

Maîtrisez les concepts fondamentaux de la cybersécurité et de la sécurité de l'information appliqués à la lutte contre la fraude à l'assurance

DURÉE : 1 Jour (7H)

Prix : 780,00 € HT



PRÉSENTIEL



Objectifs et compétences visés

- Connaître les principaux risques de cybersécurité, savoir les évaluer et identifier les fraudes associées.
- Connaître les principales mesures de sécurité en place dans les entreprises.
- Identifier les données utiles dans le cadre de la détection de la fraude.
- Comprendre le fonctionnement d'une expertise informatique après sinistre.

À qui s'adresse la formation ?

Profils

Correspondants anti-fraude, enquêteurs, assureurs, chefs de projet sécurité ou consultants sécurité en assurance, toute personne souhaitant se familiariser avec le rôle de la cybersécurité dans la lutte contre la fraude à l'assurance.

Cette formation répond à la directive européenne DDA (Décret n° 2018-431 du 1er juin 2018) visant le public des assureurs.



Prérequis

Aucun prérequis n'est nécessaire à cette formation. Il est nécessaire de venir muni d'un ordinateur portable.

Contenu de la formation

Les concepts fondamentaux de la sécurité de l'information

- L'information comme actif essentiel de l'entreprise.
- Les besoins en termes de disponibilité, d'intégrité, de traçabilité et de confidentialité.
- Présentation et décryptage d'une cyberattaque.

Les risques cyber et l'estimation d'un dommage

- Les différents types de menaces (fraude interne, attaque informatique, ...).
- L'évaluation et la hiérarchisation des risques.
- Exercice « cas pratique » :
 - création de scénarios de risque (Actifs > Vulnérabilités > Menaces > Impacts) ;
 - estimation d'un dommage (détermination des exagérations).

Les mesures de sécurité en place et l'applicabilité des garanties

- Les mesures techniques.
- Les mesures organisationnelles.

- Le contrôle de l'implémentation des mesures dans le cadre du contrat souscrit.
- Exercice pratique.

L'investigation dans le cas d'un sinistre

- La vérification de la réalité d'un dommage.
- La collecte de preuves en informatique (date d'incident, analyse des causes, gestion des logs).
- Les aspects contractuels et juridiques :
 - les garanties d'un contrat cyber ;
 - le cumul d'assurance ;
 - collusion entre la victime et le cybercriminel.

Modalités

Modalités d'évaluation

Cette formation ne donne pas lieu à un contrôle de connaissances.

Nos plus

- Formation animée par un consultant CNPP expert dans la sécurité des systèmes d'information et la recherche de preuves dans le cadre d'investigations numériques.
- Disponible également en visioconférence.

En bref

21000

stagiaires / an



Des infrastructures
pédagogiques uniques

+ de 500

diplômés / an

+ de 400

intervenants

Nos formations complémentaires

Management de la sécurité de l'information

Classe virtuelle cybersécurité : les fondamentaux organisationnels de la sécurité de l'information

1H30

Classe virtuelle

Sensibilisation à la cybersécurité - Classe virtuelle

-
Protection des données personnelles (RGPD)

Fondamentaux du RGPD

1 Jour

Présentiel

Découvrez les fondamentaux du Règlement Général à la Protection des Données (RGPD)

-

Besoin d'informations sur une formation en cybersécurité ?

Nous sommes à votre écoute pour échanger sur votre prochaine formation en cybersécurité.

Contactez-nous !

+33 (0)8 06 00 03 80