Laho
TERRE DE FORMATIONS
CCI HAUTS-DE-FRANCE

WEB, DIGITAL ET IA

FORMATION INTRA

5 jours

Cybersécurité : Référent TPE/PME

1500 € net de taxe par jour

OBJECTIFS DE LA FORMATION

- Identifier et analyser des problèmes de cybersécurité dans une perspective d'intelligence et de sécurité économiques
- Connaître les obligations et responsabilités juridiques de la cybersécurité
- Identifier et comprendre les menaces liées à l'utilisation de l'informatique et des réseaux internet, réseaux privés d'entreprises ou réseaux publics
- Mettre en œuvre les démarches de sécurité inhérentes aux besoins fonctionnels
- Savoir présenter les précautions techniques et juridiques à mettre en place pour faire face aux attaques éventuelles

PUBLIC VISÉ

Tout public

PRÉ-REQUIS

Sans niveau spécifique

AIDES AU FINANCEMENT **

Cap Emploi
Opérateurs de Compétences (OPCO)
France Travail
Entreprise

*** sous conditions*

MODALITÉS PÉDAGOGIQUES

100% Présentiel

MÉTHODES ET OUTILS PÉDAGOGIQUES

Mise en situation
Alternance d'apports théoriques et d'exercices pratiques

MODALITÉS D'ÉVALUATION

Remise d'une grille d'auto-évaluation des acquis sur les compétences travaillées lors de la formation
Processus d'évaluation des acquis tout au long de la formation
Evaluation de fin de formation individuelle par le formateur

MODALITÉS D'ACCÈS

Bulletin d'inscription
Demande de devis

ACCESSIBILITÉ ET HANDICAP

Contactez-nous

FORMATION INTRA

Cybersécurité : Référent TPE/PME

5 jours

PROGRAMME DE LA FORMATION

Les TPE/PME évoluent aujourd'hui dans un environnement de plus en plus numérique, qui favorise incontestablement leur compétitivité et leur croissance. Pour autant, les nouvelles technologies de l'information et de la communication lorsqu'elles sont mal maîtrisées, peuvent être à l'origine de vulnérabilités et faciliter les attaques sur l'entreprise.Il convient, aujourd'hui, de mettre en place une organisation et un pilotage de la sécurité du système d'information (SI) de l'entreprise.

Cybersécurité : notions de bases, enjeux et droit commun

- Identifier l'articulation entre cybersécurité, sécurité économique et intelligence économique
- Comprendre les motivations et le besoin de sécurité des systèmes d'information (SI)
- Connaître les définitions et la typologie des menaces
- Cartographier le paysage institutionnel de la cybersécurité

Hygiène informatique pour les utilisateurs

- Appréhender et adopter les notions d'hygiène de base sur la cybersécurité pour les organisations et les individus
- Comprendre le Nomadisme et les problématiques liées au BYOD (Bring Your Own Devices)

Gestion et organisation de la cybersécurité

- Appréhender les multiples facettes de la sécurité au sein d'une organisation
- Connaître les métiers directement impactés par la cybersécurité
- Anticiper les difficultés courantes dans la gestion de la sécurité
- Acquérir la méthodologie pour responsabiliser et diffuser les connaissances ainsi que les bonnes pratiques internes
- Gérer un incident, des procédures judiciaires

Protection de l'innovation et cybersécurité

- Appréhender la protection de l'innovation à travers les outils informatiques.
- Découvrir la cyber-assurance.
- Administration sécurisée du système d'information (SI) interne d'une entreprise
- Savoir sécuriser le SI interne
- Savoir détecter puis traiter les incidents
- Connaître les responsabilités juridiques liées à la gestion d'un SI

La cybersécurité des entreprises ayant externalisé tout ou une partie de leur SI

- Connaître les techniques de sécurisation d'un SI, partiellement ou intégralement externalisé

Sécurité des sites internet gérés en interne

- Connaître les menaces propres au site internet
- Connaître les règles de sécurité pour gérer un site internet