

** Cette fiche à été générée sur formation-cn.fr le 08/12/2021 à 01:12 **

Ref : CN2048

Durée : 1 journée

Tarif : 910 €HT

Formation intelligence économique

Objectifs de la formation intelligence économique :

Assurer la protection du patrimoine de l'entreprise en interne et en externe. Organiser la recherche d'information et en connaître les limites. Anticiper les risques et gérer les situations de crise.

Programme de la formation intelligence économique :

Identifier les notions d'intelligence économique et de sécurité informatique

- **Définitions, marché, droit**

- Distinguer IE et espionnage
- Cerner les impacts de l'IE sur la sécurité informatique, la convergence et ses effets

Assurer la protection du patrimoine de l'entreprise

- **La protection de l'entreprise vis-à-vis de ses acteurs**

- Actionnaires, administrateurs : encadrer, gérer leur accès et leur utilisation de l'information
- Définir quel accès à l'information laisser aux salariés

- **Gérer le risque informatique en interne**

- Contrôle des salariés
- Usurpation d'identité...

- **Faire le point sur les créations et les inventions des salariés**

- **Étude de cas** : analyse des obligations des salariés d'une société suivant le type d'information visé

Recourir à la justice pour obtenir des informations

- **Dans le cadre d'une procédure civile**

- Ordonnance sur requête, référé, saisie contrefaçon
- Collecter des preuves en toute légalité

-

Dans le cadre d'une procédure pénale

- Plaintes, instructions, perquisitions
- **La compétence des juges et des tribunaux**
 - **Étude de cas** : analyse de la gestion de la preuve dans le cadre d'un procès afin d'optimiser l'utilisation de l'information

Cerner les limites du droit à la recherche d'information

- **Le respect de la vie privée**
 - La nouvelle loi Informatique et libertés du 06/08/04
 - Les risques de concurrence déloyale
 - Concilier knowledge management et protection du capital immatériel
- **Le cryptage**

Anticiper une opération de désinformation

- **En interne**
 - Gérer la désinformation du fait des salariés
 - Faire le point sur les nouveaux risques liés au développement des technologies en réseau
- **En externe**
 - Le rôle de la presse écrite ou parlée
 - La diffusion via Internet
 - Gestion de la rumeur : les mesures de contre-influence à mettre en place
- **Identifier les responsabilités et les sanctions**
 - **Exercice d'application** : mise en place d'une cellule de crise suite à un cas de dénigrement d'une entreprise sur Internet

Méthodes pédagogiques

La formation est décomposée en séquences qui respectent une progression pédagogique et agissent sur les trois niveaux d'apprentissage : savoir, savoir-faire et motivation. Notre approche alterne apports théoriques, exercices pratiques et/ou études de cas utilisant des méthodes d'animation actives et permettant une meilleure compréhension des concepts et une appropriation accélérée. Tous les cas pratiques seront adaptés à votre contexte.