

Sécuriser et Assurer les Cyber-Risques en Entreprise



OBJECTIFS VISÉS

- Identifier les différents types de cyber-risques et leur impact sur les entreprises.
- Connaître le cadre réglementaire applicable à ces risques.
- Maîtriser les solutions de prévention et d'assurance pour une gestion efficace des cyber-risques.

PUBLIC

Collaborateurs en charge de la gestion des assurances en entreprise.

PRÉREQUIS

Aucun prérequis.

COMPÉTENCES ACQUISES

Connaissance approfondie des solutions réglementaires et assurantielles adaptées.

FORMATEURS

Cette formation est animée par un , formateur expert de Venus Consulting.

TARIF :

A partir de 1400 € HT

MODALITÉ D'ACCÈS : Les inscriptions se font par mail à conseiller@venusconsulting.fr ou en ligne sur notre site. Toutes les démarches administratives et financières doivent être réglées avant le début de la formation. Veuillez noter qu'en cas de demande de financement à un organisme financeur, la démarche de prise en charge est à réaliser par le candidat ou l'entreprise et doivent être réalisées à l'avance. Les formations sont confirmées 3 semaines avant le début de la formation.

Pour les personnes en situation de handicap souhaitant réaliser une formation en e-learning : Nous vous invitons à prendre contact avec notre référent handicap (conseiller@venusconsulting.fr) afin de déterminer les formations accessibles.

PROGRAMME

1. IDENTIFICATION DES CYBER-RISQUES

- Définir ce que sont les cyber-risques.
- Explorer les typologies des risques informatiques :
 - Détériorations accidentelles.
 - Vols et piratages.
 - Virus et logiciels malveillants.
 - Erreurs de manipulation et autres risques humains.
- Analyser les secteurs les plus exposés.
- Comprendre les enjeux stratégiques pour les entreprises.

2. LE CADRE RÉGLEMENTAIRE

- Étudier les directives européennes en matière de cyber-sécurité.
- Comprendre leur transposition dans le droit français.
- Évaluer l'impact de la réglementation sur l'assurabilité des cyber-risques.

• 3. GESTION ET ASSURANCE DES CYBER-RISQUES

- Mettre en place des stratégies de prévention :
 - Mesures de sécurité informatique.
 - Sensibilisation et formation des équipes.
- Explorer les solutions de transfert des risques :
 - Garanties proposées par les assurances.
 - Exclusions et limitations courantes.
 - Extensions et garanties annexes (pertes d'exploitation, responsabilité civile, etc.).

PERSONNALISATION DE LA FORMATION

Un questionnaire préparatoire sera remis en amont de la formation au participant lui permettant de faire remonter auprès du formateur ses attentes et besoins spécifiques.

VALIDATION DES ACQUIS

Évaluation des acquis de la formation par des cas pratiques, exercices, QCM... - Questionnaire d'évaluation à chaud proposé à la fin de formation - Une attestation sera remise au stagiaire à la fin de la formation

