

# Le diagnostic I.A.



... pour optimiser les compétences de vos collaborateurs

# Les 6 étapes du Diagnostic

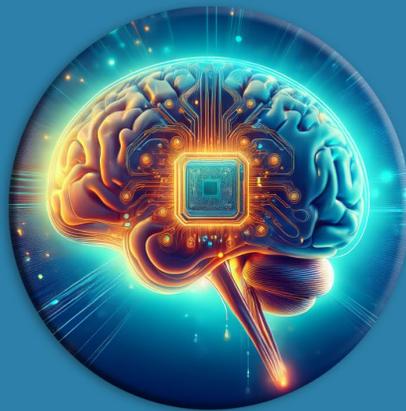
1 - Définir le périmètre et les objectifs du diagnostic



2 - Evaluer la gouvernance des données et de l'IA



6 - Formuler des recommandations et un plan d'action



3 - Analyser la qualité des données

5 - Evaluer la sécurité des données et des systèmes IA



4 - Examiner les modèles IA potentiels



...pour maximiser la productivité de votre entreprise

# Les 6 étapes en détail

## 1. Définir le périmètre et les objectifs de l'audit

- **Clarifier les objectifs** : Pourquoi cet audit ? (conformité réglementaire, évaluation des risques, optimisation des performances, etc.)
- **Délimiter le périmètre** : Quels systèmes, données et modèles d'IA sont concernés ?
- **Identifier les parties prenantes** : Qui sont les acteurs clés (équipes DATA, développeurs IA, responsables métiers, etc.) ?

## 2. Évaluer la gouvernance des données et de l'IA

- **Politiques et procédures** : Existence et application de politiques de gestion des données et de l'IA.
- **Rôles et responsabilités** : Clarification des responsabilités en matière de qualité, sécurité et éthique des données et de l'IA.
- **Conformité réglementaire** : Respect des réglementations en vigueur (RGPD, etc.).

## 3. Analyser la qualité des données

- **Collecte et stockage** : Évaluation des processus de collecte, stockage et gestion des données.
- **Intégrité et exactitude** : Vérification de l'intégrité, de l'exactitude et de la cohérence des données.
- **Documentation** : Qualité et exhaustivité de la documentation des données.

## 4. Examiner les modèles d'IA potentiels

- **Développement et déploiement** : Évaluation des processus de développement, test et déploiement des modèles.
- **Performances et biais** : Analyse des performances des modèles et détection des éventuels biais.
- **Explicabilité et transparence** : Évaluation de la capacité à expliquer et comprendre les décisions des modèles.

## 5. Évaluer la sécurité des données et des systèmes d'IA

- **Accès et authentification** : Contrôle des accès aux données et aux systèmes d'IA.
- **Protection contre les menaces** : Évaluation des mesures de protection contre les cyberattaques.
- **Gestion des incidents** : Existence et efficacité des procédures de gestion des incidents de sécurité.

## 6. Formuler des recommandations et un plan d'action

- **Identifier les points faibles** : Synthèse des principales lacunes et risques identifiés.
- **Proposer des recommandations** : Formulation de recommandations claires et réalisables pour améliorer la gouvernance, la qualité, la sécurité et l'éthique des données et de l'IA.
- **Faire évoluer les compétences humaines** : Former / Accompagner les personnes concernées par la mise en place de l'IA.
- **Établir un plan d'action** : Définition des priorités, des responsabilités et des échéances pour la mise en œuvre des recommandations.

« L'I.A. au service de vos collaborateurs  
et non l'inverse... »

