



Plan d'Assurance Qualité et Sécurité

PAQS-V3

Sommaire

1.	LE PAQS	3
1.1.	Objet du PAQS.....	3
1.2.	Référentiel.....	3
1.2.1.	Version du document	3
1.2.2.	Documents applicables	3
1.2.3.	Terminologie	3
2.	GOUVERNANCE DE LA PHASE DE RUN	5
2.1.	Organisation opérationnelle	5
2.1.1.	Les équipes et les acteurs.....	5
2.1.2.	Comité de pilotage (COPI)	5
3.	SERVICES ET ENGAGEMENTS	7
3.1.	Attestation de conformité aux normes légales :	7
3.2.	Localisation du service d'hébergement	7
3.3.	Architecture.....	7
3.3.1.	Schéma d'architecture	7
3.4.	Réseaux / Télécoms.....	8
3.4.1.	Lien WAN.....	Erreur ! Signet non défini.
3.4.2.	Réseau LAN	Erreur ! Signet non défini.
3.4.3.	Internet	8
3.5.	Engagements de service.....	8
3.5.1.	Stratégie de développement et déploiement :	8
3.5.2.	Stratégie Assurance Qualité (AQ) et Tests :	9
3.5.3.	Monitoring, Alerting et Supervision	10
3.5.4.	Organisation du service d'astreinte :	11
3.5.5.	Politique d'archivage, de sauvegarde des données et Plan de Reprise d'Activité (PRA) :	11
3.5.6.	Traitement des demandes	12
3.5.7.	Développement de nouveaux services.....	12

Confidentialité

Chacune des parties s'engage à garder confidentielles toutes les informations, toutes les données, tout document, quelle qu'en soit la nature et l'objet, dont elles ont eu connaissance dans le cadre de l'exécution des prestations, par quelque moyen que ce soit, sur quelque support que ce soit, par écrit ou oralement.

1. Le PAQS

1.1. Objet du PAQS

Le Plan d'Assurance Qualité Sécurité, « PAQS», est le document qui décrit et précise les conditions opérationnelles de délivrance des services fournis par ADORIA.

Le PAQS décrit :

- Les services délivrés et l'organisation associée,
- Les références contractuelles aux plages de service et SLA
- Les règles d'organisation, de gestion et de communication entre ADORIA et ses clients pour les différents types de prestations,

1.2. Référentiel

1.2.1. Version du document

Date	Objet des modifications	Version
01/01/2023	Version initiale V1	1
01/01/2025	Version – V2	2
01/05/2025	Version – V3- hébergement AWS	3

1.2.2. Documents applicables

Les documents listés ci-après sont les documents référencés dans ce « PAQS», leur bonne application est imposée et vérifiable, en particulier lors des audits et revues.

Nom du document	Nature de l'information
CONTRAT	Offre
DAT	Document d'architecture technique
PAS	Plan d'assurance sécurité

1.2.3. Terminologie

La terminologie qui suit se réfère aux pratiques et procédures d'adoria :

CP	Chef de Projet
PO	Product Owner
QA	Quality Assurance
COPIL	Comité de pilotage
Recette	Constat du bon fonctionnement de l'environnement et de ses services associés au terme des actions de mise à disposition de la plateforme technique.
Direction Commerciale	La direction commerciale est chargée de superviser l'ensemble des activités commerciales de la société
Direction Informatique	La direction informatique est chargée de superviser l'ensemble des activités techniques de la société

2. Gouvernance de la phase de RUN

2.1. Organisation opérationnelle

2.1.1. Les équipes et les acteurs

2.1.1.1. adoria

La Hotline

- Centralise les appels et les enregistre dans la base de maintenance,
- Qualifie les incidents en lien avec LE CLIENT ou son représentant,
- Effectue la maintenance de 1er niveau,
- Transfère aux équipes techniques pour la maintenance de 2nd niveau.

Le Chef de Projet

- Organise et anime les comités de suivi avec le client selon les modalités contractuelles prévues
- Centralise l'ensemble des demandes du client
- Suit l'activité :
 - Etablit le bilan et le compte-rendu sur les activités et les prestations fournies aux clients
 - Explicite et communique les indicateurs
 - Gère les évolutions de la documentation
- Gère la relation client :
 - Contribue à la prise en compte des besoins exprimés par le client lors des Comités
 - Participe si nécessaire, en relation avec la direction commerciale, à toute évolution dans les contrats de services et engagements d'Adoria
 - Réalise les actions de communication

Les Supports Techniques

Adoria fournit les moyens en homme et matériels, les ressources techniques et les outils de travail nécessaires au bon fonctionnement pendant la durée du contrat : supervision, outil de gestion des tickets, sauvegarde, etc.

Les supports techniques appliquent les processus, procédures et guides opératoires du système qualité d'adoria.

Le PO (Product Owner)

- Qualifie, généralise, estime, les demandes d'évolutions techniques
- Suit la réalisation, le test et la mise à disposition de nouvelles fonctionnalités

La Direction Informatique

- Participe aux réunions de travail concernant son domaine d'expertise
- Participe aux comités de suivi si demandé par le client
- Valide les demandes soumises par les PO
- Définit et demande les modifications ou évolutions d'infrastructures permettant de garantir la sécurité et la fiabilité de l'hébergement et des services mis à disposition.

2.1.2. Comité de pilotage (COPIL)

2.1.2.1. Organisation

Dès lors que le projet passe en phase opérationnelle RUN, le comité de pilotage est constitué.

Comité de pilotage	
Son rôle	Suivi des prestations en phase récurrente
	Suivi des indicateurs
	Analyse des indicateurs sur une période en rapport avec le contrat
Fréquence	Selon contrat

<i>Sa composition</i>	
- ADORIA	Chef Projet, DirCom, (PO)
- Client	Chargé Relation adoria, responsable achat
<i>Lieu</i>	ADORIA ou Client ou Visio
<i>Modalité</i>	Sur site ou réunion téléphonique/visio
<i>Entrée</i>	Document support au comité,
<i>Sortie</i>	Compte rendu
<i>Outil</i>	Tableau de bord, événements, compte rendu.

2.1.2.2. Ordre du jour

Il est décrit ici les éléments essentiels abordés lors du Comité de Suivi.

- Indicateurs de performance
- Suivi des tickets (demandes et incidents)
- Projets en cours
- Evolutions des entreprises et Nouveaux Projets
- AOB

3. Services et engagements

3.1. Attestation de conformité aux normes légales :

Adoria atteste que la solution proposée est conforme aux normes légales et réglementaires applicables, notamment en matière de sécurité des données et de protection des informations personnelles.

3.2. Localisation du service d'hébergement

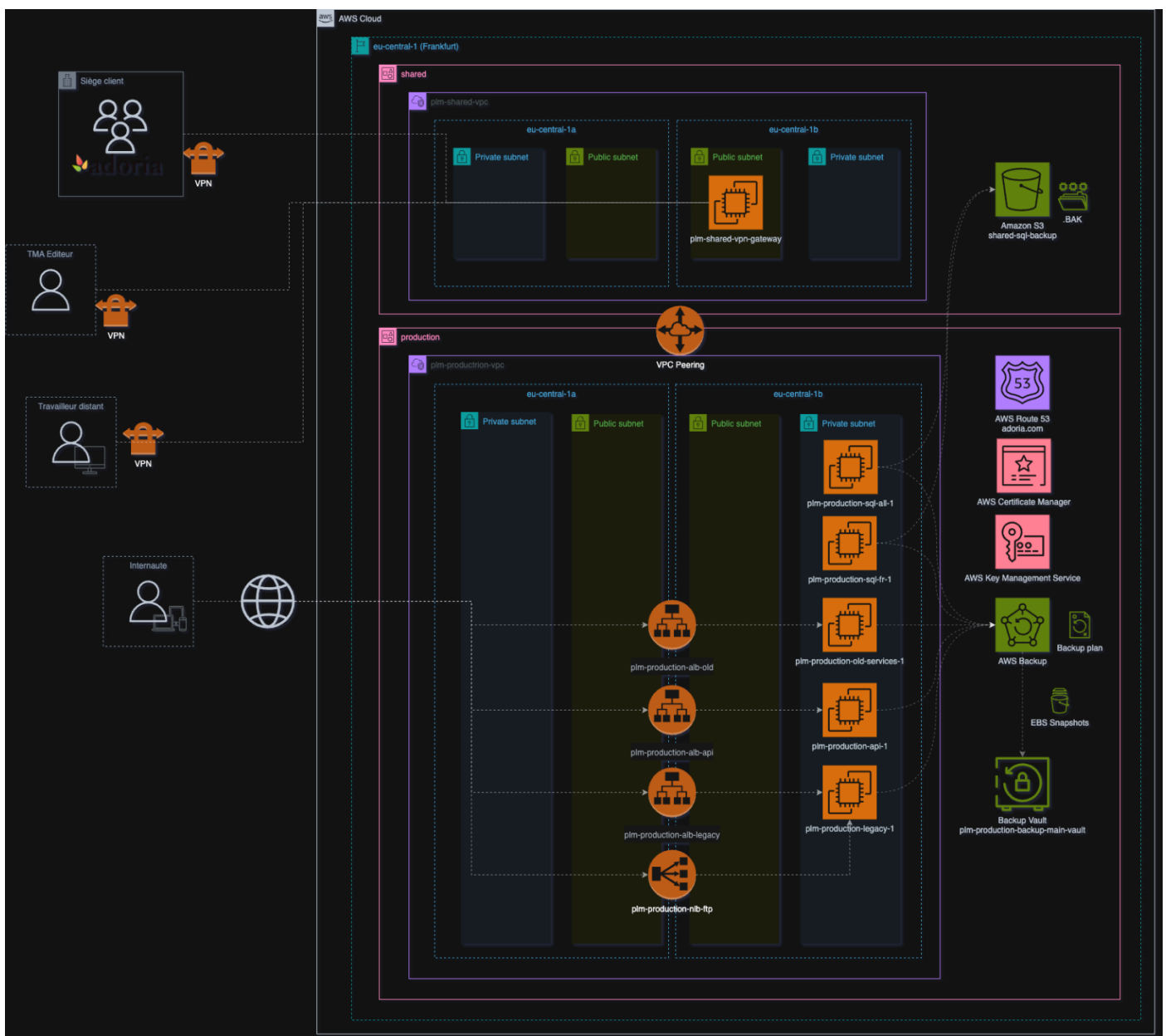
L'hébergement des données à caractère personnel et/ou des applications informatiques est réalisé en France. La description et l'adresse de l'hébergeur se trouve dans le contrat.

3.3. Architecture

3.3.1. Schéma d'architecture

3.3.1.1. Infrastructure actuelle

L'infrastructure actuelle repose sur une solution on-premise, gérée par un infogérant, et comprend deux serveurs ESXI avec un stockage mutualisé en cluster. Cette architecture assure une haute disponibilité des services.



3.3.1.2. Ségrégation des données :

Séparation des Environnements

Les environnements de production sont strictement isolés de ceux de test et développement, avec un réseau dédié et un accès limité à quelques responsables qualifiés (« lead developers » et responsables infrastructure).

Architecture des Données Clients

L'environnement de production dispose d'un serveur SQL Server centralisé avec une segmentation logique en instances par pays.

Ségrégation des données clients

Les données de chaque client sont stockées séparément à l'exception des références qui peuvent-être communes, permettant à chacun de profiter d'un catalogue fournisseur commun.

Sécurité et Contrôle d'Accès

- Gestion centralisée des accès via Active Directory avec politique de droits basée sur les rôles
- Séparation stricte des responsabilités pour les données sensibles
- Accès limité au personnel qualifié selon leurs fonctions

3.4. Réseaux / Télécoms

L'hébergeur met à disposition les équipements réseau et de sécurité tels que les commutateurs, les firewalls, les équilibreurs de charge, les routeurs et les équipements permettant les connexions distantes.

3.4.1. Internet

Liens télécoms Internet		
Réseau internet	☒ Souscrit	☐ Responsabilité Client
	☐ Non souscrit	☒ Responsabilité hébergeur
Bande passante souscrite	Bande passante dédiée garantie	

3.5. Engagements de service

3.5.1. Stratégie de développement et déploiement :

- **Organisation du Développement** Pipeline CI/CD (Continuous Integration/Continuous Delivery)
 - Approche gitflow Development
 - Workflow de développement structuré et sécurisé
 - Process de validation multi-niveaux incluant :
 - Tests automatisés

- Code review systématique
- Validation fonctionnelle
- Déploiement progressif
- **Stratégie de Déploiement**
 - Déploiements planifiés et contrôlés
 - Infrastructure robuste d'intégration continue-CI/CD (Continuous Integration / Continuous Delivery)
 - Gestion sécurisée des secrets et configurations

Architecture des Environnements

- **TestX** : Environnement d'intégration continue avec tests automatisés initiaux.
- **Recette** : Tests fonctionnels et de non-régression approfondis.
- **Préproduction** : Tests de performance avant mise en production.
- **Production/Sandbox** : Environnement client final avec monitoring constant.

Infrastructure et pipeline d'intégration continue (CI/CD)

- **GitLab** pour la gestion des pipelines de build, des tests et des déploiements automatisés.
- **Scripts de Déploiement** : Automatisation sur Windows/IIS avec gestion des configurations et rollback automatisé.

3.5.2. Stratégie Assurance Qualité (AQ) et Tests :

Tests Unitaires

- **Backend (.NET Core)** : Tests unitaires systématiques sur les APIs avec validation des comportements attendus.
- **Frontend** : Tests unitaires avec Jest et React Testing Library.

Tests d'Intégration et API

Utilisation de Cerberus pour les tests fonctionnels automatisés, et de Robot Framework pour la validation des flux API. Swagger et Postman sont employés pour les tests manuels.

Tests End-to-End (E2E)

Sahi et Cerberus pour l'automatisation des scénarios utilisateur complexes. Maestro est utilisé pour les tests mobiles.

Analyse de Code et Qualimétrie

CAST permet l'analyse statique, la détection des anti-patterns, et le suivi des bonnes pratiques de développement.

Tests de Charge

Utilisation de JMeter pour simuler des scénarios de charge et mesurer les temps de réponse.

Métriques de Performance

Surveillance du système (RAM, CPU, IOPS) et performance applicative (temps de réponse SQL, API, taux d'erreur).

3.5.3. Monitoring, Alerting et Supervision

L'hébergeur a déployé une solution de supervision permettant de couvrir les fonctionnalités indispensables au pilotage de votre environnement, que sont :

- **La Disponibilité** : Supervision temps réel, et Remontée des alarmes sur apparition des incidents potentiels.
- **La Gestion des SLAs** : Définition, Reporting et Supervision des éléments de pilotage, de la qualité de conformité des SLAs.
- **La Gestion de la Performance** : Publication de Rapports temps réels et historisation des métriques de performance.

De nombreuses Sondes et Points d'entrée fournissent les données nécessaires de l'infrastructure et des données Utilisateur pour contrôler les Services Point-à-Point, leur disponibilité et la conformité des SLAs. Le périmètre en supervision couvre l'ensemble des composants suivants ;

- Infrastructure (stockage, LAN, SAN, serveur)
- VMs
- OS Windows
- Middleware applicatifs suivants : SQL Server et Active Directory

Un évènement de remontée d'alarme de supervision est systématiquement analysé et le cas échéant une demande d'incident est créée par L'hébergeur.

La mesure du taux de disponibilité s'effectue à partir des outils de supervisons et monitoring mis en place par L'hébergeur. Ils sont complétés de mesures réalisées par adoria ainsi que des mesures par des outils indépendants et externes. Cette mesure est calculée en sortie de plateforme.

Stack de Surveillance :

- **Grafana** : Tableaux de bord et visualisation en temps réel.
- **Prometheus** : Collecte des métriques et règles d'alerting.
- **Loki** : Centralisation des logs et corrélation avec les métriques.

Dashboards de Monitoring

Solutions de monitoring complètes couvrant :

- Infrastructure serveurs
- Applications
- APIs
- Services
- Métriques applicatives

Surveillance des flux EDI :

- Surveillance 7/7 24/24 des flux EDI normé Edifact/GS1.
- Adoria est alerté automatiquement, si Agena 3000 ne vient pas prendre en charge les commandes qu'on leur met à disposition.
- Agena 3000 réalise des reprises d'erreurs automatiques, en cas d'échec des premiers envois.
- Par ailleurs, Agena 3000 alerte Adoria en cas de problème de plus grande ampleur.

- Mise en œuvre d'un fichier de dépannage qui permet d'exporter les commandes en csv sur une journée pour les transmettre rapidement à un fournisseur en cas de souci technique sur l'EDI
- Projet en cours de suivi individuel et par API des fichiers envoyés, avec rapport disponible dans Adoria permettant le suivi et la surveillance des Flux / messages entrants.
- Pour mémoire, Concernant l'EDI Adoria préconise aux fournisseurs de passer par un réseau à valeur ajoutée (type AS2) qui est plus fiable et permet de s'assurer qu'un fichier soit transmis en totalité (=sans partie manquante).

Système d'Alerte

- Système de priorisation des incidents structuré
- Métriques Surveillées : Erreurs HTTP, saturation des ressources, temps de réponse
- Processus d'Escalade : Notification automatique et communication client structurée

Support et Maintenance

- Collaboration étroite avec l'infogérant pour la surveillance proactive et le support
- Expertise DBA dédiée pour l'optimisation des performances
- Maintenance préventive planifiée

3.5.4. Organisation du service d'astreinte :

Structure et Planning

- Équipe d'astreinte de 4 personnes, en rotation hebdomadaire.
- Couverture de 9h à 20h pour assurer la continuité des opérations hors heures ouvrées.

Temps de Réponse et Processus d'Intervention

- **Temps de Réponse** : Intervention garantie en 30 minutes.
- **Processus d'Escalade** : Déclenché après 10 minutes d'incident, avec communication directe à la direction pour la gestion client.

Périmètre de Couverture

Surveillance des applications principales : application web, mobile, APIs, et services de traitement automatisé.

Documentation et Procédures

Procédures d'intervention documentées et guides de résolution adaptés aux différents niveaux de criticité.

Outils et Communication

Système de monitoring automatisé, support téléphonique pour les remontées clients, et procédures de communication définies.

3.5.5. Politique d'archivage, de sauvegarde des données et Plan de Reprise d'Activité (PRA) :

La stratégie de sauvegarde comporte plusieurs niveaux pour une protection optimale des données :

- Immuabilité des sauvegardes
- Durée : 7 jours
- Mode : COMPLIANCE
- Effet : Chaque fichier de sauvegarde est verrouillé dès son upload : aucune suppression ou modification possible pendant 7 jours, même par un compte admin.
- Cela garantit une protection forte contre toute suppression accidentelle ou malveillante (type ransomware).

- Optimisation du stockage (S3 Intelligent-Tiering)
- Règle de cycle de vie activée
- Transition automatique vers Archive Tier après 90 jours
- Objectif : les sauvegardes plus anciennes en glacier, tout en les gardant accessibles en cas de besoin.

Plan de Reprise d'Activité (PRA)

- **RTO (Recovery Time Objective)** : 2 heures
- **RPO (Recovery Point Objective)** : 15 minutes
- **Site de Secours** : Réplication synchrone dans un datacenter distant, géographiquement séparé, pour assurer la continuité de l'activité.

3.5.6. Traitement des demandes

Il faut distinguer les différents types de demandes :

- Les demandes d'informations : Toute demande d'information concernant le service délivré ou la configuration peut être adressé par le client à son CP.
- Les demandes d'incidents : adoria assure, à la suite d'une alerte de supervision ou à la déclaration d'un incident par le client, un plan de gestion des d'incidents conforme aux engagements décrits dans le contrat.
- Les demandes de services et les demandes de changements peuvent avoir un impact sur le périmètre initialement défini et donc la redevance mensuelle. Elles peuvent concerner :
 - De l'assistance
 - Des demandes de fourniture de nouveaux services existants.
 - Des demandes de créations de nouveaux services

3.5.7. Développement de nouveaux services

3.5.7.1. Méthodologie de développement utilisée

Adoria utilise une méthode de développement agile pour assurer une flexibilité et une réactivité maximale aux besoins des utilisateurs finaux et assurer une qualité et adéquation du logiciel réalisé.

Cela permet d'impliquer l'ensemble de l'équipe et le client final lors des différentes étapes, de la conception aux livraisons intermédiaires, en passant par les maquettes et le fonctionnel.

3.5.7.2. Outils et environnement de développement

Adoria utilise des outils de développement modernes et performants dans leurs dernières versions pour faciliter le processus de développement, tels que des IDE (Visualstudio, Rider, Webstorm), des outils de gestion de code source (Gitlab), des outils de gestion de projet (Jira), etc.

3.5.7.3. Processus de gestion de code source et de configuration

Adoria utilise une méthode de gestion de code source et de configuration pour garantir la cohérence et l'intégrité du code. Les serveurs Gitlab sont sauvegardés et répliqués.

Les développeurs sont tenus de suivre des règles de codage strictes pour garantir la qualité du code et l'application de Clean Code.

Une relecture de chaque code produit (Code Review) est obligatoire pour que le code soit testé et intégré.

L'ensemble des développements sont intégrés continuellement (CICD).

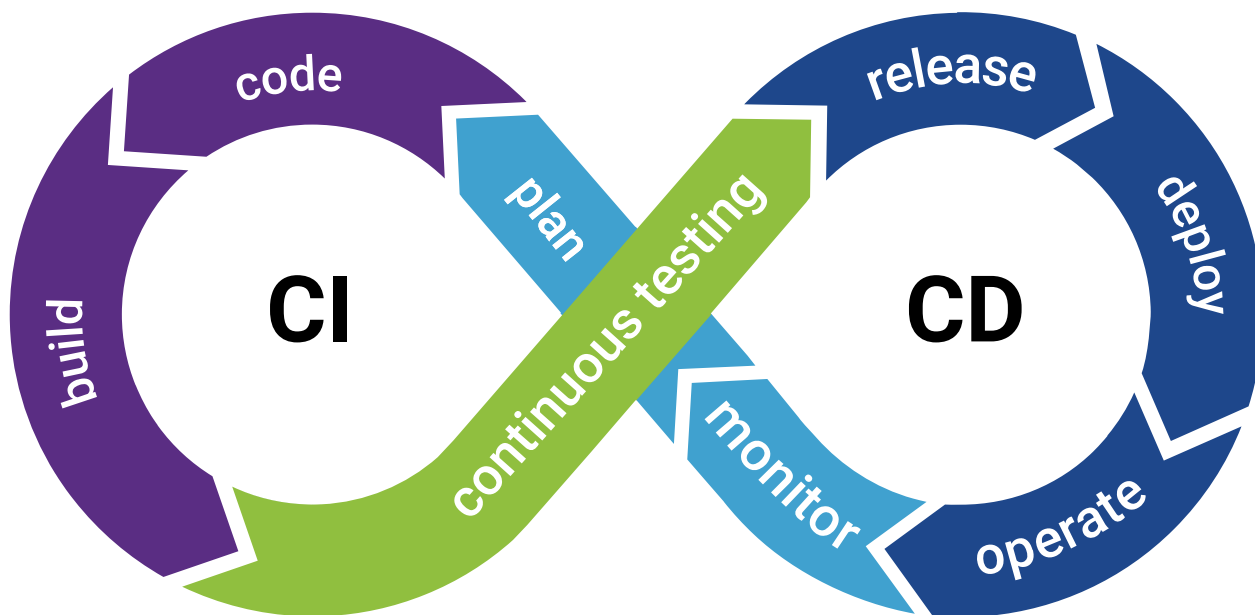
- **Organisation du Développement** Pipeline CI/CD (Continuous Integration/Continuous Delivery)
 - Approche Trunk Based Development
 - Workflow de développement structuré et sécurisé
 - Process de validation multi-niveaux incluant :
 - Tests automatisés
 - Code review systématique
 - Validation fonctionnelle
 - Déploiement progressif
- **Stratégie de Déploiement**
 - Déploiements planifiés et contrôlés
 - Infrastructure robuste d'intégration continue-CI/CD (Continuous Integration / Continuous Delivery)
 - Gestion sécurisée des secrets et configurations

Architecture des Environnements

- **TestX** : Environnement d'intégration continue avec tests automatisés initiaux.
- **Recette**: Tests fonctionnels et de non-régression approfondis.
- **Preprod**: Tests de performance avant mise en production.
- **Production/Sandbox** : Environnement client final avec monitoring constant.

Infrastructure et pipeline d'intégration continue (CI/CD)

- **GitLab** pour la gestion des pipelines de build, des tests et des déploiements automatisés.
- **Scripts de Déploiement** : Automatisation sur Windows/IIS avec gestion des configurations et rollback automatisé.



3.5.7.4. Processus de test et validation

Adoria utilise une méthode de test et de validation rigoureuse pour s'assurer que les logiciels proposés sont exempts d'erreurs et répondent aux exigences de qualité.

Chaque fonctionnalité est décomposée en User Story (US) qui contient ses conditions de satisfactions.

Tous les développements contiennent des Tests Unitaires (TU) afin de protéger de régressions.

Les développements sont testés par les développeurs puis par les membres de l'équipe QA (tests d'intégrations, test fonctionnels), puis par les équipes opérationnelles et peut être recetté par le client sur un environnement bac à sable (Sandbox).

L'équipe QA réalise en parallèle du développement de la fonctionnalité des tests automatisé qui couvrent cette fonctionnalité.

Ces tests automatisés tournent quotidiennement sur les environnements de développement et à chaque livraison des environnements de production.