PRÉSIDENCE DE LA RÉPUBLIQUE

SECRETARIAT GENERAL

Projet de Gouvernance Digitale et de Gestion de l'Identité Malagasy
(PRODIGY)

Unité de Gouvernance Digitale (UGD)

Termes de référence pour le recrutement d'un Head Manager CIRT

1. Contexte

Madagascar s'est engagé à asseoir une Administration de proximité, à l'écoute de la population et de ses besoins, et à améliorer la qualité de vie des citoyens. Pour se faire, la Présidence a élaboré une stratégie pour améliorer l'accès aux services publics, à travers la réforme du système de gestion de l'identité, et la simplification et la digitalisation des services publics clés pour la population et les entreprises.

En effet, une Unité de Transformation des Services Publics a été créée pour travailler en étroite collaboration avec tous les Ministères et institutions. Avec l'appui de la Banque Mondiale, la Présidence entend mettre en place une première équipe au sein de l'Unité à travers le PRODIGY qui pourra rapidement développer et tester de nouveaux projets pilotes et en démontrer la faisabilité. Elle sera également chargée de coordonner et d'appuyer techniquement les initiatives digitales de l'ensemble du gouvernement, afin d'assurer un contrôle qualité, une interopérabilité et une approche harmonisée.

Suivant la communication verbale relative aux modalités de mise en place du cadre structurel en charge de la cyber sécurité à Madagascar, du 26 Juillet 2023, le Computer Incident Response Team (CIRT) transitoire est placé au sein de l'Unité de Gouvernance Digitale (UGD) jusqu'à l'adoption du Plan Stratégique du Numérique. Les présents TDR ont pour objet le recrutement de son head manager.

2. Objectif du poste

Le Directeur Général du CIRT National est responsable de la définition et de la mise en œuvre de la stratégie globale du centre, visant à renforcer la résilience nationale face aux cybermenaces. Il dirige une équipe spécialisée dans la détection, l'analyse et la réponse aux incidents de cybersécurité, tout en collaborant avec des partenaires nationaux et internationaux pour assurer une cybersécurité robuste.

3. Responsabilités principales

3.1. Leadership stratégique :

- Définir la vision, la mission et les objectifs stratégiques du CIRT National.
- Élaborer des plans stratégiques pour renforcer la posture de cybersécurité nationale.

3.2. Gestion opérationnelle :

- Superviser toutes les activités opérationnelles du CIRT, y compris la détection, l'analyse et la réponse aux incidents de cybersécurité.
- Coordonner les équipes spécialisées pour assurer une réactivité efficace aux menaces.

3.3. Partenariats et collaborations :

- Établir et entretenir des partenariats stratégiques avec d'autres CIRT nationaux, organismes gouvernementaux, entreprises privées et organisations internationales.
- Collaborer avec les parties prenantes pour partager des informations et renforcer la cyber-résilience nationale.

3.4. Veille technologique :

- Assurer une veille constante sur les évolutions technologiques et les tendances en matière de cybersécurité.
- Intégrer les nouvelles technologies et méthodologies pour maintenir l'efficacité opérationnelle du CIRT.

3.5. Gestion budgétaire et financière :

- Élaborer et gérer le budget du CIRT en assurant une utilisation efficiente des ressources financières.

3.6. Communication et représentation :

- Être le porte-parole du CIRT auprès des médias, des autorités gouvernementales et des organismes internationaux.
- Participer à des conférences et événements pour promouvoir la cybersécurité nationale.

4. Résultats attendus

4.1. Gouvernance et cadre stratégique

- Élaboration, validation et publication de la Stratégie Nationale de Cybersécurité, puis mise à jour annuelle.
- Élaboration d'une feuille de route opérationnelle alignée avec les objectifs du Plan Stratégique du Numérique et du projet PRODIGY.
- Élaboration de documents de référence (politique de gestion des incidents, protocoles d'escalade, guides de bonnes pratiques, etc.).

4.2. Opérations du CIRT

- Mise en place d'un centre opérationnel fonctionnel avec procédures claires pour la détection, l'analyse et la réponse aux incidents.
- Rapports réguliers d'incidents (mensuels et trimestriels), incluant des indicateurs de performance (nombre d'incidents traités, délai moyen de réponse, etc.).
- Déploiement d'outils de supervision, d'alerte et de corrélation d'événements (SIEM, sondes, etc.).

4.3. Coopération nationale et internationale

- Signature d'au moins 3 partenariats formels avec des entités nationales ou internationales (CIRT, OI, agences sectorielles, etc.).
- Organisation d'au moins 2 exercices de simulation (cyber drill) par an avec les parties prenantes nationales.

4.4. Sensibilisation et renforcement des capacités

- Lancement et animation d'une campagne annuelle de sensibilisation à la cybersécurité auprès des administrations publiques et du grand public.
- Conception et mise en œuvre de programmes de formation à destination des agents publics, incluant au moins 3 modules thématiques par an.

4.5. Indicateurs du projet PRODIGY

- Contribution directe à l'atteinte des indicateurs du projet PRODIGY relatifs à la cybersécurité (nombre de structures publiques connectées, niveau de maturité SSI, etc.).
- Transmission trimestrielle de rapports d'activités et tableaux de bord à l'UGD et à la Banque Mondiale.

5. Profil du candidat

Critères obligatoires

- Avoir un diplôme bac +5 en Informatique ou Gestion ou Droit
- Au moins 10 années d'expérience dans le domaine des technologies de l'information et du numérique
- Au moins une expérience avérée dans la gestion de la cybersécurité à un niveau national ou international
- Au moins 5 années d'expérience en gestion d'équipes multidisciplinaires et en leadership
- Au moins une expérience de projets en matière d'élaboration, de révision ou d'analyse de textes législatifs et réglementaires
- Capacité de communiquer en Anglais, Français et Malagasy, à l'écrit et à l'oral

Atout optionnels

- Solide compréhension des enjeux géopolitiques liés à la cybersécurité
- Excellentes compétences en communication et en négociation

6. Durée de la mission

La durée de la mission est jusqu'au 30 Juin 2026 sous réserve d'une évaluation satisfaisante des performances du consultant après trois (3) mois .

Le poste est basé à Antananarivo.

7. Modèle de curriculum vitae de la Banque mondiale

Titre du Poste et No.	*[parex. PC 1 - Chef d'équipe]*
Nom de l'expert :	*Mme, Mr [Insérer le nom complet]*
Adresse physique :	
Adresse émail et numéro téléphone	
Date de naissance :	*[Jour/mois/année]*
Nationalité/Pays de résidence	

: [Résumer les études universitaires et autres études spécialisées suivies, en indiquant le nom de l'école ou université, les années d'étude et les diplômes obtenus]

Expérience professionnelle pertinente à la mission : *[Dresser la liste des emplois exercés depuis la fin des études, dans un ordre chronologique inverse, en commençant par le poste actuel ; pour chacun, indiquer les dates, le nom de l'employeur, le titre professionnel de l'employé et le lieu de travail ; pour les emplois des dix dernières années, préciser en outre le type de travail effectué et fournir, le cas échéant, les noms des clients à titre de références. Les emplois tenus qui sont sans rapport avec la mission peuvent être omis.]*

Période	**Nom de l'employeur, titre professionnel/poste tenu. Renseignements sur contact pour références**	**Pays**	**Sommaire des activités réalisées, en rapport avec la présente mission**
[par ex. Mai 2011- présent]	*[par ex. Ministère de ……, conseiller/consultant pour… Pour obtenir références : Tél……./courriel…… ; M. xxxx, Directeur]*		

Affiliation à des associations professionnelles et publications réalisées :

Langues pratiquées (indiquer uniquement les langues dans lesquelles vous pouvez travailler) : Compétences/qualifications pour la mission :

Tâches spécifiques incombant à l'expert parmi les tâches à réaliser par l'équipe d'experts du Consultant :	**Référence à des travaux ou missions antérieures illustrant la capacité de l'expert à réaliser les tâches qui lui seront attribuées**

Renseignements pour contacter l'expert : (courriel, Téléphone)

Certification :

Je soussigné, certifie que le présent CV me décrit de manière correcte, ainsi que mes qualifications et mon expérience professionnelle ; je m'engage à être disponible pour réaliser la mission lorsque cela sera nécessaire, au cas où le contrat serait attribué. Toute fausse déclaration ou renseignement fourni incorrectement dans le présent CV pourra justifier ma disqualification ou mon renvoi par le Client, et/ou des sanctions par la Banque.

[jour/mois/année]

Nom de l'expert Signature Date

[jour/mois/année]

Nom du représentant autorisé du Consultant Signature Date

(la même personne qui est signataire de la Proposition)