ASIN AGENCE DES SYSTÈMES D'INFORMATION ET DU NUMÉRIQUE
RÉPUBLIQUE DU BÉNIN

01 BP 8088 Cotonou
+ 229 21 31 10 13
contact@asin.bj

AVIS DE RECRUTEMENT

Type de contrat : CDI **Disponibilité immédiate**

Ingénieur(e) sécurité en Gouvernance, Risque et Conformité	
Employeur	Agence des Systèmes d'Information et du Numérique (ASIN)
Direction	Pôle Sécurité Numérique
Superviseur Hiérarchique	Chef Département Confiance et Conformité / Responsable conformité
Lieu d'affectation	Cotonou
Candidature	Postulez en ligne sur le portail national des services publics https://service-public.bj/public/services/service/PS01334 en joignant CV détaillé, lettre de motivation, références et attestations, au plus tard le 15 septembre 2023 à 18h00 (heure de Cotonou).

INFORMATIONS GENERALES

La République du Bénin a lancé un programme ambitieux de développement de l'économie numérique visant à positionner le pays comme la référence en matière de plateforme de services numériques de l'Afrique de l'Ouest et de faire des Technologies de l'Information et de la Communication le principal levier de son développement socio-économique.

L'Agence des Systèmes d'Information et du Numérique (ASIN) est une agence gouvernementale sous la double tutelle du Ministère de l'Économie et des Finances et du Ministère du Numérique et de la Digitalisation, chargée d'assurer la mise en œuvre opérationnelle des programmes et projets entrant dans le cadre des stratégies de développement des services et systèmes d'information sécurisés au Bénin.

MISSION & RESPONSABILITES

- Rattaché directement au Responsable de la conformité du Pôle Sécurité Numérique, l'ingénieur(e) GRC a pour mission principale d'assurer la conformité aux politiques de sécurité et de protection, aux normes et aux meilleures pratiques en matière de Sécurité Numérique. Il participe activement aux activités relevant du Laboratoire des Opérations de Conformité dans le cadre de l'atteinte des objectifs qui lui sont assignés.

ACTIVITES ET TACHES

- Participer à la définition, à l'élaboration, à la mise en œuvre et au contrôle du plan d'inspection de Sécurité Numérique.
- Réaliser les audits de conformité, présenter les analyses d'écarts au regard des référentiels en vigueur, exposer les conclusions aux structures auditées et aux équipes de contrôle.
- Participer à l'analyse des risques, à la mise en œuvre et au suivi des plans de traitement des risques en Sécurité Numérique.
- Contribuer à l'élaboration, à la mise en œuvre, au suivi, à la mise à jour et à l'amélioration des documents de gouvernance de sécurité et des cadres de références (stratégie de Sécurité Numérique, politiques de sécurité, politiques de protection, documents de spécification).
- Contribuer à l'élaboration des processus et des procédures concernant les activités de sécurité de l'information.
- Participer à la définition et à la gestion des KPI de sécurité.
- Réaliser en autonomie des diagnostics de sécurité des fonctions informatiques et des processus métiers informatisés.
- Mener des contrôles permanents et/ou périodiques de sécurité, notamment sur la base de revues documentaires, de collecte de preuves et des rapports des outils de contrôle de

01 BP 8088 Cotonou
+ 229 21 31 10 13
contact@asin.bj

conformité.
- Participer au programme de sensibilisation/formation en sécurité de l'information.
- Exécuter toutes autres tâches liées à la Sécurité Numérique assignées par le supérieur hiérarchique.

FORMATION, EXPÉRIENCES ET LANGUES

Formation

- Être titulaire au moins d'un Master (BAC + 5) portant sur le « management des SI » ou « en Ingénierie Informatique », avoir au moins l'une des certifications suivantes serait un atout :
  - CISA,
  - ISO 27001- Lead Auditor,
  - ISO 27001- Lead Implementer.

Expérience professionnelle

- Une expérience de 3 à 5 ans minimum dans le domaine de la Sécurité Numérique dont au moins 1 à 2 ans en audit, gouvernance, risque et conformité de la Sécurité Numérique
- Une bonne connaissance des outils, normes, référentiels et standards de l'industrie : ISO 27001, ISO 27002, ISO 20000, Top10 OWASP
- Une bonne connaissance des cadres nationaux : Stratégie nationale de sécurité numérique, Politique de sécurité des systèmes d'information de l'état, Politique de protection des infrastructures critiques
- Une bonne connaissance du Code du Numérique
- Une bonne expérience de la gouvernance de la sécurité Numérique
- Une bonne compréhension des dispositifs de contrôle et de gestion des risques

Langues

- Une excellente maîtrise de la langue française aussi bien à l'oral qu'à l'écrit est exigée.
- Une bonne maîtrise de l'anglais à l'oral et à l'écrit est un atout.

ETHIQUE ET APTITUDES

- Être passionné de la sécurité des technologies de l'information, avoir la volonté d'apprendre et être capable de travailler en équipe pour l'atteinte des objectifs.
- Avoir un bon sens de l'analyse et une bonne capacité de traitement des urgences.
- Avoir une excellente capacité rédactionnelle.
- Avoir l'esprit de confidentialité et d'auto-formation.
- Avoir une excellente capacité de communication.
- Avoir une bonne capacité de gestion du temps et des priorités.
- Avoir un bon sens de la synthèse.
- Être de bonne moralité.