UIMM
PÔLE FORMATION
Adour
LA FABRIQUE DE L'AVENIR

Sensibilisation à la cybersécurité pour les managers

OBJECTIFS

- Définir la cybersécurité et ses enjeux pour l'entreprise.
- Identifier les menaces numériques courantes.
- Reconnaître les comportements à risque.
- Analyser les impacts d'une cyberattaque.
- Comprendre les obligations légales (RGPD, LPM, ISO 27001).
- Adopter des bonnes pratiques en cybersécurité.
- Promouvoir une culture de sécurité dans son équipe.

PUBLIC

Managers, responsables d'équipe, cadres opérationnels ou fonctionnels souhaitant acquérir les clés de compréhension des enjeux de cybersécurité afin d'identifier les risques, adopter les bonnes pratiques et sensibiliser leurs équipes.

PRÉREQUIS

Avoir une compréhension du fonctionnement d'un système d'information (SI), incluant ses composantes, son périmètre fonctionnel, et les principales interactions avec les utilisateurs.

STAGIAIRES PAR SESSION

De 5 à 10 personnes

TARIF

Les tarifs d'inscription en inter-entreprises sont disponibles sur notre site internet.

Pour plus de renseignements, pour étudier votre projet en formation, pour la mise en place d'intra-entreprise nous contacter :
par téléphone au 05.59.14.04.44
ou par mail : afpiadour.pau@metaladour.org

DURÉE

7h soit 1 jour

ÉVALUATION DES ACQUIS

QCM / QUIZZ

FORMALISATION DES RESULTATS

Attestation de formation

ACCESSIBILITE AUX PERSONNES EN SITUATION DE HANDICAP

Pour toute situation de handicap, pour plus d'information contactez nous au 05.59.14.04.44 ou consultez notre site internet : Accessibilité (formation-industries-adour.fr)

MÉTHODES ET MOYENS PÉDAGOGIQUES

Alternance d'apports théoriques et de cas pratiques
Formateur expert dans le domaine de l'informatique : Cybersécurité, RGPD, Gouvernance

UIMM
PÔLE FORMATION
Adour
LA FABRIQUE DE L'AVENIR

Sensibilisation à la cybersécurité pour les managers

CONTENU DE LA FORMATION

Introduction à la cybersécurité

- Définition et enjeux pour l'entreprise
- Statistiques et impact croissant des cyberattaques

Identification des menaces et comportements à risque

- Types de cybermenaces : phishing, ransomware, malware
- Erreurs humaines et cas concrets d'attaques

Conséquences des cyberattaques sur l'entreprise

- Coût financier, atteinte à la réputation, interruption des opérations

Partie légale et conformité réglementaire

- **Cadre légal** : Règlementation applicable (RGPD, LPM, ISO 27001)
- **Obligations de l'entreprise** : Protection des données, notification des violations
- **Sanctions en cas de non-conformité** : Amendes, risques juridiques
- **Bonnes pratiques légales** : Politiques de sécurité, respect des normes

Prévention et bonnes pratiques

- Culture de cybersécurité, formations et outils de protection

Conclusion et session de questions-réponses

POUR ALLER PLUS LOIN

Autres formations proposées en Intra-Inter-entreprises :
- Sensibilisation aux enjeux numériques
- Initiation à l'Intelligences Artificielles

ACCES AU PLANNING DE FORMATION

Siège Social
PAU
4 rue des Frères d'Orbigny
BP7502 - 64075 Pau Cedex

Agences
ASSAT
TARBES
TARNOS

05.59.00.01.01
pole-formation-adour@metaladour.org
www.formation-industries-adour.fr