RÉPUBLIQUE DE GUINÉE
Travail - Justice - Solidarité
PRÉSIDENCE

ANIES
Agence Nationale d'Inclusion Economique et Sociale

PRESIDENCE DE LA REPUBLIQUE

AGENCE NATIONALE D'INCLUSION ECONOMIQUE ET SOCIALE (ANIES)

PROJET DE RIPOSTE D'URGENCE ET D'APPUI AU PROGRAMME NAFA (PRU-APN)

Financement : Banque Mondiale IDA D6540-GN

AVIS A MANIFESTATIONS D'INTERET
SERVICES DE CONSULTANTS POUR LE RECRUTEMENT D'UN ADMINISTRATEUR SYSTEMES ET RESEAUX

Date de début : 16 août 2022 **Date limite : 30 août 2022**

Le Gouvernement de la République de Guinée bénéficie, dans ce cadre, d'un don de soixante-dix (70) millions de dollars américains de la part de la Banque mondiale, au titre du Projet de Riposte d'Urgence et d'Appui au Programme NAFA (PRU-APN).

La Direction Générale de l'ANIES compte utiliser une partie de cet appui dans le cadre de sa composante 4, Gestion du projet, pour le recrutement d'un **Administrateur Systèmes et Réseaux** pour le Projet de Riposte d'Urgence et d'Appui au Programme NAFA (PRU-APN), et lance ainsi un appel à candidatures ouvert à cet effet.

Nature et étendue des tâches :

Sous l'autorité de la Directrice des Systèmes d'Information (DSI) et le Coordinateur du Projet, l'Administrateur Systèmes et Réseaux devra :

a- Gestion de l'infrastructure informatique

- Administrer les infrastructures informatiques (physique) et le patrimoine applicatif en vue de leur maintien en condition opérationnelle ;
- Installer, paramétrer et configurer les ressources informatiques (matériels, logiciels…) ;
- Guider et former tous les utilisateurs et réaliser le support aux utilisateurs ;
- Assurer l'entretien du matériel et anticiper le renouvellement ;
- Aider à évaluer les besoins en équipement (spécifications techniques) et suivre en permanence l'évolution du matériel informatique en termes de besoin en équipement et d'adéquation entre les équipements utilisés et les besoins réels des utilisateurs ;
- Détecter, analyser et comprendre l'origine d'un dysfonctionnement, incident ou accident et proposer une solution permettant de résoudre le problème ;
- Anticiper les défaillances techniques et proposer des solutions d'amélioration ;

Cameroun en face de la station Total
Commune de Dixinn-Conakry-Rep.Guinée - BP 75.
Tél. : +224 629 00 57 00
Site web : www.anies.gov.gn
E- mail : contact@anies.gov.gn

- Anticiper les failles sécuritaires en procédant périodiquement des tests de sécurité et de contrôle, et en présentant aux responsables hiérarchiques les résultats suivis de propositions de solutions ;
- Mettre en place une application de gestion de l'infrastructure et de support informatique pour répertorier et suivre tous les équipements du système. L'application doit être capable d'enregistrer toutes les interventions faites sur chaque équipement ;

b- Administration du réseau informatique

- Optimiser le réseau par la conduite de projet d'installation ou de refonte de certains éléments du réseau de l'agence, matériels ou logiciels ;
- Prendre en compte les exigences des utilisateurs en termes d'exigence de performances du réseau (puissance, rapidité, stabilité) ;
- Intégrer de nouvelles applications afin d'améliorer les performances des réseaux ;
- Assurer l'interface entre les équipes internes et externes (sous-traitants) lors de la mise en place de réseaux ;
- Mettre en place les interconnexions entre les différents réseaux de l'agence pour assurer leur compatibilité ;
- Apporter son expertise technique et fonctionnelle sur la partie réseaux lors du lancement de projets transverses ;
- Mettre en place les normes de sécurité, notamment celles liées aux conditions d'accès ;
- Assurer la bonne gestion des droits d'accès, pour les machines d'une part, et pour les utilisateurs d'autre part, dans le respect des règles de sécurité de l'agence ;
- Mettre en place des tableaux de bord de suivi des performances et de qualité du réseau (pannes, flux, disponibilité des ressources, sécurité, etc.) ;
- Installer les logiciels d'administration de réseaux et assurer l'ensemble des sauvegardes nécessaires pour maintenir la sécurité des données circulant dans le réseau de l'agence ;
- Informer le budget lié aux opérations sur le réseau ;
- Assister les utilisateurs (hotline) sur la partie réseau afin de les aider en cas de panne ou de difficultés ;
- Former et sensibiliser les utilisateurs aux réseaux et à la sécurité ;
- Assurer une veille technologique afin d'anticiper les évolutions nécessaires à l'optimisation du réseau ;
- Proposer les investissements informatiques relatifs au réseau informatique.

c- Sécurité des système et réseaux

- Diagnostiquer, prévenir et réparer les pannes et les dysfonctionnements des réseaux ;
- Analyser les risques et les dysfonctionnements, les marges d'amélioration des systèmes de sécurité ;
- Définir, faire évoluer et mettre en œuvre la politique de sécurité des systèmes d'information ;
- Établir un plan de prévention des risques informatiques et un plan de continuité d'activité (PCA) (ou plan de maintien en conditions opérationnelles du Système d'Information) ;

- Définir ou faire évoluer les mesures et les normes de sécurité (charte), en cohérence avec la nature de l'activité de l'agence et son exposition aux risques informatiques (nomadisme, BYOD (Bring your own device), transferts de données, transactions financières, etc.) ;
- Choisir les dispositifs techniques sécuritaires les plus appropriés aux besoins de l'agence (firewall, programmes de back up, cryptographie, authentification…) ;
- Mettre en place les méthodes et outils de sécurité adaptés, et accompagner leur implémentation auprès des utilisateurs ;
- Mettre en place un mécanisme de sauvegarde automatique de l'ensemble des données du système d'information ;
- Gérer les incidents de sécurité et proposer des solutions pour rétablir rapidement les services ;
- Définir les actions à mener afin de réparer les dommages causés au SI en cas de survenance d'un sinistre de sécurité S.I. (intrusion dans le système, contamination par un virus, défaillance d'un équipement…), mettre en œuvre le plan de reprise d'activité (PRA) ;
- Faire analyser les causes des incidents et consolider les mesures de sécurité ;
- Faire tester régulièrement le bon fonctionnement des mesures de sécurité mises en place pour en détecter les faiblesses et les carences ;
- Auditer le respect des normes de sécurité informatique imposées aux sous-traitants de l'agence ;
- Réaliser le référentiel de sécurité, l'actualiser régulièrement, en assurer la diffusion et veiller à son application ;
- Mettre en place des actions de communication (en concertation avec sa hiérarchie) auprès du personnel de l'Agence en cas de risque majeur ou de dommages au SI causés par une attaque ou par des dégâts matériels ;
- Assurer une veille technologique, de manière à garantir la sécurité logique et physique du système d'information ;
- Identifier les nouveaux risques sur la sécurité du système d'information : apparition de nouveaux virus, lancement d'attaques informatiques sur le réseau mondial... ;
- Rechercher des solutions innovantes pour répondre aux problématiques induites par l'introduction de toute nouvelle technologie ;
- Suivre les évolutions juridiques du marché en termes de sécurité informatique afin de garantir la conformité du Système d'Information au droit individuel et collectif
- Rédiger des notes technologiques de sécurité ;
- Participer au choix et l'évaluation des sous-traitants (sélection des SSII ou cabinets conseil, participation à la rédaction de l'appel d'offre et au dépouillement des réponses, sélection et réception des candidats) ;
- Analyser les technologies de sécurité mises en œuvre par les fournisseurs, rechercher les faiblesses des systèmes et signaler les menaces et les problèmes logiciels éventuels
- S'assurer que tous les documents du projet, y compris les documents d'appel d'offres, les contrats, les artefacts de conception, intègrent l'importance de la sécurité.
- Mettre en œuvre et contrôler les tableaux de bord techniques des incidents de sécurité rencontrés (virus, tentatives d'intrusion, …) ;
- Assurer le reporting des problèmes de sécurité en estimant les pertes financières (pertes engendrées et coût de mise en place d'une parade).

d- **Autres tâches**

Assurer toutes autres tâches professionnelles que la DSI ou les responsables jugeraient utiles de lui confier.

Qualifications requises :

Les « savoirs » :

Au moins cinq (5) années d'études universitaires (Bac+5) sanctionnées par un diplôme en informatique, réseaux et sécurité ou ingénieur en informatique option réseau et/ou sécurité.

Les « savoir-faire » :

- ✓ Avoir une expérience d'au moins 5 ans dans le domaine des réseaux et de la sécurité informatique à un poste similaire ;
- ✓ Avoir les certifications telles que ITIL, CCNA, CND (Certified Network Defender), CCISCO (Certified Chief Information Security Officer) et CISA (Certified Information Systems Auditor) seraient un atout ;
- ✓ Avoir une maitrise des technologies switching Aruba & Cisco (vlan, spanning-tree…), des systèmes de Stockage, Monitoring (Nagios, CENTREON), Load balancing (F5, Haproxy…), Veeam Backup ;
- ✓ Avoir une maitrise de l'administration des serveurs (DNS, Active directory, DHCP, WSUS), Oracle (RMAN sauvegarde et Restore) et des plateformes Virtuel (ESXI,Vcentre…) ;
- ✓ Avoir une bonne connaissance de l'architecture et des fonctionnalités d'un système d'information ;
- ✓ Avoir une maîtrise des normes et procédures de sécurité informatiques et télécommunications, des techniques de chiffrement et signature de données et des outils et technologies qui s'y rapportent : GPO, Matrice des flux, WAF, firewall, antivirus, cryptographie, serveurs d'authentification, tests d'intrusion, PKI, filtrages d'URL...) ;
- ✓ Avoir une bonne connaissance en matière de cyber sécurité (menaces et leur traitement) ;
- ✓ Avoir une bonne connaissance en technologies télécoms, Internet, serveur web, serveur de base de données ;
- ✓ Avoir une très bonne connaissance des principaux systèmes d'exploitation (Windows, Unix, …) ;
- ✓ Avoir une connaissance des principaux prestataires du marché de la sécurité informatique (éditeurs, sociétés de service...) ;
- ✓ Avoir une bonne connaissance des réseaux et systèmes, des outils d'évaluation et de maîtrise des risques ;

- ✓ Avoir une connaissance des méthodologies (ex : OSSTMM, OWASP…) ;
- ✓ Une connaissance des normes juridiques en matière de sécurité et de droit informatique serait un atout ;
- ✓ Avoir une connaissance des normes ISO 27001, CEH, CISSP, de l'évaluation de la vulnérabilité et des tests de pénétration ;
- ✓ Avoir une maîtrise de l'anglais technique ;
- ✓ Avoir une expérience avec les centres de données (Datacenter) serait un atout.

Les « savoir-faire » comportementaux :

- Avoir un sens de responsabilité et d'engagement ;
- Avoir un sens de l'écoute et bonnes aptitudes à la communication et aux relations interpersonnelles ;
- Avoir une bonne réactivité ;
- Avoir le sens de la rigueur et de précision ;
- Avoir une bonne appréhension du risque ;
- Savoir gérer son stress et travailler en équipe ;
- Avoir une bonne capacité d'analyse, de synthèse et de résolution de problèmes ;

  Adaptabilité et curiosité car les évolutions technologiques sont rapides et doivent être assimilées afin de pouvoir optimiser l'existant.

Evaluation des performances :

Les performances du Consultant seront évaluées trimestriellement par la DSI et le Coordinateur du Projet, sur la base du plan de travail et des résultats attendus et séquencés trimestriellement. Les résultats de l'évaluation seront partagés avec le Gouvernement et l'IDA.

Nature et durée du contrat :

Le contrat de Consultant aura une durée initiale d'un (1) an éventuellement renouvelable en cas de prestations jugées satisfaisantes et ce pour la durée du Projet.

Les Consultants intéressés peuvent obtenir les termes de référence auprès du siège de l'ANIES, à Cameroun en face de la Station TOTAL du lundi au vendredi de 09h00 à 16h00 ou par e-mail à l'adresse : recrutement@anies.gov.gn

Dossiers à fournir :

Le dossier de candidature devra comporter les pièces ci-après :

- ✓ Une lettre de motivation ;
- ✓ Un CV détaillé ;
- ✓ Une copie du ou des diplômes et attestations ou tout autre document attestant les expériences et qualifications acquises.

Méthode de sélection :

Le recrutement du consultant se fera suivant la méthode Sélection de Consultants Individuels conformément aux dispositions décrites dans le Règlement de Passation de Marchés de la Banque Mondiale pour les Emprunteurs sollicitant le Financement de Projets d'Investissement (FPI), édition Novembre 2020.

Lieu du travail : Le poste sera basé à Conakry.

Date limite et lieu de remise des candidatures :

Les candidatures doivent être adressées à Monsieur le Directeur Général de l'ANIES et déposées au **siège de l'ANIES à Cameroun, en face de la station TOTAL** ou envoyées par voie électronique à l'adresse suivante : recrutement@anies.gov.gn au plus tard **le 30 août 2022 à 12 heures GMT** avec la mention en objet « ***CANDIDATURE POUR LE RECRUTEMENT D'UN ADMINSTRATEUR SYSTEMES ET RESEAUX*** ».

P/Le Directeur Général p.o.
La Directrice Générale Adjointe

M'Mah DOPAVOGUI