implantació *10*
3.3.1 Pla d'implantació general *10*
3.3.2 Cronograma d'implantació *10*
3.3.3 Servei de suport *11*
3.4 Documentació *11*
3.4.1 Documentació a lliurar durant el projecte *11*
3.4.2 Documentació a lliurar al final del projecte *11*
3.5 Formació *12*
3.6 Garantia *12*
3.7 SLA *13*
3.8 Confidencialitat *13*

1 CONTRACTE

1.1 Objecte del contracte

L'objecte del contracte és l'execució dels serveis per a la migració a una nova plataforma de Prevenció de Riscos Laborals i Salut Laboral per a l'Hospital Clínic de Barcelona i subscripció al programari.

L'objectiu d'aquest concurs és l'execució de serveis per a l'actualització del programari PREVEN a un aplicació en modalitat SAAS.

La contractació dels serveis que és liciten en aquest expedient, permetran realitzar els següents accions:

1. Migració de les dades de Preven CS
2. Enllaç de dades de treballadors amb RRHH (sistema origen)
3. Càrrega d'analítiques
4. Exàmens de Salud i aptituds
5. Antecedents
6. Investigació d'accidents i comunicacions COMTA
7. Gestió de formacions
8. Lliuraments d'EPI's
9. Avaluacions i gestió de riscos
10. Gestió de mesures

La Direcció per les Persones proposa licitar un contracte per cobrir aquestes necessitats.

1.2 Subscripció i Llicenciament

El llicenciament de l'eina haurà de ser un import fix anual, que no variarà al llarg del contracte independentment del número de persones treballadores.

2 Projecte

2.1 Introducció

El present plec de prescripcions tècniques té per objecte descriure els requisits funcionals i tècnics, per al correcte disseny, definició i implantació d'un sistema de Salut Laboral, que permeti facilitar, millorar i controlar tota la gestió de prevenció de riscos laborals.

És requisit indispensable per a l'Hospital Clínic que totes les tasques que es realitzin en l'àmbit de la configuració durant aquest projecte, siguin compatibles i reutilitzables en el futur desplegament de noves funcionalitats/mòduls de l'eina de Salut Laboral.

2.2 Requeriments de manteniment

Els Requeriments Generals que NECESSÀRIAMENT haurà de complir la solució desenvolupada.

I. Que EL PRESTADOR DE SERVEIS, ha de ser una empresa que s'hagi especialitzat en el desenvolupament, venda i manteniment de programari de Prevenció de Riscos i Salut Laboral, la principal funcionalitat del qual consisteix en el control de la Prevenció i la Salut a les empreses.

II. Que Clínic Barcelona necessita per a la seva eficient organització empresarial del programari de Prevenció de Riscos i Salut Laboral, així com l'assistència tècnica i el manteniment del mateix.

III. Que Clínic Barcelona, està interessat en la contractació d un servei de programari, per al desenvolupament de determinades funcions en el marc de la seva activitat empresarial.

IV. Que EL PRESTADOR DE SERVEIS ha de ser una entitat que es dediqui, entre altres activitats, a la provisió i la llicència de programari especialitzat en el sector sanitari mitjançant el procediment Programari de Servei, des d'un centre de processament de dades (Data Center).

2.3 Seguretat i confidencialitat

El programari per la Gestió de riscos laborals i vigilància de la Salut desenvolupada peel proveïdor ha de ser una solució accessible de manera segura des de qualsevol navegador (versió posterior a progr) a través d'HTTPS.

2.3.1 Gestió i Seguretat de la identitat

La gestió d'usuaris s'haurà de realitzar seguint l'esquema de seguretat que proporciona l'Hospital Clínic de Barcelona i que es regeix per les normes de l'esquema nacional de seguretat. En aquest sentit s'hauran de complir els següents punts:

Usuaris

La gestió dels usuaris es realitzarà mitjançant la federació amb el directori actiu d'Azure del Clínic Barcelona, tenint en compte les següents tipologies d'usuaris:

- Usuaris administradors – Aquells que configuraran la plataforma i el seu funcionament essencial.
- Usuaris – Departament de Salut Laboral: Podran accedir als expedients de la plataforma així com podran realitzar les configuracions bàsiques de funcionament de la plataforma.
- Usuaris – Professionals del Clínic Barcelona: Podran accedir exclusivament a les dades referents al seu expedient.

2.4 Seguretat

En generà els requisits que s'hauran de complir referents a la seguretat de la plataforma en quan a comunicació, emmagatzematge de dades i gestió d'accessos queden recollits en el següent document de requisits de seguretat del Clínic Barcelona d'obligat compliment:

[CA]Requisits Generals Seguretat (

A mode resum del document caldrà complir els següents criteris.

2.4.1 Seguretat de les dades

- Complir les guies del CCN-STIC (Centre Criptològic Nacional)
- Realitzar auditories de proves de penetració.
- Ser transparent en quant a facilitar informació relativa al servei i infraestructures prestada
- Utilitzar xifratge de dades i gestionar les claus d'acord amb les guies del CCN-STIC
- Facilitar una avaluació d'impacte associada al servei que es presta

2.4.2 GDPR

Tota la infraestructura i dades han d'estar desplegats a la regió d'Europa i a través de directives de la plataforma, caldrà que s'impedeix que cap recurs o servei passi a fora d'Europa.

La plataforma ha de mantenir un registre històric d'activitats i transaccions en la base de dades i ha de permetre comprovar quines operacions ha realitzat cada usuari.

D'altra banda, cal disposar disposar d'un procediment d'esborrat de dades totals en el cas que així es sol·liciti.

Els accessos a les dades han d'estar controlats a través d'un sistema de rols d'usuari d'aplicació que restringint i delimitin el tipus de dades que pot consultar cada tipus d'usuari.

2.4.3 Encriptació End-to-End

Totes les comunicacions estan encriptades End-to-End a través de SSLv3/TLS 1.2-1.3, des del navegador fins a les bases de dades en qualsevol tram de comunicació inclòs el tram des del portal de l'empleat al servidor web.

El certificat ha d'usar en les comunicacions SSL des del navegador al WAF i des del WAF als servidors web que es renoven cada 3 mesos.

En el cas del certificat SSL, el servidor web genera el certificat mitjançant let's Encrypt sobre el corresponent nom DNS.

Com el certificat s'autogenera cada vegada que es desplega, cap administrador de l'equip tècnic de l'aplicació ha de tenir les claus d'aquests certificats per a garantir la seguretat al màxim.

2.4.4 Backup de Bases de dades

Caldrà tenir definida una política de còpia o Backup de base de dades de manera encriptada.

Es realitza una còpia de seguretat de la base de dades diariàriament, amb un període de retenció d'entre 7 dies i fins a 35 dies. Aquestes còpies hauran d'estar encriptades usant FIPS 140-2 (Xifratge AES de 256 BITS amb les claus gestionades directament per Microsoft).

2.4.5 Auditories

El proveïdor del programari ha de permetre realitzar per part del Clínic Barcelona totes les auditories necessàries de seguretat.

2.5 Idioma

Els idiomes en els que haurà d'estar disponible el programari per l'usuari seran:

- Català
- Castellà
- Anglès

3 Estructura de la oferta tècnica

En aquest capítol es detalla l'estructura que haurà de seguir la proposta tècnica que presenti la licitadora. En tot moment, l'empresa licitadora podrà aportar Annexes amb tota aquella informació que consideri d'interès, i que no hagi estat sol·licitada explícitament.

3.1 Resum de gestió

A continuació es fa un resum general del que es requereix com a exposició inicial de la licitadora en la seva oferta, i que sónels següents punts clau:

Els punts Claus per garantir l'èxit de la migració de dades i la correcta implantació de l'aplicació es defineixen en:

1. Configuració i parametrització migrant les configuracions actuals de Preven CS que siguin compatibles.
2. Migració de dades dels entorn de QUALITAT i PRODUCCIÓ des de l'antiga plataforma de Preven CS.
3. Formació dels diferents usuaris del departament de Prevenció i dels diferents mòduls que componen el programari i el seu funcionament.
4. Entrega dels materials de formació i manuals necessaris per al funcionament del programari.

5. Posada en marxa del servei a producció (o entorn real) i posterior suport post posada a producció (garantia).
6. Seguiment i control. Incloent la gestió d'incidències, correctius i possibles evolutius.

3.2 Descripció de la solució

A continuació es detalla la Solució Tècnica que l'empresa proveïdora implementarà per donar resposta als requeriments plantejats en aquest plec.

L'aplicació serà una plataforma associada a SaaS de Gestió de riscos laborals i vigilància de la Salut; sent una solució accessible de manera segura des de qualsevol navegador (versió posterior a 2020) a través d'HTTPS i estant desplegada sobre Microsoft Azure (regió Oest d'Europa). El desenvolapament ha d'estar realitzat mittjançant Python i Django.

L'aplicació tindrà dues parts principals, la part general on accedeixen els usuaris del departament de Salut Laboral, i un mòdul de Portal de Prevenció que permeti als professionals interactuar amb la plataforma per consultar les dades i participar de la prevenció.

Les dades de l'aplicació hauran d'estar desplegades en dues bases de dades:

Azure Database for PostgreSQL en modalitat de Servidor Flexible, un servei de base de dades relacional basada en el motor de base de dades de Postgres. És un servei totalment gestionat per Microsoft (base de dades com servei) que realitza un backup diari de les dades en una finestra de 7 dies. La versió actual de Postgresql es la 15.4.

Mongo DB, emmagatzema dades històriques (logging y auditoria) i altres dades de configuració (dades no sensibles). S'utilitzarà una màquina virtual con Mongo, un servei de base de dades NoSQL i es realitzaran còpies de seguretat diàries amb una finestra de 7 dies. La connexió a la base de dades Mongo es realitzarà mitjançant l'usuari ADMIN i un Password especificat en les variables de entorn del propi servidor en Azure. La connexió requerirà mode SSL.

Serà una solució accessible de forma segura des de qualsevol navegador (versió posterior a 2020, que son els tipus de navegadors que podem trobar dins el Clínic de Barcelona) a través de HTTPS i està desplegada en Microsoft Azure (regió Oest de Europa).

A nivell funcional, es requerirà la gestió dels àmbits de:

- Vigilància de la Salut: reconeixements mèdics; gestió assistencial; agenda, campanyes i citacions)
- Gestió de les Formacions (cursos, informes, treballadors pendents de formació...)
- Gestió per a la Coordinació activitats empresarials (CAE)
- Gestió dels accidents i incidents (notificació, comunicació de riscs, ,investigació...)
- Filiacions (eina per la traçabilitat dels professionals –noves incorporacions, llistats de professionals,...-)
- Memòria activitat, auditories, inspeccions, planificacions d'activitats
- Assistencial (receptes, vacunes, informes, estudis de salut, ...)
- Generació de informes, estadístiques, explotació de dades de professionals...
- Gestió de professionals especialment sensibles (T.E.S)
- Avaluació i gestió dels riscos laborals: fitxes informatives, mesures correctores, informes de riscos
- Agents: generació de fitxes de característiques i propietats dels d'agents físics, químics i biològics. Riscos associats, EPI's.
- Gestió i lliurament d'Equips de Protecció Individual: Inventaris d'EPI's, fitxes dels EPI's, Gestió de lliuraments d'EPI's, alertes de caducitats i lliuraments.
- Alertes (vacunes, baixes obertes, caducitat epi's...)
- Manteniment (usuaris, paraules clau, parametritzacions,...)
- Gestió del Pla de prevenció, planificació, memòria
- Gestió del pla d'emergència, definició dels Equips d'emergència.

3.2.1 Gestió i Seguretat de la identitat

<u>Usuaris Administradors</u>

La identitat és el nou perímetre de seguretat. Actualment, la majoria d'atacs tenen èxit al comprometre's la identitat d'accés. Per l'aplicació, es seguiran les recomanacions principals propostes per Microsoft per a gestionar i securitzar la identitat dels usuaris (basat en Azure Activi Directory) que s'utilitzarà per administrar i operar la plataforma de l'aplicació en Azure.

Concretament, les mesures principals que s'adoptaran per a securizar la identitat són les següents:

1. Servei de Protecció d'Identitat

Per a detectar i remeiar atacs a la identitat dels usuaris administradors de l'aplicació en Azure, s'usa el Servei de Protecció d'Identitat de Microsoft Azure. Aquest servei permet automatitzar la detecció i remediació de riscos basats en identitat, investigar aquests riscos i exportar aquestes dades a un SIEM.

Els riscos detectats entre altres són ús d'adreces d'IP anònimes, ubicacions d'origen sospitoses, propietats d'inici de sessió no usuals, etc. D'aquesta manera es detecta el nivell de risc d'inici de sessió.

2. Servei d'Azure AD Password Protection

Està implementat el servei d'Azure AD Password Protection que permet detectar i bloquejar contrasenyes considerades dèbils.

3. Multifactor Authentication i Accés condicional

Tots els usuaris administradors de l'aplicació en Azure, requereixen d'una identificació multifactor que, a més comprova una sèrie de condicions per mitigar potencials atacs (ubicació i nivell de risc d'inici de sessió detectant a través del Servei de protecció d'identitat).

4. Privilegis mínims

Per defecte, els usuaris administradors de la plataforma de l'aplicació en Azure, només tenen permís de lectura i estan organitzats per grups de rols (desenvolupament i producció) en Azure.

5. Servei d'Azure AD Privileged Identity Management

Està implementat el servei d'Azure AD Privileged Identity Management de manera que davant la necessitat d'administrar o realitzar qualsevol operació en Azure que necessiti permisos, l'usuari corresponent sol·licita el nivell d'accés que precisa de manera temporal i es rebutja a les 4 hores. Així, es redueix l'exposició a possibles atacs d'identitat.

Usuaris del programari

Els usuaris de l'aplicació estan organitzats per rols (treballador/pacient com a administrador i personal sanitari) i s'autentiquen a través d'usuari i contrasenya. L'inici de sessió pot protegir-se amb diversos mecanismes (validadores) configurables pel Clínic Barcelona.

L'accés a la informació està securitzada en tres nivells en funció del rol corresponent: a nivell de taula, a nivell de camps i a nivell de registre. D'aquesta manera es pot controlar d'una forma més granular l'accés a les dades sensibles.

Si el Clínic Barcelona el requereix, l'autenticació d'usuaris pot realitzar-se a la plataforma Azure AD mitjançant Oauth.

Single sign on (AZURE AD)

Per configurar el programari de l'aplicació, a mode que s'identifiqui com usuari de l'Azure AD del Clínic Barcelona, necessitem per la seva part, seguir els passos i proporcionar-nos la informació següent:

- Crear un registre del programari en Azure Active Directory
- Configurar el Redirect URI per redirigir a l'usuari una vegada autentificat.

El redirect URL es definirà segons estableixi la URL del domini pertinent.

Proporcionar els següents identificadors que s'obtenen del registre del programari:

- CLIENT_ID

- CLIENT_SECRET (VALUE)
- TENANT_ID

Pot establir-se el MFA sense que afecti al procés d'identificació del programari, ja que el sistema redirigeix automàticament a la pantalla de Login d'Azure del Clínic Barcelona.

3.2.2 Seguretat de la xarxa

Topologia Hub and Spoke

La topologia de xarxa utilitzada per l 'aplicació Azure és la d'Hub&Spoke recomanada per Microsoft. En aquest tipus d'arquitectura el Hub actua de punt central de comunicacions i allotja serveis de comunicació i seguretat comuns com Web Application Firewall, Azure Bastion o la màquina de salt (es detalla en les següents seccions). La plataforma està aïllada en la seva pròpia xarxa virtual (spoke) de manera que augmenta el nivell de seguretat font atacs. Existirà un spoke (xarxa virtual independent i aïllada) per cada entorn (desenvolupament, Pre-producció u producció). Les subxarxes dins de la xarxa virtual, està securitzada mitjançant grups de seguretat de xarxa, tal i com recomana Microsoft.

3.2.3 Accessos privats

Tots els serveis tenen punts d'accés privats i només són accessibles des del backbone d'Azure i la xarxa virtual privada corresponent. Tots aquests accessos privats estan securitzats mitjançant grups de xarxa (regles de filtrat nivell 4 de OSI).

Azure Bastion: Accessos administratiu i despagaments

L'accés a les màquines virtuals i del Portal de Prevenció tant per a administrar-les com per als corresponents desplegaments de codi es realitza mitjançant el servei de Azure Bastion, un servei totalment administrat per Microsoft que proporciona un accés segur a través del protocol SSH evitant l'exposició a través d'adreces IP públiques. Per a accedir i administrar els serveis de PostgreSQL i altres serveis PAAS, s'utilitza addicionalment una màquina de salt Ubuntu a la qual s'accedeix a través de Azure Bastion i en la qual estan instal·lades les corresponents eines. D'aquesta manera s'evita exposar cap servei amb direccions de xarxa públiques (principal vector d'atac).

Web Application Firewall i Application Gateway

L'Azure Application Gateway és un balancejador de trànsit web que permet gestionar i enrutar el trànsit a aplicacions web (operen en capa 4 de OSI)
Azure Web Application Gateway és un servei natiu d'Azure que permet protegir les aplicacions web enfront d'atacs comuns com a injecció de codi SQL, scripts entre llocs, etc.

En el hub de l'aplicació estan desplegats tots dos serveis per a protegir tant el servidor web principal de l'aplicació com el portal de l'empleat.
L'única adreça IP pública en la plataforma és la del Web Application Firewall i la del servei de Azure Bastion.

3.2.4 Encriptació End-to-End

Totes les comunicacions estan encriptades End-to-End a través de SSLv3/TLS 1.2-1.3, des del navegador fins a les bases de dades en qualsevol tram de comunicació inclòs el tram des del portal de l'empleat al servidor web de l'aplicació. El certificat usat en les comunicacions SSL des del navegador al WAF i des del WAF als servidors web es renoven cada 3 mesos.

En el cas del certificat SSL, el servidor web genera el certificat mitjançant let's Encrypt sobre el corresponent nom DNS. Com el certificat s'autogenera cada vegada que es desplega, cap administrador de l'equip tècnic té les claus d'aquests certificats per a garantir la seguretat al màxim.

3.2.5 Seguretat de les dades i GDPR

Encriptació de dades en repòs
Les dades en les bases de dades de PostgreSQL estan encriptats a dos nivells. De base usen l'encriptació de disc per defecte (FIPS 140-2, xifratge AES de 256 bits amb les claus gestionades directament per Microsoft) que té el servei de Azure Database for PostgreSQL (dades, còpies de seguretat i fitxers temporals). Addicionalment, s'encripten les dades sensibles a través de pgcrypto. En Redis Cache no es guardaran dades sensibles només referències a aquests. Per a accelerar la càrrega dels treballadors i que l'experiència de l'usuari sigui més còmode existeix un sistema d'emmagatzematge de referències mitjançant hash que impedeix la identificació directa entre treballador i les seves dades sensibles.

3.2.6 Backup de Bases de dades

Es realitza una còpia de seguretat de la base de dades de PostgreSQL diari amb un període de retenció de 7 dies que podria arribar a configurar-se fins a 35 dies a petició del Clínic Barcelona.

Es realitza una còpia de seguretat diària de la base de dades de Mongo amb un període de retenció de 7 dies.

Les còpies de seguretat estan encriptades usant FIPS 140-2 (Xifratge AES de 256 BITS amb les claus gestionades directament per Microsoft).

La solució ha de disposar d'un procediment paral·lel de còpies de seguretat segur de PostgreSQL en una plataforma descentralitzada de les pròpies BB.DD. de manera que es garanteix la integritat davant un possible atac de Ransomware o xifratge malintencionat d'aquestes còpies de seguretat. Aquest consisteix en aprovisionar una màquina virtual amb l'eina pg_dump i automatitzar en els horaris que es designin les còpies de seguretat de les diferents BBDD.

3.2.7 GDPR

Tota la infraestructura i dades estan desplegats a la regió d'Oest d'Europa, i a través de directives d'Azure s'impedeix que cap recurs o servei es desplegui fora d'Europa.

La plataforma manté un registre històric d'activitats i transaccions realitzades que està emmagatzemada en una base de dades Mongo en una màquina virtual d'Azure, dins de la mateixa xarxa privada virtual, i que permet comprovar quines operacions ha realitzat cada usuari.

D'altra banda, es la solució ha de disposar d'un procediment d'esborrament de dades totals en el cas que el sol·liciti el Hospital Clínic de Barcelona.

Finalment, els accessos a les dades estan controlats a través d'un sistema de rols d'usuari d'aplicació que restringeixen i delimiten el tipus de dades que pot consultar cada tipus d'usuari.

3.2.8 Validadors de contrasenyes

A més dels estàndards de Django, les validacions de contrasenya que incorpora l'aplicació, són:

- La contrasenya ha d'estar formada com a mínim per un número, un caràcter especial i una lletra majúscula.
- No es pot repetir l'anterior contrasenya.
- Llista de paraules prohibides, sent configurables pel Clínic Barcelona.
- No poder-se repetir contrasenya en els últims X dies, sent aquest dies configurables pel Clínic Barcelona.

Camps encriptats

El disc físic que allotja la base de dades, està encriptat, a més tenim encriptats via PGP, els següents camps de la :

- Taula consulta, contrasenya de l'informe.
- Taula dades personals (para treballadors): nom, cognoms, nacionalitat, telèfon, DNI, tipo de documento, data de naixement.
- Taula de dades de contacte (per tots els usos que puguin donar-se): carrer, número, codi postal.

3.2.9 Custodia segura de claus, secrets i certificats

Totes les claus, secrets i certificats estan allotjats en un servei de custòdia segura proporcionat per Microsoft, Azure Key Vault. Aquest servei usa mòduls maquinari de seguretat FIPS 140-2 (nivell 2 i 3) i impedeix que les aplicacions i usuaris tinguin un accés directe a les claus i secrets.

3.2.10 Directives de Seguretat

Per a assegurar la consistència i persistència de les mesures de seguretat preses, s'han fet ús de les directives de Azure per a forçar totes les recomanacions de seguretat corresponents.

3.2.11 Monitorització de Seguretat

L'estratègia de monitoratge de seguretat (detecció i remediació d'amenaces) de l'aplicació estarà basat en Microsoft Defensar for Cloud. Aquesta plataforma de Microsoft permet protegir les càrregues de treball desplegades en Azure. És una eina que comprova i verifica la postura de seguretat per a detectar vulnerabilitats, suggereix recomanacions per a reforçar la seguretat i detecta i resol amenaces sobre els recursos i serveis corresponents.

3.3 Pla d'implantació

En aquest punt es detallarà les tasques que s'inclouen i qui les ha de realitzar: proveïdora i/o Clínic Barcelona.

L'empresa licitadora haurà de presentar en la seva oferta un calendari detallat de tasques i terminis d'execució previstos.

La proveïdora afrontarà el projecte de migració i implementació de l'aplicació a Clínic de Barcelona en les següents fites:

1. Configuració i parametrització del nou programari
2. Migració de dades actuals al nou programari
3. Formació al personal
4. Posada en funcionament del programari a l'entorn de producció i suport post producció
5. Seguiment i control

Per la seva banda, el Clínic Barcelona posarà a disposició del proveïdor les dades referents a recursos humans des del Sistema actual (SAP) mitjançant la crida a serveis web del programari.

A fi d'ajustar l'eina i carrega de l'aplicació amb les dades provinents del sistema de Recursos Humans del clínic Barcelona, es facilitarà l'accés als entorns de proves pertinents per tal de poder realitzar la integració de dades.

3.3.1 Pla d'implantació general

Per a començar la implantació de l'aplicació en el Clínic Barcelona es proposarà una reunió d'inici de projecte anomenada KickOff on es presentarà el projecte, es fixaran els principals rols de gestió i s'establiran les primeres dates d'implantació, amb l'objectiu de donar per iniciat el projecte i les següents accions.

3.3.2 Cronograma d'implantació

La licitadora haurà de presentar en la seva oferta un calendari detallat de tasques i terminis d'execució previstos.

Dintre d'aquesta planificació, la licitadora haurà d'especificar la durada prevista per a la realització de cada fase, i la posada en productiu.

S'espera que inicialment la durada total del projecte de migració sigui d'aproximadament de 3 mesos.

Activtiats i fites	M1	M2	M3	M4 i posteriors
Inici del projecte				
Kick Off				
Consultoria inicial - Fase d'analisis				
Integracións				
Sessions amb usuaris i tecnics				
Fase de desenvolupament				
Desenvolumanet de moduls i integracions				
Configuració de taules mestres				
Migració de dades				
Pla de formació				
Formació Key Users				
Formació Usuaris de perfil sanitari				
Formació Usuaris técnics				
Suport posada en Productiu				
Servei de suport				

3.3.3 Servei de suport

- Horari: de dilluns a divendres de 9h a 18h
- Modalitat: telèfon, correu electrònic i presencial en cas necessari
- Perfils: han de ser els perfils que hagin tingut participació directa en el projecte

3.4 Documentació

En la documentació a elaborar durant el projecte, es diferenciarà la realitzada durant el mateix desenvolupament del projecte i la lliurada en finalitzar aquest.

El Clínic Barcelona facilitarà plantilles que l'empresa licitadora haurà de seguir per tot entregable, podent afegir el seu logotip a la part de la capçalera, cantó esquerre, i podent modificar el peu de pàgina, part esquerra, on s'indica "qui" genera el document.

Tota documentació haurà de ser en català.

3.4.1 Documentació a lliurar durant el projecte

- Pla de Projecte: inclourà un calendari detallat de projecte, el pla de qualitat, el pla de riscos, el pla de contingència, pla de comunicació, pla de formació i aquells documents que el Clínic Barcelona consideri adients a l'inici del projecte.
- Actes: documents resum de totes les reunions de pressa de requeriments o de qualsevol altre tipus de reunió.
- Informe de Seguiment: inclourà tota la informació de l'avanç del projecte, així com tots els aspectes rellevants que calgui destacar.
- Disseny Funcional i Tècnic: especificarà la solució a implementar i els desenvolupaments necessaris tant des del punt de vista funcional com tècnic. En aquest punt s'hauran d'entregar tots els documents actualitzats referents a les passarel·les de dades entre els sistema de Recursos Humans i l aplicació.
- Prototip: inclourà a escala visual, com quedarà la solució final que es lliurarà.
- Document de Proves: inclourà totes les proves i evidencies realitzades, per garantir que totes les funcionalitats han estat testejades, i el resultat en les proves ha estat satisfactori.

3.4.2 Documentació a lliurar al final del projecte

- Documentació Projecte: document que haurà d'incloure, detalladament, totes les modificacions i parametritzacions dutes a terme, així com els programes font empleats. Aquest document ha de permetre que tant el Clínic Barcelona com qualsevol altra empresa, vegi quina és la solució final, i com s'ha arribat a ella pas per pas i de totes les funcionalitats implementades.

- Manual Usuari: document que descriu l'accés a l'aplicació, les pantalles, els camps dins d'aquestes, i com l'usuari hi pot interactuar, per conèixer pas a pas, quines són les accions que es poden fer i com s'han de dur a terme de totes les funcionalitats implementades.
- Manual Administrador: document que descriu la informació d'ús i manteniment de la solució proposada pel personal encarregat d'administrar i mantenir la solució per part del Clínic Barcelona de totes les funcionalitats implementades.
- Mapa Global d'Interdependències: document que contingui el mapa global d'interdependències entre aplicacions i processos funcionals.
- Diccionari de dades mestres: document on s'enumeren els diferents camps de sistema d'informació amb el seu descriptiu, significat, característiques, format i valors possibles. Per exemple: camp data de naixement, la data en que va néixer el professional, format DD/MM/AAAA, on DD=dia, MM=mes, AAAA=any, els valors que compren D són 1 a 31, M 1 a 12 i any 1900 a 9999.
- Vídeos tutorials: per a l'usuari final.

3.5 Formació

L'empresa adjudicatària, en coordinació amb Clínic Barcelona, precisarà la durada i contingut de les formacions necessàries per a una correcta explotació i manteniment de la solució proposada. En concret caldrà la formació dels mòduls de PRL i VS.

La formació s'efectuarà utilitzant com a suport la documentació tècnica i els manuals d'usuaris lliurats i aprovats per Clínic Barcelona.

La formació no es donarà per finalitzada fins que Clínic Barcelona validi que els professionals corresponents han obtingut els coneixements necessaris per dur a terme les tasques i activitats definides en el pla de formació. L'empresa adjudicatària haurà de fer tantes formacions com sigui necessari fins a obtenir l'aprovació de Clínic Barcelona.

L'empresa adjudicatària, haurà de formar als usuaris de Clínic Barcelona en la ubicació i data prèviament establerta, tenint en compte que no s'incorrerà en cap cost addicional per l'execució i desplaçaments d'aquestes formacions.

L'idioma de totes les formacions haurà de ser en català o castellà.

3.6 Garantia

L'empresa adjudicatària haurà de garantir el correcte funcionament dels sistemes i programari subministrat durant el període d'oferiment del servei.

L'empresa adjudicatària haurà de corregir els errors detectats pel Clínic Barcelona durant el termini de garantia (12 mesos posteriors a la posada en producció i aprovació per part del Hospital Clínic de Barcelona, de la finalització de la implantació) realitzant les modificacions i configuracions necessàries per garantir el correcte funcionament de la solució.

El dia de la posada en productiu de la solució informàtica, i un cop Clínic Barcelona, hagi validat i aprovat el correcte funcionament del sistema, es firmarà un document de recepció provisional, que indicarà el començament del període de garantia contractual. En aquest punt s'activarà el contracte de manteniment del programari dins el contracte de llicencies.

La recepció definitiva es realitzarà un cop finalitzi el període de garantia contractual, de manera que Clínic Barcelona es compromet a no realitzar cap modificació dels desenvolupaments objectes del plec, sense previ acord amb l'empresa adjudicatària.

Durant el període de garantia, el proveïdor assumirà els costos derivats de les incidències del programari. Aquesta garantia tindrà una durada igual al període de vigència de les llicències.

3.7 Manteniment

S'inclou, dins del cost de les llicencies, el manteniment del programari de l'aplicació per part del proveïdor allargant el suport a les incidències del programari a la durada de la llicencia d'explotació del programari. El cost associat a la resolució d'aquestes incidències no es repercutirà al Clínic Barcelona.

3.8 SLA

Els temps de resposta durant el període de Suport posada en Productiu i Garantia han de ser els següents:

- Prioritat Urgent
  - Resposta → abans de 2h
  - Solució → abans de 8h
- Prioritat No Urgent
  - Resposta → abans de 8h
  - Solució → abans de 16h

3.9 Confidencialitat

La informació obtinguda a conseqüència de la prestació dels serveis objecte d'aquest contracte té caràcter confidencial i l'empresa adjudicatària ha de mantenir en tot moment el secret professional.

L'adjudicatària serà responsable de qualsevol violació del deure de secret que es pugui produir per part del personal a càrrec seu. Per evitar-ho, s'obliga a aplicar sobre el personal vinculat al projecte les mesures que siguin necessàries per a garantir el compliment dels principis de mínim privilegi i necessitat de conèixer.

Un cop finalitzat el contracte, l'adjudicatària es compromet a destruir o retornar la totalitat de la informació facilitada per l'administració, així com qualsevol altre producte resultant de l'execució del present contracte.

En el cas que l'adjudicatària, a conseqüència de l'execució del present contracte tingui accés a dades de caràcter personal de Clínic Barcelona, ostentarà la posició de sub-encarregat/encarregat de tractament envers aquestes dades de conformitat amb la llei orgànica 3/2018 (RGPD). En conseqüència l'adjudicatària es compromet a utilitzar les dades única i exclusivament amb les finalitats i obligacions establertes en aquest contracte, a tractar les dades d'acord amb les instruccions de Clínic Barcelona, i a no aplicar-les ni utilitzar-les amb una finalitat diferent de la d'aquest contracte, ni comunicar-les ni cedir-les, ni tan sols per a la seva conservació, a qualsevol tercer aliè al contracte.

L'adjudicatària vetllarà per tal que les persones que tinguin accés a dades de caràcter personal siguin les estrictament imprescindibles per a la correcta execució de les tasques derivades del contracte. Totes aquestes persones hauran de ser advertides de la naturalesa confidencial i reservada de les dades i del deure de secret al qual estan sotmeses, essent l'adjudicatària el responsable del compliment d'aquestes obligacions per part del seu personal i de les conseqüències d'una eventual violació d'aquestes.

L'adjudicatària haurà de comunicar a Clínic Barcelona quins treballs seran objecte de subcontractació i quines seran les empreses que els realitzaran. Amb el permís exprés de Clínic Barcelona i actuant en nom i representació d'aquest, l'adjudicatària formalitzarà els corresponents contractes amb les empreses subcontractades que, als efectes de l'aplicació de la normativa en matèria de protecció de dades, tindran la consideració d'encarregats del tractament. Aquests contractes s'afegiran com annex al contracte administratiu que formalitza aquesta adjudicació.

Davant qualsevol incompliment d'aquesta clàusula, l'adjudicatària serà considerada responsable del tractament i respondrà personalment de les infraccions que hagi comès i de les possibles reclamacions que es puguin produir al respecte. Clínic Barcelona repercutirà a l'adjudicatària tots els costos corresponents a sancions o indemnitzacions a les quals hagi de fer front que s'haguessin originat directament o indirectament per un tractament deficient o negligent de les dades de caràcter personal per part de l'adjudicatària.

Barcelona, 27 de setembre de 2024

David Vidal Fernández
Director de Sistemes d'Informació