

TALENTS PLUS CONSEILS CÔTE D'IVOIRE filiale de **TALENTS PLUS AFRIQUE** recherche pour la **Caisse de Retraite par Répartition Avec Épargne de l'Union Monétaire Ouest Africaine (CRRAE-UMOA)** des candidats pour les postes suivants basés à **ABIDJAN-CÔTE D'IVOIRE**:

UN (01) CHEF DE LA DIVISION DES OPÉRATIONS ET DE LA SÉCURITÉ ET NUMÉRIQUE (H/F) Réf. TPCI : 2510R01CDOSN

PRINCIPALES MISSIONS :

Sous la supervision du Directeur du Digital et des Systèmes d'Information, le/la candidat(e) aura pour activités principales de :

- Veiller au bon fonctionnement des systèmes et des réseaux, à la sécurité du système informatique, assurer leur évolution et leur optimisation
- Administrer au quotidien le datacenter (serveurs physiques et système de virtualisation hyperconvergée), ainsi que les services réseaux (DNS, DHCP, VPN, SD-WAN)
- Administrer et exploiter l'infrastructure des réseaux filaires (commutateurs, routeur et pare-feu), sans fil (contrôleur wifi, points d'accès) et télécom (téléphonie IP, trunks SIP)
- Définir et déployer les évolutions matérielles ou logicielles nécessaires
- Administrer, maintenir et optimiser les solutions collaboratives Office 365 (Teams, SharePoint, Exchange) et des services connexes
- Administrer, maintenir et optimiser les services d'annuaire d'entreprise (Active Directory et Entra ID) pour la gestion des comptes utilisateurs, dans le respect des droits et procédures établis
- Administrer des bases de données et serveurs d'application
- Structurer et organiser les activités d'exploitation (notamment la sauvegarde des données), de support (service desk et gestion des incidents) et de sécurisation et de maintenance des infrastructures
- Contribuer à la mise en œuvre et au suivi des politiques de sécurité des SI
- Assurer la veille technologique et participer aux décisions concernant les orientations stratégiques technologiques

PROFIL EXIGÉ

- Être âgé de 35 ans, titulaire d'un Bac+5 (Master ou Diplôme d'ingénieur) en réseaux télécom, ingénierie système ou équivalent
- Justifier d'une expérience professionnelle de sept (07) ans au minimum dans l'administration des systèmes, réseaux et télécom dont cinq (05) ans en qualité de manager ou chef de projet
- Parfaite maîtrise des Architectures réseaux (LAN/WAN/VoIP/VPN/SD-WAN) et des équipements Cisco, Fortinet, Sophos (avoir des certifications réseaux serait un plus)
- Excellente connaissance des systèmes d'exploitation Linux, Windows, Nutanix AOS et les hyperviseurs (Hyper-V, Nutanix AHV)
- Maîtrise de l'administration de l'infrastructure logicielle de base Microsoft (Windows Server, Active Directory, Entra ID, Office 365, Exchange, SharePoint, DNS, DHCP), de PowerShell pour l'automatisation des tâches, les concepts de gestion des utilisateurs, des groupes et des stratégies de groupe (GPO)
- Avoir une certification Microsoft (MCSE/MCSA) serait un plus
- Maîtrise des architectures HCI (Hyper Converged Infrastructure) Microsoft, Nutanix et leur déploiement
- Bonne connaissance en administration et conception de bases de données relationnelles (MySQL, PostgreSQL, SQL Server ou équivalents)
- Bonne connaissance des principes ITIL et des processus ITSM
- Bonne connaissance des référentiels de sécurité (ISO 27001, NIST, etc.)
- Avoir une certification sécurité serait un plus
- Avoir une expérience dans les outils de sauvegarde (Veeam, Veritas)
- Disposer des qualités et aptitudes suivantes : forte capacité d'analyse, de synthèse et d'animation en environnement multi-acteurs, aisance rédactionnelle, capacité à produire des livrables structurés, esprit "doer" et pragmatique, capable de faire avancer les sujets de manière concrète, capacité d'écoute, de respect de l'autre, disponibilité, esprit d'équipe et d'initiative, honnêteté, loyauté, rigueur

UN (01) CHEF DE LA DIVISION DE L'INNOVATION ET DE LA GESTION DES DONNÉES (DIGITAL FACTORY & DATA) (H/F) Réf. TPCI : 2510R02CDIGD

PRINCIPALES MISSIONS :

Sous la supervision du Directeur du Digital et des Systèmes d'Information, le/la candidat(e) aura pour activités principales de :

- Accompagner la Caisse dans l'usage des outils SI et Digitaux pour améliorer l'efficacité des processus, la création de valeur et d'accompagner une transformation digitale et numérique
- Coconstruire les roadmaps digitales et data avec les directions métiers, en proposant des solutions innovantes adaptées à leurs besoins
- Délivrer les projets digitaux et data dans les délais en respectant les exigences de qualité
- Concevoir des solutions logicielles (applications web/mobile), rédiger des spécifications techniques, et développer les applications end-to-end (frontend + backend) en relation avec son équipe, en utilisant des langages de programmation adaptés
- Effectuer des tests unitaires, d'intégration et de performance pour garantir la qualité et la fiabilité des logiciels développés

→ 2

- Définir la stratégie data et les règles d'usage associées
- Piloter la gouvernance des données, notamment transactionnelles et référentielles
- Structurer les processus et outils pour répondre aux obligations contractuelles et réglementaires ; participer à la mise en conformité (RGPD, sécurité, archivage)
- Formaliser les règles d'accès, de traitement, de sécurité, et de cycle de vie des données
- Définir et superviser des indicateurs clés de performance et construire des tableaux de bord (Power BI, Tableau Software, QlikView, OBIEE...)
- Identifier et développer les sujets d'innovation puis diriger des Labs et des POC
- Assurer la veille technologique, participer aux décisions concernant les orientations stratégiques technologiques

PROFIL EXIGÉ

- Être âgé de 35 ans, titulaire d'un Bac+5 (Master ou Diplôme d'ingénieur) en informatique, développement, génie logiciel, ou ingénierie système ou équivalent
- Justifier d'une expérience professionnelle de sept (07) ans au minimum dans le développement d'applications, la gestion des projets digitaux (Product owner) dont trois (3) ans en qualité de responsable d'un service delivery pour des développements d'applications informatiques
- Maîtrise des langages de programmation (Java, Python, C++, PHP etc.) et des architectures modernes : SOA, microservices, API REST, cloud, conteneurisation (Docker, Kubernetes)
- Bonne connaissance des systèmes d'exploitation, bases de données, middleware, et serveurs d'applications
- Avoir une bonne connaissance des sciences des données, des outils ETL et BI
- Capacité à modéliser et à formaliser des architectures (UML, ArchiMate...).
- Bonne connaissance des frameworks modernes (Spring, Quarkus, Angular, React, Vue.js, Django, Laravel, Node.js etc.).
- Connaissance des architectures logicielles : Modèles MVC, client-serveur, etc.
- Compétences en bases de données : SQL (SqlServer, Postgres Sql, MySql, Oracle) , NoSQL (MongoDB, Cassandra)
- Bonne maîtrise des méthodes de gestion de projet (Agile, Scrum, Cycle en V)
- Avoir des notions de BPM (Business Process Management)
- Maîtrise des outils de développement: IDE, gestionnaires de versions (Git)
- Une expérience dans le domaine de la gestion des régimes de retraite, des fonds de pension ou de l'assurance vieillesse serait un atout
- Disposer des qualités et aptitudes suivantes : travail en équipe (collaboration avec les chefs de projet, les designers et les autres développeurs), capacité d'analyse et de résolution de problèmes techniques, qualités relationnelles et communication avec les utilisateurs, bonne organisation, capacité d'écoute et de respect de l'autre, disponibilité, esprit d'initiative, honnêteté, loyauté, rigueur, excellentes capacités rédactionnelles.

UN (01) INGÉNIEUR AMOA SENIOR (H/F) Réf. TPCI :

PRINCIPALES ACTIVITÉS

Sous la supervision du Chef de la Division de Pilotage des Projets et de l'Accompagnement Métier, le/la candidat(e) aura pour activités principales de :

- Accompagner la maîtrise d'ouvrage (MOA) dans la définition, le pilotage et la mise en œuvre de projets stratégiques en garantissant l'alignement entre les besoins métier et les solutions informatiques
- Recueillir, analyser et formaliser les besoins métiers
- Rédiger les cahiers des charges, les spécifications fonctionnelles et user stories
- Assurer la liaison entre les équipes métier, la DDSI et les prestataires
- Contribuer à la rédaction et au suivi des appels d'offres (sélection de prestataires)
- Participer à la conception des processus métier, des évolutions et changements
- Animer des ateliers de travail avec les utilisateurs pour identifier les besoins et les axes d'amélioration
- Assurer la coordination entre les équipes métier, les équipes techniques internes et les prestataires externes
- Préparer et accompagner les phases de recette fonctionnelle complète (rédaction stratégie de tests, plan de tests, pilotage de l'exécution, validation des livrables et des PV de recette)
- Identifier et qualifier les anomalies, assurer le suivi de leur résolution en collaboration avec les équipes de maintenance
- Assurer la conduite du changement (formations, communication, documentation utilisateur)
- Suivre les risques, plannings et budgets liés aux projets
- Produire des reportings clairs à la Direction et aux parties prenantes.

PROFIL EXIGÉ

- Être âgé de 35 ans, titulaire d'un Bac+5 en informatique, systèmes d'information, gestion de projet, école d'ingénieur ou école de commerce avec spécialisation SI)
- Justifier d'une expérience de 5 ans minimum dans la gestion de projets SI complexes, idéalement dans les secteurs bancaire, assurances, retraites ou secteur public
- Expérience confirmée en AMOA sur des projets de transformation digitale

3

→

- (ERP, CRM, dématérialisation, cybersécurité, modernisation SI)
- *Maîtrise des approches Agile (Scrum, SAFe) et traditionnelles (cycle en V).*
 - *Maîtrise de l'analyse métier : recueil des besoins, modélisation des processus (BPMN, UML), priorisation*
 - *Expérience en gestion du changement et accompagnement d'équipes non techniques.*
 - *Bonne compréhension des architectures SI et des processus métiers*
 - *Expérience en urbanisation et cartographie des systèmes d'information (idéalement TOGAF, BPMN)*
 - *Certifications appréciées :*
 - *Gestion de projet : PMP, Prince2, Agile/Scrum Master, Architecture SI et processus métiers : TOGAF, BPMN*
 - *Gouvernance et sécurité : ITIL, COBIT, ISO 27001*
 - *Gestion des risques et continuité : ISO 31000, ISO 22301*
 - Disposer des qualités et aptitudes suivantes : travail en équipe pluridisciplinaire, excellente communication écrite et orale, capacité à vulgariser les sujets techniques auprès des métiers, forte capacité d'analyse, esprit de synthèse et rigueur, leadership et autonomie, bonne organisation (gestion du temps), autonomie et réactivité, capacité d'analyse et de synthèse, bonnes qualités relationnelles, faire preuve de diplomatie, d'écoute, de respect de l'autre, disponibilité, esprit d'équipe et d'initiative, grande discrétion, honnêteté, loyauté, rigueur.

UN (01) RESPONSABLE DE LA SÉCURITÉ OPÉRATIONNELLE DES SYSTÈMES D'INFORMATION (H/F) RÉF. TPCI : 2510R04RSOSI

PRINCIPALES ACTIVITÉS

Sous la supervision du Chef de la Division de la Sécurité et des Opérations Numériques, le/la candidat(e) aura pour activités principales de :

- Superviser et administrer les solutions du Centre des Opérations de Sécurité
- Piloter les projets de mise en place, d'évolution ou d'amélioration du SOC (XDR, EDR, NDR, SIEM, SOAR, outils de détection...)
- Concevoir et assurer l'amélioration continue des stratégies de collecte et de détection, gérer et optimiser les interconnexions entre outils (SOAR, XDR, EDR, NDR, SIEM) et des processus de traitement opérationnel
- Détecter, analyser et qualifier les incidents
- Coordonner la réponse aux incidents de sécurité selon un plan de gestion de crise structuré
- Respecter et faire appliquer la politique et les procédures de sécurité des systèmes d'information, contribuer à la rédaction et à la mise à jour de ces dernières
- Assurer une veille technologique et réglementaire permanente sur les menaces émergentes et évolutions légales
- Définir l'architecture de sécurité globale de l'entreprise (modèle de sécurité en couches, zéro trust)
- Valider les choix technologiques et architecturaux des projets IT sous l'angle sécurité
- Concevoir et implémenter les politiques de segmentation réseau, DMZ et zones de confiance
- Définir les standards de sécurisation pour les infrastructures cloud, hybrides et on-premise
- Superviser l'intégration sécurisée des nouvelles technologies (IoT, IA, blockchain)
- Assurer la cohérence technique entre les différentes briques de sécurité déployées

PROFIL EXIGÉ

- Être âgé de 35 ans, titulaire d'un Bac+5 en informatique, réseaux télécoms, sécurité informatique ou cybersécurité
- Expérience confirmée (5 ans minimum) en cybersécurité idéalement dans un contexte SOC
- Bonne connaissance des outils de supervision et de détection (SIEM, EDR, XDR, NDR, SOAR...)
- Bonne maîtrise des normes et référentiels de sécurité (ISO 27001, NIST, etc.)
- Expérience confirmée en SOC ou en cybersécurité avec une expertise technique avancée.
- Bonne maîtrise des outils SIEM, SOAR, des solutions de détection d'intrusion et des outils de vulnerability management (Nessus, Qualys, Rapid7)
- Parfaite maîtrise des parefeux Fortigate et Sophos
- Bonne maitrise des Architectures réseaux (LAN/WAN/VoIP/VPN/SD-WAN.),
- Bonne connaissance des systèmes d'exploitation Linux, Windows, Nutanix AOS et les hyperviseurs (Hyper-V, Nutanix AHV)
- Certifications sécurité souhaitées CISSP, CISM ou CISA + ISO 27001 Lead Auditor/Implémenter
- Certifications techniques appréciées : CISSP, CEH, GCIH, GIAC, SANS, et certifications des constructeurs (Fortinet, Cisco, Sophos, Microsoft, AWS Security)
- Disposer des qualités et aptitudes suivantes : Bonne organisation (gestion du temps) et leadership, bonnes qualités relationnelles, diplomatie, capacité d'écoute et de respect de l'autre, disponibilité, esprit d'équipe et d'initiative, grande discrétion, honnêteté, loyauté, rigueur, excellentes capacités rédactionnelles

UN (01) RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (H/F) RÉF. TPCI : 2510R05RSSI

PRINCIPALES ACTIVITÉS

Sous l'autorité du Directeur du Contrôle Permanent, de la Conformité et de la Gestion des Risques, le/la titulaire du poste aura pour missions principales de : ➡ 4

- Définir, piloter et mettre en œuvre la politique globale de sécurité des systèmes d'information en alignement avec la stratégie de la CRRAE-UMOA
- Mettre en place le système de management de la sécurité de l'information (SMSI) selon la norme ISO 27001
- Conduire les analyses de risques approfondies sur l'ensemble du SI avec méthodologies reconnues (EBIOS, ISO 27005)
- Élaborer et maintenir la cartographie des risques numériques et cyber avec scenarios de menaces actualisées
- Mettre en place un système de management de la continuité d'activité (SMCA) selon la norme ISO 22301 et piloter les PRA/PCA
- Piloter les audits de sécurité internes et externes, coordonner les tests de sécurité et d'intrusion
- Assurer la conformité aux réglementations : RGPD, loi ivoirienne sur la cybersécurité, directives CEDEAO
- Gérer les relations avec les autorités de régulation (ARTCI, ANSSI-CI, CERT-CI)
- Superviser les processus de classification et de protection des données sensibles
- Coordonner les diligences de réponse en cas d'incidents graves, de crises ou d'attaques
- Piloter la gouvernance sécurité via des comités dédiés et reporting régulier à la Direction Générale
- Assurer une veille technologique et réglementaire permanente sur les menaces émergentes et évolutions légales
- Participer activement aux instances dirigeantes pour intégrer la dimension sécurité dans toutes les décisions stratégiques
- Encadrer les équipes, coordonner les prestataires, sensibiliser le personnel

PROFIL EXIGÉ

- Être âgé de 35 ans, titulaire d'un Bac+5 ou d'un Diplôme d'Ingénieur en informatique, cybersécurité, télécommunications ou domaines connexes (réseaux, systèmes, sécurité des données)
- Justifier d'une expérience professionnelle d'au moins sept (07) ans dans la sécurité des systèmes d'information, dont trois (03) ans à un poste de responsabilité
- Disposer d'une excellente connaissance des référentiels et normes de sécurité (ISO 27001/27002, NIST, COBIT, EBIOS, RGPD, loi ivoirienne sur la cybersécurité)
- Avoir une connaissance des technologies de sécurité : firewalls nouvelle génération, IDS/IPS, WAF, SIEM, EDR/XDR, gestion des identités et des accès (IAM, PAM)
- Maîtriser la sécurisation des environnements cloud (AWS, Azure, GCP), des systèmes d'exploitation (Windows, Linux) et des applications critiques
- Avoir une bonne maîtrise de la norme ISO 22301 sur la SMSCA
- Avoir une bonne maîtrise de la gestion des risques numériques (ISO 27005)
- Certifications sécurité requises CISSP, CISM ou CISA + ISO 27001 Lead Auditor/Implémenter
- Posséder une très bonne pratique des outils bureautiques (Word, Excel, PowerPoint), ainsi que des outils et plateformes de sécurité.
- Une expérience dans les secteurs des finances, régimes de retraite, fonds de pension ou de l'assurance serait un atout
- Disposer des qualités et aptitudes suivantes : Sens de l'organisation et bonne gestion des priorités, qualités relationnelles et aptitude à travailler en équipe, diplomatie, écoute, respect de l'autre, esprit d'initiative et capacité à fédérer, discrétion, honnêteté, loyauté et rigueur, excellentes capacités rédactionnelles et de communication

DOSSIER DE CANDIDATURE ET DÉPÔT

Tout (e) candidat (e) intéressé (e) par l'une des offres devra, au risque d'irrecevabilité, produire :

- La **preuve de la nationalité** de l'un des pays de l'espace UEMOA (Bénin, Burkina Faso, Côte d'Ivoire, Guinée-Bissau, Mali, Niger, Sénégal, Togo)
- Une **lettre de motivation signée** indiquant la référence du poste concerné adressée au Directeur Général de la CRRAE-UMOA ,
- Un **CV chronologique** (indiquant la période exacte de chaque expérience) détaillé mettant en exergue les activités pertinentes pour le poste,
- Les **copies du (s) diplôme (s) exigé (s) pour le poste,**
- Les **attestations ou certificats de travail** justifiant les expériences.

NB : Les dossiers incomplets seront, purement et simplement, déclarés irrecevables et les expériences non justifiées ne seront pas prises en compte.

Les dossiers sont reçus au siège du cabinet **Talents Plus Conseils Côte d'Ivoire (TPCI)** sis à Abidjan, Cocody Angré 9^e Tranche, Immeuble contigu à l'immeuble CGK, 2^e étage, porte de droite ou par mail : recrutement-tpci@talentsplusafrique.com

Date limite de dépôt : 23 octobre 2025 à 16 h 00 TU.

Infos line : (+225) 27 22 41 01 52-07 09 21 17 27

DÉROULEMENT DU PROCESSUS

Le processus se déroulera en trois (03) phases principales :

- une phase de dépouillement et présélection
- une phase de tests et d'entretiens individuels/candidats présélectionnés
- une dernière phase d'entretiens/candidats retenus à l'issue de la phase précédente

NB : Exclusivement les candidats présélectionnés seront contactés et aucun dossier ne sera retourné.