

# Formation cybersécurité pour la fonction juridique

PROGRAMME DE FORMATION

DURÉE : 1 jour (7 heures) – en centre de formation  
ou en entreprise.

Présentiel

## Objectif

Contribuer à la cybersécurité de mon entreprise pour les responsables de la fonction juridique (Rôle et responsabilité dans le domaine).

## Pré-requis

Compréhension de l'informatique de base.

## Participants

Direction juridique.

## Validation

L'évaluation du cours se fera à travers des exercices : des phases de quizz et de questions/réponses.

## Modalités

Nos formateurs utilisent les méthodes andragogiques suivantes : la démonstration, l'étude de cas, le projet, le questionnement de groupe et le quizz.

## Infos complémentaires

Délai d'accès :  
Entre 15 et 45 jours. Formation accessible aux personnes en situation de handicap.  
Plus d'informations au 0692 22 55 83.

Débouchés :  
Cette formation permet une montée en compétences mais ne permet pas de se former à un métier.

Passerelles :  
Aucune passerelle disponible.

## Programme synthétique

### Module 1

Les cyberattaques locales récentes,  
Témoignages de victimes de cyberattaques  
Un site pour se tenir informé de l'actualité cyber

### Module 2

L'environnement numérique des entreprises, et transformation digitale de la fonction finance,  
Comprendre la révolution numérique à travers une brève histoire ,  
Comprendre le rôle des géants de la tech., des opérateurs telco's, des entreprises de Services numériques, des plates-formes « legalltech »  
Comprendre les usages privés et professionnels (les réseaux sociaux, WEB, Darkweb,...)  
Comprendre Les apports concrets des technologies (WEB, Cloud, 5G, Big Data, Opendata, Intelligence Artificielle la justice prédictive, la « blockchain-smart-contracts », registres) et leur impact.  
Comprendre les usages (WEB, Darkweb, réseaux sociaux..),  
Les tendances, le juriste augmenté ou juriste 2.0  
Connaître les usages locaux ( à La Réunion)

### Module 3

Panorama des menaces  
Définir Les sources de risques, les effets recherchés d'une attaque par type (sabotage, espionnage, atteinte à l'image, cybercriminalité, cyberguerre..)  
Qualifier brièvement les attaquants, et les menaces qu'ils peuvent faire peser sur les entreprises  
Connaître les principales menaces ( et les autres) sur les données et les processus Finance

### Module 4

Les essentiels de la cybersécurité  
Connaître les actifs essentiels d'un système d'information  
Définir Les critères de sécurité (les exemples pour la fonction par un exercice  
Mettre en œuvre (impérativement) des processus de cybersécurité quelle que soit la taille de l'entreprise,  
Connaître les activités, les domaines, quelques outils  
Différencier cybersécurité et cyber résilience

### Module 5

Mise en pratique de manipulation des concepts (actifs, critères, risques..)

### Module 6

La cybersécurité de la fonction juridique:  
Les aspects juridiques de la sécurité  
La sécurité sur la communication électronique  
La sécurité des données  
Les différents outils de sécurité pour le juriste

### Module 7

La participation de la fonction à la gestion de crise (exercice)

### Module 8

Les bonnes pratiques de cybersécurité au quotidien  
Connaître les principaux vecteurs pour les attaquants (le hameçonnage, les supports amovibles, et mots de passe..),  
Sécuriser mes informations,  
Actions à réaliser en cas de fuite de données,  
Utiliser internet en sécurité, pour mes opérations