CAHIER DES CHARGES

Projet : Plateforme Numérique de Gestion Documentaire Sécurisée intégrant des Techniques d'Intelligence Artificielle

Organisme : Direction des Systèmes d'Informations et de la Transformation Numérique (DSITN)
Version : 2.0 – Version Institutionnelle Conforme Sécurité & Réglementation

Version	Auteur	Statut
2.0	• Ouassou oussama • Masnaoui Ismail • Mataich Anas • Bnitir mohamed	

1. Introduction

1.1 Contexte

Dans le cadre de la stratégie nationale de transformation digitale menée sous l'impulsion de :

- Agence de Développement du Digital
- Direction Générale de la Sécurité des Systèmes d'Information
- Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel

La **DSITN** doit moderniser la gestion documentaire interne afin de :

- Garantir la sécurité des données sensibles
- Assurer la conformité réglementaire
- Optimiser les processus métiers
- Renforcer la traçabilité et la gouvernance des informations

La gestion actuelle présente :

- Risque de fuite d'informations
- Manque de traçabilité
- Archivage non structuré
- Accès non centralisés

1.2 Objectif du document

Ce Cahier des Charges a pour objectif de :

- Définir les besoins fonctionnels et non fonctionnels
- Encadrer les exigences réglementaires
- Garantir la conformité aux normes nationales et internationales
- Servir de document contractuel de référence

2. CADRE RÉGLEMENTAIRE ET NORMATIF

La solution devra respecter :

Référence	Désignation	Exigence
Loi 09-08	Protection des données personnelles	Déclaration CNDP obligatoire
Loi 53-05	Échange électronique des données juridiques	Intégrité & valeur probante
Directive DGSSI	Sécurité des SI publics	Conformité PSSI
ISO/IEC 27001	Management sécurité de l'information	Bonnes pratiques
ISO 27002	Contrôles de sécurité	Mesures techniques
Loi 05-20		

3. Présentation Générale du Projet

3.1 Objectif Général

Développer une plateforme sécurisée permettant :

- Centralisation documentaire
- Contrôle d'accès avancé
- Automatisation par IA
- Recherche intelligente
- Archivage sécurisé
- Journalisation conforme aux exigences DGSSI

3.2 Objectifs Spécifiques

N°	Objectif
O1	Authentification forte (MFA recommandé)
O2	Gestion RBAC conforme ISO 27001
O3	Chiffrement des données au repos et en transit
O4	Versioning sécurisé
O5	Intégrer un module OCR
O6	Classification automatique IA / recherche intelligente
O7	Sauvegarde & Plan de Reprise d'Activité

4. Périmètre du Projet

4.1 Inclus dans le projet

La solution devra inclure :

- Gestion utilisateurs
- Gestion rôles & permissions
- Gestion documentaire complète
- Module IA (OCR + classification)
- Audit complet
- Recherche plein texte
- Sauvegarde automatique
- Archivage sécurisé

4.2 Hors périmètre

Élément	Justification
Signature électronique légale	Complexité juridique
Application mobile native	Hors scope du stage
Intégration ERP complète	Projet trop étendu
Blockchain	Non prioritaire

5. Parties Prenantes

5.1 Identification des Parties Prenantes

Les parties prenantes du projet regroupent l'ensemble des acteurs impliqués dans la définition, la conception, la réalisation, la validation et l'exploitation de la plateforme numérique sécurisée de gestion documentaire au sein de la **Direction des Systèmes d'Informations et de la Transformation Numérique (DSITN)**.

Le tableau ci-dessous présente les principaux acteurs du projet :

Acteur	Rôle
Direction des Systèmes d'Informations et de la Transformation Numérique (DSITN)	Maîtrise d'Ouvrage – Expression du besoin et validation
Étudiant (Chef de projet)	Conception, développement et implémentation

Encadrant académique	Validation pédagogique et suivi académique
Responsable Sécurité des SI (RSSI)	Validation conformité sécurité et réglementaire
Administrateurs système	Exploitation technique et maintenance
Utilisateurs finaux	Exploitation fonctionnelle de la plateforme
Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel	Autorité de contrôle pour la conformité Loi 09-08

5.2 Rôles et Responsabilités

5.2.1 Direction des Systèmes d'Informations et de la Transformation Numérique (DSITN)

- Définition des besoins fonctionnels
- Validation du Cahier des Charges
- Validation des livrables
- Participation à la recette finale

5.2.2 Étudiant

- Analyse des besoins
- Conception UML et architecture
- Développement backend et frontend
- Intégration du module IA
- Mise en œuvre des exigences de sécurité
- Rédaction des livrables (CDC, SFG, SFD, Rapport)

5.2.3 Encadrant Académique

- Validation méthodologique
- Suivi pédagogique
- Validation des livrables académiques
- Participation à l'évaluation finale

5.2.4 Responsable Sécurité des Systèmes d'Information (RSSI)

- Validation des mécanismes de sécurité
- Vérification conformité aux directives nationales

- Validation des politiques de gestion des accès
- Validation des mécanismes de journalisation

5.2.5 Utilisateurs Finaux

- Utilisation quotidienne de la plateforme
- Tests fonctionnels
- Remontée des anomalies
- Participation à la validation opérationnelle

5.3 Organisation du Pilotage

Le projet est piloté selon une structure simplifiée adaptée au cadre d'un stage PFE :

Niveau	Responsable	Mission
Stratégique	DSITN	Validation et orientation
Technique	Étudiant	Réalisation du projet
Pédagogique	Encadrant académique	Encadrement académique

Des réunions de suivi périodiques seront organisées afin de :

- Contrôler l'avancement
- Identifier les risques
- Valider les étapes intermédiaires

6. Acteurs du Système

6.1 Identification des Acteurs

Les acteurs du système représentent les entités qui interagissent directement avec la plateforme numérique de gestion documentaire. Ils peuvent être humains ou systèmes externes.

Acteur	Type	Description	Niveau d'accès
Administrateur	Interne	Responsable de la gestion globale du système	Accès complet
Gestionnaire documentaire	Interne	Responsable de la gestion et validation des documents	Accès avancé

Utilisateur standard	Interne	Utilisateur métier exploitant les documents	Accès limité selon rôle
Responsable Sécurité (RSSI)	Interne	Supervision sécurité et audit	Accès aux logs et audits
Système IA	Système interne	Analyse automatique (OCR + classification)	Accès contrôlé aux documents
Système de sauvegarde	Système technique	Sauvegarde automatique des données	Accès base de données et stockage

6.2 Description des Acteurs

6.2.1 Administrateur

L'administrateur dispose des privilèges les plus élevés.
Il est responsable de :

- Création et gestion des utilisateurs
- Attribution des rôles et permissions
- Supervision globale du système
- Suppression définitive des documents
- Consultation des journaux d'audit

6.2.2 Gestionnaire Documentaire

Il assure :

- Validation des documents
- Organisation des catégories
- Suivi du cycle de vie documentaire
- Archivage

6.2.3 Utilisateur Standard

Il peut :

- Téléverser des documents
- Rechercher des documents
- Consulter les documents autorisés
- Modifier ses propres documents (selon permissions)

6.2.4 Responsable Sécurité des SI (RSSI)

Il est chargé de :

- Contrôler les accès
- Vérifier les journaux d'audit
- Superviser la conformité réglementaire
- Valider les mécanismes de sécurité

6.2.5 Système IA

Le module IA agit automatiquement pour :

- Extraire le texte via OCR
- Classifier les documents
- Indexer le contenu

Il ne possède pas de rôle humain mais interagit avec les données selon des règles strictes.

6.3 Synthèse des Droits par Acteur

Fonctionnalité	Admin	Gestionnaire	Utilisateur	RSSI
Créer utilisateur	✓	✗	✗	✗
Attribuer rôles	✓	✗	✗	✗
Upload document	✓	✓	✓	✗
Modifier document	✓	✓	Selon rôle	✗
Supprimer définitif	✓	✗	✗	✗
Consulter logs	✓	✗	✗	✓

7. Organisation du Projet

7.1 Phases du Projet

Phase	Description	Durée
Étude	Analyse des besoins	3 semaines
Conception	Modélisation UML	3 semaines

Développement	Implémentation	6 semaines
Tests	Validation & correction	2 semaines
Intégration	Déploiement & documentation	2 semaines

8. Livrables

8.1 Livrables d'Entrée

Les livrables d'entrée correspondent aux éléments nécessaires au démarrage du projet.

N°	Type	Livrable	Description
LE1	Documentaire	Sujet de stage validé	Intitulé officiel du projet et validation académique
LE2	Documentaire	Expression des besoins	Description des attentes fonctionnelles
LE3	Organisationnel	Planning prévisionnel	Planification des phases du projet
LE4	Technique	Environnement de développement	IDE, serveur local, base de données
LE5	Technique	Contraintes techniques	Technologies imposées ou recommandées
LE6	Sécurité	Politique de sécurité (si disponible SMSI) / Audit / Règlementation	Règles internes de gestion des données

8.2 Livrables de Sortie

Les livrables de sortie correspondent aux résultats attendus à la fin du projet.

8.2.1 Livrables Documentaires

N°	Livrable	Description	Validation
LS-D1	Cahier des Charges (CDC)	Définition complète des besoins	Encadrant
LS-D2	SFG	Spécifications fonctionnelles générales	Encadrant
LS-D3	SFD	Spécifications détaillées	Encadrant
LS-D4	Diagrammes UML	Cas d'utilisation, classes, séquences	Encadrant
LS-D5	Document d'architecture	Architecture technique détaillée	Encadrant
LS-D6	Rapport final	Rapport académique complet	Jury

8.2.2 Livrables Techniques

N°	Livrable	Description	**Critère** de Validation
LS-T1	Backend sécurisé	API REST fonctionnelle	Tests API réussis
LS-T2	Base de données	Modèle relationnel implémenté	Intégrité validée
LS-T3	Module IA	OCR + classification automatique	Tests fonctionnels
LS-T4	Système de stockage	Stockage sécurisé des fichiers	Sécurité validée
LS-T5	Interface utilisateur	Application web opérationnelle	Tests utilisateurs
LS-T6	Système d'authentification	Gestion JWT / RBAC	Tests sécurité

8.2.3 Livrables de Qualité et Validation

N°	Livrable	Description	Indicateur
LS-Q1	Tests unitaires	Couverture des fonctionnalités critiques	>70% couverture
LS-Q2	Tests d'intégration	Validation des modules interconnectés	Aucun bug critique
LS-Q3	Tests de sécurité	Vérification des accès et permissions	Accès contrôlé
LS-Q4	Documentation technique	Guide d'installation et d'utilisation	Document validé

LS-Q5	Démonstration finale	Présentation fonctionnelle du système	Validation jury

8.3 Synthèse Générale des Livrables

Catégorie	Nombre	Objectif
Livrables d'entrée	6	Lancer le projet
Livrables documentaires	6	Formaliser le projet
Livrables techniques	6	Implémenter la solution
Livrables qualité	5	Garantir conformité

9. Exigences Fonctionnelles détaillées avec Règles de Gestion

9.1 Gestion des Utilisateurs

9.1.1 Description

Ce module permet l'administration des comptes utilisateurs et la gestion des accès à la plateforme.

9.1.2 Règles de Gestion – Utilisateurs

Réf RG	Règle de Gestion
RG-U1	Un utilisateur doit posséder un identifiant unique.
RG-U2	Le mot de passe doit être stocké sous forme chiffrée (hash sécurisé).
RG-U3	Un utilisateur doit être associé à au moins un rôle.
RG-U4	Un administrateur peut créer, modifier ou désactiver un utilisateur.
RG-U5	Un utilisateur ne peut accéder qu'aux ressources autorisées par son rôle.
RG-U6	Après 5 tentatives de connexion échouées, le compte est temporairement bloqué.
RG-U7	Toute action utilisateur doit être enregistrée dans le journal d'audit.

9.2 Gestion des Rôles et Permissions

9.2.1 Description

Ce module permet d'attribuer des droits d'accès selon le principe RBAC (Role-Based Access Control).

9.2.2 Règles de Gestion – Rôles

Réf RG	Règle de Gestion
RG-R1	Un rôle définit un ensemble de permissions.
RG-R2	Un rôle peut être attribué à plusieurs utilisateurs.
RG-R3	Un utilisateur peut avoir plusieurs rôles.
RG-R4	Seul l'administrateur peut créer ou modifier un rôle.
RG-R5	Les permissions sont définies par type d'action (lecture, écriture, suppression).
RG-R6	Toute modification d'un rôle doit être journalisée.

9.3 Gestion des Documents

9.3.1 Description

Ce module assure la gestion complète du cycle de vie des documents.

9.3.2 Règles de Gestion – Documents

Réf RG	Règle de Gestion
RG-D1	Chaque document doit posséder un identifiant unique.
RG-D2	Un document doit être associé à un propriétaire.
RG-D3	Un document peut contenir plusieurs versions.
RG-D4	Seul le propriétaire ou un utilisateur autorisé peut modifier un document.
RG-D5	La suppression définitive est réservée à l'administrateur.
RG-D6	Les documents archivés ne peuvent pas être modifiés.
RG-D7	Les fichiers doivent être stockés de manière sécurisée (chiffrement).
RG-D8	La taille maximale d'un fichier doit être définie par configuration.

9.4 Gestion du Versioning

9.4.1 Description

Permet de conserver l'historique des modifications d'un document.

9.4.2 Règles de Gestion – Versioning

Réf RG	Règle de Gestion
RG-V1	Chaque modification crée automatiquement une nouvelle version.
RG-V2	Les versions précédentes doivent rester accessibles en lecture seule.
RG-V3	Une version doit contenir la date et l'auteur de modification.
RG-V4	La suppression d'une version doit être journalisée.

9.5 Gestion de la Recherche

9.5.1 Description

Permet de rechercher efficacement les documents.

9.5.2 Règles de Gestion – Recherche

Réf RG	Règle de Gestion
RG-S1	La recherche doit fonctionner sur le titre et les métadonnées.
RG-S2	La recherche plein texte doit analyser le contenu extrait par OCR.
RG-S3	Les résultats doivent respecter les permissions utilisateur.
RG-S4	Les résultats peuvent être filtrés par date, catégorie ou type.
RG-S5	Le temps de réponse ne doit pas dépasser 2 secondes.

9.6 Gestion du Module IA

9.6.1 Description

Ce module automatise l'analyse et le classement des documents.

9.6.2 Règles de Gestion – IA

Réf RG	Règle de Gestion
RG-IA1	Tout document uploadé déclenche automatiquement une analyse IA.
RG-IA2	Le texte extrait via OCR doit être sauvegardé dans la base.

RG-IA3	Le système doit proposer une catégorie automatique.
RG-IA4	L'utilisateur peut modifier la catégorie proposée.
RG-IA5	La classification doit être enregistrée dans les métadonnées.
RG-IA6	L'analyse IA ne doit pas bloquer l'upload du document.

9.7 Gestion de l'Audit et Journalisation

9.7.1 Description

Permet d'assurer la traçabilité complète des actions.

9.7.2 Règles de Gestion – Audit

Réf RG	Règle de Gestion
RG-A1	Toute connexion doit être enregistrée.
RG-A2	Toute modification de document doit être journalisée.
RG-A3	Les logs doivent inclure : utilisateur, date, action.
RG-A4	Les logs ne peuvent pas être modifiés par un utilisateur standard.
RG-A5	Les journaux doivent être conservés pendant une durée définie.

10. Exigences Non Fonctionnelles

10.1 Sécurité

Réf	Exigence
NF1	Chiffrement des fichiers
NF2	Hash des mots de passe
NF3	HTTPS obligatoire
NF4	Journalisation des accès
NF5	RBAC

10.2 Performance

Réf	Exigence	Description	Critère de Validation
PERF-1	Temps de réponse	Le temps de réponse moyen des requêtes ne doit pas dépasser 2 secondes en charge normale.	< 2 secondes pour 95% des requêtes
PERF-2	Indexation rapide	L'indexation d'un document après upload doit être réalisée automatiquement et rapidement.	Indexation < 5 secondes après upload
PERF-3	Support fichiers volumineux	Le système doit accepter des fichiers de grande taille sans dégradation critique des performances.	Support fichiers ≥ 50 MB sans erreur

10.3 Scalabilité

Réf	Exigence	Description	Critère de Validation
SCAL-1	Architecture modulaire	Le système doit être conçu en modules indépendants.	Séparation claire des couches (API, IA, DB)
SCAL-2	Extensibilité	Possibilité d'ajouter de nouvelles fonctionnalités sans refonte majeure.	Ajout module sans modification cœur système
SCAL-3	Compatibilité Cloud	Le système doit être déployable sur infrastructure cloud.	Déploiement via Docker ou serveur distant validé

10.4 Disponibilité

Réf	Exigence	Description	Critère de Validation
DISP-1	Sauvegarde automatique	Mise en place de sauvegardes régulières des données.	Sauvegarde quotidienne configurée
DISP-2	Gestion des erreurs	Le système doit gérer les erreurs sans interruption critique.	Aucun crash système lors d'erreurs contrôlées
DISP-3	Récupération après incident	Le système doit permettre la restauration des données en cas de panne.	Restauration testée avec succès

11. Architecture du Système

11.1 Vue Générale

La plateforme adopte une architecture modulaire multicouche respectant les principes de :

- Séparation des responsabilités
- Sécurité par conception (Security by Design)
- Scalabilité
- Maintenabilité

L'architecture repose sur une approche **API RESTful** avec séparation entre :

- Couche Présentation
- Couche API
- Couche Métier
- Couche IA
- Couche Données

11.2 Architecture Logique

Couche	Description	Technologies
Présentation	Interface utilisateur web	React / HTML / CSS
API	Exposition des endpoints sécurisés	Python (Fast API / Django REST)
Métier	Logique applicative et règles de gestion	Services Python
IA	OCR + Classification automatique	Python (Tesseract, Scikit-learn, TensorFlow)
Base de données	Stockage structuré des métadonnées	PostgreSQL
Stockage fichiers	Stockage sécurisé des documents	MinIO
Sécurité	Authentification & autorisation	JWT + RBAC

11.3 Architecture Physique

L'architecture physique pourra être déployée selon le schéma suivant :

- Serveur Backend (API Python)
- Serveur Base de Données PostgreSQL
- Serveur de stockage MinIO
- Serveur Web (Nginx en production)
- Conteneurisation via Docker

Cette architecture permet :

- Isolation des services
- Déploiement cloud ou on-premise
- Scalabilité horizontale

11.4 Sécurisation de l'Architecture

L'architecture intègre les mécanismes suivants :

- HTTPS (TLS 1.3)
- Chiffrement AES-256 pour les fichiers
- Hash sécurisé des mots de passe (Argon2 / bcrypt)
- Journalisation centralisée
- Séparation des environnements (Dev / Test / Production)

11.5 Justification des Choix

Le choix de Python pour le backend permet :

- Intégration native des modules IA
- Rapidité de développement
- Écosystème riche et mature
- Performance adaptée aux API REST

L'utilisation de PostgreSQL garantit :

- Intégrité transactionnelle
- Sécurité avancée
- Indexation performante

MinIO est retenu pour :

- Stockage objet sécurisé
- Compatibilité S3
- Facilité de déploiement

12. Contraintes Techniques et Organisationnelles

12.1 Contraintes Techniques

Domaine	Contrainte
Backend	Développement en Python
Architecture	Respect architecture REST
Base de données	PostgreSQL obligatoire
Stockage	Stockage sécurisé compatible S3
Sécurité	Implémentation JWT + RBAC
Performance	Temps de réponse < 2 secondes
Fichiers	Support ≥ 50 MB
Déploiement	Conteneurisation Docker

12.2 Contraintes de Sécurité

12.2.1 Conformité Réglementaire et Normative

Référence	Désignation	Exigence
Loi 09-08	Protection des données à caractère personnel	Déclaration et conformité aux exigences de protection des données
Directives nationales SSI	Directives de sécurité des systèmes d'information	Respect des politiques nationales de sécurité
ISO/IEC 27001	Système de management de la sécurité de l'information	Application des bonnes pratiques de sécurité

ISO/IEC 27002	Code de bonnes pratiques	Mise en œuvre des contrôles de sécurité

12.2.2 Exigences Techniques de Sécurité

Réf	Exigence	Description	Critère de Validation
SEC-1	Chiffrement des données en transit	Utilisation du protocole HTTPS (TLS 1.3)	Communication sécurisée activée
SEC-2	Chiffrement des données au repos	Chiffrement AES-256 des fichiers stockés	Données non lisibles sans clé
SEC-3	Journalisation	Enregistrement des connexions et actions	Logs horodatés disponibles
SEC-4	Politique mot de passe	Complexité minimale (majuscule, minuscule, chiffre, caractère spécial)	Validation automatique lors création
SEC-5	Blocage après échecs	Blocage après 5 tentatives infructueuses	Compte temporairement verrouillé
SEC-6	Sauvegarde automatique	Sauvegarde quotidienne des données	Procédure testée et validée

12.3 Contraintes Organisationnelles

12.3.1 Contraintes liées au Cadre du Stage

Réf	Contrainte	Description	Impact
ORG-1	Durée limitée	Stage de 6 mois maximum	Planification rigoureuse requise
ORG-2	Projet individuel	Réalisé par un seul étudiant	Limitation de charge et priorisation
ORG-3	Validation académique	Encadrement et soutenance obligatoires	Respect des livrables académiques

12.3.2 Contraintes Environnementales

Réf	Contrainte	Description
ENV-1	Environnement technique imposé	Respect des technologies validées par l'organisme d'accueil
ENV-2	Infrastructure disponible	Déploiement sur serveur interne ou environnement défini
ENV-3	Accès aux ressources	Accès contrôlé aux données et systèmes internes

12.4 Contraintes de Performance

Réf	Exigence	Critère
PERF-1	Temps de réponse API	< 2 sec (95%)
PERF-2	Indexation document	< 5 sec
PERF-3	Charge normale	≥ 100 utilisateurs simultanés

13. Analyse des Risques

Risque	Impact	Solution
Complexité IA	Retard	Modèle pré-entraîné
Failles sécurité	Critique	Tests approfondis
Volume fichiers	Performance	Optimisation stockage

14. Critères d'Acceptation

Le projet sera validé si :

- Toutes les fonctionnalités sont opérationnelles
- Les exigences de sécurité sont respectées
- Les performances sont conformes
- Les tests sont validés
- La démonstration finale est concluante

15. Conclusion

Ce cahier des charges constitue le document de référence du projet. Il définit l'ensemble des exigences nécessaires à la conception et au développement de la plateforme numérique de gestion documentaire sécurisée intégrant des techniques d'intelligence artificielle.