PARCOURS

JURISTE EN DROIT DE L'INNOVATION TECHNOLOGIQUE

Certifiez vos compétences juridiques à l'ère du digital

JURISTE EN DROIT DE L'INNOVATION TECHNOLOGIQUE

—

Tarif préférentiel : 3 500 € HT

- 2 jours — **CULTURE IT POUR LES MÉTIERS JURIDIQUES** — Code : 63146
- 1 jour — **BLOCKCHAIN : LES ENJEUX JURIDIQUES ET COMPLIANCE** — Code : 63257
- 1 jour — **OPEN INNOVATION** — Code : 63140
- 1 jour — **LA CYBERCRIMINALITÉ** — Code : 63147

Ceci est une suggestion de parcours – Si une de ces formations mérite d'être remplacée, vous pourrez sélectionner celle de votre choix parmi la gamme afin que le parcours soit le plus adapté à vos besoins. Pour plus d'informations, veuillez nous consulter.

La Cybercriminalité

Quel plan d'actions pour renforcer son dispositif de sécurité ?

OBJECTIFS

- Identifier les différentes formes de cyberattaques
- Savoir quelles actions mettre en œuvre suite à une attaque informatique
- Savoir quelles mesures mettre en place pour prévenir les attaques informatiques
- Anticiper un contrôle de la Commission nationale de l'informatique et des libertés suite à une violation de données à caractère personnel rendue possible par l'exploitation d'une faille de sécurité

FORMATEUR(S)

Virginie BENSOUSSAN-BRULE, Avocat, Directrice du pôle Contentieux numérique, Cabinet LEXING ALAIN BENSOUSSAN AVOCATS

PUBLIC

- Responsable juridique, juriste
- Avocat, DSI, DG
- Développement / Innovation

DURÉE :	1 jour
SESSIONS	18 mars 17 juin 16 septembre 18 novembre
TARIF :	1020 € HT
CODE :	63147

PROGRAMME / 1 jour

1 Les infractions pénales

Panorama des atteintes aux systèmes de traitement automatisés de données (STAD) :
- la notion de STAD
- la notion de maître du système
- la question de la protection du STAD
- l'accès frauduleux
- le maintien frauduleux
- l'atteinte à l'intégrité du système
- l'atteinte à l'intégrité des données
- l'association de malfaiteurs informatiques
- la détention d'un programme informatique conçu pour commettre une atteinte à un STAD
- la tentative

L'infraction spécifique de vol d'informations

2 Les actions à mettre en œuvre suite à une attaque informatique

Dépôt de plainte auprès du Procureur de la République
Déclaration de sinistre
Plan de communication interne et externe
***Mise en situation** : rédaction d'un plan média*

3 Les mesures à mettre en place pour prévenir les attaques informatiques

Sécurisation du SI contre les risques externes :
- charte des moyens informatiques et des outils numériques
- charte des administrateurs
- charte des tiers

Sécurisation du SI contre les risque internes

4 La notification de violations de données

Notification à la Cnil :
- notifications initiale et complémentaire
- information des personnes concernées

Notification à l'Anssi :
- par les organismes d'importance vitale (OIV)
- par les organismes de service essentiel (OSE)
- par les fournisseurs de service numérique (FSN)

Le lanceur d'alerte informatique