

FICHE DE FONCTION

Responsable des systèmes d'information

Référence : SG/SI/03

Supérieur hiérarchique : Secrétaire général

Positionnement

Responsable de fonction transverse. Pilote les prestataires d'infrastructure, d'hébergement, de support, de cybersécurité et de solutions numériques.

Nature du recrutement : cette fonction sera confiée à une société / firme spécialisée en systèmes d'information. Les compétences, l'expérience et les exigences décrites dans la présente fiche s'appliquent à l'entité prestataire retenue et à l'équipe qu'elle mobilise pour le compte de CGLU Afrique.

Finalité du poste

Garantir à CGLU Afrique la maîtrise de ses actifs numériques, la disponibilité de ses services, la sécurité de ses données et sa capacité à poursuivre ou rétablir ses activités. Le Responsable SI réduit toute dépendance à une personne, un compte privé ou un prestataire non réversible.

Responsabilités fonctionnelles

1. **Gouvernance SI :** établir la cartographie du système d'information, la feuille de route, le budget, les standards techniques et les règles de décision.
2. **Maîtrise des actifs :** inventorier les équipements, applications, domaines, hébergements, licences, comptes maîtres, contrats, administrateurs et moyens de récupération.
3. **Identités et accès :** rendre les comptes nominatifs, déployer l'authentification multifacteur, organiser les habilitations et supprimer rapidement tout accès indu.
4. **Cybersécurité :** évaluer les risques, corriger les vulnérabilités, surveiller les services, gérer les incidents et préserver les traces utiles aux investigations.
5. **Continuité :** définir les sauvegardes, objectifs de reprise, procédures de crise et tests de restauration adaptés à la criticité des services.
6. **Applications et données :** sécuriser les outils métiers, la gestion documentaire, les échanges avec les partenaires et les règles de conservation définies avec les métiers et le Juridique.
7. **Services et prestataires :** organiser le support, les niveaux de service, les contrats, les coûts, la réversibilité et le transfert de connaissances.
8. **Projets et adoption :** piloter les projets numériques, accompagner les utilisateurs, documenter les changements et mesurer la valeur, les risques et les coûts complets.

Résultats attendus et indicateurs clés

- Registre exhaustif des actifs numériques, comptes administrateurs, contrats, propriétaires, sauvegardes et dépendances.
- Matrice des habilitations actualisée et revue formellement pour tous les accès critiques.

- Comptes privilégiés nominatifs, protégés par authentification multi-facteurs et dépourvus de moyens de récupération personnels.
- Sauvegardes surveillées et tests de restauration documentés selon un calendrier fondé sur la criticité.
- Plan de continuité et de reprise testé, registre des incidents tenu et actions correctives suivies jusqu'à clôture.
- Dossier de réversibilité complet pour chaque prestataire critique et tableau de bord mensuel de service, sécurité, coûts et projets.

Aptitudes, compétences et connaissances

Requises

- Maîtrise de la gouvernance SI, des infrastructures hybrides et cloud, des réseaux, des identités et accès et de la gestion des services.
- Compétences confirmées en cybersécurité, sauvegarde, continuité, réponse aux incidents, journalisation et gestion des vulnérabilités.
- Capacité à contractualiser et piloter des prestataires en intégrant disponibilité, sécurité, propriété, réversibilité et niveaux de service.
- Pratique de l'architecture, de la documentation, de la gestion de projets et de l'accompagnement des utilisateurs.
- Connaissance des enjeux de protection des données, de conservation documentaire, de preuve électronique et de souveraineté numérique.
- Méthode, sens du service, sang-froid, confidentialité et capacité à expliquer les risques techniques à une gouvernance non spécialiste.

Souhaitables

- Certifications pertinentes en sécurité, gouvernance, gestion des services, cloud ou continuité.
- Expérience d'une organisation internationale, multisite ou répartie dans plusieurs pays.

Formation académique

- Diplôme de niveau Bac+5 en systèmes d'information, informatique, cybersécurité, télécommunications ou domaine équivalent.

Expérience

- Huit à douze années d'expérience, dont au moins trois dans la responsabilité d'un SI, d'une équipe ou de prestataires critiques.
- Une expérience de reprise de contrôle d'actifs et d'accès numériques est recherchée.

Langues

- Maîtrise professionnelle du français et de l'anglais.
- La capacité à produire une documentation claire dans les deux langues est requise.

Conditions d'exercice

- Poste basé à Rabat.

- Astreinte ou disponibilité ponctuelle en cas d'incident critique.
- Déplacements occasionnels auprès des bureaux, partenaires et prestataires.

Comment postuler

- Veuillez envoyer votre CV et votre lettre de motivation à l'adresse suivante : recruitments@uclg-africa.org
- Date limite : 29 octobre 2026