



## AVIS DE RECRUTEMENT

Type de contrat : CDD 2 ans

Disponibilité immédiate

| PKI SECURITY COMPLIANCE OFFICER (SCO) (H/F) |                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Employeur                                   | Agence des Systèmes d'Information et du Numérique (ASIN)                                                                                                                                                                                                                                                                                  |
| Superviseur Hiérarchique                    | Responsable Département Confiance et Conformité                                                                                                                                                                                                                                                                                           |
| Direction                                   | Pôle Sécurité Numérique                                                                                                                                                                                                                                                                                                                   |
| Relation fonctionnelle                      | Tous directeurs et autres collaborateurs                                                                                                                                                                                                                                                                                                  |
| Lieu d'affectation                          | Cotonou - BENIN                                                                                                                                                                                                                                                                                                                           |
| Candidature                                 | Postulez en ligne sur le portail national des services publics <a href="https://service-public.bj/public/services/service/PS01334">https://service-public.bj/public/services/service/PS01334</a> , en joignant CV actualisé, lettre de motivation, références et attestations, au plus tard le 23 octobre 2026 à 20h00 (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 de la Transformation Digitale et de l'Innovation, 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. À ce titre, elle conçoit, déploie et maintient les plateformes nationales de services publics numériques, les référentiels et les briques d'interopérabilité qui permettent aux administrations d'échanger leurs données et de servir les usagers de manière simple, sécurisée et continue.

### CONTEXTE ET PORTÉE DE LA MISSION DU POSTE

Le/La Security Compliance Officer (Responsable de la conformité en matière de sécurité PKI) est chargé(e) de définir, piloter et contrôler la conformité et la sécurité des infrastructures PKI de l'organisation. Il/Elle est ainsi garant(e) du respect des exigences, normes et bonnes pratiques en matière de sécurité et de confiance de l'infrastructure PKI.

### PRINCIPALES RESPONSABILITÉS

- Examiner, maintenir et archiver les journaux d'audit de l'infrastructure PKI ;
- Administrer et maintenir les solutions de gestion des événements et informations de sécurité (SIEM) ;
- Effectuer ou superviser les audits internes de conformité afin de vérifier que les opérations respectent les pratiques de certification ;
- Définir et piloter le programme d'audit interne et préparer les audits et évaluations externes (ETSI EN 319 401/411, WebTrust for CA ou référentiel applicable) ;
- Assurer le suivi des constats d'audit et des plans d'actions correctives jusqu'à leur clôture ;
- Contribuer à la rédaction et à la mise à jour de la politique de certification (CP) et de la déclaration des pratiques de certification (CPS) selon le cadre RFC 3647 ;
- Contribuer à l'analyse de risques selon une méthodologie reconnue (ISO/IEC 27005, EBIOS RM) ;
- Organiser les revues périodiques des habilitations, de la séparation des rôles et du double contrôle ;
- Vérifier la conformité aux exigences légales et réglementaires applicables en matière de signature électronique et de certification ;
- Produire le reporting de conformité à destination de la hiérarchie et des instances de gouvernance ;
- Assurer la veille réglementaire et normative ;



- Exécuter toutes autres tâches assignées par le superviseur.

## FORMATION, CONNAISSANCES, EXPÉRIENCES ET LANGUES

### FORMATION & CERTIFICATIONS

- Être titulaire au moins d'un Master (BAC + 5) en Sécurité des systèmes d'information, en Audit ou toute autre formation de niveau équivalent.
- Être certifié(e) ISO/IEC 27001 Lead Implementer et EBIOS RM.

### CONNAISSANCES & COMPÉTENCES

- Bonne connaissance des infrastructures à clés publiques, du cadre RFC 3647 (structure CP/CPS) et de la norme X.509 ;
- Bonne connaissance des référentiels d'évaluation des autorités de certification (ETSI EN 319 401/411, WebTrust for CA) ;
- Bonne maîtrise des normes ISO/IEC 27001, et des méthodologies d'analyse de risques ;
- Bonne connaissance du cadre juridique de la signature électronique et de la protection des données personnelles ;
- Bonne connaissance des services de confiance électronique, du cadre EIDAS ;
- Maîtrise des techniques d'audit et de la rédaction de rapports de conformité ;
- Aptitude à respecter des processus rigoureux et des standards de sécurité.

### EXPÉRIENCES

Avoir au minimum cinq (05) années d'expérience dans l'audit, la conformité ou la gouvernance de la sécurité des systèmes d'information, idéalement en environnement PKI.

### LANGUES

Une excellente maîtrise de la langue française aussi bien à l'oral qu'à l'écrit est exigée et une bonne maîtrise de l'anglais dans un contexte professionnel est requise.

## ETHIQUE, MANAGEMENT ET LEADERSHIP

- Sens élevé de la rigueur, de l'objectivité et de l'indépendance dans la conduite des contrôles
- Sens de l'éthique, de l'intégrité et de la confidentialité dans le traitement de tous les sujets sous sa responsabilité
- Esprit de synthèse et d'analyse, capacité à formaliser des constats et des recommandations
- Capacité à travailler en équipe et à communiquer avec l'ensemble des parties prenantes
- Bonne gestion du temps, des priorités et capacité à traiter les urgences
- Volonté d'auto-formation et d'actualisation continue des connaissances.

## USAGE RESPONSABLE DE L'INTELLIGENCE ARTIFICIELLE

- N'utiliser que les outils d'IA explicitement autorisés par l'ASIN et dans les conditions définies
- Ne soumettre aucune donnée d'incident, donnée à caractère personnel, preuve numérique ou information classifiée à un service d'IA externe non autorisé
- Soumettre à revue humaine toute analyse, tout code ou toute règle de détection produits avec l'assistance de l'IA, et en assumer la responsabilité technique
- Tracer l'usage de l'IA dans les travaux d'investigation et ne jamais présenter une sortie de modèle comme un fait observé.

## CADRE LÉGAL ET RÈGLES D'ENGAGEMENT

- Aucune action offensive ne peut être engagée sans mandat écrit préalable définissant le périmètre, les adresses et systèmes concernés, les fenêtres d'intervention, les actions interdites et les points de contact d'urgence
- Interdiction absolue de toute action hors périmètre, de toute exfiltration de données réelles au-delà de la preuve minimale nécessaire, et de toute action susceptible de dégrader un service en



production sans autorisation explicite

- Journalisation exhaustive et horodatée de toutes les actions menées, conservée et communicable à l'entité testée et à la hiérarchie
- Destruction sécurisée des données collectées à l'issue de la mission, selon la procédure de rétention définie
- Notification immédiate à la hiérarchie et à l'entité en cas de découverte d'une compromission préexistante, avec bascule vers le processus de réponse à incident
- Interdiction d'utiliser les compétences, les accès, l'outillage ou les informations obtenus dans le cadre du poste à toute autre fin ; engagement de non-divulgation permanent, y compris après la fin du contrat
- Poste soumis à une enquête de moralité approfondie et à la production d'un extrait de casier judiciaire.

#### CONDITIONS PARTICULIERES D'EXERCICE

- Interventions possibles en dehors des heures ouvrables en cas de crise ou afin de limiter l'impact sur les services en production, et déplacements sur le territoire national.