Lefebvre Dalloz
Compétences.

Tél.: 01 83 10 10 10
src-formation@lefebvre-dalloz.fr
formation.lefebvre-dalloz.fr

Confiance numérique : de quoi parle-t-on ?

Instaurer une confiance solide est essentiel pour le secteur public à l'ère du numérique

Code	Durée	Tarif Inter*
702047	3 heures 30 / 3 heures	319 € HT

Repas inclus (en présentiel)

PUBLIC

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

PRÉ-REQUIS

Aucun prérequis nécessaire

NIVEAU D'EXPERTISE

Fondamentaux

LES POINTS FORTS

Docaposte Institute propose plusieurs dispositifs pédagogiques adaptés aux apprenants :

Formation en présentiel

En groupe (inter-entreprises ou intra-entreprise)

En individuel (monitorat)

En journée ou en cours du soir (sur demande spécifique)

Formation en distanciel

Distanciel synchrone

Distanciel asynchrone

MOYENS PÉDAGOGIQUES

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Objectifs pédagogiques

- Définir le concept de confiance numérique et son importance pour le secteur public.
- Explorer les principaux défis en matière de cybersécurité et de protection des données.
- Découvrir les meilleures pratiques et cadres légaux pour assurer une transformation digitale sécurisée.
- Engager une réflexion sur les stratégies à adopter pour renforcer la confiance des usagers.

Programme de la formation

Séquence 1 : Introduction à la Confiance Numérique dans le Secteur Public

Objectif : Poser les bases de la confiance numérique, sa définition, et son importance dans le contexte du secteur public.

- Définition de la confiance numérique : sécurité, fiabilité et protection des données.
- Pourquoi la confiance est-elle cruciale pour la transformation digitale des services publics ?
- Enjeux et attentes des citoyens en matière de sécurité et de transparence numérique

.

Séquence 2 : Défis de la Cybersécurité et de la Protection des Données

Objectif : Identifier les principaux risques liés à la cybersécurité et à la gestion des données personnelles dans le secteur public.

- Analyse des menaces actuelles : cyberattaques, violations de données, usurpation d'identité.
- Impacts potentiels sur les services publics et sur la confiance des citoyens.
- Exemples récents de cyberincidents touchant les collectivités locales et leurs conséquences.

SATISFACTION ET EVALUATION

- En amont de la formation
  - Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
  - Auto-positionnement des apprenants afin de mesurer le niveau de départ.
- Tout au long de la formation
  - Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...
- A la fin de la formation
  - Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
  - Evaluation par le formateur des compétences acquises par les apprenants.
  - Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
  - Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

ACCOMPAGNEMENT FORMATION À DISTANCE

En cas de nécessité, une assistance technique et pédagogique est joignable entre 8h30 et 18h (jours ouvrés):

- par téléphone : 01 83 10 10 10
- par mail : care-formation@lefebvre-dalloz.fr

Une réponse immédiate est apportée ; si besoin, le demandeur est mis en relation avec un expert dans un délai maximum de 48h.

Séquence 3 : Cadres Légaux et Normes de Sécurité

Objectif : Comprendre les exigences légales et les bonnes pratiques en matière de sécurité numérique et de protection des données.

- Présentation des principales régulations : RGPD, Loi Informatique et Libertés, directives européennes.
- Normes et certifications de sécurité applicables au secteur public (ISO 27001, ANSSI).
- Rôle et responsabilité des collectivités dans la mise en conformité.

Séquence 4 : Stratégies et Meilleures Pratiques pour Renforcer la Confiance

Objectif : Proposer des solutions pratiques et des stratégies pour renforcer la sécurité des données et la confiance des citoyens dans les services digitaux.

- Mise en place de politiques de sécurité robustes : audit, gestion des accès, protection des données sensibles.
- Solutions technologiques pour améliorer la cybersécurité : chiffrement, authentification forte, gestion des identités.
- Communication proactive et transparente sur les mesures de sécurité mises en place.

Séquence 5 : Construire une Stratégie de Confiance Numérique Durable

Objectif : Aider les participants à élaborer une stratégie de confiance numérique adaptée à leur organisation.

- Élaboration d'un plan d'action pour renforcer la confiance numérique dans les services publics.
- Ateliers de réflexion sur les bonnes pratiques et les outils à mettre en place.
- Approches collaboratives pour renforcer la confiance entre les administrations et les citoyens.

Séquence 6 : Perspectives Futures et Évolutions de la Confiance Numérique

Objectif :Aborder les évolutions futures de la confiance numérique et les nouveaux défis à venir.

- Anticipation des nouvelles menaces : intelligence artificielle malveillante, deepfakes, cyberespionnage.
- Opportunités offertes par les technologies émergentes (blockchain, zero-trust architecture).
- Discussion sur le rôle du secteur public dans la création d'un écosystème numérique de confiance.