Cyberattaques et responsabilités : Maîtriser le cadre juridique et ses obligations

Programme de formation

Objectifs :

- Comprendre le cadre juridique des cyberattaques
- Maîtriser les obligations légales en matière de cybersécurité (RGPD, NIS 2)
- Savoir réagir légalement et opérer les notifications nécessaires aux autorités de contrôle en cas d'incident
- Connaître les responsabilités juridiques en cas de cyberattaque
- Mettre en place une stratégie de sécurité conforme à la réglementation

Durée : 1 jour soit 8 heures

Public : Professionnels du droit (juristes, avocats) souhaitant se spécialiser en cybersécurité, Responsables de la conformité, de la sécurité des systèmes d'information (RSSI) et Délégués à la protection des données (DPO), Dirigeants d'entreprise et managers désireux de comprendre leurs responsabilités juridiques face aux cyber risques et de mettre en place des plans d'anticipation et de réaction

Prérequis : Compréhension de base du fonctionnement d'un système informatique et d'un réseau, connaissance élémentaire du Règlement général sur la protection des données (RGPD) serait un atout, familiarité avec le vocabulaire de base de la cybersécurité (cyberattaque, vulnérabilité, hameçonnage)

Moyens et outils pédagogiques : Présentation numérique, Démonstrations pratiques, Etudes de cas, Mises en situation, Exercices pratiques, Quiz

Nombre de formateurs : 1 + 1 intervenant

Lieu et date : en vidéoconférence

Coût : à partir de 584 € HT (soit 700,80 € TTC)

A l'issue de la formation chaque participant recevra un certificat de réalisation, un livret de formation, un questionnaire de satisfaction et un questionnaire de validation des acquis

AJ Consulting s'engage à rendre ses formations accessibles aux personnes en situation de handicap. N'hésitez pas à contacter notre référent handicap pour discuter de vos besoins spécifiques.

AJ Consulting
Conseil – Audit – Formation
27 rue Jean Jaurès – 29120 Pont l'Abbé
Tél : 02 22 94 12 21
SIRET : 511 588 295 00028 – APE 6202A – NDA 53 29 10088 29 – TVA FR 515 511 588 295

Déroulé de la formation

Module 1 : Enjeux, risques et obligations réglementaires (Matin)

Objectif : comprendre la menace pour se protéger

- Définitions, contexte et menaces
- Evaluation des impacts : financiers, réputationnels, juridiques et opérationnels
- Conformité réglementaire : RGPD, NIS 2
- Présentation des autorités de référence : cyberdéfense, ANSSI, CNIL
- Identification des menaces et des vulnérabilités

Module 2 : Pratiques à mettre en place pour sécuriser son environnement informatique (Matin)

Objectif : Anticiper pour éviter une cyberattaque par l'analyse des risques, adopter des comportements sécurisés

- Stratégie de sécurisation et définition des priorités
- Méthodologie et outils : les plans d'anticipation
- Les plans de continuité d'activité (PCA) et de reprise d'activité (PRA)
- Pratiques indispensables pour se protéger

Module 3 : Faire face à une cyberattaque (Après-midi)

Objectif : Savoir réagir en cas de cyberattaque

- Les bons gestes à adopter lors de la découverte de la cyberattaque
- Les notifications aux autorités de contrôle
- La mise en pratique des plans et les poursuites judiciaires

Module 4 : Etude de cas et mise en situation (Après-midi)

Objectif : A partir d'études de cas et mise en situation, mettre en pratique les pratiques et les obligations apprises dans les modules 1, 2 et 3, savoir identifier une situation à risque

- Etude de cas pratique
- Mise en situation
- Evaluation finale

AJ Consulting
Conseil – Audit – Formation
27 rue Jean Jaurès – 29120 Pont l'Abbé
Tél : 02 22 94 12 21
SIRET : 511 588 295 00028 – APE 6202A – NDA 53 29 10088 29 – TVA FR 515 511 588 295