

ANNEXE 1 :



Développement d'une application de gestion et de 03 sites Web

1.1 Le contexte

Le ministère de l'Intérieur a entrepris avec l'appui du PNUD un processus de réforme du secteur de la sécurité ce qui a permis de réaliser des avancées considérables notamment en ce qui concerne le modèle tunisien de police de proximité, de promotion du cadre juridique et institutionnel du secteur de la sécurité améliorant les aspects de l'intégration de l'approche genre et de l'égalité des chances entre les femmes et les hommes, de la redevabilité, de la déontologie, de l'intégrité et du respect des droits humains.

Cependant, le contexte socio-économique actuel aggravé par les répercussions des crises sanitaires est caractérisé par des défis majeurs liés à la qualité de vie et à la sécurité de la communauté notamment au niveau local impactant la capacité des personnes notamment les plus vulnérables à accéder aux droits et services ainsi que leur confiance dans les institutions et favorisant les risques de tensions, font que les efforts en matière de gouvernance du secteur de la sécurité sont toujours d'actualité et devraient être consolidés et promus.

Afin de répondre proactivement à ces défis de plus en plus complexes et multidimensionnels, le projet essaiera à travers une approche centrée sur les personnes ralliant les solutions intégrées au niveau national et local en harmonie avec le cadre général d'appui au ministère de l'intérieur à savoir « la gouvernance en tant que levier du développement socio-économique » et spécifiquement l'effet qui stipule que « Les services de sécurité et de justice sont centrés sur la personne et les individus peuvent faire valoir leurs droits ».

1.2 Contexte spécifique

Le PNUD appui le ministère de l'intérieur dans son parcours pour la réforme du secteur de la sécurité par l'implémentation de l'approche « police de proximité » qui s'appuie sur les piliers suivants :

- Le Partenariat ;
- L'action orientée vers la Résolution des problèmes ;
- La Communication ;
- La prestation de Services de qualité.

L'intégration du numérique est cruciale pour garantir un service de qualité au citoyen. Dans ce sens le PNUD entend appuyer le ministère de l'intérieur pour le développement d'une nouvelle version d'une application appelée « Tableau de Bord de Gestion » qui est déployée au niveau d'un ensemble de structures régionales et locales.

L'application offre aux agents une aide à la gestion en incluant des activités et les demandes des citoyens pour l'obtention de documents officiels, et offre à la chaîne de commandement des tableaux récapitulatifs et des statistiques.

Cette nouvelle version, appelée « casier numérique des postes de la sécurité publique », inclura des fonctionnalités, tel que GED, qui vont permettre d'avancer dans le processus de numérisation des postes afin de minimiser au maximum le recours aux papier (registres, boîtes d'archives, ...etc).

En plus, le PNUD entend appuyer le ministère de l'intérieur pour le développement de sites Web orientés aux citoyens pour leur permettre d'accéder en ligne à des services divers et qui seront énumérés par la suite.

1.3 Méthodologie et tâches

La méthodologie de gestion du projet de développement de l'application informatique s'appuiera sur une approche agile, favorisant la collaboration et l'adaptation aux besoins du client. Le projet sera découpé en sprints de courte durée (2 à 4 semaines), permettant une livraison progressive de fonctionnalités et une validation continue par le client.

Les principales phases du projet seront les suivantes :

- Phase d'initialisation : Définition des objectifs du projet, des besoins du client et des fonctionnalités à développer ;
- Phase de planification : Détailler les tâches, estimation du temps et des ressources nécessaires, création du planning du projet ;
- Phase de développement : Réalisation des sprints de développement, avec des livraisons régulières au client pour validation ;
- Phase de tests : Tests unitaires, tests d'intégration et tests de recette pour garantir la qualité de l'application ;
- Phase de déploiement : Mise en production de l'application et formation des utilisateurs ;
- Phase de maintenance : Correction des bugs et évolution de l'application en fonction des besoins du client.

Outils et méthodes :

- Outils de gestion de projet : Trello, Jira, ...etc ;
- Outils de communication : Slack, Zoom, ... etc ;
- Outils de développement : Git, GitHub, IDE (Visual Studio, IntelliJ IDEA), ...etc ;
- Méthodes de développement : Agile, Scrum, Kanban, ... etc ;
- Méthodes de test : TDD, BDD, ... etc.

Suivi et reporting :

- Des points d'avancement réguliers seront organisés avec le client pour suivre l'état du projet et identifier les points d'amélioration.
- Des reportings d'activité seront transmis au client à chaque fin de sprint.

Gestion des risques :

- Une analyse des risques sera réalisée en amont du projet.
- Un plan de gestion des risques sera mis en place pour identifier les risques et définir des actions correctives.

Communication :

- Une communication transparente et régulière sera établie avec le client tout au long du projet.
- Le client sera impliqué dans les phases de validation et de recette.

Rôles et responsabilités :

- Le chef de projet sera responsable de la planification, du suivi et de la coordination du projet.
- Le client sera responsable de la validation des livrables et de la fourniture des feedbacks.
- L'équipe de développement sera responsable de la réalisation des tâches et de la qualité de l'application.
- Le choix de la méthodologie agile permettra de garantir une meilleure flexibilité et adaptabilité du projet aux besoins du client. La collaboration étroite entre le client et l'équipe de développement sera un facteur clé de succès du projet.

1.4 Spécifications fonctionnelles métier

1.4.1 Le casier numérique des postes de la sécurité publique

La nouvelle version de l'application doit permettre la saisie et le suivi des activités des postes de la sécurité publique et des demandes déposés par les citoyens et l'exécution de recherches multicritères. En plus, elle offrira des **tableaux récapitulatifs et des statistiques à la chaîne de commandement** pour l'aide à la prise de décisions. Les statistiques seront :

- Soit générées automatiquement (tableaux, graphiques, ...etc) depuis la base de données et au niveau de chaque niveau hiérarchique présentation des détails et des récapitulatifs ;
- Soit saisies manuellement au niveau des postes et présentées en détails et en récapitulatifs aux différents niveaux hiérarchiques.

Liste des services et activités inclus dans l'application :

Services type 1 :

- Service 1.1 ;
- ...
- Service 1.5.

Pour chacun des menus il y aura :

- Un formulaire de saisie de données alphanumériques, de dates, liste déroulante, ...etc, avec des contrôles sur les données en termes de formes, de composition, de contenu, la date ne doit pas dépasser la date du système, génération automatique de numéro d'ordre, ... etc ;
- Une impression des données sur des préimprimés officiels et impression d'un état journalier des dossiers ou pour une durée déterminée, et des résultats des recherches ;
- Un scan de documents et archivage avec indexation et OCR des identifiants avec possibilité d'archivage par lot de l'archive papier des préimprimés anciens ;
- Une interface de suivi qui permettra de mettre à jours l'état de la demande (avec sélection simple et multiples) et d'exécuter des recherches multicritères et trie ;
- Génération d'alertes concernant les dossiers en cours de traitement et ceux qui dépassent des délais spécifiques.

Services type 2 :

- Service 2.1 ;
- ...

- Service 2.6.

Pour ces menus il y aura :

- Un formulaire de saisi de données alphanumériques, de dates, liste déroulante, ...etc, avec des contrôles sur les données en termes de formes, de composition, de contenu, la date ne doit pas dépasser la date du système, génération automatique de numéro d'ordre, ... etc ;
- Une impression des données sur des préimprimés officiels et impression d'un état journalier des dossiers ou pour une durée déterminée, et des résultats des recherches ;
- Un scan de documents et archivage avec indexation et OCR des identifiants avec possibilité d'archivage par lot de l'archive papier des préimprimés et dossiers anciens ;
- Une interface de suivi qui permettra de mettre à jours l'état de la demande (avec sélection simple et multiples) et d'exécuter des recherches multicritères et trie ;
- Génération d'alertes concernant les dossiers en cours de traitement et ceux qui dépassent des délais spécifiques.

Services type 3 :

- Service 3.1 ;
- Service 3.2 (06 types) ;
- Services 3.3.

Pour ces menus il y aura :

- Un formulaire de saisi de données alphanumériques, de dates, liste déroulante, ...etc, avec des contrôles sur les données en termes de formes, de composition, de contenu, la date ne doit pas dépasser la date du système, génération automatique de numéro d'ordre, ... etc ;
- **L'accès à certains types du service 3.2 sera avec une authentification supplémentaire (code différent du mot de passe) ;**
- Une impression des données sur des préimprimés officiels et impression d'un état journalier des dossiers ou pour une durée déterminée, et des résultats des recherches ;
- Un scan de documents et archivage avec indexation et OCR des identifiants avec possibilité d'archivage par lot de l'archive papier des préimprimés et dossiers anciens ;
- Une interface de suivi qui permettra de mettre à jours l'état de la demande (avec sélection simple et multiples) et d'exécuter des recherches multicritères et trie ;
- Génération d'alertes concernant les dossiers en cours de traitement et ceux qui dépassent des délais spécifiques.

Services type 4

- Service type 4.1 ;
- ... ;
- Service type 4.3.

Pour ce menu il y aura :

- Un formulaire de saisi de données alphanumériques, de dates, liste déroulante, ...etc, avec des contrôles sur les données en termes de formes, de composition, de contenu, la date ne

doit pas dépasser la date du système, génération automatique de numéro d'ordre, ... etc ;

- Impression d'un état des dossiers pour une durée déterminée, et des résultats des recherches ;
- Un scan de documents et archivage avec indexation et OCR des identifiants avec possibilité d'archivage par lot de l'archive papier des préimprimés et dossiers anciens ;
- Une interface de suivi qui permettra de mettre à jours l'état (avec sélection simple et multiples) et d'exécuter des recherches multicritères et trie ;
- Génération d'alertes concernant les dossiers en cours de traitement et ceux qui dépassent des délais spécifiques.

Gestion des équipements

- Liste des différents types d'équipements classées par catégorie avec suivi du cycle de vie : création, réparation, épave, remplacement, réaffectation, ...etc.

Pour ce menu il y aura :

- Un formulaire de saisi de données alphanumériques, de dates, liste déroulante, ...etc, avec des contrôles sur les données en termes de formes, de composition, de contenu, la date ne doit pas dépasser la date du système, génération automatique de numéro d'ordre, ... etc ;
- Une impression des données sur des préimprimés officiels et impression d'un état global des équipements ou pour une durée déterminée ou une catégorie spécifique, et des résultats des recherches ;
- Un scan de documents et archivage avec indexation et OCR des identifiants avec possibilité d'archivage par lot de l'archive papier des préimprimés anciens ;
- Une interface de suivi qui permettra de mettre à jours l'état des équipements (avec sélection simple et multiples) et d'exécuter des recherches multicritères et trie ;
- Génération d'alertes concernant les équipements en cours de réparation et qui dépassent des délais spécifiques.

Gestion de personnels

- Liste des différents types d'équipements classées par catégorie avec suivi du cycle de vie : création, réparation, épave, remplacement, réaffectation, ...etc.

Pour ce menu il y aura :

- Un formulaire de saisi de données alphanumériques, de dates, liste déroulante, ...etc, avec des contrôles sur les données en termes de formes, de composition, de contenu, la date ne doit pas dépasser la date du système, ... etc ;
- Une fonction de scan de photo et de documents ;
- Impression d'un état des dossiers pour une durée déterminée, et des résultats des recherches ;
- Une interface de suivi qui permettra de mettre à jours l'état de la personne (avec sélection simple et multiples) et d'exécuter des recherches multicritères et trie ;

Statistiques (50 cas de figure) :

- Générées automatiquement d'une façon périodique (programmable) ou à la demande à partir

des activités enregistrées et validation avant soumission au niveau hiérarchique supérieur ;

- Formulaires (sous forme de tableau) à remplir par le poste de la sécurité publique et validation avant soumission au niveau hiérarchique supérieur ;
- Au niveau des structures hiérarchiques les tableaux récapitulatifs et statistiques seront affichées sous forme détaillées et récapitulatif et validation avant soumission au niveau hiérarchique supérieur.

Pour ce menu il y aura :

- Un formulaire de saisi de données alphanumériques, de dates, liste déroulante, ...etc, avec des contrôles sur les données en termes de formes, de composition, de contenu, la date ne doit pas dépasser la date du système, génération automatique de numéro d'ordre, ... etc ;
- Impression d'un journal journalier ou pour une durée déterminée, et des résultats des recherches ;
- Un scan de documents et archivage avec indexation et OCR des identifiants ;
- Jointure de fichiers de différents types et optimisation et compression des fichiers de type médias (photo, vidéo, ...etc) ;
- Une interface de suivi avec possibilité de mise à jour (avec sélection simple et multiples) et d'exécuter des recherches multicritères et trie ;
- Génération d'alertes concernant le dépassent des délais spécifiques pour chaque type de tableau récapitulatif et statistiques.

Bibliothèque électronique des manuels de procédures et de thèmes de formation

- Liste de manuels de procédures ;
- Liste de documents (pdf, images, vidéos, ...etc), de formation pour les agents du poste de la sécurité publique y compris un document de formation sur l'utilisation de l'application.

1.4.2 Sites Web

Les sites web qui vont être développés donnerons accès aux services suivants :

- Dépôt de plaintes en ligne ;
- Demandes en ligne du bulletin N°3 ;
- Le bulletin N°3 en ligne.

Dépôt de plaintes en ligne

Consciente de l'importance de l'écoute des soucis des citoyens pour lui rendre des services de qualité et renforcer la relation de confiance avec lui, le ministère de l'intérieur à décider de mettre à la disposition du citoyen de nouveaux canaux de dépôt des plaintes, plus proche et rapide.

Dans ce sens, Il est demandé dans le cadre de ce projet de développer un site Web en Extranet et une application mobile pour le dépôt et le suivi des plaintes en ligne.

L'accusateur peut déposer une plainte anonyme, ou il peut créer un compte pour le dépôt et le suivi de ses plaintes et que des fichiers de natures diverses (pdf, doc, vidéos, images, ...etc)

peuvent être joint à la plainte comme pièces justificatives. De plus, les deux nouveaux moyens doivent offrir la possibilité de l'enregistrement et l'envoi de messages vocaux.

Une gestion particulière des plaintes doit être offerte à des groupes restreints de personnes ou organisations préenregistrées, pour envoyer et suivre, individuellement, les plaintes déposées. Selon le groupe, les plaintes seront redirigées vers une structure spécifique pour la prise en charge.

La gestion particulière des utilisateurs des groupes restreints nécessite la mise à disposition d'une interface d'administration en back-office pour assurer plusieurs fonctions tel que la création et la désactivation des groupes, la validation des demandes d'inscription, l'activation et la désactivation des comptes, la réinitialisation des mots de passes, ...etc.

La solution doit offrir des statistiques spatiotemporelles sur les requêtes reçues via ces deux nouveaux moyens de dépôt des plaintes tel que : nombre de téléchargement avec une dispersion géographique, nombre des requêtes anonymes et requêtes authentifiés et comparaison avec des périodes précédentes et évolution dans le temps, nombre des requêtes par localisation géographique selon l'IP de connexion (localisation approximative par gouvernorat), nombre d'utilisateurs inscrits (hors groupes), requêtes par groupes, temps de réponse moyen aux requêtes pour les utilisateurs enregistrés et pour les groupes, ...etc.

En termes d'autorisations, l'application mobile ne doit avoir accès qu'aux ressources nécessaires pour assurer l'authentification forte, joindre des fichiers et afficher des notifications. L'application n'utilisera pas la fonction de géolocalisation des appareils mobiles pour localiser le gouvernorat de connexion mais s'appuiera plutôt sur l'IP. Cette information est recueillie uniquement pour des fins de statistiques en termes d'adoption des nouvelles technologies par région.

Le soumissionnaire doit prendre en considération qu'il se chargera des frais d'enregistrement de l'application auprès des 03 centres de téléchargement, à savoir : PlayStore, AppStore et AppGallery, pour une année qui peut être renouvelée.

Demandes en ligne du bulletin N°3

Cette nouvelle version du site, reprendra les mêmes rubriques du site existant avec enrichissement des fonctionnalités, tel que le suivi de la livraison du courrier et l'intégration d'un nouveau Framework de paiement en ligne plus fiable et plus sécurisé.

Bulletin N°3 en ligne

Ce site reprendra les fonctionnalités du précédent site avec la différence en termes de modalité de livraison qui sera un document signé électroniquement.

1.5 Fonctionnalités applicatives

Dans cette section sera énumérée une liste, non exhaustive, de fonctionnalités qui doivent être intégrées dans l'application et les sites Webs.

Le prestataire doit prendre en considération qu'au cours du développement, de nouvelles fonctionnalités peuvent s'avérer nécessaires et il faut les intégrer dans la version finale.

1.5.1 Import des données et interfaçage

L'application « casier numérique des postes de la sécurité publique » remplacera l'ancienne version appelée « Tableau de Bord de Gestion ».

Pour ce faire, le prestataire est tenu d'intégrer le contenu de la base existante dans la nouvelle application pour garder l'historique des dossiers à des fins de recherches et de statistiques.

L'import des données se fera de deux manières, soit en effectuant une transition brusque par l'import de la totalité de la base existante vers la nouvelle base et l'exploitation de la nouvelle application, soit par une transition fluide qui dure dans le temps, et ce selon la complexité de la tâche et la criticité de l'exploitation de la base de données existante.

Le prestataire, en étroite collaboration avec l'équipe IT du ministère, préparera les scénarios et les outils nécessaires pour cette tâche et lui fournira l'assistance nécessaire pour effectuer, conjointement, cette tâche. La base existante est de type Oracle 11 ;

De plus, l'application échangera des données avec d'autres applications et bases de données via des **APIs et des Web-Services (05 Webs services)**. Cette tâche se fera au fur et à mesure de l'avancement de mise en exploitation des modules et s'étalera dans le temps.

Pour le site Web de dépôt en ligne des demandes du bulletin N°3, le prestataire doit prévoir un scénario pour une transition fluide et sans arrêt du service (juste le temps du basculement) et sans perte des données des demandes en cours.

1.5.2 Gestion de contenu, numérisation et OCR

L'application « casier numérique des postes de la sécurité publique » doit intégrer un Framework ou une solution open-source de bonne réputation, robuste et stable, pour gérer les documents scannés et archivés.

La solution doit intégrer un module permettant la gestion des opérations de numérisation via des scanners et un module de reconnaissance de caractère OCR dont le but de reconnaître des identifiants numérique ou alphanumérique.

1.5.3 Métadonnées

La solution devra prendre en compte des métadonnées pour les dossiers et les documents associés (images, vidéos, ...etc). Ces métadonnées devront être proposées automatiquement à l'utilisateur et pourront être modifiées manuellement.

1.5.4 Bibliothèque électronique

Une bibliothèque électronique contenant un ensemble de documents, classés par thématiques et sous thématiques et qui peuvent être marquer par des métadonnées.

La bibliothèque s'appuiera sur la plateforme de gestion électronique des documents open-source, sujet du point 5.2, et offrir toutes les fonctionnalités d'un GED.

1.5.5 Gestion des utilisateurs

La gestion des utilisateurs se fera totalement au niveau des applications et aucune interaction avec un autre système d'authentification n'est envisageable actuellement.

De plus, chaque corps ou ensemble de structure, aura sa propre interface d'administration des utilisateurs avec une gestion des droits d'accès.

1.5.6 Didacticiel

Pour l'application « casier numérique des postes de la sécurité publique » et afin d'assister les utilisateurs tout au long de leur expérience d'utilisation des applications en mettant à leur

disposition un cours interactif et exploitable dans un navigateur. Ce cours doit être axé sur la simplicité du contenu pour une meilleure assimilation par les utilisateurs et ce via des Pop-Ups didactiques qui doivent se présenter pour chaque fonctionnalité et assister à son exploitation. La langue utilisée pour le didacticiel est l'Arabe.

Pour les sites Web, des Popups doivent être prévus, selon la langue choisie par l'utilisateur (arabe, français et anglais).

1.5.7 Consultation et recherche de données

Un moteur de recherche devra être intégré, que ce soit en Front-office ou en Back-office et doit répondre aux différentes exigences quant aux modes de recherche simple et avancée (multicritère) :

- La recherche se fera principalement en arabe et doit être adaptée pour les noms propres en utilisant un système de transcription phonétique et linguistique.
- Les documents « non-image » stockés dans le système doivent être indexés par leurs index prédéfinis (métadonnées) et/ou par leurs contenus permettant ainsi des recherches en texte intégral ;
- Les fonctions de recherche doivent être disponibles dans les interfaces web ;
- Les recherches doivent être possibles avec les opérations (booléennes et autres) standards de recherche ; on doit retrouver les deux modes de recherche : la recherche simple et avancée ;
- L'enregistrement des requêtes est spécifique à la recherche avancée ;
- Une prévisualisation de l'information (présentation des identifiants du document) pratiquement immédiate ;
- Une recherche full-texte sur les entités et les documents associés ;
- Les propriétés des recherches multicritères doivent être personnalisables ;
- Les propriétés affichées dans les résultats de recherches doivent être administrables ;
- Les résultats de recherches peuvent être exportés et téléchargés sous forme de fichiers standards CSV, PDF, DOCX, XLSX, JPG, ODT, ...etc.

1.5.8 Administration

L'interface doit intégrer un module d'administration convivial assurant toutes les fonctions nécessaires à la gestion de toutes ces composantes et nomenclatures tel que :

- Gestion des utilisateurs ;
- Gestion des droits d'accès via une matrice détaillée permettant la création et la modification des rôles. Cette matrice indiquera en détails les interfaces disponibles pour chaque module ;
- Création et mise à jour intuitive et assistée des catégories des événements et des procédures d'intervention, de la façon la plus simple et sans nécessité des connaissances en informatique ;
- Création de modèles de rapports ;
- Alimentation et mise à jour des nomenclatures ;
- Assignation d'un code de sécurité supplémentaire pour l'accès à certains menus
- ...etc.

De plus, toutes les informations traitées par le module d'administration peuvent être exportées sous formats électroniques avec mise en page (page de garde, date, identité de l'administrateur, ...etc), pour des besoins de documentation, de reporting et d'archivage.

Le prestataire doit prendre en considération que la gestion des ressources sera décentralisée, c'est-à-dire que pour chaque structure ou un ensemble de structures est affecté un administrateur qui se chargera de la gestion des utilisateurs et des droits d'accès aux rubriques de l'application.

1.6 SPECIFICATIONS TECHNIQUES

1.6.1 Architecture

L'application « casier numérique des postes de la sécurité publique » sera déployée en Intranet et sera implémentée selon une architecture centralisée et les données seront stockées dans une seule base de données.

Pour les sites Web, l'architecture proposée doit prendre en considération qu'il y aura une partie, Extranet, exposée aux internautes et une autre partie, Intranet, qui récupérera les données de la partie extranet et pour un usage de suivi et gestion en interne. Dans ce sens, le prestataire une fois sélectionné, est appelé à proposer une architecture virtualisée sécurisée selon les règles de sécurité les plus strictes et doit s'appuyer sur un bureau d'études expérimenté et certifié dans le domaine.

Le prestataire doit prendre en charge la création et la configuration des VMs, de type « VmWare », nécessaires y compris la haute disponibilité et l'équilibrage de charge si nécessaire.

1.6.2 Interfaces et IHM

Les interfaces doivent supporter les langues, arabe, français et anglais (en Intranet et en Extranet) et doivent être responsive (Responsive Web Design). Le prestataire devra proposer et implémenter une solution permettant d'adapter automatiquement la mise en page et le contenu des pages à la taille et résolution des écrans des supports numériques utilisés (Ordinateurs, Tablettes et Smartphones).

La charte graphique ainsi que les chartes ergonomiques et de navigation qui seront structurées et développées en respectant la structure et l'apparence actuelle de l'application « Tableau de Bord de Gestion » et pour les sites Web la charte du site actuel du ministère.

Les solutions proposées devront répondre aux standards du W3C, HTML5 et CSS3 afin de permettre une compatibilité des interfaces avec les navigateurs actuels et futurs (minimum les versions supportées par **Windows 7**) :

- Mozilla Firefox ;
- Google Chrome ;
- Microsoft EDGE ;
- Safari ;
- Opera.

Les interfaces doivent mettre l'accent sur la facilité, la simplicité d'utilisation, l'ergonomie, la clarté et le bon agencement des interfaces. Le choix de la technologie « one page » avec rafraîchissement automatique et exécution du côté du client est basée, entre autres, sur ces critères.

Ceci se traduit, entre autres, au niveau des interfaces par un agencement clair des champs, composition en zones identifiées, gestion des symboles et couleurs (pour le suivi), mise en surbrillance, animation des symboles et des couleurs, ...etc.

La conception des interfaces ne doit pas privilégier la représentation hiérarchique selon la modélisation, elle doit être plutôt axé sur la facilité de lecture et l'accès rapide aux informations et aux fonctionnalités. Plus une fonctionnalité est sollicitée, plus elle doit paraître en premier plan et soit accessible avec le minimum de manipulations et de transitions des interfaces.

La simplicité de l'utilisation peut être assurée par différents moyens en privilégiant :

- L'accès par raccourcis clavier ;
- La codification des listes ;
- L'utilisation de la propriété « AutoComplete » et mise à jour automatique des tables paramètres pour toute nouvelle entrée ;
- Passage automatique au champ suivant par suite d'une validation par clavier ;
- Navigation entre les champs en utilisant les touches flèches ;
- Effacement de l'historique de saisie une fois un formulaire est validé ;
- Pour certains champs, tel que les dates, le formulaire affichera la date du jour ou la dernière date choisie ;
- Pour les dates de naissance le prestataire doit proposer la méthode d'entrée la plus adéquate avec les contrôles nécessaires ;
- ...etc.

Le développement doit adopter un codage universel multilingues et l'interface doit supporter le LTR et RTL pour s'adapter à certains cas de figure, tel que l'affichage des résultats des requêtes avec les bases existantes.

Le prestataire doit tenir en compte l'option de la conception d'une interface modulaire permettant la modification de l'agencement des différentes zones, champs et fonctionnalités ainsi que d'autres aspects graphiques (polices, couleurs, symboles, ...etc), et ce au fur et à mesure de l'utilisation de l'application et du recueil des feedback des utilisateurs.

1.6.3 Outils de développement

En conformité avec les outils adoptées par le ministère de l'intérieur, les outils de développement qui seront utilisés pour le développement seront les suivants :

- Environnement et Framework de développement Java 8.

Pour des raisons de respect de délais du développement de l'application de gestion et de modernisation des outils de développement de l'équipe IT du ministère de l'intérieur, le prestataire doit s'appuyer sur un outil ou une plateforme de type Low-coding ou No-Code, pour la génération des formulaires et de Workflow (comme décrit dans le paragraphe X.6.5). L'outil ou la plateforme sera livré avec la solution et mis à disposition de l'équipe de développement avec l'accompagnement nécessaire.

La génération du code automatique sera autorisée si elle dépend d'un outil de développement libre et qui répond aux recommandations précédentes. Il est impératif de

pouvoir générer le code source sans se trouver bloqué par l'indisponibilité de l'environnement de développement.

Le prestataire ne doit faire recours à des bibliothèques non-standards (JAR, JavaScript, CSS, ...etc) que si besoin et qu'elles ont montrées une fiabilité prouvée. De plus, elles doivent disposer d'une communauté étendue et active.

1.6.4 Les codes sources et les binaires

Le ministère de l'intérieur doit disposer de l'intégralité du code source et des éléments permettant de générer les binaires.

Convention de codage

L'objectif principal des conventions de codage est de permettre une bonne compréhension et une bonne maintenabilité du code (couplage très faible des méthodes, ...etc).

Il est important que l'application respecte les bonnes pratiques du codage.

Les outils de contrôle

Les conventions de codage et de structuration devront être contrôlé par des outils standards les plus efficaces.

1.6.5 Outils de développement complémentaire

Le prestataire aura à utiliser des outils de développement complémentaire (FrameWork, SDK, ...etc) dont le but de bénéficier des avantages suivants :

- Faciliter la tâche de développement ;
- Un code source bien organisé et plus fiable ;
- Rapidité de développement ;
- Optimisation du temps et du coût.

Le prestataire peut utiliser des FrameWork et SDKs, open-source de préférence, permettant :

- Gestion des identités : Keycloak, ...etc ;
- Le reporting ;
- La génération de statistiques ;
- La génération de formulaires : génération et modification à partir d'une interface Web ;
- Edition de Workflow : Edition et modification à partir d'une interface Web ;
- Déploiement de l'application à partir d'une interface Web ;
- Gestion de projet : assure un meilleur suivi des différents projets et tâches en offrant des présentations graphiques multiples, à savoir : Kanban, Gantt, ...etc ;
- Monitoring open-source : serveur applicatif, base de données, liste des Beans disponibles, détails des threads (dump), l'état de l'application, les compteurs systèmes (RAM, les valeurs du heap Java, nombre de classes java, variables d'environnement, uptime, etc ...) ;
- Et tout autre FrameWork ou SDK jugé utile et efficace.

Le choix des FrameWorks et des SDKs doit répondre aux critères suivants :

- Robustesse et fiabilité réputés ;
- Communauté active et support assuré au moyen terme ;
- Ne présente pas de failles ou de vulnérabilités ;
- Facilité d'exploitation avec un effort minimale de la part du développeur.

1.6.6 Système d'exploitation

Toutes les machines virtuelles qui seront déployées que ce soit pour la phase de production ou de préproduction utiliseront le système d'exploitation Linux.

Le prestataire doit prendre en considération le choix d'une distribution parmi les plus robustes pour une meilleure stabilité et fiabilité de la solution.

1.6.7 Serveur d'application

Le ministère de l'intérieur dispose du serveur d'application IBM WebSphere Application Server v9.5 pour Linux sur lequel sera déployée l'application.

Durant le développement le déploiement et les tests doivent utiliser WebSphere Liberty Profile, pour assurer une meilleure compatibilité lors de du déploiement en production.

Pour les sites Web, le soumissionnaire doit s'appuyer sur un serveur d'application réputé pour sa sécurité et robustesse.

1.6.8 Base de données

Il est indispensable d'utiliser DB2 11.5 dont dispose le ministère de l'intérieur. Il faut noter que le SGBD peut intégrer les fichiers qui seront joints aux dossiers (PDF, JPEG, DOCX, MPEG, ...etc) et que cette jointure ne doit en aucun cas influencer sur la performance de la base de données et les temps de réponse des requêtes des utilisateurs.

Pour des raisons de sécurité et de protection des données, le prestataire doit prévoir un mécanisme de protection des données tel que le chiffrement.

1.6.9 Sites web

Les sites web doivent être développés avec les mêmes choix technologiques précédemment cités. Il est demandé d'utiliser en plus les techniques suivantes :

- Un outil pour le blocage des robots et l'authentification des utilisateurs enregistrés (Captcha, ...etc) ;
- Double-authentification : Google/Microsoft authenticator ;
- Blocage des robots par l'utilisation des mécanismes de génération de codes aléatoires ;
- ...etc.

Le prestataire est tenu de mettre en place, en commune concertation avec le ministère de l'intérieur, une architecture applicative hautement sécurisée et permettant de synchroniser les bases de données des sites Web (Extranet) avec les bases de données centrale situées dans la partie Intranet et ce en optant à différentes technologies tel que les proxys, les tokens, ...etc.

1.6.10 Application mobile de dépôt de plaintes en ligne

Le prestataire devra proposer le mode de développement (hybride ou natif) avec les arguments nécessaires pour défendre sa proposition.

La sécurité du code doit être la priorité et l'axe principal sur lequel doit se focaliser le prestataire afin de mettre en place une application hautement sécurisée et ce dès le début de la conception et tout au long du processus de développement.

Le prestataire doit intégrer des mécanismes de sécurité renforçant l'authentification et la confidentialité des données, à savoir : l'authentification forte, gestion des sessions, gestions des identités, communications sécurisées (SSL, TLS et certificats)

L'application doit prendre en considération les fonctionnalités et mécanismes suivants :

- Authentification simple ;
- Authentification forte ;
- Désactivation des PrintScreen ;
- Compatibilité à partir des versions suivantes : Android 8, iOS 8 ;
- Désactivation de l'enregistrement automatique des login et mots de passes ;
- Demande de réinitialisation de mot de passe ;
- Prise en charge des fonctions d'accès sécurisé à l'application (schéma, PIN, empreinte, reconnaissance faciale) ;

Le prestataire doit assister le ministère de l'intérieur pour la publication de l'application dans les Stores les plus utilisés afin qu'elle soit accessible au maximum de personnes, à savoir : Google Play, AppStore et AppGallery. Cette assistance couvrira la création de comptes au nom du ministère et aussi les frais d'enregistrement et d'abonnement pour une année.

1.6.11 Sécurité

Sécurité des données

Les solutions manipulent des données personnelles et des faits qui nécessitent une protection maximale à l'accès et la consultation et ce conformément avec les lois et directives de protection des données personnelles en Tunisie.

Pour ce faire les champs confidentiels doivent être chiffrer au niveau de la base de données, rendant les données protégées contre la consultation, la création, la suppression et la modification. Le prestataire est tenu d'assurer cette fonctionnalité en intégrant un algorithme fiable qui protège les données mêmes des tentatives de restitution des données originales via des moulinettes qui sont disponibles même en ligne.

Le prestataire concevra une solution sécurisée contre les tentatives de violation des données, les injections de code ou toute autre technique d'intrusion. Il décrira précisément la politique de sécurité mise en œuvre. Il doit prendre en considération et respecter les chartes de sécurité de l'ANCS (couche de données, connexions, HTTPS) et garantir l'impossibilité d'entrer du script au niveau d'un formulaire ou d'une url (Protéger contre l'url injection et SQL injection).

Le prestataire doit mettre en place tous les mécanismes pour éliminer les 10 domaines de risques identifiés par l'OWASP à savoir :

- Injection :
 - SQL Injection (WASC-19)
 - XML Injection (WASC-23)

- Null Byte Injection (WASC-28)
- LDAP Injection (WASC-29)
- Mail Command Injection (WASC-30)
- OS Commanding (WASC-31)
- XPath Injection (WASC-39)
- XQuery Injection (WASC-46)
- Cross-Site Scripting : Cross-Site Scripting (WASC-08) ;
- Violation de Gestion d'Authentification et de Session :
 - Insufficient Authentication (WASC-01)
 - Brute Force (WASC-11)
 - Credential/Session Prediction (WASC-18)
 - Session Fixation (WASC-37)
 - Insufficient Session Expiration (WASC-47) ;
- Référence directe à un objet non sécurisée :
 - Insufficient Authentication (WASC-01)
 - Insufficient Authorization (WASC-02)
 - Path Traversal (WASC-33)
 - Predictable Location (WASC-34) ;
- Falsification de requêtes intersites : Cross-Site Request Forgery (WASC-09) ;
- Gestion de configuration non sécurisée :
 - Server Misconfiguration (WASC-14)
 - Application Misconfiguration (WASC-15) ;
- Stockage de données non sécurisé : Insufficient Data Protection (WASC-50) ;
- Défaillance de restriction d'accès à une URL :
 - Insufficient Authorization (WASC-02)
 - Denial of Service (WASC-10)
 - Brute Force (WASC-11)
 - Insufficient Anti-automation (WASC-21)
 - Predictable Location (WASC-34) ;
- Communications non sécurisées : Insufficient Transport Layer Protection (WASC-04) ;
- Redirection et renvoi non validés : URL Redirector Abuse (WASC-38).

De plus les solutions doivent intégrer les mécanismes de renforcement de sécurité suivants :

- Limitation à une unique connexion d'un même équipement (PC, Tablette, SmartPhone, ...) ;

- Association entre le compte utilisateur et le site de connexion par la vérification de l'adresse IP source ;
- Blocage, génération d'alerte et reporting de la source ayant émis plusieurs tentatives de connexions simultanées ;
- Communications sécurisées TLS ;
- Protection contre les vulnérabilités TLS du RFC 7457 ;
- Implémentation de la spécification FIPS 202 pour la vérification de l'intégrité des données ou tout autre standard équivalent ;
- Contrôle d'accès aux informations selon les standards internationaux tel que le modèle NIST RBAC ;
- Tout autre mécanisme que le prestataire recommande.

Le prestataire doit assurer l'implémentation d'un système de sécurité sur plusieurs couches dans un API. Ce système assure l'élimination des failles et bugs lors de l'exposition des données à partir d'un API grâce à des mécanismes de sécurité multicouche, tel que la disposition suivante :

- Première couche : L'API d'extraction vérifie l'utilisateur et ses différents rôles pour pouvoir vérifier s'il a les bons droits de consulter ces informations. Si ce n'est pas le cas, l'API retourne un message d'erreur.
- Deuxième couche : Lors du premier contact entre la couche de données et l'API d'extraction, ce dernier fournit une proposition d'un plan de requête mais avant l'exécution de cette requête, la base de données assure la présence d'un certain nombre de filtres. Dans le cas contraire, cette proposition est rejetée.
- Troisième couche : Lorsque la couche de données interroge la base de données, elle utilise des jointures (pour le cas des bases de données SQL) sur les données de l'utilisateur qui fait appel à cet API, pour garantir que tous les objets interrogés correspondent à cet utilisateur.
- Quatrième couche : Tous les enregistrements renvoyés par la base donnée sont convertis en modèles visibles par l'utilisateur via une couche de mappage. Cette couche peut éliminer des informations sensibles ou des détails qui ne devaient pas être visible à l'utilisateur.
- Cinquième couche : les modèles générés par la couche de mappage sont examinés par le filtre de réponse de l'API. Ce filtre assure que tous les enregistrements font partie des données que l'utilisateur peut consulter. Cette couche rejette tous les modèles qui ne sont pas explicitement signalés comme visibles par le l'utilisateur.

Chaque couche empêche contre un type d'erreur différent :

- Les tests de l'API détectent des discordances accidentelles.
- L'analyseur de requêtes protège contre un oubli où vous oubliez d'ajouter la sécurité de la couche de données.
- La couche SQL vérifie le contexte utilisateur par rapport à son magasin de données
- La couche de mappage empêche l'exposition accidentelle des détails d'implémentation.
- La réponse API revérifie le travail de chacune des couches au-dessus.

Chaque couche lève des exceptions par elle-même, on peut définir exactement où se produit chaque bug et erreur et à quelle fréquence les risques de sécurité sont présents.

Droits d'accès

Le système doit assurer un contrôle d'accès renforcé en adoptant les mesures suivantes :

- Une seule session est autorisée par utilisateur ;
- Changement du mot de passe lors de la première connexion ;
- Déconnexion de la session après un temps d'inactivité ;
- **Association du nom d'utilisateur avec une @IP ou une adresse réseau ;**
- Signalisation des tentatives de connexion échouées ;
- Et tout autres mécanismes proposés par le prestataire.

Traçabilité

Les solutions doivent enregistrer toutes les actions applicatives dans un journal dédié : connexion, consultation, modification, insertion, changement de mot de passes, interfaces utilisées, recherches effectuées, export, impression, ... etc.

Une interface dédiée doit être développée pour faciliter la lecture, le tri, la filtration et la recherche multicritères du journal et la fourniture d'un résultat pertinent.

1.6.12 Tests et intégration

Le prestataire est tenu d'effectuer une série de tests sur le code source et les différents modules de l'application afin de vérifier la bonne structuration, la conformité aux normes internationales, l'optimisation et la sécurité du code source. Ce qui garantit la mise en place d'une application performante, robuste, fiable, sécurisée et facilement maintenable.

- Tests unitaires : il est recommandé d'utiliser un outil de gestion de tests unitaires. Cet outil fournit un support à l'écriture, l'évaluation, et à l'exécution des tests unitaires. Ceux-ci vérifient qu'un package ne comporte pas d'erreurs de conception ou de programmation. Les tests unitaires doivent être prévus au moment du développement pour les composantes importantes de l'application. Ceux-ci doivent permettre aussi la vérification des composantes techniques et de contrôler la connectivité (SGBD, serveur d'application, ...etc). Livrable : rapport.
- Tests de performance : ce type de tests vérifie que les contraintes de temps de réponse, de tenu en charge et de stress sont respectées. Lorsque cela est pertinent, l'application ou le composant technique seront testés avec des outils prévus à cet effet. Livrable : rapport.
- Mesure de qualité du code : Il existe un ensemble de raisons justifiant la mesure de la qualité du code. Les principales sont :
 - Un code mal maîtrisé entraîne mécaniquement une augmentation régulière et constante de la dette technique ;
 - Une surveillance des métriques permet une diminution du coût de maintenance à moyen et long terme ;
 - Une accélération de la prise en main du code : un code homogène sera mieux pris en charge par l'équipe, et l'intégration de nouveaux arrivant s'en retrouve également facilitée ;

- Un refactoring plus aisé : c'est un effet de bord direct du point précédent. En facilitant la prise en main, on diminue l'effet boîte noire. Combiné au précepte YagNi d'XP et aux garde-fous de l'intégration continue, l'adaptation permanente du code au besoin s'en retrouve fortement facilité ;
- Qui dit approche quantitative dit processus automatisable et donc peu coûteux ;
- Livrable : rapport.
- Intégration continue : Elle repose souvent sur la mise en place d'une brique logicielle permettant l'automatisation de tâches : compilation, tests unitaires et fonctionnels, validation produit, tests de performances ...etc. À chaque changement du code, cette brique logicielle va exécuter un ensemble de tâches et produire un ensemble de résultats, que le développeur peut par la suite consulter. Cette intégration permet ainsi de ne pas oublier d'éléments lors de la mise en production et donc ainsi améliorer la qualité du produit³. Pour appliquer cette technique, il faut d'abord que :
 - Le code source soit partagé (en utilisant des logiciels de gestion de versions tels que CVS, Subversion, git, Mercurial, ...etc) ;
 - Les développeurs intègrent (commit) quotidiennement (au moins) leurs modifications ;
 - Des tests d'intégration soient développés pour valider l'application (avec JUnit par exemple).

Un outil d'intégration continue est ensuite nécessaire, tel que CruiseControl, Jenkins ou Travis CI. Les principaux avantages d'une telle technique de développement sont :

- Le test immédiat des modifications ;
- La notification rapide en cas de code incompatible ou manquant ;
- Les problèmes d'intégration sont détectés et réparés de façon continue, évitant les problèmes de dernière minute ;
- Une version est toujours disponible pour un test, une démonstration ou une distribution.
- Tests de sécurité : le code de l'application doit subir une série de tests de sécurité afin de renforcer sa robustesse. L'inspection doit être de type Full-Stack et vise à rechercher les vulnérabilités potentielles du code, des dépendances, des Frameworks, SDKs, conteneurs, systèmes d'exploitation, ...etc. Dans ce sens une prise en considération des guides de l'OWASP est fortement recommandée.
- Tests fonctionnels : le prestataire est tenu de réaliser une série de tests fonctionnels via des outils dédiés et ce pour chaque livraison. La création des campagnes de tests couvrant les fonctionnalités à valider en exécutant un plan de tests qui permet de découvrir les éventuelles anomalies de manière rigoureuse et organisée. L'exécution d'une campagne de test donne un aperçu du nombre de problèmes techniques et fonctionnels, et permet de renseigner un traceur de bogues (comme Mantis).

1.6.13 Audit de sécurité

Le prestataire est tenu d'effectuer un audit de sécurité approfondi de l'application et des sites Web auprès d'un bureau d'audit spécialisé et accrédité par l'Agence Nationale de la Cyber Sécurité (ANCS). L'application et les sites Web ne peuvent être considérées comme sûres et peuvent être mises en exploitation que par la suite d'un audit valide et conforme aux normes de sécurité les plus exigeantes, adoptées par l'ANCS.

En plus, le prestataire doit tenir en compte que l'audit de sécurité sera une activité qui accompagnera le processus de maintenance curative et évolutive prévus dans le présent RFQ.

1.6.14 Journaux

Traces et journaux

Il est important de pouvoir avoir deux niveaux de lecture des traces générées par l'applicatif :

- Un niveau interprétable par un administrateur système ne connaissant pas le langage de développement ;
- Un niveau de lecture dédié à l'analyse de l'applicatif par le développeur.

Les traces servant au débogage doivent être désactivable lors de la production.

Structure des journaux

Les journaux doivent respecter les critères de structuration suivants :

- Notion de priorité : Debug, Info, Warning, Error, Fatal ;
- L'horodatage ;
- La catégorie ;
- Les messages.

1.7 Prestations et conditions PARTICULIERES

1.7.1 Accompagnement, garantie et support technique

Il est attendu que l'équipe technique du ministère de l'intérieur sera capable, à l'issu des travaux de développement, de conduire de façon autonome les activités techniques requises pendant tout le cycle de vie de l'application depuis l'expression des besoins jusqu'à l'exploitation et les tests de conformité et de performance applicative.

Accompagnement

Afin d'assurer une maîtrise maximale de la technologie par l'équipe technique du ministère de l'intérieur, le prestataire doit assurer une série d'activités tout au long des processus de développement à savoir :

- L'équipe technique du ministère de l'intérieur doit être impliqué durant toutes les phases de développement de l'application : étude, conception, développement, testing, et mise en production ;
- Reproduire les travaux de préparation de l'environnement de développement et de production ;
- Périodiquement, le prestataire doit assurer une journée pour présenter et expliquer en détails, l'avancement des travaux, le codage, les tests, et effectuer une série d'exercices pratiques à l'équipe technique pour une meilleure assimilation et maîtrise. La journée sera organisée dans les locaux du ministère de l'intérieur.

Garantie

Le prestataire est tenu d'assurer une période de garantie de 12 mois après la livraison, de chaque solution, couvrant la résolution des problèmes de fonctionnement, bugs, failles, ...etc.

Maintenance et Support technique

Après la livraison et la fin de garantie, le prestataire doit assurer, durant une année, un support technique couvrant la mise à jour et l'assistance technique aux différentes requêtes de l'équipe technique pour éclaircissement concernant les modules logiciels utilisés pour la mise en place du système de gestion des plaintes et des inspections (FrameWorks, SDKs, SGBD, ...etc).

En cas d'incident, Le Titulaire doit en effet, mettre à la disposition du Ministère, un numéro ou plusieurs numéros permettant de joindre un interlocuteur qui devra être en mesure de résoudre le problème constaté et d'intervenir rapidement.

Les prestations d'assistance devront être assurées durant les jours ouvrés du lundi au vendredi (hors jours fériés) de 8 heures à 12 heures et de 14 heures à 18 heures.

Le Titulaire mettra à la disposition du Ministère un point d'entrée unique pour la gestion de l'assistance utilisateurs et la gestion de la maintenance sur l'ensemble de la solution. Les demandes d'assistance se feront via un système de ticketing (outils type PMS, Mantis, Quality Center...) permettant la description de la demande, ainsi que le suivi de son avancement.

Le Titulaire assurera les services suivants :

- Accusé de réception du message signalant l'incident ;
- Notification de la prise en charge de la demande, dans le respect du délai de Garantie de Temps d'Intervention.

A l'issue du diagnostic établi par le service support sur la base des informations complémentaires éventuelles, et dans le cas d'un dysfonctionnement avéré du produit, une notification d'incident doit être envoyée

Maintenance évolutive

De plus il est prévu d'assurer 12 mois de maintenance évolutive en parallèle avec la période de garantie, dont le but d'apporter des améliorations aux applications et d'ajouter de nouvelles fonctionnalités. Le nombre de jours est calculé à la base 20% du nombre de jours total pour le développement de chaque application.

1.8 Hébergement

Le prestataire doit assurer un hébergement provisoire (dans un environnement similaire à l'environnement de production), d'au moins 06 mois, des 03 sites web pendant la période de développement et de test, avec un accès privé et avec une possibilité d'un accès public.

1.9 Documentation

Une documentation technique très détaillée, structurée et bien commenté concernant les solutions à développer doit être fournie et doit respecter les règles d'écriture standard.

Le prestataire doit fournir entre autres les détails suivants :

- Documentation UML 2.0 avec format d'échange XML ;
- Architecture technique ;
- Modélisation et spécifications fonctionnelle ;
- Livrable de chaque itération ;
- Rapports de tests consolidés ;
- Product BackLog final ;

- Rapport d'intégration ;
- Etats d'édition des rapports ;
- Code source bien commenté et effectuer une passation complète et efficace permettant à l'équipe IT du ministère d'assurer la maintenance et la mise à jour de l'application. En plus il doit une documentation détaillée des nominations spécifiques des nomenclatures ;
- Guide de déploiement détaillé avec tous les incidents rencontrés et leurs remèdes.
- Scripts, fichiers de config ;
- ...etc.

Il faut bien noter que le diagramme de classes doit être présent dans la documentation UML, et le diagramme de séquences est obligatoire pour mieux comprendre l'interaction dans l'application.

1.10 Formation

Pour chacune des solutions, le prestataire sera chargé d'assurer une formation :

- Des formateurs qui se chargent de former les utilisateurs finaux. Un guide d'utilisation doit être élaboré pour assister les formateurs et les utilisateurs ;
- Formation sur l'administration de l'application. Un guide doit être élaboré.

1.11 Qualification de l'Equipe intervenante et de l'entreprise

Il est demandé dans le cadre de ce cahier des charges de développer, **simultanément**, une application de gestion et 03 sites Web au profit de bénéficiaires différents. Il est demandé du prestataire de mettre à la disposition de ces projets, au minimum, les compétences suivantes :

- Un point focal avec une expérience minimale de 5 années en gestion de projets ;
- Un Product Owner avec une expérience minimale de 5 années en tant que PO ;
- Un Scrum Master avec une expérience minimale de 3 années en tant que SM ;
- Deux développeurs seniors certifiés Oracle Certified Professional avec une expérience minimale de 3 années en développement ;
- Deux développeurs juniors avec un minimum de 2 années d'expérience en développement ;
- Développeur mobile avec une expérience minimale de 2 années en cette spécialité ;
- Testeur certifié ISTQB avec une expérience minimale de 2 années en développement mobile ;
- Spécialiste UX avec une expérience minimale de 2 années en cette spécialité ;
- Un ingénieur infrastructure et système.

Cette liste n'est pas restrictive et le prestataire est tenu de mettre en place les ressources nécessaires pour assurer la livraison dans les délais contractuels.

L'entreprise doit satisfaire au moins les critères suivants :

- Une expérience d'au moins 04 années dans le domaine du développement des applications informatique dans l'environnement Java ;
- Au moins 06 projets clôturés durant les 03 dernières années ;
- Une équipe stable ;

- Un projet achevé avec une agence onusienne ou à l'échelle internationale durant les 03 dernières années.

1.12 Échéances

| Projet | Échéance |
|---|------------------|
| Casier numérique des postes de la sécurité publique | 10 décembre 2024 |
| Site Web et application mobile : Plaintes en ligne | 31 octobre 2024 |
| Site Web : demandes en ligne du bulletin N°3 | 10 décembre 2024 |
| Site Web : bulletin N°3 en ligne | 10 décembre 2024 |

1.13 Modalités de paiement

| Livrable/ Description de l'activité | Délais de livraison | % de paiement |
|--|------------------------|---------------|
| Casier numérique des postes de la sécurité publique | | |
| Chronogramme et plan de travail | 30 août | 15 % |
| Préparation de l'infrastructure virtualisée | | |
| Déploiement de la rubrique statistiques | 30 septembre | 15 % |
| Déploiement des rubriques Services type 1 et type 2 | 31 octobre | 20 % |
| Déploiement des rubriques Services type 3 et type 4 | 29 novembre | 20 % |
| Gestion des équipements, gestion du personnel et bibliothèque | 10 décembre | 20 % |
| Formation | 20 décembre | 10 % |
| Garantie et maintenance corrective de 12 mois après réception finale | - | - |
| Maintenance évolutive de 12 mois après réception finale | - | - |
| Total | | 100 % |
| Site Web et application mobile : Plaintes en ligne | | |
| Chronogramme et plan de travail | 30 août | 15 % |
| Préparation de l'infrastructure virtualisée | | |
| Déploiement du site Web | 18 octobre | 75 % |
| Formation | Octobre | 10 % |
| Garantie et maintenance corrective de 12 mois après réception finale | - | - |
| Maintenance évolutive de 12 mois après réception finale | - | - |
| Total | | 100 % |
| Site Web : demandes en ligne du bulletin N°3 | | |
| Chronogramme et plan de travail | 30 août | 15 % |
| Préparation de l'infrastructure virtualisée | | |
| Déploiement du site Web | 15 novembre | 75 % |
| Formation | Octobre | 10 % |
| Garantie et maintenance corrective de 12 mois après réception finale | - | - |
| Maintenance évolutive de 12 mois après réception finale | - | - |
| Total | | 100 % |
| Site Web et application mobile : Bulletin N°3 en ligne | | |
| Chronogramme et plan de travail | 30 août | 15 % |
| Préparation de l'infrastructure virtualisée | | |
| Déploiement du site Web | 15 novembre | 75 % |
| Formation | Octobre | 10 % |
| Garantie et maintenance corrective de 12 mois après réception finale | - | - |
| Maintenance évolutive de 12 mois après réception finale | - | - |
| Total | | 100 % |



1.13.1 Format de réponse

Le soumissionnaire doit détailler sa réponse pour répondre rubriques suivantes :

- Méthodologie ;
- Spécifications fonctionnelles métiers ;
- Spécifications fonctionnelles applicatives ;
- Spécifications techniques ;
- Prestations et conditions particulières ;
- Documentation ;
- Formation ;
- Qualification de l'entreprise et de l'équipe intervenante.

Critères d'évaluation technique

| Résumé des formulaires d'évaluation des propositions techniques | | Points Maximum |
|---|--|----------------|
| 1. | Qualification, capacité et expérience du soumissionnaire | 200 |
| 2. | Méthodologie, approche et plan de mise en œuvre proposés | 400 |
| 3. | Structure de gestion et personnel clé | 400 |
| Total | | 1000 |

| Section 1. Qualification, capacité et expérience du soumissionnaire | | Points Maximum |
|---|--|----------------|
| 1.1 | Nombre d'années d'expérience dans le développement et la fourniture de solutions logicielles : <ul style="list-style-type: none"> 04 - 08 ans -> 20 points ; Plus de 08 ans -> 30 points. | 30 |
| 1.2 | Capacité organisationnelle générale susceptible d'influer sur la mise en œuvre : structure de gestion, gestion du personnel, contrôles de gestion de projet, mesures dans laquelle tout travail serait sous-traité : <ul style="list-style-type: none"> Structure organisationnelle -> 15 points ; Procédures de formation du personnel -> 15 points ; Manuels de procédures -> 15 points ; Système d'information de gestion et outils de suivi des projets -> 15 points. | 60 |
| 1.3 | Procédures et mécanismes d'assurance de la qualité, de protection des données personnelles et mesures d'atténuation des risques. Des certifications seront une plus-value (ISO 9001, PMP, PECB, GDPR, ...etc) : <ul style="list-style-type: none"> ISO 9001 -> 10 points ; PMP ou équivalent -> 10 points ; PECB ou équivalent -> 10 points ; GDPR -> 10 points ; Organisation et mécanismes d'atténuation des risques et de protection des données personnelles -> 10 points. | 50 |
| 1.4 | Nombre de projets nationaux et internationaux similaires clôturés en termes de complexité pendant les 03 dernières années : <ul style="list-style-type: none"> Plus que 6 -> 30 points ; de 4 - 6 -> 20 points ; <= 3 -> 15 points. | 30 |
| 1.5 | Nombre de projets clôturés à l'international pendant les deux dernières années : <ul style="list-style-type: none"> 3 ou plus -> 30 points ; 1 ou 2 -> 15 points ; 0 -> 0 points. | 30 |
| Total Section 1 | | 200 |

| Section 2. Méthodologie, approche et plan de mise en œuvre proposés | | Points Maximum |
|---|--|----------------|
| 2.1 | Compréhension de l'exigence : les aspects importants de la tâche ont-ils été abordés avec suffisamment de détails ? Les différents éléments du projet sont-ils suffisamment pondérés par rapport à l'autre ? | 60 |
| 2.2 | Description de l'approche et de la méthode de l'offrant pour satisfaire ou dépasser les exigences du mandat. | 80 |
| 2.3 | Précisions sur la façon dont les différents éléments de service seront organisés, contrôlés et livrés. | 60 |
| 2.4 | Description des mécanismes et des outils de suivi et d'évaluation des performances disponibles ; comment ils seront adoptés et utilisés pour une exigence spécifique. | 80 |

| | | |
|------------------------|--|------------|
| 2.5 | Évaluation du plan de mise en œuvre proposé, y compris si les activités sont correctement séquencées et si celles-ci sont logiques et réalistes. | 70 |
| 2.6 | Démonstration de la capacité de planifier, d'intégrer et de mettre en œuvre efficacement les mesures de durabilité dans l'exécution du contrat. | 50 |
| Total Section 2 | | 400 |

| Section 3. Structure de gestion et personnel clé | | Points Maximum |
|---|---|-----------------------|
| 3.1 | Qualifications du personnel clé proposé | |
| 3.1 a | Point focal | 60 |
| | Expérience générale : <ul style="list-style-type: none"> 5 ans ou plus -> 10 points ; <=5 ans -> 0 points. | 10 |
| | 5 années d'expérience en gestion et suivi des projets : <ul style="list-style-type: none"> Plus que 7 ans -> 30 points ; Entre 5 et 7 ans -> 20 ans ; <5 ans -> 0 points. | 30 |
| | Nombre d'expériences Internationale en tant que gestionnaire de projets : <ul style="list-style-type: none"> 2 ou plus -> 10 points ; 1 -> 5 points ; 0 -> 0 points. | 10 |
| | Qualifications linguistiques : <ul style="list-style-type: none"> Français et anglais lu et écrit -> 10 ; Sinon 0 points. | 10 |
| 3.1 b | Product Owner | 60 |
| | Expérience générale : <ul style="list-style-type: none"> 5 ans ou plus -> 10 points ; <5 ans -> 0 points. | 10 |
| | 5 années d'expérience en tant que PO : <ul style="list-style-type: none"> Plus que 7 ans -> 30 points ; Entre 5 et 7 ans -> 20 ans ; <5 ans -> 0 points. | 30 |
| | Nombre d'expériences internationale en tant PO : <ul style="list-style-type: none"> 2 ou plus -> 10 points ; 1 -> 5 points ; 0 -> 0 points. | 10 |
| | Qualifications linguistiques : <ul style="list-style-type: none"> Français et anglais lu et écrit -> 10 ; Sinon 0 points. | 10 |
| 3.1 c | Scrum Master | 60 |
| | Expérience générale : <ul style="list-style-type: none"> 3 ans ou plus -> 10 points ; <5 ans -> 0 points. | 10 |
| | 3 années d'expérience en tant que SM : <ul style="list-style-type: none"> Plus que 5 ans -> 30 points ; Entre 3 et 5 ans -> 20 ans ; <3 ans -> 0 points. | 30 |

| | | | |
|-------|---|----|----|
| | <p>Nombre d'expérience internationale en tant que SM :</p> <ul style="list-style-type: none"> • 2 ou plus -> 10 points ; • 1 -> 5 points ; • 0 -> 0 points. | 10 | |
| | <p>Qualifications linguistiques :</p> <ul style="list-style-type: none"> • Français et anglais lu et écrit -> 10 ; • Sinon 0 points. | 10 | |
| 3.1 d | Développeur senior 1 certifié OCP | | 60 |
| | <p>Expérience générale :</p> <ul style="list-style-type: none"> • 3 ans ou plus -> 10 points ; • <3 ans -> 0 points. | 10 | |
| | <p>3 années d'expérience en développement :</p> <ul style="list-style-type: none"> • Plus que 5 ans -> 30 points ; • Entre 3 et 5 ans -> 20 ans ; • <3 ans -> 0 points. | 30 | |
| | <p>Nombre d'expériences internationale en tant que développeur senior :</p> <ul style="list-style-type: none"> • 2 ou plus -> 10 points ; • 1 -> 5 points ; • 0 -> 0 points. | 10 | |
| | <p>Qualifications linguistiques :</p> <ul style="list-style-type: none"> • Français et anglais lu et écrit -> 10 ; • Sinon 0 points. | 10 | |
| 3.1 e | Développeur senior 2 certifié OCP | | 60 |
| | <p>Expérience générale :</p> <ul style="list-style-type: none"> • 3 ans ou plus -> 10 points ; • <3 ans -> 0 points. | 10 | |
| | <p>3 années d'expérience en développement :</p> <ul style="list-style-type: none"> • Plus que 5 ans -> 30 points ; • Entre 3 et 5 ans -> 20 ans ; • <3 ans -> 0 points. | 30 | |
| | <p>Nombre d'expériences internationale en tant que développeur senior :</p> <ul style="list-style-type: none"> • 2 ou plus -> 10 points ; • 1 -> 5 points ; • 0 -> 0 points. | 10 | |
| | <p>Qualifications linguistiques :</p> <ul style="list-style-type: none"> • Français et anglais lu et écrit -> 10 ; • Sinon 0 points. | 10 | |
| 3.1 f | Testeur certifié ISTQB | | 50 |
| | <p>Expérience générale :</p> <ul style="list-style-type: none"> • 2 ans ou plus -> 10 points ; • <2 ans -> 0 points. | 10 | |
| | <p>2 années d'expérience en tant que testeur ISTQB :</p> <ul style="list-style-type: none"> • Plus que 2 années -> 30 points ; • 2 années -> 20 points ; • Moins de 2 années -> 0 points. | 30 | |
| | <p>Qualifications linguistiques :</p> <ul style="list-style-type: none"> • Français et anglais lu et écrit -> 10 ; • Sinon 0 points. | 10 | |
| 3.1 g | Spécialiste UX | | 50 |

| | | | |
|------------------------|--|----|------------|
| | Expérience générale : <ul style="list-style-type: none"> • 2 ans ou plus -> 10 points ; • <2 ans -> 0 points. | 10 | |
| | 2 années d'expérience spécifique pertinente à l'affectation : <ul style="list-style-type: none"> • Plus que 2 années -> 30 points ; • 2 années -> 20 points ; • Moins de 2 années -> 0 points. | 30 | |
| | Qualifications linguistiques : <ul style="list-style-type: none"> • Français et anglais lu et écrit -> 10 ; • Sinon 0 points. | 10 | |
| Total Section 3 | | | 400 |