

La formation en résumé

Les TPE et les PME représentent une source importante d'emplois et d'innovations. Elles 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. Pour y faire face, les TPE/PME n'ont pas toujours la possibilité de recruter des profils dédiés à la sécurité informatique. Qui plus est, l'approche qu'elles ont de la gestion des infrastructures informatiques varie en fonction de l'utilisation qui en est faite, de leur taille, du secteur économique et du budget qui y est consacré. De fait, à l'exception de certains secteurs très spécifiques, le niveau de perception et de prise en charge du cyber-risque dans les TPE/PME est aujourd'hui faible. Afin de promouvoir un environnement favorable au développement économique et de préserver le patrimoine immatériel de ces entreprises, il convient aujourd'hui, dans une démarche d'intelligence économique, de mettre en place des solutions humaines et techniques adaptées aux spécificités des TPE/PME.

Objectifs :

- 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.

Participants :

Salariés et demandeurs d'emploi,
Dirigeants de TPE ou PME,
manager, Responsables informatique

Prérequis :

Connaissance de base en informatique.
Il est recommandé d'avoir des compétences sur l'organisation d'un système informatique.

Le contenu

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.

Hygiène informatique pour les utilisateurs

- Appréhender et adopter les notions d'hygiène de base sur la cybersécurité pour les organisations et les individus.

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.

Protection de l'innovation et cybersécurité

- Appréhender la protection de l'innovation à travers les outils informatiques.

2 750 €

(non assujetti à la TVA)

Cycle intégrant le passage de la Certification - Éligible CPF

**35 heures****5 jours**Initiative Data
Compétences

Éligible au CPF

Financement
FNE-Formation
(nous consulter)

Dates et villes

Lyon - 04 72 53 88 00

Sessions à venir - Nous contacter

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 règles de sécurité pour gérer un site internet

Moyens pédagogiques et d'encadrement

Formation avec alternance d'apports théoriques et pratiques.

Pédagogie active : Echanges, analyses de pratiques, mises en situation, cas réels d'entreprises

Support de formation remis aux participants.

Formation animée par un formateur expert de son domaine sélectionné selon un processus qualité certifié. Les formateurs sont accompagnés par notre pôle pédagogique intégré « [Agir et Apprendre](#) ». Parcours du formateur disponible sur simple demande.

Suivi et évaluation de la formation :

Les acquis sont évalués en cours et en fin de formation et les stagiaires passeront un examen menant à la certification IDC (Initiative Data Compétences) :

Référent en Cybersecurite

