Ref : DNDASECUDROIT	**Durée :** 3 Jours	**Tarif :** 2 070 €HT

Formation Droit de la cybersécurité

Objectifs de la formation Droit de la cybersécurité:

- Apprendre les règles juridiques encadrant la sécurité informatique
- Permettre à des personnes n'étant pas juristes de comprendre les règles de droit s'appliquant à la sécurité informatique
- Savoir comment assurer le respect du droit de manière efficace et opérationnelle
- Pouvoir améliorer le niveau de conformité de son organisme ou de ses clients

Programme de la formation Droit de la cybersécurité:

1 - Introduction
Présentation de la formation
Présentation du cadre juridique français
Articulation du droit national avec les droits étrangers

2 - Les atteintes à la sécurité du SI
Notion essentielle : responsabilité pénale et civile / infractions
Les infractions d'atteintes au SI
La collecte des preuves
Le dépôt de plainte
Les services spécialisés
Les obligations de signalement des atteintes au SI

3 - Les obligations de sécurité
Les obligations légales de sécurité : sécurité des données personnelles, des données de santé, des données bancaires, etc.
Les obligations contractuelles : disponibilité du service, confidentialité des données, etc.
Les responsabilités de chacun :

- de l'organisme
- de l'employeur
- des salariés
- du RSSI, du DSI, de l'administrateur système

4 – La protection des données personnelles
Le cadre légal : les textes, les principes fondamentaux, les risques associés aux manquements
Les principales notions : données à caractère personnel, traitement, responsable de traitement, sous-traitant, personnes concernées, DPO, CNIL.
Les obligations :

- La cartographie des traitements

La conformité des traitements
La responsabilité des acteurs : responsable de traitement, co-responsable, sous-traitant, DPO
Les études d'impact (PIA)
La sécurité des données
Les prestataires et sous-traitants
Les transferts internationaux Les droits des personnes concernées
Les contrôles de la CNIL
Pour aller plus loin : Gouvernance, Code de conduite, Certifications

5 - Les obligations de conservation des traces
Données relatives au trafic
Données d'identification des créateurs de contenus
Accès administratif aux données de connexion
Autres traces

6 - Surveillance des salariés
Le pouvoir et devoir de contrôle de l'employeur
Le respect de la vie privée des salariés
L'accès au poste et aux données des salariés
Les règles encadrant l'usage du SI
La responsabilité du salarié
La Charte informatique :

son rôle
son contenu
son entrée en vigueur
sa valeur contraignante

7 - Conclusion
Conclusion
Démarche documentaire
Outils de veille

Public

RSSI, DSI, Administrateurs systèmes et réseaux, astreintes opérationnelles, Maîtrises d'œuvre de la SSI, chefs de projet, responsables de compte, Consultants en sécurité, Juristes amenés à intervenir dans le domaine de la cybersécurité, Toute personne impliquée dans la sécurité informatique.

Pré-requis

Aucun pré-requis n'est demandé. Il n'est pas nécessaire de disposer de connaissances en droit ou en sécurité informatique pour suivre cette formation. Cependant, une connaissance générale de l'informatique est souhaitable.

Méthodes pédagogiques

Le cours se veut avant tout pratique. Chaque thème est abordé en partant des dispositions juridiques, qui sont expliquées en langage courant. Le formateur conseille les stagiaires sur le comportement qu'il estime le plus pertinent en pratique, en prenant en compte l'ensemble des aspects (coûts, image, risques, etc.). Le cours est conçu pour être totalement interactif : les stagiaires peuvent

constamment poser des questions, et le formateur soumet souvent des cas pratiques aux stagiaires, afin qu'ils réfléchissent au comportement le plus adapté.