DU CYBERCRIMINALITE : DROIT, SECURITE DE L'INFORMATION ET INVESTIGATION NUMERIQUE LEGALE

Durée
1 an

Structure de formation
Faculté de Droit et de Science politique

Présentation

L'essor d'Internet a incontestablement accéléré et facilité les accès et les échanges de l'information. Cette fulgurante réussite dans la communication a favorisé l'apparition de nouvelles menaces criminelles. Ces menaces font courir des risques considérables pour les entreprises, les administrations publiques et les particuliers. La lutte contre la cybercriminalité est devenue un défi majeur mondial en raison de la dimension internationale de cette nouvelle délinquance souvent organisée.

La cybercriminalité évolue chaque jour, faisant apparaître de nouvelles formes de risques et de techniques de contournement de la loi, que le droit se doit de prendre en considération et auxquelles il doit s'adapter.

Les + de la formation

Site du diplôme (candidature et information) : https://cybercrime.edu.umontpellier.fr/

Secrétariat du diplôme - Courriel

Objectifs

Mis en place dans le cadre du projet Européen 2CENTRE, le diplôme d'Université « Cybercriminalité : Droit, Sécurité de l'information et investigation numérique légale » est une formation pluridisciplinaire permettant de comprendre les enjeux de la sécurité de l'information et de la cybercriminalité et d'appréhender les différentes infractions et responsabilités liées à l'utilisation frauduleuse des réseaux numériques et des systèmes d'information.

Elle apporte aux acteurs économiques, aux étudiants, aux professionnels du droit, aux forces de l'ordre, aux experts judiciaires, aux responsables des systèmes d'information et à toutes les personnes confrontées à la cybercriminalité un éclairage sur :

* La nature des menaces liées aux réseaux numériques,
* Les techniques d'intrusion dans les systèmes d'information,
* Les dispositifs juridiques de lutte contre la cybercriminalité,
* Les enjeux de la sécurisation et les obligations légales et réglementaires de la sécurisation d'un système d'information,
* La protection des données personnelles (RGPD, etc.),
* Les techniques d'investigation numérique et les procédures d'établissement de la preuve,
* L'impact économique de la cybercriminalité (blanchiment d'argent, cyber-fraudes financières…),
* Les questions et les réponses juridiques qui se mettent en place aux plans national, européen et mondial.

Ce diplôme bénéficie de l'appui de l'Ecole Nationale de la Magistrature (diplôme inscrit au catalogue de formation de l'ENM pour la formation des Magistrats), de la Gendarmerie Nationale (formation d'officiers de la Gendarmerie Nationale) et de plusieurs organismes nationaux et internationaux. C'est le seul diplôme (domaine Cyber) de l'Université soutenu par ces deux institutions.

Adel JOMNI, Responsable de la formation

Enseignant-chercheur (Université de Montpellier)

Expert auprès du Conseil de l'Europe

Membre de l'European Cybercrime Training and Education Group

Organisation

Contrôle des connaissances

Un examen final (écrit) se déroule lors de la première semaine du mois de juillet. Il concerne les conférences proposées pendant l'année universitaire. Le redoublement n'est pas autorisé.

Aménagements particuliers

50 % de la formation peut être suivie à distance

Admission

Conditions d'accès

Formation initiale :

Étudiants ayant validé une Licence 3 (ou équivalent).

Formation continue :

Licence 3 validé (ou équivalent) ; ou au minimum bac + 2 avec au moins deux années d'expérience professionnelle.

Public cible

Formation initiale :

Étudiants ayant validé une Licence 3 (ou équivalent)

Formation continue :

Cette formation s'adresse aux professionnels qui souhaitent développer des compétences dans le domaine de la lutte contre la cybercriminalité et la sécurité des systèmes d'information. Les professionnels peuvent ainsi valoriser l'expérience professionnelle qu'ils ont acquise, par l'obtention d'un diplôme universitaire.

Exemples de professionnels concernés par cette formation :

Les salariés de l'industrie ou des collectivités locales qui sont responsables de la sécurité des systèmes d'information

Le personnel chargé des enquêtes (experts judiciaires, officiers de la Gendarmerie et la Police nationale, enquêteurs privés) ou de leur supervision dans les affaires de criminalité informatique

Les professionnels du droit (Magistrats, Avocats, responsables de services juridiques) amenés à traiter des dossiers liés à la cybercriminalité

Les personnes chargées de la régulation des réseaux sociaux et des plates-formes de signalements

Pré-requis recommandés

Un goût pour les nouvelles technologies. Des connaissances de base (bureautique) sur les ordinateurs et sur Internet sont souhaitées.

Un programme de mise à niveau technique, pour les juristes, est prévu, de même qu'un programme de mise à niveau juridique pour les étudiants et les professionnels non juristes. La mise à niveau se déroule lors du premier mois de la formation.

Infos pratiques

Contacts

Responsable pédagogique

Adel Jomni

+33 4 34 43 29 53

adel.jomni@umontpellier.fr

Secrétariat DU CYBERCRIMINALITE

du-cybercrime@umontpellier.fr

Lieu(x)

Montpellier - Faculté de Droit et de Science politique

En savoir plus

https://cybercrime.edu.umontpellier.fr/

Programme

Organisation

Le planning prévisionnel de la formation est disponible sur le site : https://cybercrime.edu.umontpellier.fr/ »

UE1 : Introductions aux réseaux et à l'Internet

* Organisation et structure physique des réseaux
* Caractéristiques techniques du réseau Internet (TCP/IP, DNS, WiFi…)
* RFID et réseaux de capteurs sans fils
* Caractéristiques des applications Web2.0 (réseaux sociaux, blogs, Twitter…)
* Les réseaux Peer to peer (P2P ou pair à pair)
* Caractéristiques et modes d'utilisation des outils de recherche et de veille sur Internet (moteurs, méta-moteurs...)
* Les fournisseurs de services de la société de l'information : rôles et catégories de services proposés et qualification juridique.

UE2 : Introduction au Droit et à la sécurité juridique (Mise à niveau juridique)

* Les différentes branches du droit
* Introduction au Droit pénal
* Introduction à la procédure pénale
* Introduction au Droit de la propriété intellectuelle
* Les diverses formes de responsabilité juridique

UE3 : Introduction aux aspects techniques de la sécurité des systèmes d'information et de la cybercriminalité

* Logiciels malveillants : principes et techniques
* Techniques d'intrusion dans un réseau et moyens de protection.
* Système d'information : définition, rôle et normes de sécurisation
* Cybercriminalité : menaces (piratage informatique, usurpation d'identité, e-réputation, « social engineering », fraudes, APT, Botnets…)
* Introduction à la signature électronique et à la cryptologie

UE4 : Aspects juridiques et économiques de la sécurité des systèmes d'information

* Contexte juridique de la sécurité des systèmes d'information
* Les obligations légales, réglementaires de sécurisation
* Les enjeux de la sécurisation
* Les aspects juridiques de la démarche de sécurisation (cryptologie, chartes, préservation de la preuve, signalement des incidents…)
* Principes et aspects techniques, juridiques et réglementaires de la dématérialisation des échanges (contrats électroniques, preuve électronique, signature électronique…)
* Sécurité de l'information et intelligence économique

UE5 : Cybercriminalité : dispositifs juridiques, enjeux économiques et sociaux

* Panorama de la cybercriminalité (statistiques, évolution…)
* Menaces et qualification juridique
* Lutte contre la cybercriminalité et Droits et Libertés fondamentaux
* Instances de régulation, de prévention et de répression
* Cybercriminalité et coopérations nationales et internationales
* Droits et obligations des acteurs de la société de l'information
* Impact économique de la cybercriminalité (blanchiment d'argent, cyber-fraudes...).
* Réseaux sociaux : impacts pour l'entreprise, risques et responsabilités
* Risques spécifiques aux paiements en ligne et réglementations.

UE6 : Informatique légale, investigation et enquête

* Introduction aux techniques d'investigation numériques légales (computer forensics)
* Panorama de la criminalistique
* Missions et déroulement de l'expertise judiciaire
* Interception des données sur le réseau Internet

UE7 : Traitement et protection des données personnelles sur le réseau internet

* Cadre juridique et enjeux (RGPD, loi informatique et libertés, etc.)

* Statut et missions du délégué à la protection des données (DPO)
* Définition et mise en place d’un plan d’action de conformité
* Faire face à un contrôle de la CNIL