PROTEGER ET SECURISER L'INFORMATION ET SON SAVOIR-FAIRE

Objectifs :

- Sensibiliser les employés aux enjeux de la protection de l'information et du savoir-faire.
- Adopter de bonnes pratiques pour sécuriser les données et les échanges d'informations.
- Comprendre les risques liés aux fuites d'informations et aux cyberattaques.
- Protéger le savoir-faire et les connaissances stratégiques de l'entreprise.

Durée :
7 heures

Public & Pré-requis :
Les salariés

Modalité pédagogiques :
pédagogie active
En présentiel ou à distance

Modalités de suivi :
Attestation de fin de Formation.
Evaluation de fin de formation par le formateur

Profil formateur :
2 à 3 ans d'expérience mini dans le domaine. Et professionnels en poste dans le domaine enseigné

1. Introduction à la protection de l'information
   - Pourquoi la protection de l'information est essentielle ?
   - Les enjeux pour l'entreprise et les employés.
   - Exemples concrets de fuites d'informations et de leurs conséquences.

2. Sécurisation des données et bonnes pratiques
   - Les différents types de données et leur classification (confidentielles, sensibles, publiques, etc.).
   - Bonnes pratiques pour sécuriser les fichiers et les documents.
   - Gestion des accès et des mots de passe (création et gestion sécurisée).
   - Utilisation des outils de chiffrement et de stockage sécurisé.

3. Cyberattaques et risques
   - Principales menaces : phishing, ransomware, espionnage industriel, social engineering.
   - Identifier et éviter les tentatives de fraude.
   - Mettre des procédures de sécurité en place.
   - Sécuriser ses communications : emails, connexions distantes, VPN.
   - Bonnes pratiques pour la navigation sur Internet et l'utilisation des réseaux sociaux.

4. Préserver le savoir-faire de l'entreprise
   - Définition du savoir-faire et de la propriété intellectuelle.
   - Importance de la confidentialité des processus et des innovations.
   - Gestion des documents stratégiques et des accès aux informations critiques.
   - Sensibilisation aux risques liés au départ des employés (départ volontaire, licenciement, etc.).

5. Sensibilisation aux obligations légales et réglementaires

- Lois et réglementations sur la protection des données (RGPD, confidentialité des données professionnelles, etc.).
- Droits et devoirs des employés en matière de protection de l'information.
- Impact du non-respect des règles (sanctions, responsabilité juridique, etc.).

6. Mise en pratique et études de cas

- Exercices interactifs : identification des bonnes et mauvaises pratiques.
- Analyse de scénarios réels et simulation de cyberattaques.
- Discussion et échanges sur les expériences et difficultés rencontrées.

7. Conclusion et engagements

- Récapitulatif des bonnes pratiques à adopter.
- Engagement des employés à appliquer les mesures de protection.
- Questions/réponses et recommandations finales.