L'USINEDIGITALE EVENTS

CADRE JURIDIQUE DE LA CYBERSÉCURITÉ

Quels leviers juridiques activer pour protéger le patrimoine de votre entreprise

,

CYBER SÉCURITÉ

Objectifs de la formation

- Déterminer le cadre juridique applicable aux enjeux techniques de protection et de défense de votre système d'information
- Comprendre son évolution au regard du développement des nouvelles technologies et des nouveaux usages associés : Objets connectés, Big data, Cloud computing,...
- Appréhender les enjeux juridiques liés aux données et à leur exploitation
- Anticiper les risques juridiques encourus par vous ou votre organisation en cas de problème d'intrusion, vol, modification ou destruction de données

Animée par

- VÉRET DANIELE
  Avocate,

Public concernés

- Directeur des Systèmes d'Information,
- Responsable de la sécurité des systèmes d'information
- Directeur Juridique, Juriste, correspondant CNIL
- Expert/consultant en système d'information...

Dates

Critères d'admission

- Cette formation entre dans le champ

Accueil des participants

Evolution de la réglementation en matière de sécurité des systèmes d'information et projets de réglementation (droit français et règles européennes)

- Les lois et réglementations directrices en matière de protection des individus
- L'évolution du cadre juridique de la protection des données à caractère personnel
- Le contour des notions de confidentialité et de secret
- Les grands principes qui régissent la propriété intellectuelle
- Déontologie, loyauté

Panorama des différentes approches existantes sur la protection des données dans les principaux pays

d'application des dispositions relatives à la formation professionnelle continue car considérée comme une action d'adaptation et de développement des compétences des salariés.

Prérequis

- Aucun prérequis n'est nécessaire

Modalités pédagogiques

- Un questionnaire préalable sera envoyé aux participants pour recueillir leurs besoins et attentes spécifiques, et sera transmis au(x) formateur(s) avant la formation
- Tous nos stages de formations sont limités, dans la mesure du possible, à une douzaine de participants
- Les formations sont déroulées en présentiel ou en classe virtuelle et étayées, chaque fois que cela est pertinent, d'études de cas et de mise en pratique ou en situation
- Un formulaire d'évaluation du formateur et du déroulé du programme suivi sera proposé aux participants à la fin du stage

Quelle position pour le RSSI en matière de cybersécurité

- Missions du RSSI et chaîne des responsabilités dans l'entreprise au regard de la cybersécurité
- Les bons réflexes à adopter pour exercer sa mission de façon sécurisée
- Quels sont les risques encourus et fautes possibles pouvant entrainer la responsabilité du RSSI

Déjeuner

Les risques d'infractions pénales

- Accès et maintien frauduleux, suppression ou modification de données, introduction frauduleuse de données, altération du fonctionnement d'un système, etc.
- Contrefaçon
- Collecte, finalité, proportionnalité et données à caractère personnel
- Violation d'un secret

Quelles précautions juridiques prendre au regard des différents outils numériques (Cloud, Big Data, Objets connectés)

- L'information des personnes et les demandes d'autorisation
- Les précautions contractuelles
- La constitution de preuves
- Le renforcement de la charte d'utilisation des moyens de communication
- La sensibilisation et la responsabilisation des utilisateurs

Comment prouver et valoriser un préjudice

- L'atteinte à l'image de la personne et à sa dignité
- La perte d'un emploi
- La perte de commande voire de clientèle
- La concurrence déloyale et parasitaire

Quelles actions mener en cas de litige

- La recherche du responsable ou du coupable
- Comment parvenir à un accord amiable
- Les poursuites judiciaires

Fin de journée