REPUBLIQUE DU SENEGAL

Un Peuple-Un But-Une Foi

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR DE LA RECHERCHE, ET DE L'INNOVATION

DIRECTION GENERALE DE LA RECHERCHE ET D EL'INOVATION

CYBER-INFRASTRUCTURE NATIONALE POUR L'ENSEIGNEMENT SUPÉRIEUR, LA RECHERCHE ET L'INNOVATION
(CINERI)

Projet Enseignement Supérieur Professionnel Orienté Insertion et Réussite des Jeunes (ESPOIR-Jeunes)

TERMES DE REFERENCES

Recrutement d'un (1) ingénieur cyber-sécurité sénior pour la sécurité du SIGESR

Avril 2024

1. CONTEXTE ET JUSTIFICATION

L'enseignement supérieur sénégalais a connu plusieurs réformes ces dernières années dont, notamment, le passage au système Licence-Master-Doctorat (LMD), la mise en place de nouveaux textes réglementaires organisant les universités, la réforme des grades du personnel enseignant, etc.

L'un des axes majeurs des réformes de politiques du sous-secteur de l'enseignement supérieur est l'utilisation des TIC pour accompagner leur mise en œuvre et permettre leur suivi. En effet, le pilotage de l'enseignement supérieur et de la recherche nécessite une maitrise, en temps réel, de l'information relative à ce secteur.

La gouvernance de l'Enseignement supérieur et de la Recherche peut se décliner en :

- gouvernance institutionnelle ;
- gouvernance de l'activité.

La **gouvernance institutionnelle** couvre le domaine des processus de conformité en termes de responsabilité publique et d'assurance qualité (Ministère, Conseils d'Administration des universités, ANAQ-Sup) et s'adresse au Ministre et aux Conseils d'Administration des différentes universités. La **gouvernance d'activité** couvre le domaine du processus de performance en termes de pédagogie, d'utilisation de ressources et s'adresse aux rectorats et aux autres directions opérationnelles du Ministère. L'utilisation de ressources de la gouvernance d'activité regroupe les thèmes suivants : planification stratégique et alignement, prise de décision stratégique, gestion des risques stratégiques, systèmes stratégiques, tableaux de bords, amélioration continue.

Quatre principaux piliers peuvent être identifiés, pour la gouvernance de l'Enseignement supérieur et de la Recherche (ESR) :

1. Les Étudiants ;
2. L'offre de formation ;
3. Les établissements d'enseignement supérieur publics et privés ;
4. La Recherche.

Pour chacun de ces piliers, il y a plusieurs composantes à gérer, avec à chaque fois un volet opérationnel (dont la gestion repose sur les établissements et structures concernés: gouvernance d'activité) et un volet informationnel (à destination du ministère et ses instances de gouvernance de l'ESR : gouvernance institutionnelle).

Un bon système de gouvernance passe nécessairement par une bonne circulation de l'information et la mise à disposition de tableaux de bord permettant l'analyse en temps réel de différents indicateurs préétablis.

La mise en place d'un Système intégré de Gouvernance de l'ESR (SIGESR) est un moyen pour prendre en charge la plupart des problèmes actuels du secteur. En effet, cela pourrait permettre de suivre en temps réel les différents indicateurs de performance et de gestion des différentes structures dépendant du MESRI.

Plusieurs actions ont déjà été menées depuis quelques années. Le socle du SIGESR est complètement opérationnel et quelques objets métiers de base sont déjà implémentés. D'autres objets ont commencé à être implémentés, mais n'ont pas été finalisés. Enfin, nous avons des objets dont l'implémentation n'a pas encore commencé.

Dans le cadre du projet Enseignement supérieur professionnel orienté Insertion et Réussite des jeunes (Espoir-Jeunes), le Ministère, avec l'appui de la Banque Mondiale, a consacré une rubrique au SIGESR. L'accent est mis, pour une meilleure gouvernance de l'Enseignement Supérieur et de la Recherche (ESR), sur la finalisation du SIGESR et son interconnexion aux applications de gestion utilisées dans les universités.

Nous souhaitons, dans ce contexte, prendre toutes les dispositions nécessaires pour assurer la sécurité du dispositif applicatif.

2. Objectifs

Les objectifs de cette mission sont d'assurer la sécurité des applications déployées dans le cadre du SIGESR et celle des interactions avec les Systèmes des établissements. Pour cela, nous souhaitons recruter, pour compléter l'équipe en place, le profil suivant, **pour une durée de 12 mois**.

INGÉNIEUR CYBER-SECURITE SENIOR (1 POSTE)

Poste : Sous la responsabilité de l'Architecte logiciel, l'ingénieur cyber-sécurité sénior prend en charge la mise en œuvre de la Sécurité du SIGESR et du déploiement du dispositif. Il a une connaissance en sécurité et systèmes.

Tâches : Les principales tâches sont :

- Définir des procédures et normes de sécurité adaptées, les documenter et veiller à leur respect ;
- Sensibiliser les acteurs sur les bonnes pratiques et les enjeux de sécurité ;
- Protéger les systèmes d'information, les données et les réseaux contre les menaces et les attaques cybernétiques ;
- Surveiller les activités suspectes ;
- Réagir rapidement en cas d'incident de sécurité ;
- Assurer une veille sur les menaces et suivre les vulnérabilités des infrastructures et systèmes.

Profil : Titulaire d'un diplôme de niveau Bac+5 en informatique avec une spécialisation en sécurité ou systèmes, l'ingénieur cyber-sécurité dispose d'une expérience d'au moins 3 ans dans des fonctions similaires. Il a un esprit d'équipe et est capable d'apprendre et de comprendre de nouvelles technologies.

Il a :

- Une connaissance approfondie des protocoles et technologies de sécurité (pare-feu, VPN, IDS/IPS, cryptographie, etc.) ;
- Une maîtrise des outils et des techniques de test de pénétration ;
- Des compétences en matière de gestion de la sécurité de l'information et de conformité réglementaire (RGPD, PCI-DSS, etc.) ;
- De bonnes compétences en communication pour la sensibilisation à la sécurité auprès des utilisateurs et la communication avec les autres membres de l'équipe informatique ;
- Des connaissances des techniques de détection des menaces et de réponse aux incidents ;
- Des connaissances des technologies de sécurité Cloud, des architectures Cloud et des pratiques de sécurité associées ;
- Une capacité à travailler sous pression et à résoudre des problèmes rapidement ;
- Des capacités rédactionnelles.

Les certifications (CompTIA Security+, CISSP, CEH, CCSP, GSEC…) sont un atout.

3. Activités

Les principales activités de l'ingénieur cyber-sécurité comprennent, mais sans s'y limiter, celles listées ci-après :

- Élaboration de procédures et normes de sécurité adaptées ;
- Tests d'intrusion ;
- Sensibilisation des acteurs sur les bonnes pratiques et les enjeux de sécurité ;
- Protection des systèmes d'information, des données et des réseaux ;
- Surveillance des activités suspectes ;
- Participation aux ateliers et réunions ;
- Veille sur les menaces et vulnérabilités des infrastructures et des systèmes.

Les travaux dans le tableau ci-dessous seront réalisés durant la mission.

1.	Mise à niveau du socle du SIGESR et des plateformes en production
2.	Sécurisation de CAMPUSEN
3.	Mise en œuvre de la sécurité du SIGESR

4. Résultats attendus

Au terme de cette mission :

- Le SIGESR est mis à niveau ;
- Le SIGESR et les applications connectées sont sécurisées ;
- Les échanges de données entre le SIGESR et les systèmes des établissements sont sécurisés ;
- La documentation technique est disponible ;
- Les membres de l'équipe SIGESR sont sensibilisés sur les normes de sécurité.

5. Procédure de Sélection

La sélection se fera suivant la méthode basée sur la Qualification des consultants par avis à manifestation d'intérêt publié sur le site de la Banque et dans les journaux.

Les candidats seront notés suivant le barème ci-après :

Qualifications générales du candidat	**40 points**
•Titulaire d'un BAC+5 en informatique avec une spécialisation en sécurité ou systèmes	20 points

• Certifications : CompTIA Security+, CISSP, CEH, CCSP, GSEC (4 points chacune)	20 points
Expérience du candidat	**60 points**
•Expérience d'au moins 3 ans dans des fonctions similaires (05pts / année)	15 points
• Connaissance approfondie des protocoles et technologies de sécurité (pare-feu, VPN, IDS/IPS, cryptographie, etc.)	10 points
• Maîtrise des outils et des techniques de test de pénétration, de détection des menaces et de réponse aux incidents	10
• Autres compétences utiles pour le poste dont la connaissance des technologies de sécurité Cloud, des architectures Cloud et des pratiques de sécurité associée	5 points
• Interview	20 points
TOTAL	**100 points**

La note minimale requise pour être retenu dans la liste des pré-qualifiés est de 80 points /100. Le candidat ayant obtenu la note totale la plus élevée et supérieure à la note minimale ci-dessus sera invité à une négociation.

En cas d'égalité entre deux ou plusieurs candidats, ces derniers seront départagés par le nombre d'année d'expérience dans des fonctions similaires. A défaut d'être départagés par ce critère, il sera fait recours au nombre d'années d'expérience professionnelle en général.