

RESPONSABLE DES INFRASTRUCTURES NUMERIQUES ET SECURITE INFORMATIQUE (H/F)

Structure : **Sèmè City Institute of Technology and Innovation (SCITI)** Lieu : **Cotonou (Bénin)**

CONTEXTE

Sèmè City est le projet phare du Gouvernement Béninois visant à relever les défis de la formation, de l'employabilité et de l'innovation des jeunes dans des secteurs reconnus comme porteurs pour les économies africaines. Sèmè City rassemble des établissements d'enseignement supérieur et de formation technique et professionnelle, des centres d'incubation, laboratoires et espaces d'innovation ouverte, pour créer un environnement où l'excellence, la créativité et la collaboration permettent de repousser les limites de ce qui est possible. L'objectif est de former ainsi une nouvelle génération de talents, d'encourager l'émergence d'entreprises innovantes, et de promouvoir un modèle de croissance durable fondé sur l'innovation locale.

Les campus de démarrage, dont Sèmè One, situé à Cotonou, accueillent déjà des milliers d'étudiants, de chercheurs et d'entrepreneurs dans des infrastructures modernes. Le campus principal, en cours de développement à Ouidah, sur un site de 336 hectares, a vocation à devenir une référence en matière de campus durable en Afrique, à l'horizon 2030.

Dans le cadre de sa récente restructuration institutionnelle, le projet entre dans une nouvelle phase s'appuyant sur quatre types d'entités complémentaires afin de permettre un déploiement des activités à plus grande échelle :

- **La Fondation Sèmè City**, garante de la vision stratégique, de la coordination globale et du financement à long terme ;
- **L'Agence de Développement de Sèmè City (ADSC)**, responsable de la conception, du développement des infrastructures et du pilotage des programmes ;
- **La Commission Académique**, chargée de l'agrément des formations et du contrôle qualité académique ;
- **Les établissements d'enseignement publics et privés**, dont le **Sèmè City Institute of Technology and Innovation (SCITI)**, établissement public dédié à la formation d'ingénieurs et aux activités de recherche scientifique.

Implanté au cœur de Sèmè City, SCITI a pour vocation de former une nouvelle génération d'ingénieurs, de chercheurs et d'innovateurs capables d'apporter des solutions technologiques et scientifiques aux défis du développement durable.

En mettant l'accent sur la recherche appliquée, l'apprentissage par la pratique et les partenariats avec le secteur productif, SCITI ambitionne de devenir une référence régionale en matière de formation technologique et d'innovation industrielle.

Dans cette perspective, la mise en place d'une équipe dédiée aux infrastructures numériques et à la sécurité informatique constitue une priorité stratégique pour SCITI.

Cette démarche vise à garantir la disponibilité, la performance et la résilience des systèmes d'information, tout en assurant la protection des données et des services numériques. Elle a également pour objectif de soutenir efficacement les activités pédagogiques, de recherche et d'innovation de l'établissement. Enfin, cette démarche répond à la fois aux exigences immédiates liées au lancement des premières activités de SCITI et à la nécessité d'anticiper les conditions techniques, organisationnelles et sécuritaires indispensables à une opérationnalisation complète et durable de l'établissement.

C'est dans cette optique que s'inscrit le présent processus de recrutement, qui vise à doter Sèmè City Institute of Technology and Innovation d'un(e) responsable des infrastructures numériques et sécurité informatique pour l'accompagner dans la mise en œuvre efficace de ses missions et à son déploiement institutionnel, académique et administratif au sein de l'écosystème Sèmè City.

Vous êtes proactif, rigoureux, dynamique, analytique et ingénieux(se). Vous aimez travailler en équipe tout en offrant des résultats d'excellente qualité.

Rejoignez Sèmè City Institute of Technology and Innovation!

Le poste

Le/la Responsable des Infrastructures Numériques et Sécurité Informatique est directement rattaché(e) à la Direction des Systèmes d'Information et de l'Innovation Pédagogique (DSIIP) et entretient des liens fonctionnels avec les autres départements de SCITI.

Il/Elle devra intégrer l'organisation administrative mise en place pour garantir la réalisation de toutes les activités liées aux Infrastructures Numériques et à la Sécurité Informatique en conformité avec la réglementation en vigueur dans le domaine.

Les missions principales

Le/la Responsable des Infrastructures Numériques et Sécurité Informatique sera spécifiquement chargé de :

- Concevoir, déployer et maintenir en condition opérationnelle les infrastructures réseaux, les serveurs, la messagerie, les postes de travail, les systèmes de stockage et le cloud de SCITI ;
- Garantir la disponibilité, la performance et la fiabilité des systèmes d'information ;
- Assurer le dimensionnement, l'évolutivité et l'anticipation des besoins ;
- Définir et mettre en œuvre la politique de sécurité informatique de SCITI ;
- Superviser les audits de sécurité, les tests d'intrusion et les analyses de vulnérabilité ;
- Assurer la configuration des équipements et des systèmes ;
- Assurer la conformité aux normes, standards et réglementations ;
- Elaborer et suivre les plans de continuité d'activité et de reprise après sinistre ;
- Identifier, évaluer et réduire les risques informatiques ;
- Coordonner les prestataires, fournisseurs et partenaires technologiques ;
- Participer à la définition du budget infrastructures numériques et informatiques et en assurer le suivi ;
- Conseiller la direction sur les choix technologiques et stratégiques ;
- Assurer une veille technologique et réglementaire ;

- Proposer des solutions innovantes pour améliorer la sécurité, l'efficacité opérationnelle et la résilience du système d'information de SCITI ;
- Former et sensibiliser les utilisateurs aux bonnes pratiques de sécurité informatique ;
- Développer une culture de cybersécurité au sein de SCITI ;
- Accompagner la transformation numérique de SCITI ;
- Superviser les opérations de maintenance préventive et corrective.

Formation et expériences professionnelles minimales

- Être titulaire d'un diplôme d'ingénieur ou de Master (BAC+5) en Informatique, réseaux et télécommunications, cybersécurité, système d'information ou tout autre domaine connexe ;
- Avoir une excellente connaissance aussi bien théorique que pratique en administration réseaux, sécurité informatique et gestion des infrastructures complexes ;
- Avoir au minimum 05 années d'expériences professionnelles prouvées en gestion des infrastructures numériques et sécurité informatique d'une université ou d'une grande organisation ;
- Avoir une solide connaissance des réseaux informatiques (TCP/IP, VLAN, routage, Wi-Fi entreprise, etc.), des systèmes (Linux, Windows Server, etc.), du Cloud (AWS, Azure, Google Cloud, etc.), en virtualisation (VMware, Hyper-V, Proxmox, etc.) et en sécurité informatique ;
- Avoir une excellente capacité rédactionnelle en français, ainsi qu'une bonne aptitude pour la communication et le travail sous pression ;
- Avoir une bonne capacité d'analyse, de synthèse et de résolution pratiques des éventuels problèmes liés aux infrastructures numériques et sécurité informatique.

Qualités personnelles et aptitudes professionnelles

- Solide sens du leadership, de la planification, de l'organisation et de la rigueur, avec un niveau élevé d'exigence et de recherche de l'excellence ;
- Intègre, honnête et attaché(e) aux valeurs éthiques ;
- Aisance relationnelle et capacité à communiquer avec des interlocuteurs de tous profils ;
- Capacité à faire preuve d'agilité et de réactivité face aux imprévus ;
- Bonne aptitude à l'écoute, à l'adaptation, de tempérance et à la compréhension des enjeux ;
- Goût marqué pour le travail collaboratif et excellente qualité relationnelle ;
- Autonome, curieux(se), force de proposition, capable d'intervenir sur des missions variées ;
- Capacité à gérer le stress de manière constructive.

Atouts complémentaires

Détenir des certifications ou des preuves de connaissances en :

- ISO 27001 Lead Implementer / Lead Auditor ;
- CISSP, CISM, CEH ;
- ITIL foundation / Expert ;
- CCNA / CCNP ;
- Certifications Cloud (AWS, Azure etc.).

Dossier à fournir

- Une lettre de motivation adressée au Directeur général de SCITI ;
- Un CV actualisé avec noms et contacts de trois (03) personnes références ;
- Une copie légalisée du diplôme ;
- Les preuves des expériences citées dans le CV.

Merci de postuler par mail en envoyant votre dossier de candidature à l'adresse suivante : recrutement.sciti@sciti.edu.bj avec pour objet du mail, la mention : « **Candidature pour le poste de Responsable des Infrastructures Numériques et Sécurité Informatique** ». Les candidatures doivent être déposées **au plus tard le 26 février 2026**. Un accusé confirmera la réception de votre candidature (tout dossier non conforme ne sera pas étudié).

Postulez dès maintenant !

Les candidatures féminines sont fortement encouragées ;

- Durée du mandat : deux (02) renouvelables suivant une évaluation satisfaisante ;
- Contrat CDD ;
- Rémunération : selon le profil des candidatures ;
- Seul(e)s les candidat(e)s présélectionné(e)s seront contacté(e)s ;
- SCITI se réserve le droit de ne pas donner une suite à cet avis de recrutement, sans aucun préjudice.