



AVIS DE RECRUTEMENT

Type de contrat : CDD 2 ans

Disponibilité immédiate

ARCHITECTE SECURITE (H/F)	
Employeur	Agence des Systèmes d'Information et du Numérique (ASIN)
Direction	Pôle Sécurité Numérique
Superviseur Hiérarchique	Responsable Département Confiance et Conformité / Responsable conformité
Relation fonctionnelle	Tous directeurs et autres collaborateurs
Lieu d'affectation	Cotonou - BENIN
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 23 octobre 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 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.

OBJECTIF ET PORTEE DE LA MISSION

L'Architecte Sécurité a pour mission principale de définir, formaliser et accompagner la mise en œuvre de systèmes d'information, de plateformes numériques et de projets critiques, en cohérence avec la stratégie de sécurité nationale ; les exigences de gouvernance, de gestion des risques, de conformité et de résilience de l'Agence des Systèmes d'Information et du Numérique (ASIN) ; les normes et les meilleures pratiques en matière de conception sécurisée et de sécurité numérique. Il/Elle conçoit, élabore et surveille la mise en œuvre des structures de sécurité des réseaux et des systèmes d'information pour une organisation, s'assure que les exigences de sécurité sont prises en compte adéquatement dans tous les aspects de l'infrastructure et que le système soutient les processus organisationnels.

PRINCIPALES RESPONSABILITES

- Définir les principes, modèles et standards d'architecture de sécurité applicables aux projets numériques et aux systèmes d'information
- Elaborer les dossiers d'architecture de sécurité pour tous les projets
- Contribuer à l'analyse des besoins de sécurité dès les phases de conception des projets
- Évaluer les architectures techniques proposées et formuler des recommandations de sécurité adaptées.
- Accompagner les équipes projets et techniques dans l'intégration des exigences de sécurité.
- Participer à l'identification, l'évaluation et la réduction des risques liés aux architectures applicatives, réseaux, cloud, IA et infrastructures.



- Produire ou mettre à jour les référentiels, dossiers d'architecture, avis de sécurité, feuilles de route et rapports associés.
- Examiner la conformité des livrables finaux des projets par rapport à l'architecture sécurité validée et signaler les écarts.
- Rendre compte à la hiérarchie de l'état d'avancement, des risques identifiés et des arbitrages nécessaires.
- Exécuter toutes autres tâches liées à la Sécurité Numérique assignées par le supérieur hiérarchique.
- Contribuer à l'élaboration, la mise en œuvre, le suivi, la mise à jour et 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).

FORMATION, CONNAISSANCES, EXPÉRIENCES ET LANGUES

Formation

- Être titulaire au moins d'un Master (BAC + 5) portant sur la cybersécurité, sécurité des systèmes d'information, architecture des systèmes d'information, réseaux et télécommunications, informatique ou tout autre domaine équivalent ;
- Détenir une ou plusieurs certifications de sécurité ou d'architecture serait un atout : CISSP, CISM, CISA, ISO 27005, CRISC, TOGAF, SABSA ou équivalent.

Connaissances

De solides connaissances sont attendues dans les domaines suivants :

- Plans stratégiques et d'activités
- Méthodes d'évaluations des menaces et des risques
- Architectures de système
- Outils et applications de mise en correspondance des TI
- Processus et procédures de gestion des incidents, des systèmes de gestion des événements et des incidents de sécurité ou systèmes et réseaux de signalement des incidents
- Processus et politiques de gestion des incidents de cybersécurité
- Lois relatives à la sécurité et au respect de la vie privée
- Infrastructure de sécurité organisationnelle et systèmes de production de rapports
- Connaissance des référentiels et bonnes pratiques de sécurité, notamment ISO/IEC 27001, ISO/IEC 27005, NIST, CIS Controls, Zéro Trust ou équivalents ;
- Cadres nationaux : Stratégie nationale de sécurité numérique, Politique de sécurité des systèmes d'information de l'état, Politique de protection des infrastructures critiques ;
- Code du Numérique

Compétences Techniques

- Besoins opérationnels en matière de sécurité
- Capacité à analyser les risques d'architecture et à formuler des recommandations pragmatiques et documentées
- Exigences juridiques et relatives aux politiques et à la conformité
- Concepts, principes et pratiques de sécurité intégrée ou organisationnelle (logiciels, systèmes, données, matériel et personnel)
- Contrôles préventifs techniques, opérationnels et de gestion disponibles et responsabilités organisationnelles pour ces contrôles
- Menaces, infrastructures techniques et besoins opérationnels liés au secteur ou au contexte
- Gestion de projet et exigences de sécurité tout au long du cycle de vie du projet
- Concepts de la cryptographie et de la gestion des clés cryptographiques
- Dispositifs de réseau privé virtuel et chiffrement



- Concepts et pratiques d'ingénierie appliqués à la sécurité et à l'architecture des systèmes
- Concepts d'architecture de sécurité et modèles de référence relatifs à l'architecture d'entreprise
- Processus d'évaluation et d'autorisation de sécurité
- Authentification, autorisation et méthodes de contrôle de l'accès
- Méthodes et processus de mise à l'essai et d'évaluation de la sécurité
- Concepts et fonctions des systèmes de sécurité des applications
- Principes de gestion du cycle de vie des systèmes, y compris la sécurité et la convivialité des logiciels
- Normes de l'industrie, et principes et méthodes d'analyse acceptés par l'organisation
- Configuration et utilisation des outils de protection informatique basés sur des logiciels
- Conception de solutions matérielles et logicielles
- Gestion, mesures et suivi du programme de cybersécurité
- Gestion des incidents et planification et exécution de la reprise des systèmes

Expérience professionnelle

- Une expérience avérée de plus de trois (03) ans dans la conception, l'évaluation ou la mise en œuvre d'architectures de sécurité des systèmes d'information ;
- Une bonne maîtrise des architectures applicatives, réseaux, cloud, identité et accès, sécurité périmétrique, chiffrement, journalisation et supervision de sécurité ;
- Une expérience dans l'accompagnement de projets numériques ou de transformation sécurisée serait un atout ;
- Une bonne expérience de la gouvernance de la sécurité Numérique.

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, MANAGEMENT ET LEADERSHIP

- Être de bonne moralité et passionné(e) de la sécurité des technologies de l'information ;
- Être proactif, avoir la volonté d'apprendre, et assurer une veille technologique continue ;
- Être capable de communiquer clairement sur les exigences, procédures et recommandations de sécurité ;
- Avoir la capacité de gérer les demandes urgentes et de respecter les délais ;
- Avoir la capacité de travailler de manière autonome et de s'adapter aux différents contextes professionnels ;
- Avoir la capacité de travailler en équipe et sous pression pour l'atteinte des objectifs organisationnels ;
- Avoir l'esprit de confidentialité et une excellente capacité rédactionnelle ;
- Avoir un bon sens de synthèse et d'analyse.

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-divulgaration 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 PARTICULIÈRES 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.