

IA - Gouvernance technique

Référence : **PYIA093**

Durée : **2 jours (14 heures)**

Certification : **Aucune**

CONNAISSANCES PRÉALA

Avoir de l'expérience en développement Python
Connaissances des architectures cloud (AWS/Azure/GCP)
Connaître les fondamentaux de l'IA

PROFIL DES STAGIAIRES

DSI, architectes IA, DevOps, ingénieurs MLOps, ingénieurs données, responsables infrastructure, RSSI

OBJECTIFS

Concevoir et implémenter un framework de gouvernance IA
Définir des processus de validation et d'audit
Établir des métriques de conformité
Sécuriser les déploiements IA selon les standards réglementaires

CERTIFICATION PRÉPARÉE

Aucune

MÉTHODES PÉDAGOGIQUES

Mise à disposition d'un poste de travail par stagiaire
Remise d'une documentation pédagogique papier ou numérique pendant le stage
La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions
Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-formateur expert IA

MÉTHODES D'ÉVALUATION DES ACQUIS

Auto-évaluation des acquis par le stagiaire via un questionnaire
Attestation des compétences acquises envoyée au stagiaire
Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

1. Cadre réglementaire et framework de gouvernance IA

AI Act européen : obligations techniques, classification des systèmes, documentation obligatoire
Standards ISO/IEC 23053 et 23894 : processus de gouvernance, évaluation des risques
Framework organisationnel : rôles AI Officer/DPO, comités de gouvernance, processus décisionnels
Processus de validation : validation qualité, critères d'approbation, escalade des risques
Métriques de gouvernance : définition des KPIs éthiques, SLA de conformité, indicateurs de performance
💡 *Conception d'un framework de gouvernance adapté à l'organisation - matrice de responsabilités, processus d'approbation, grille d'évaluation des risques, templates de documentation conformité*

2. Architecture et processus de gouvernance technique

Principes d'architecture gouvernée : séparation des responsabilités, traçabilité, auditabilité

Processus de sélection technologique : critères de choix, matrice de décision, validation architecture

Patterns d'architecture pour la gouvernance : microservices, API Gateway, observabilité distribuée

Stratégies de déploiement contrôlé : gates de validation, rollback automatique, environnements de test

Sécurité by design : chiffrement, authentification, autorisation, limitation d'accès

💡 *Définition d'une architecture de référence gouvernée - critères de sélection d'outils, processus de validation technique, mise en place de surveillance de base avec métriques de conformité*

3. Processus MLOps et traçabilité pour la gouvernance

Gouvernance du cycle de vie ML : processus de développement, validation, déploiement contrôlé

Traçabilité obligatoire : versioning des modèles, lignage des données, audit trail complet

Critères de choix d'outils MLOps : gouvernance, sécurité, intégration, conformité réglementaire

Documentation automatisée : standards de documentation, génération automatique, templates conformes

Processus CI/CD gouverné : tests automatisés, validation de conformité, approbations requises

💡 *Conception d'un pipeline MLOps gouverné - définition des processus, mise en place de la traçabilité, création de templates de documentation, validation par tests automatisés*

4. Surveillance et gestion des risques en production

Processus de surveillance continue : métriques techniques et éthiques, seuils d'alerte, escalade

Gestion de la dérive : détection, évaluation d'impact, processus de correction, validation

Framework de détection d'anomalies : techniques statistiques, seuils adaptatifs, corrélation d'événements

Processus d'alerte et d'escalade : classification des incidents, procédures d'intervention, communication

Tests en production : méthodologies A/B, shadow mode, validation continue des performances

💡 *Conception d'un système de surveillance gouvernée - définition des métriques critiques, processus d'escalade, mise en place d'alertes intelligentes avec validation réglementaire*

5. Audit automatisé et processus de conformité

Framework d'audit IA : méthodologies, fréquence, critères d'évaluation, rapport standardisé

Processus de tests de conformité : détection de biais, robustesse, explicabilité, validation éthique

Analyse de sécurité : évaluation des vulnérabilités, tests de pénétration, audit de sécurité

Processus de documentation : traçabilité des décisions, justifications, rapports d'audit automatisés

Intégration dans les workflows : points de contrôle, validation continue, certification

💡 *Mise en place d'un processus d'audit automatisé - définition des tests, critères de validation, génération de rapports conformes, intégration dans les pipelines de développement*

6. Sécurisation et optimisation des déploiements

Processus de déploiement sécurisé : validation préalable, environnements isolés, tests de sécurité

Architecture haute disponibilité : répartition de charge, redondance, continuité de service

Stratégies d'optimisation : mise en cache, optimisation des inférences, gestion des ressources

Déploiement edge : critères de choix, sécurisation, synchronisation avec le cloud

Surveillance de sécurité : détection d'intrusions, audit des accès, journalisation de sécurité

💡 *Conception d'une architecture de déploiement sécurisée - processus de validation, configuration haute disponibilité, mise en place de la surveillance de sécurité*

7. Tableaux de bord et processus de reporting

Framework de métriques : KPIs techniques, éthiques, opérationnels, définition des seuils

Processus de reporting : fréquence, destinataires, format, escalade automatique

Intégration organisationnelle : ITSM, systèmes de surveillance, bases de données métier

Automatisation du reporting : génération automatique, distribution, archivage

Gouvernance des alertes : classification, corrélation, réduction du bruit, processus d'intervention

💡 *Conception d'un système de reporting gouverné - définition des métriques stratégiques, automatisation des rapports, création de tableaux de bord conformes aux exigences réglementaires*

8. Migration et industrialisation gouvernée

Méthodologie de migration : évaluation des risques, stratégies de transition, coexistence des systèmes

Processus d'industrialisation : validation technique, tests de charge, certification de production

Stratégies de rollback : critères de déclenchement, procédures automatisées, plan de continuité

Infrastructure as Code : gouvernance des configurations, auditabilité, reproductibilité

Documentation opérationnelle : procédures d'exploitation, gestion des incidents, formation des équipes

💡 *Élaboration d'un plan de migration gouvernée - analyse de risques, définition des étapes, processus de validation, procédures opérationnelles et de conformité*

Notre référent handicap se tient à votre disposition au [01.71.19.70.30](tel:01.71.19.70.30) ou par mail à referent.handicap@edugroupe.com pour vos éventuels besoins d'aménagements, afin de vous offrir la meilleure .