



AVIS DE RECRUTEMENT

ASSI19092019-08

INGÉNIEUR EN CYBER-SÉCURITÉ

Date de démarrage du poste : Immédiatement

Type de contrat : CDI

Employeur : Agence de Services et Systèmes d'Information- ASSI
(Présidence de la République)

Lieu de travail : Agence des Services et Systèmes d'Information- En face
du Trésor Public

FICHE DE POSTE	
Superviseur Global	Direction Générale
Supérieur hiérarchique	Direction des Opérations
Relation fonctionnelle	Directeurs, gestionnaires de projets, autres collaborateurs de ASSI, autres entités gouvernementales (agence, instituts, ministères), partenaires techniques
Lieu d'affectation	Cotonou
Informations générales	
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 en Afrique de l'Ouest à l'horizon 2021 et de	

faire des Technologies de l'Information et de la Communication le principal levier de son développement.

L'Agence des Services et Systèmes d'Information (ASSI) est une agence gouvernementale sous la tutelle de la Présidence de la République et sous la supervision du Ministère de l'Economie et de la Communication, chargée d'assurer la mise en œuvre opérationnelle des programmes et projets du Gouvernement du Bénin, entrants dans le cadre de ses stratégies de développement des services et systèmes d'information sécurisés. A ce titre, elle est chargée de :

- l'assistance stratégique, méthodologique et opérationnelle de toutes les structures gouvernementales et des opérations d'importance Vitale (OIV) ;
- la conception et l'implémentation des services et systèmes d'information répondant aux priorités stratégiques nationales ;
- l'assurance de la cohérence technique, applicative et financière des services et systèmes d'information nationaux ;
- l'hébergement et l'accès sécurisé aux données ;

la promotion des technologies, des systèmes et des savoir-faire contribuant au développement de la confiance numérique.

Objectif et portée de la mission du poste

Sous la supervision directe de la Direction des Opérations, définir et mettre en œuvre la Politique de Sécurité des Systèmes d'Information de l'Agence au sein des différentes directions et projets qu'elles mènent.

Principales Responsabilités

Sous la supervision directe du Directeur des Opérations, les principales responsabilités de l'Ingénieur en cyber-sécurité informatique se résument aux tâches suivantes :

Identification des risques et définition de la politique de sécurité

- Réaliser des audits du système de sécurité dans le périmètre défini par la Direction des Opérations et plus particulièrement sur les projets menés par l'Agence.
- Analyser les risques et les dysfonctionnements, les marges d'amélioration des systèmes de sécurité de l'Agence et des projets menés par l'Agence.
- Établir et tenir à jour la cartographie des menaces.
- Définir et faire évoluer la politique de sécurité des systèmes d'information de l'Agence (PSSI).
- Définir et implémenter les différentes procédures relatives à la sécurité informatique sur les projets menés par l'Agence.
- Etablir un plan de prévention des risques informatiques et un plan de continuité d'activité (PCA) (ou plan de maintien en conditions opérationnelles du S.I.).

- 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...).
- Choisir les dispositifs techniques les plus appropriés aux besoins de l'Agence (firewall, programmes de back up, cryptographie, authentification...).
- Participer à la définition et au contrôle de la gestion des habilitations.
- Participer au comité des risques.
- Assurer un rôle de veille en matière de cyber-sécurité, de conseil, d'assistance, d'information, de formation et d'alerte sur les risques de malveillance et d'intrusion.

Mise en œuvre et suivi du dispositif de sécurité

- Faire appliquer les normes et standards de sécurité en vigueur.
- Mettre en place les méthodes et outils de sécurité adaptés, et accompagner leur implémentation auprès des utilisateurs.
- Elaborer et suivre des tableaux de bord des incidents sécurités.
- Superviser ou auditer les programmes de sauvegarde (back-up).
- Gérer les incidents sécurités 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...), et formaliser 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.

Formation, expériences et langues

Education

- Être titulaire au moins d'un Master, d'un diplôme d'une Grande École d'Ingénieur ou toute autre formation de niveau équivalent dans les domaines des systèmes d'information.
- Avoir fait un BAC scientifique.

Expériences professionnelles

- Une bonne expérience en audit systèmes et analyses de risque

- Une bonne expérience en établissement de procédures et politiques de sécurité ou le cas échéant leur mise en œuvre
- Une bonne expérience en évaluation des vulnérabilités et Tests de pénétration.
- Bonne connaissance des différents systèmes d'exploitation (Microsoft Windows Server, MS Cluster, LINUX et Redhat Cluster)
- Bonne connaissances des technologies de virtualisation (Vmware Esxi, Microsoft HyperV, Oracle Virtual box, etc...)
- Bonne connaissance des protocoles réseaux majeurs, leurs forces et faiblesses.
- Une bonne expérience de l'exploitation des systèmes de sécurité (Firewall, Web Application Firewall, IDS, IPS, SIEM, et système de control d'accès).
- Certifications souhaitées : CISSP, CISA, CEH, CHFI, etc....

Langue

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

Ethique, Management et Leadership

- Excellente communication et capacité à travailler en équipe pour atteindre les objectifs organisationnels ;
- Disposer d'une forte aptitude d'organisation, d'une maturité de jugement et de comportement ;
- Avoir l'aptitude à établir et maintenir des relations de travail efficaces avec les collègues ;
- Démontrer d'un esprit d'ouverture face au changement et avoir des aptitudes à gérer des dossiers complexes ;
- Disposer des aptitudes de maîtrise de soi et être de bonne humeur, même sous pression ;
- Avoir un sens aigu de l'éthique et de l'intégrité dans le traitement de tous les dossiers à lui confier ;
- Etre disposé à effectuer des travaux de nature confidentielle, à traiter un grand volume de travail et à respecter les délais ;
- Avoir une capacité à se concentrer sur les résultats attendus et à répondre positivement aux diverses préoccupations dans son domaine de compétence ;
- avoir d'excellentes capacités d'analyse, de raisonnement, de prise de décision et de rédaction ;



- Travailler avec une énergie et une attitude positive et constructive ;
- Avoir le goût d'anticipation ;
- Maîtriser les outils du numérique (l'outil informatique et les technologies de la communication).

NB : Les dossiers de candidature doivent comporter les pièces suivantes :

- 1- Lettre de motivation ;
- 2- Un Curriculum Vitae détaillé ;
- 3- Copies des diplômes ;
- 4- Extrait d'acte de naissance ;
- 5- Copie de la carte d'identité ou du passeport en cours de validité ;
- 6- Casier Judiciaire daté de moins de trois (3) mois.

Tous les dossiers de candidature doivent parvenir par courrier électronique à l'adresse: **assi.rh@presidence.bj** au plus tard le **30 sept 2019 à 17H30** (Heure de Cotonou, Benin).

Pour plus d'information, visitez notre site internet suivant l'adresse: <https://www.assi.bj>