Après le master

Les types d'emplois

- Consultant en sécurité - Ingénieur d'études
- Ingénieur R&D en sécurité
- Ingénieur en conseil, service ou intégration dans le secteur de la cybersécurité
- Assistant-expert en informatique légale
- Ingénieur en administration sécurité système et réseaux

EMPLOYEURS POTENTIELS

- Entreprises spécialisées dans les domaines de la sécurité informatique
- PME et grand groupe (sécurité des systèmes d'informations)
- Grands comptes : assurances, banques, grands groupes.
- Agences gouvernementales

Exemples de sujet de mission

- Implantation sécurisée de chiffrement AES dans une suite logicielle pour smartphones et validation.
- Gestion de la sécurité chez un hébergeur de sites web et audit de l'infrastructure.
- Gestion automatisée de détection de vulnérabilité et validation pour des applications web sensibles.
- Extraction et analyse de données provenant de smartphones (mémoires, cartes SD, données GPS).
- Méthodologie de tests d'intrusions sur des systèmes d'informations.

Informations pratiques

MODALITÉS D'ACCÈS

Ce master de type professionnel s'adresse aux titulaires d'au moins un M1, d'un diplome de master ou d'ingénieur avec une majeure en Informatique ou Mathématiques.
Il est préférable de maîtriser un langage de programmation et d'avoir des connaissances de bases en développement logiciel et en réseaux.

L'admission se fait en deux temps : il y a une première sélection sur dossier, suivi d'un entretien devant une commission. Cet entretien obligatoire détermine l'admissibilité à la formation. L'admission a lieu lorsque votre contrat d'apprentissage est validé.

Le dossier de candidature est à télécharger sur le site de l'établissement ou à demander par courrier

CONTACTS

UFR IM²AG / Unité de Formation et de recherche Informatique, Mathématiques et Mathématiques Appliquées de Grenoble
60, rue de la Chimie - CS 40700
38028 Grenoble Cedex 9

Service Gestion de l'étudiant
Tél. 04 76 53 57 01
im2ag-service-formation@univ-grenoble-alpes.fr

Site web de l'UFR IM²AG :
https://im2ag.univ-grenoble-alpes.fr

UFR IM²AG
UNIVERSITÉ Grenoble Alpes

MASTER (M2) INFORMATIQUE

PARCOURS CYBERSÉCURITÉ ET INFORMATIQUE LÉGALE (CSI)

EN ALTERNANCE

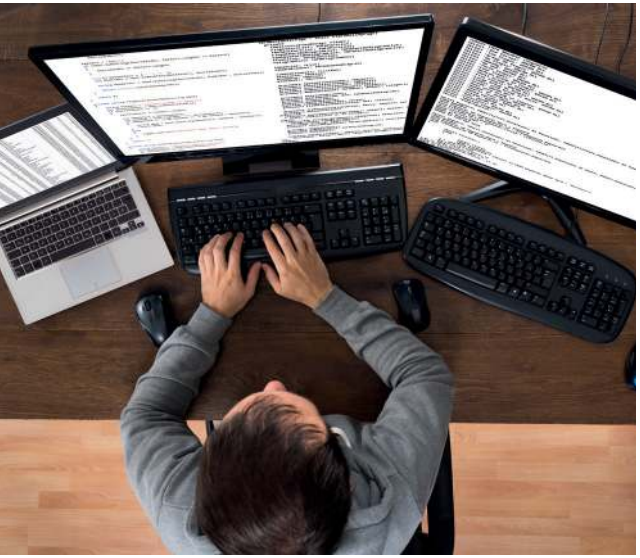
Crédits photos : Shutterstock / UGA

UFR IM²AG
UNIVERSITÉ Grenoble Alpes

Le master CyberSécurité et Informatique légale (CSI) est un parcours de la mention Informatique du master Sciences, technologies et santé de l'Université Grenoble Alpes.

Présentation

Le master CSI est exclusivement proposé en apprentissage et alternance.
Cette formation permet aux étudiants issus d'un niveau M1 ou équivalent, avec une majeure Informatique ou Mathématiques, de se former lors de leur deuxième année de master aux métiers de la cybersécurité (sécurité des systèmes et des réseaux, l'audit, analyse de risques, sécurités logiciel et matériel) et de l'informatique légale (forensic, investigation numérique) avec une spécialisation sur la lutte contre la cybercriminalité et la sécurité des composants et des logiciels, incluant aussi une formation sur les aspects juridiques de la cybersécurité.



Objectifs de la formation

Nous formons les étudiants à l'utilisation des techniques mathématiques et informatique de la cryptologie et de la sécurité des systèmes d'information, ainsi que des concepts et techniques d'informatique légale (forensic), de sécurité réseau, sécurités logiciel et matériel. L'accent de la formation est mis sur la lutte contre la cybercriminalité, la conception et l'analyse d'architectures de sécurité et la protection des composants matériels et logiciels.

À l'issue de cette formation, les diplômés seront des spécialistes des questions de cybersécurité et d'informatique légale qui occuperont des fonctions d'ingénieur ou de consultant dans les secteurs de l'industrie informatique ou des services.

Les métiers et les entreprises visés se situent dans les catégories suivantes : constructeurs et fournisseurs de composants de sécurité; expertises et audits de sécurité informatique, services spécialisés où la sécurité est critique ; administration du système d'information et réseau au sein d'une entreprise ; expertise informatique légale ; conception d'architecture de sécurité.

Les enseignements

La formation comporte cinq parties :

- **1. Ingénierie cryptographiques et protocoles.**
- **2. Architectures de sécurité.**
  Incluant l'administration de réseaux sécurisés et les infrastructures à clefs publiques.
  Systèmes biométriques.
- **3. Audit et analyse de risques.**
  Incluant les méthodologies d'audit (ISO 27005, EBIOS, OSSTMM,...) et les outils permettant de traiter les menaces (intrusions, logiciels malveillants, virus, botnet, …).
- **4. Sécurité des composants et des logiciels.**
  Applications multimédias. Sécurités des OS, des systèmes embarqués, des smartphones.
- **5. Informatique légale et aspects législatifs et politiques de la cybersécurité.** Techniques de l'investigation numérique. Cadre juridique. Géopolitique d'internet. Intelligence économique et sûreté numérique. Protection de la vie privée.

La mission en entreprise se déroule en alternance durant l'année. La formation comporte aussi un enseignement d'anglais, ainsi que du tutorat individuel.