



AVIS DE RECRUTEMENT

Type de contrat : **CDD 02 ans**

Disponibilité immédiate

INGENIEUR RESEAU ET SECURITE SENIOR	
Employeur	Agence des Systèmes d'Information et du Numérique (ASIN)
Superviseur Hiérarchique	Responsable Service Support et Assistance
Entité	Service Support et Assistance
Relation fonctionnelle	Tous directeurs et autres collaborateurs de l'Agence
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, lettre de motivation, références et attestations, au plus tard le 24 mars 2026 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 en 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.	
OBJECTIFS ET PORTEE DE LA MISSION DU POSTE	
• Apporter son expertise aux sectoriels, et institutions étatiques dans l'exploitation des environnements Réseaux & sécurité • Définir et mettre en œuvre la sécurité relative au périmètre Réseaux et sécurité • Traitement des demandes de modifications Réseaux, les supports relatifs au périmètre réseau et sécurité, en assurant la qualité de services ainsi que le maintien en condition opérationnelle. • Participer à l'audit réseaux et sécurité	
PRINCIPALES RESPONSABILITES	
• Définition, actualisation et mise en place d'une approche formelle pour implémenter des solutions nécessaires au développement et à l'exploitation de l'architecture des SI (transversaux et sectoriels) ; • Évolution des systèmes (sectoriels et/ou transversaux) des Administrations à l'aune de l'ambition de transformation numérique de l'Etat béninois ; • Identification des modifications nécessaires et des composants concernés : matériels, logiciels ou la plateforme technologique ; • Prise en compte de l'interopérabilité, l'adaptabilité, la facilité d'utilisation et la sécurité. • Concevoir et mettre en place des architectures réseau sécurisées.	



- Administrer et maintenir les équipements réseau (routeurs, commutateurs, pare-feu, WAF, plateforme de sécurité de messagerie, PAM etc.).
- Assurer la surveillance proactive des réseaux pour détecter et résoudre les problèmes de performance et de sécurité.
- Mettre en œuvre et gérer les politiques de sécurité réseau, incluant la gestion des accès et des identités.
- Effectuer des audits de sécurité réguliers et des tests de pénétration pour identifier les vulnérabilités.
- Répondre aux incidents de sécurité et coordonner les actions de remédiation.
- Documenter les configurations réseau, les procédures de sécurité et les incidents de sécurité.
- Former et sensibiliser le personnel aux bonnes pratiques de sécurité informatique.
- ✓ **Installation et tests**
 - Installation et configuration des commutateurs, routeurs, firewall, WAF selon les cahiers de charges validés ;
 - Respect des procédures d'installation, de connexion... des matériels et des logiciels ;
 - Installation des mises à jour ;
 - Tests des équipements réseaux et sécurité.
- ✓ **Exploitation**
 - Gestion de l'exploitation sur incident ;
 - Diagnostic des causes de dysfonctionnements, proposition des corrections et solutions de rechange ;
 - Information des équipes sur les évolutions techniques du système ;
 - Traitement des incidents sur les réseaux informatiques ;
 - Elaboration de politiques, procédures et guides
 - S'assurer du monitoring des ressources réseaux et sécurité ;
 - Support niveau 3 aux sectoriels.
- ✓ **Administration et sécurité**
 - Contrôle du respect de la sécurité d'accès aux locaux techniques et signale les anomalies
 - Gestion et maintien des infrastructures techniques
 - Veille technologique et évaluation prospective technologique ;
 - Exploitation et administration du réseau sur son périmètre ;
 - Contrôle de la conformité des équipements avec les référentiels.
- ✓ **Participation aux études et développement**
 - Conduite des études pour la définition des systèmes en fonction des besoins ;
 - Intervention dans le choix des fournisseurs

FORMATION, EXPÉRIENCES, ET LANGUES

FORMATION

Être titulaire au minimum d'un Master (BAC + 4/5), d'un diplôme d'une Grande École d'Ingénieur ou toute autre formation de niveau équivalent en informatique avec (si possible) une spécialité en architecture des réseaux, et une bonne maîtrise des techniques et méthodes d'analyse.



EXPÉRIENCE

Avoir au minimum cinq (05) années d'expérience en administration de Réseaux / sécurité et disposer des compétences dans les domaines suivants :

- Organisation, rigueur et réactivité, sens du service client, facilité et rapidité d'adaptation aux évolutions techniques, facilité de communication (orale et écrite), d'écoute et d'expression, facilité à résoudre des situations complexes, prise de décision, gestion de projets ;
- Capacité à entretenir des relations avec plusieurs partenaires (Vendeur, Opérateurs), concernant les aspects projets et opérationnels ;
- Capacité de synthèse écrite sur des sujets techniques complexes.

CONNAISSANCES ET COMPETENCES TECHNIQUES

- Forte expertise & expérience des réseaux TCP/IP, LAN/WAN, DMVPN, SD-WAN, VPN/Solutions SSL, CISCO commutateurs, CISCO/FORTIGATE Firewalls ;
- Equipements HUAWEI, PAM/IAM, WAF, sécurité messagerie
- Forte expertise sur les protocoles de routage OSPF, EIGRP, BGP ;
- Forte expertise & expérience dans les aspects diagnostics pour les équipements de type routeur, commutateur et firewall de la marque CISCO/FORTIGATE ;
- Forte expertise & expérience de l'administration réseau et de leur usage (Infoblox, IPAM, ACE, Wireshark), des solutions de sécurité, et des bonnes pratiques dans l'industrie.
- Certification(s) en réseaux et sécurité (CCNA, CCNP, NSE4, NSE6, etc.) est un atout
- Connaissance des normes ISO 27001 /2 est un atout

LANGUE

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

ETHIQUE, MANAGEMENT ET LEADERSHIP

- Une excellente capacité à travailler de manière autonome et à s'adapter aux différents contextes culturels et professionnels
- Une capacité à travailler en équipe pour l'atteinte des objectifs organisationnels
- Une capacité à gérer des projets complexes et bonne gestion du temps et des priorités
- Un esprit de synthèse et d'analyse et bonne communication orale et écrite
- La rigueur, l'éthique et de l'intégrité dans le traitement de tous les sujets sous sa responsabilité
- Une aptitude à effectuer des travaux de nature confidentielle, à traiter un grand volume de travail et à respecter les délais.