

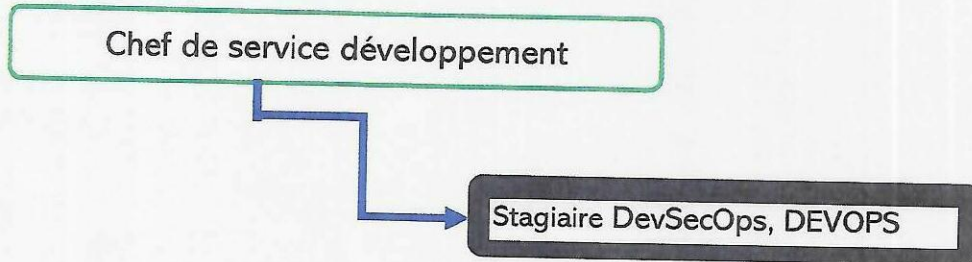
APPEL A CANDIDATURE EXTERNE

Dans le cadre du renforcement des ressources humaines de la Direction des Systèmes d'Information (DSI), la Direction de la Logistique et des Ressources Humaines lance un appel à candidature pour cinq (05) postes de **stagiaires développeurs, sécurité et opérations**.

Intitulé de Poste : **Stagiaire, DevSecOps, DEVOPS**

Lieu du poste : **Abidjan**

Relation Hiérarchique : Sous-Direction du Développement des Application



Relations fonctionnelles : Toutes les Directions

Mission principale

- Assurer les activités la sécurisation des solutions digitalisées (en équipe ou en maitre)

Activités principales

- Concevoir et réaliser des documents publicitaires et de marketing ;
- Apporter, à la demande, son appui technique aux directions sur la réalisation graphique de leurs documents ;
- Effectuer le reporting de son activité auprès de sa hiérarchie.
- Respecter les cahiers des charges ;
- Former les agents de la digitalisation à l'utilisation des solutions clients ;
- Assurer le suivi de maintenance opérationnelle sur les applications développées ;
- Diagnostiquer les dysfonctionnements des applicatifs ;
- Former les agents supports aux solutions à déployer ;
- Veiller à la qualité des programmes et applications ;
- Coder ou programmer des solutions ou applications souhaitées selon le cahier des charges ;
- Gérer l'évolution des environnements technologiques et les fonctionnalités logicielles ;
- Tester et faire évoluer les applications métiers ou externes ;
- Matérialiser le cahier de charge ou le DCF par une solution logicielle ;
- Proposer des solutions innovantes.

Conditions d'accès au poste

- Au moins Bac +3 en informatique développement d'application ou informatique gestion ou génie logiciel ou tout autre diplôme équivalent avoir une qualification obligatoire en développement sécurisé (DevSecOps).

Compétences souhaitées

- Connaissance des concepts de programmation ;
- Modèle MVC ;
- Agile Scrum ;
- Création et sécurisation d'API ;
- Cloud ;
- Gestion de projet ;
- Algorithmique et structures de données ;
- Programmation orientée objet (POO).
- Gestion de configuration ;
- Modélisation informatique ;
- Architecture d'applications, mobile et web ;
- Connaissance de l'architecture technique du système d'information ;
- Connaissance de langages de programmation (PHP, JAVA, JavaScript, HTML, CSS3, Kotlin, JQuery, AJAX, PYTHON, etc.) ;
- Connaissance des techniques d'intégration telles que le responsive ;
- restframework, Flutter, React native) ;
- Bases en gestion ;
- Connaissance des Bases de données Oracle, Postgresql, Sqlserver, MariaDB, MySQL ;
- Connaissance en GitHub ;
- Connaissance des Frameworks (Tel que Laravel, Bootstrap, ReactJS, Django ;
- Architecture des applications Web, Mobile et Client/Serveur.

1. Profil DevOps (Développement + Opérations)

- **Rôle principal** : Garantir la fluidité du pipeline de livraison, de l'écriture du code jusqu'à la mise en production (CI/CD).
- **Compétences clés** :
 - **Automatisation** : Maîtrise des outils CI/CD (Jenkins, GitLab CI, GitHub Actions).
 - **Infrastructure as Code (IaC)** : Capacité à gérer des serveurs et réseaux via du code (Terraform, Ansible, CloudFormation).
 - **Conteneurisation et Orchestration** : Expertise Docker et Kubernetes pour garantir la portabilité des applications.
 - **Cloud** : Bonne connaissance des plateformes (AWS, Azure, GCP, OVH etc).
 - **Scripting** : Python, Bash ou Go pour automatiser les tâches répétitives.
- **Mindset** : Favorise la culture de l'agilité, de la collaboration et de l'amélioration continue.

2. Profil DevSecOps (Développement + Sécurité + Opérations)

- **Rôle principal** : Intégrer des contrôles de sécurité automatisés sans ralentir la vitesse du déploiement.
- **Compétences clés** :

- **Sécurité applicative (AppSec)** : Connaissance des vulnérabilités courantes (OWASP Top 10).
- **Intégration d'outils de sécurité (DevSecOps Pipeline)** : Automatisation du scan du code (SAST - Static Application Security Testing) et des dépendances (SCA - Software Composition Analysis) directement dans la CI/CD.
- **Gestion des secrets** : Savoir gérer les mots de passe, clés API et certificats de manière sécurisée (HashiCorp Vault, AWS Secrets Manager).
- **Sécurité Cloud (Cloud Native Security)** : Maîtrise des configurations de sécurité dans le Cloud (IAM, sécurisation de Kubernetes).
- **Conformité** : Capacité à appliquer des politiques de sécurité automatisées (Policy as Code).
- **Mindset** : La sécurité n'est plus la responsabilité exclusive d'une équipe dédiée, mais une responsabilité partagée par tous (le principe du « Security as Code »).

Qualités requises (Savoir être) :

- Être curieux, s'adapter, anticiper les changements
- Esprit d'apprentissage et volonté de développer ses compétences
- Capacité d'adaptation et à travailler en équipe
- Sens de l'écoute
- Être courtois et respectueux de la hiérarchie
- Discrétion, intégrité et probité
- Sens du service et de la disponibilité
- Respect de la vie privée
- Rigueur et sens de l'organisation
- Respect des procédures et de la confidentialité des données
- Respect des règles et des instructions, méthodologie et organisation
- Capacité à communiquer et documenter systématiquement

Dossiers à fournir

- Lettre de demande de stage à adresser au Directeur Général.
- CV actualisé avec les informations précises.
- Carte d'étudiant.

Lieu de dépôt de la candidature

Direction des Ressources Humaines et de la Logistique, ONECI, 8^{ème} Tranche étage auprès du Secrétariat de la Direction des Ressources humaines et de la logistique ou par mail à : ressources.humaines@oneci.ci.

Date limite de dépôt de candidature : Le 25 juillet 2026 à 17H00

NB : Les candidatures déposées au-delà de la date et de l'heure limites, ne seront pas prises en compte dans la présélection. Seuls les postulants retenus seront contactés.
Seules les candidatures retenues seront contactées.