PLEC DE PRESCRIPCIONS TÈCNIQUES

SAAS DE L'APLICACIÓ INFORMÀTICA WHISTLEBLOWER SOFTWARE DEL CONSORCI SANITARI INTEGRAL

CSI2025077S

(IMP-SC-006)

Índex

1. Introducció

L'objecte d'aquest plec és la contractació del SAAS de l'aplicació informàtica Whistleblower Software, amb l'objectiu de mantenir el servei en eficients condicions de funcionament durant tot el període contractat, i assegurant el servei d'assistència tècnica en cas d'avaria o fallida en el funcionament, per un termini de 3 anys i 5 mesos (prorrogable 1 any més) a partir de la data d'inici del contracte.

2. Abast del Subministrament

L'aplicació informàtica permet informar de manera segura i anònima sobre irregularitats dins d'una organització. Els seus trets característics han de ser:

1. Personalització
    - Adaptació a la identitat corporativa.
    - Configuració de pestanyes, contingut i elements multimèdia.
2. Formulari de Denúncia
    - Preguntes personalitzades amb opcions condicionals.
    - Diferents tipus de respostes: text, selecció múltiple, data, etc.
3. Mètodes de Denúncia
    - Opció d'enviar informes escrits o àudios.
    - Possibilitat de distorsionar gravacions per anonimat.
    - Opció de denunciar confidencial o anònimament
4. Adjuntar Arxius
    - Adjuntar documents, imatges, àudios i vídeos (fins a 100 MB).
    - Eliminació automàtica de metadades per a protegir la identitat.
5. Enviament i Seguiment de Casos
    - Contrasenya única per accedir al seguiment.
    - Comunicació xifrada amb els gestors del cas.

- Alertes per correu electrònic sobre actualitzacions.

6. Configuració de Destinataris
    - Selecció de qui rep la denúncia per evitar conflictes d'interès.
    - Selecció de qui gestiona la denúncia per evitar conflictes d'interès
7. Compatibilitat
    - Funciona en mòbils, tauletes i ordinadors.

L'aplicació informàtica ha d'implementar les següents mesures per protegir la infraestructura i garantir la confidencialitat, integritat i disponibilitat de les dades.

a. Emmagatzematge i Separació de Dades
    - Ubicació de les dades: Totes les dades s'emmagatzemen a AWS Frankfurt (Alemanya), amb còpies de seguretat en diferents zones de disponibilitat.
    - Separació de dades:
        - AWS RDS: Emmagatzema dades estructurades com títols i descripcions de casos, xifrades amb E2E (Extrem a Extrem).
        - AWS S3: Emmagatzema arxius dels casos, també amb xifratge de extrem a extrem.
        - Bases de dades independents: Separen arxius miscel·lanis (imatges de perfil, configuracions) de les dades sensibles dels casos.

b. Control d'Accés a les Dades
    - Accés restringit:
        - Només els usuaris amb permisos específics poden accedir als casos.
        - Els arxius emmagatzemats a AWS S3 estan en dipòsits privats sense accés públic.
        - Es genera accés temporal només per a usuaris autoritzats.
    - Autenticació robusta:
        - Ús de OAuth 2.0 i SAML 2.0 per a una autenticació segura.

- Autenticació multifactor (2FA) per a usuaris administratius.
- Llistes blanques d'IPs per restringir l'accés només des de ubicacions autoritzades.

c. Monitorització i Detecció d'Intrusions

- Tallafocs d'Aplicacions Web (WAF):
  - Protegeix contra atacs com injecció SQL, XSS i atacs DDoS.
- Sistemes de detecció d'intrusos (IDS):
  - Monitoratge constant del trànsit de xarxa i registres del sistema.
  - Alertes automàtiques en cas d'activitat sospitosa.
- Registres d'activitat:
  - Control detallat d'accessos i modificacions en el sistema.
  - Registres d'intents d'inici de sessió i canvis en la configuració.

d. Còpies de Seguretat i Recuperació de Dades

- Còpies de seguretat periòdiques:
  - Diàries, amb retenció de 35 dies.
  - Setmanals, amb retenció de 85 dies.
- Eliminació segura de dades:
  - S'eliminen claus de xifratge un cop complert el període de retenció, fent irreversibles les dades eliminades.
- Objectius de Recuperació:
  - RPO (Recovery Point Objective): Dades amb un màxim de 24 hores d'antiguitat.
  - RTO (Recovery Time Objective): Recuperació en menys de 1 hora en cas de fallada.

e. Protecció contra Malware i Persistència d'Amenaces

- Executables en contenidors de només lectura:

- AWS Lambda executa l'API en contenidors Docker sense escriptura.
- Cada 15 minuts es restableixen els contenidors, impedint la persistència de malware.

- Gestió de pedaços i actualitzacions:
  - Serveis administrats per AWS amb pedaços automàtics.
  - Escaneig continu de vulnerabilitats en contenidors, servidors i codi.

3. Manteniment correctiu

- Totes les configuracions, components i actualitzacions que foren necessaris per cadascuna de les reparacions.
- Assistència tècnica
- Actualitzacions de l'aplicació.
- ~~Les possibles integracions acordades.~~

4. Detall del Subministrament

El licitador ha d'oferir un únic contacte per totes les circumstàncies que puguin sorgir durant la vigència del contracte de SAAS de l'aplicació informàtica Whistleblower Software.

El licitador haurà d'acreditar estar en disposició de la ISAE 3000 Type 2 i la ISO 27001.

Per a assegurar el subministrament en òptimes condicions durant l'execució del contracte, el licitador haurà de proporcionar un telèfon i un correu de contracte, i haurà d'oferir un temps de resposta no superior a 48h (exceptuant els dissabtes, diumenges i festius).

El licitador haurà d'oferir un temps de resolució de les incidències d'acord amb les següents especificacions:

- Quan no es pugui accedir a l'aplicació: 48 hores (exceptuant els dissabtes, diumenges i festius).
- Quan alguna de les funcionalitats bàsiques de l'aplicació no estigui operativa: 1 setmana (exceptuant els dissabtes, diumenges i festius).
- Quan se li requereixi alguna millora en l'aplicació que no estigui relacionada amb les funcionalitats bàsiques: 75 dies.

El licitador haurà d'explicar el funcionament del servei:

- Procediment d'obertura de les peticions o incidències.
- Mètode de qualificació de les peticions o incidències.
- Matriu de qualificació, nivell de prioritat i temps de resposta i resolució de les incidències.
- Mètode de resolució d'una incidència.
- Indicadors de seguiment del servei (compliment de lliurament en terminis, i compliment de la qualitat)
- Procediment de revisió, proves i validació de la seva resolució.

El lloc de prestació del servei es farà de manera no presencial per a tot tipus de manteniment.

5. Termini del Subministrament

El contracte tindrà una vigència de 3 anys i 5 mesos (prorrogables 1 any més) a partir de la data d'inici del mateix, finalitzant en tot cas a 31/12/2028.