Formation « Droit de la cybersécurité »

Réf : SECUDROIT

La cybersécurité ne se gère pas qu'avec une organisation adaptée et des savoir-faire techniques, le droit en est un des piliers incontournables, et tout professionnel de la sécurité des systèmes d'information doit en connaître les bases.

Le cours aborde les principaux aspects juridiques de la sécurité informatique, de façon pratique, concrète et pragmatique. La formation est conçue conjointement par des juristes ou avocats et des ingénieurs en informatiques.

Objectifs

- **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**

Durée & horaires

- **3 jours soit 21 heures**
- **De 9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **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.**

Méthode pédagogique

- **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.**

Supports

- **Support de cours au format papier en français**
- **Extraits de documents pratiques : charte informatique, fiches de traitement, etc.**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **À l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h00 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUDROIT par HS2.**

Programme

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