BANQUE D'INVESTISSEMENT ET DE DEVELOPPEMENT DE LA CEDEAO
ECOWAS BANK FOR INVESTMENT AND DEVELOPMENT
BANCO DE INVESTIMENTO E DE DESENVOLVIMENTO DA CEDEAO

**La Banque d'investissement et de développement de la CEDEAO (BIDC), basée à Lomé, en République Togolaise, recherche des candidats qualifiés, citoyens de la Communauté, pour pourvoir au poste suivant dans la catégorie professionnelle.**

| Poste | Principales fonctions et responsabilités | Qualifications, expérience et compétences requises |
|---|---|---|
| **RESPONSABLE DE LA SÉCURITÉ DU SYSTEME D'INFORMATION (RSSI)**<br><br>**Grade P3-1)** | **Description du poste**<br><br>Sous la supervision du Directeur du département de la gestion des risques de la Banque, le titulaire du poste aura pour mission de définir et de maintenir la vision, la stratégie et les programmes de l'institution afin d'assurer une protection adéquate des actifs et des technologies de l'information. À ce titre, il fournira des orientations sur les obligations de conformité, aidera la banque à concevoir des approches fiables de gestion des risques et sera le fer de lance d'initiatives visant à protéger les données, la propriété intellectuelle et le cadre technologique de la Banque contre les risques internes et externes. Le titulaire du poste joue un rôle central en matière de suivi du respect des normes réglementaires et des critères de référence du secteur, et veille à encourager une culture de la sécurité dans l'ensemble de la Banque.<br><br>**Tâches**<br><br>**1. Planification et vision stratégiques :**<br>• Élaborer et mettre en œuvre la stratégie et la feuille de route de la Banque en matière de sécurité de | • Titulaire d'un master délivré par une université reconnue, en informatique, en technologie de l'information ou dans un domaine connexe ;<br><br>• Expérience avérée (au moins sept ans) dans des postes de direction dans le domaine de la cybersécurité, avec des expériences couronnées de succès dans la mise en œuvre et la gestion de programmes de cybersécurité.<br><br>• Bonne compréhension des principes, des cadres et des technologies de cybersécurité, y compris, mais sans s'y limiter, NIST, ISO, contrôles CIS, SIEM, IDS/IPS, DLP, chiffrement et sécurité du cloud.<br><br>• Excellentes compétences en matière de leadership, de communication et de relations interpersonnelles, avec une capacité à collaborer efficacement entre les départements |

| | | |
|---|---|---|
| | l'information en mettant en place une architecture et des politiques de sécurité fondées sur les besoins opérationnels, l'évaluation des risques et les exigences réglementaires.<br>• Définir des politiques, des normes et des procédures de sécurité alignées sur les objectifs opérationnels et les meilleures pratiques sectorielles.<br>• Évaluer les menaces et les tendances émergentes et adapter les stratégies de sécurité en conséquence.<br><br>**2. Gestion des risques :**<br>• Identifier, évaluer et hiérarchiser les risques de sécurité dans l'ensemble de l'organisation.<br>• Développer et maintenir un cadre de gestion des risques afin d'atténuer les risques de manière efficace.<br>• Conduire le programme de gestion des risques grâce à une planification, au développement, à la coordination et à la mise en œuvre de la reprise après sinistre des technologies de l'information et la planification de la continuité des activités.<br><br>**3. Opérations de sécurité :**<br>• Superviser la conception, la mise en œuvre et la maintenance des contrôles, des technologies et des processus de sécurité. | et à avoir un impact sur les parties prenantes à tous les niveaux de l'institution.<br>• Les certifications professionnelles telles que CISSP, CISM, CISA ou équivalentes seraient un atout.<br>• Expérience dans des secteurs réglementés (par exemple, la santé, la finance, la fonction publique) et connaissance des réglementations applicables (par exemple, HIPAA, RGPD, SOX) est un atout.<br>• Solides compétences en matière d'analyse et de résolution de problèmes, avec la capacité de prendre des décisions fondées sur le risque dans un environnement en évolution rapide.<br>• Capacité avérée à diriger et à développer une équipe diversifiée de professionnels de la cybersécurité. |

| | | |
|---|---|---|
| | • Assurer la coordination des activités de réponse aux incidents et diriger les efforts visant à atténuer les incidents de sécurité.<br>• Effectuer régulièrement des évaluations et des audits de sécurité pour garantir la conformité et l'efficacité.<br><br>**4. Conformité et gouvernance :**<br>• Assurer le respect des lois, des réglementations et des normes pertinentes du secteur (par exemple, RGPD, HIPAA, ISO 27001).<br>• Créer et maintenir des structures de gouvernance en appui à une gestion efficace de la sécurité de l'information.<br>• Prendre contact avec les auditeurs internes et externes et les régulateurs lors de l'examen des résultats des enquêtes spéciales, des audits internes, des travaux de recherche, des prévisions et des exercices de modélisation, afin de fournir des orientations et des conseils.<br><br>**5. Sensibilisation et formation à la sécurité :**<br>• Élaborer et mettre en œuvre des programmes de sensibilisation à la sécurité afin d'informer les employés de leur rôle et de leurs responsabilités dans le maintien de la sécurité. | |

| | | |
|---|---|---|
| | • Former le personnel informatique et les autres parties prenantes concernées aux meilleures pratiques en matière de sécurité.<br>• Exécuter toutes les autres tâches à lui confiées par le directeur du département et la haute direction. | |

❖ **AUTRES EXIGENCES**

- Être ressortissant de l'un des États membres de la CEDEAO ;
- Être âgé de 45 ans au plus à la date du recrutement ;
- Avoir une bonne maîtrise des outils informatiques (Word, Excel, Access et Power Point).

❖ **LE DOSSIER DE CANDIDATURE DOIT COMPORTER LES PIECES SUIVANTES :**

- Un curriculum vitae détaillé ;
- Une lettre de motivation ;
- Copies des diplômes académiques et certificats professionnels ;
- Une copie de la carte nationale d'identité ou du passeport ;
- Une copie de l'acte de naissance.

Les candidats intéressés doivent soumettre leur candidature par courriel à recrutbidc@bidc-ebid.org, au plus tard le 30 août 2024, avec pour objet « PROGRAMME DE RECRUTEMENT 2024 ».

**N.B**.: Seuls les candidats présélectionnés seront invités à un entretien. La BIDC se réserve le droit de retirer la vacance de poste notifiée ou de proposer un poste à un grade inférieur. Les candidatures féminines sont vivement souhaitées.