

# Conférence - Confiance numérique et IA : de quoi parle-t on ?

## Présentation

À l'ère du tout numérique et de l'IA, instaurer une confiance solide est essentiel pour le secteur public. Cette conférence abordera les défis et les solutions pour garantir la sécurité des données, protéger la vie privée des citoyens et renforcer la confiance dans les services digitaux.

Durée : 3,50 heures (1 jours)

Tarif INTRA : Nous consulter

## Objectifs de la formation

- Définir le concept de confiance numérique et son importance pour le secteur public.
- Découvrir comment l'usage de l'IA peut s'intégrer dans un environnement de confiance.
- S'approprier la définition de l'IA, son rôle, ses atouts et ses limites
- Découvrir les meilleures pratiques et cadres légaux pour assurer une transformation digitale sécurisée.
- Engager une réflexion sur les stratégies IA à adopter pour renforcer la confiance des usagers.

## Prérequis

Aucun

## Public

Toute personne travaillant ou désirant s'informer sur les avancées technologique adaptées au secteur public

## Programme de la formation

### Séquence 1 : Introduction à la Confiance Numérique et à l'IA dans le Secteur Public



Objectif : intégrer les bases de la confiance numérique en introduisant également l'IA comme un levier de transformation, tout en posant la question de la confiance.

Contenu :

- Définir la confiance numérique et l'IA de confiance : principes de sécurité, fiabilité, et éthique de l'IA.
- Pourquoi l'IA est cruciale dans la transformation digitale des services publics ?
- Enjeux et attentes des citoyens en matière de transparence et de sécurité dans l'utilisation de l'IA.

### **Séquence 2 : Défis de la cybersécurité et de la protection des données**

Objectif : étendre l'analyse des risques en incluant les spécificités de l'IA dans les problématiques de cybersécurité.

Contenu :

- Identifier les menaces liées aux IA malveillantes, deepfakes, et autres vecteurs d'attaque amplifiés par l'IA.
- Exemples de cyberincidents impliquant des IA et leurs conséquences sur la confiance des citoyens.
- Comment s'assurer que l'utilisation de l'IA respecte les principes de sécurité et de confidentialité ?

### **Séquence 3 : Cadres légaux et normes de sécurité**

Objectif : expliquer les réglementations spécifiques à l'IA et leur articulation avec les normes de cybersécurité.

Contenu :

- Cadres juridiques autour de l'IA éthique (ex : réglementations européennes sur l'IA).
- Présentation des certifications spécifiques (ex : ISO AI).
- Responsabilité des collectivités dans la mise en œuvre de l'IA de confiance.

### **Séquence 4 : Meilleures Pratiques en Sécurité et Confiance dans l'IA**

Objectif : identifier des pratiques qui intègrent IA et cybersécurité pour renforcer la confiance.

Contenu :

- Solutions technologiques spécifiques à l'IA (ex : transparence des algorithmes, auditabilité).
- Politiques de sécurité robustes incluant l'IA : évaluation des biais, surveillance des algorithmes.
- Communication transparente sur l'usage de l'IA dans les services publics.

### **Séquence 5 : Élaboration d'une Stratégie Durable d'IA de Confiance**

Objectif : aider les participants à construire une stratégie d'intégration de l'IA dans leurs services.

Contenu :

- Plan d'action pour une IA de confiance adaptée au secteur public.
- Ateliers de réflexion sur l'IA éthique et sécurisée.
- Collaboration pour renforcer la confiance entre l'IA des administrations et les citoyens.

### **Séquence 6 : Perspectives Futures : Confiance Numérique et IA de Confiance**

Objectif : explorer les avancées technologiques futures en IA et les défis de la confiance numérique.

Contenu :

- Anticipation des nouvelles menaces impliquant l'IA : deepfakes, AI-powered cyber espionnage.
- Opportunités offertes par des architectures comme le zero-trust pour l'IA.
- Rôle du secteur public dans la création d'un écosystème numérique et IA de confiance

## **Organisation**

### **Formateur**

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes.

Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétence.

### **Moyens pédagogiques et techniques**

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

### **Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation**

#### **En amont de la formation** *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

#### **Tout au long de la formation**

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

#### **À l'issue de la formation** *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

### **Accessibilité**

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.

