RÉPUBLIQUE DU SÉNÉGAL

Un Peuple – Un but – Une foi

MINISTÈRE DE LA SANTÉ
ET DE L'ACTION SOCIALE

****

Cellule de la Carte sanitaire et sociale, de la Santé digitale et de l'Observatoire de Santé (CSSDOS)

Programme de Digitalisation du Système de Santé 2023-2028 (PDSS)

Projet d'Accélération de l'Économie numérique au Sénégal 2023-2028 (PAENS, P172524)

****

TERMES DE RÉFÉRENCES

ACTIVITÉ N°4208 PTBA 2024 : RECRUTER UN EXPERT EN SECURITE ET INFRASTRUCTURE LOGICIELLE

1. CONTEXTE

Le Sénégal dispose d'un nouveau référentiel de politique économique et sociale avec : (i) le « Sénégal 2050 : Agenda national de Transformation » décliné en (ii) Masterplan 2025-2034 ; et en (iii) Stratégie nationale de Développement 2025-2029. Ce référentiel accorde une place importante à la transformation numérique du secteur de la santé.

A plusieurs occasions, les autorités ont exprimé dans des termes clairs, leur volonté d'utiliser les technologies numériques pour contribuer à la transformation systématique de la santé. Le Président de la république a prôné la *« digitalisation intégrale des services de santé et de l'information sanitaire »* lors du Conseil des Ministres du 07 août 2024.

« Une réforme profonde du système de santé pour un accès universel, en passant d'une logique de guérison à une logique de prévention, en numérisant le système, … » a été rappelé dans l'Agenda national de transformation Sénégal 2050.

Le Master Plan 2024-2034, dans son Programme 16 établit quatre projets prérequis dont le premier concerne *« Données de santé digitalisées »* avec comme résultat attendu *« 100% de la population enrôlée dans le système national digitalisé des données de santé ».*

Dans la Stratégie nationale de Développement (SND) 2025-2029 l'Etat demande de *«généraliser l'adoption du dossier patient numérique ; (ii) utiliser la technologie, en particulier, l'intelligence artificielle pour optimiser l'organisation, le fonctionnement des EPS et la prise en charge efficiente des patients ».*

Le premier Ministre, dans sa Déclaration de Politique Générale s'est engagé à mettre à l'échelle le dossier médical électronique *« Le dossier patient informatisé, déjà disponible, sera mis à l'échelle, au fur et à mesure, avec une approche régionale ».*

Lors du lancement du New Deal technologique, le Président de la République a considéré que la digitalisation du dossier patient informatisé et la télémédecine est une priorité absolue.

Ainsi, le Ministère de Santé et de l'Action sociale (MSAS) s'est résolument tourné vers la transition numérique du secteur conformément aux prescriptions de la nouvelle stratégie des politiques publiques (Agenda national de transformation Sénégal Vision 2050).

2. JUSTIFICATIONS

Pour piloter et gérer la transformation digitale de la santé, le MSAS a créé en 2017, la Cellule de la Carte sanitaire et sociale, de la Santé digitale et de l'Observatoire de la Santé (CSSDOS). La CSSDOS a atteint plusieurs résultats dont la délivrance du certificat de vaccination contre la Covid-19 à code QR, l'adoption du Programme de Digitalisation du Système de Santé (PDSS) 2023-2028 et le déploiement en phase pilote de la plateforme Dossier Patient Informatisé (DPI) pour la gestion électronique du dossier médical du patient. Cependant, elle reste confrontée à plusieurs contraintes dont le manque de ressources humaines dont des experts dans les domaines de santé numérique, de la conduite du changement, de la gestion des données de santé. Cette rareté de ces ressources est d'autant plus cruciale que la digitalisation des services de santé et de l'information sanitaire demande une expertise certaine pour

l'élaboration de la politique de santé et des projets opérationnels, la mise en œuvre et le suivi-évaluation.

En sa qualité de partenaire de mise en œuvre du PAENS au sein du MSAS, la CSSDOS élabore le PTBA et le met en œuvre avec les bénéficiaires internes au MSAS. Pour la digitalisation intégrale des services de santé et de l'information sanitaire, la CSSDOS a besoin d'être renforcée pour mettre en œuvre cette ambition de l'État de digitalisation de la santé et des systèmes d'information digitalisés de santé.

Lors de la mission de la Banque Mondiale en octobre, il a été recommandé de renforcer l'équipe de la CSSDOS en mettant l'accent sur le recrutement prioritaire d'experts chefs de projet dans un premier lot de recrutement.

Ainsi, ces présents termes de référence (TDR) ont pour objectif de décrire les principales attentes, les objectifs et les livrables des missions de l'expert en sécurité et infrastructure logicielle.

Il sera mis à la disposition de la CSSDOS et travaillera sous la responsabilité du coordonnateur de la CSSDOS. Il sera amené à travailler et appuyer les autres départements du secteur conformément aux orientations du PDSS.

3. OBJECTIFS

Le recrutement de ces experts, en appui à la CSSDOS, a pour objectif général d'appuyer de manière transversale la transformation digitale du secteur de la santé en favorisant une culture d'innovation et d'agilité.

De façon spécifique, les experts recrutés devront :

- Accompagner la transformation digitale du secteur de la santé ;
- Améliorer le cadre de management de projets de santé numérique ;
- Renforcer les compétences numériques en accompagnant les acteurs de santé dans l'adoption de nouveaux outils et technologies numériques, en renforçant leurs compétences et leur culture digitale ;
- Assurer la sécurité et la conformité des solutions numériques développées en respectant les normes de sécurité et de conformité applicables, en mettant en œuvre des mesures de protection des données et de gestion des risques ;
- Faciliter l'innovation continue au sein du MSAS en proposant des idées et des initiatives novatrices, en testant de nouveaux concepts et en explorant de nouvelles opportunités digitales ;
- Travailler en étroite collaboration avec toutes les parties prenantes du MSAS, y compris les équipes métier, les départements informatiques, les fournisseurs de technologie et les partenaires stratégiques.

4. LIVRABLES

Le recrutement de l'expert en sécurité et infrastructure logicielle pour une période d'une année renouvelable est essentiel pour garantir le succès et la pérennité des initiatives de transformation numérique dans le secteur de la santé.

Les livrables suivants sont attendus de l'expert en sécurité et infrastructure logicielle :

Catégorie	Livrables
Analyse et diagnostic	• Rapport d'audit de sécurité : évaluation des vulnérabilités des systèmes, applications et infrastructures. • Cartographie des risques : identification des menaces (internes et externes) et des impacts potentiels. • Rapport d'analyse de conformité : vérification du respect des normes et réglementations.
Conception et Mise en place des solutions de sécurité	• Architecture de sécurité : schéma détaillé des solutions techniques (pare-feu, VPN, systèmes de détection d'intrusion, segmentation réseau, etc.). • Plan de renforcement des infrastructures : recommandations et actions concrètes pour durcir la sécurité des serveurs, bases de données, API et applications. • Déploiement de solutions de cybersécurité : Antivirus, EDR (Endpoint Detection and Response), SIEM (Security Information and Event Management), etc. • Documentation technique : guide de configuration, procédures de sécurité et documentation d'intégration.
Gestion des accès et protection des données	• Plan de gestion des identités et des accès (IAM) : stratégie pour sécuriser l'accès aux ressources (authentification multi-facteurs, contrôle des privilèges, etc.). • Politique de chiffrement des données : stratégie de cryptage pour les données sensibles (au repos, en transit, et lors des traitements). • Plan de sécurisation des API et microservices : protection des échanges entre services (OAuth, JWT, etc.).
Prévention et gestion des incidents	• Plan de gestion des incidents de sécurité (PRA/PCA) : Procédure pour détecter, contenir, éradiquer et récupérer après une attaque. • Simulations d'attaques : Test d'intrusion avec rapport détaillé des failles détectées et des correctifs à appliquer. • Rapport d'analyse post-incident : Retour d'expérience après une attaque (ex : ransomware, fuite de données).
Formation et sensibilisation	• Programme de formation des équipes : Formation des développeurs et administrateurs pour intégrer les bonnes pratiques de cybersécurité (DevSecOps).

	• Guide de bonnes pratiques en cybersécurité : Pour les utilisateurs non techniques (phishing, mots de passe, accès distants, etc.).
Suivi et amélioration continue	• Tableaux de bord de sécurité • Rapport de veille technologique • Plan d'amélioration continue : Proposition d'évolutions des infrastructures et politiques de sécurité.

5. FICHE DE POSTE

L'expert en sécurité et infrastructure logicielle accompagne le PMO dans la sécurité des systèmes d'information de santé, des infrastructures numériques gérées par les ressources du MSAS. Il conçoit, implémente et supervise les solutions de sécurité pour protéger les systèmes d'information, les données sensibles et les infrastructures logicielles. Il veille à la résilience des systèmes face aux menaces et à la conformité avec les réglementations en vigueur.

A. MISSIONS

- Examen initial et cartographie des problèmes de cybersécurité et de protection des données dans les systèmes d'information sanitaire et sociale existants.
- Effectuer des évaluations des risques et des analyses de vulnérabilité.
- Examiner la conformité réglementaire.
- Évaluer les plans de réponse aux incidents et de reprise après sinistre.
- Organiser des ateliers de renforcement des capacités sur les risques cyber.
- Rédaction d'un rapport final contenant des recommandations détaillées et présentation des résultats au PMO.
- Faire l'audit continu des infrastructures logicielles des solutions numériques de santé.
- Définir des stratégies de mise en conformité des solutions numériques de santé.
- Participer à la définition de l'architecture logicielle du Système Digital Intégré de la Santé (SDIS)

B. PROFIL ET EXPERIENCES

Profil

Le candidat doit disposer d'un diplôme supérieur d'au moins Bac +5 en sécurité de l'information, en informatique, en Cybersécurité ou dans un domaine connexe.

Expériences professionnelles :

- Avoir au moins 5 ans d'expérience dans un poste similaire (infrastructure ou sécurité) ;
- Avoir au moins 5 ans d'expériences dans le domaine de la cybersécurité ;
- Avoir une expérience dans les systèmes d'information de santé est un atout ;

- Avoir une expérience pertinente dans le volet hébergement des données de santé est un atout.

Compétences professionnelles

- Solides compétences techniques en matière d'évaluation de la vulnérabilité et de cryptage
- Une certification HCISPP serait un atout majeur, à défaut disposer d'une certification ISACA (CISA,CISM,CISA) ou ISO 27001 ou CIPP/E
- Bonnes connaissances des architectures cloud et des environnements conteneurisés
- Maitrise des protocoles et outils de sécurité informatique (SSL/TLS,SIEM,IDS/IPS)
- Connaissances des normes et standards de sécurité (ISO 27001 ou NIST)
- Bonne capacité à travailler sous pression et dans les délais ;
- Avoir une bonne connaissance de la politique nationale de santé digitale du Sénégal est un atout.

6. DURÉE DU CONTRAT

Le contrat a une durée d'un an renouvelable après évaluation.

7. MÉTHODE DE SÉLECTION

La méthode de sélection choisie est la sélection de consultants individuels par mise en concurrence ouverte, conformément au Règlement de Passation des Marchés pour les Emprunteurs sollicitant le Financement de Projets d'Investissement (FPI), Edition septembre 2023.

Un avis de recrutement sera publié dans les journaux et supports électroniques appropriés à cet effet.

8. CRITÈRES DE SÉLECTION

Une commission de recrutement du MSAS procédera à l'examen et à la sélection des dossiers. Seuls les candidats retenus seront invités à prendre part à l'entretien.

9. DOSSIER DE CANDIDATURE

Le dossier de candidature comprend :

- Les copies légalisées (Police ou Gendarmerie) des diplômes et attestations
- Le Curriculum Vitae incluant au moins trois personnes références
- La Lettre de motivation

Seuls les candidats présélectionnés seront contactés.