Notre offre de formation évolue ! Les programmes pour l'année 2027-2028 sont en cours de mise à jour et peuvent encore évoluer. Les programmes de l'année universitaire 2026-2027 restent consultables en cas de besoin.

SCIENCES, TECHNOLOGIES, SANTÉ, INGÉNIERIE

Parcours Cybersécurité et informatique légale 2e année

Master Cybersécurité

Université Grenoble Alpes

Niveau d'étude visé
Bac +5

ECTS
60 crédits

Durée
1 an

Composante
UFR Informatique, mathématiques et mathématiques appliquées (IM2AG)

Langue(s) d'enseignement
Français

Présentation

Le parcours CyberSécurité et informatique légale est un parcours de la mention Informatique du master Sciences, technologies et santé de l'Université Grenoble Alpes. **Il est exclusivement proposé en apprentissage et alternance.**

Cette formation permet aux étudiants issus d'un niveau master 1re année ou équivalent, avec une majeur 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.

Les étudiants sont formés 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.

Programme :

1. **Ingénierie cryptographiques et protocoles**

2. **Architectures de sécurité**. Incluant l'administration de réseaux sécurisés et les infrastructures à clefs publiques

3. **Audit et analyse de risques** incluant les méthodologies d'audit (par ex. ISO 27001) et les outils permettant de traiter les menaces (intrusions, logiciels malveillants, virus, botnet…)

4. **Sécurité des composants et des logiciels et 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

Informations non contractuelles.
Dernière mise à jour le 21 juillet 2026

Notre offre de formation évolue ! Les programmes pour l'année 2027-2028 sont en cours de mise à jour et peuvent encore évoluer. Les programmes de l'année universitaire 2026-2027 restent consultables en cas de besoin.

6. Apprentissage et projet en entreprise

A 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.

Cette formation est dispensée par des enseignants chercheurs (maitres de conférences, professeurs d'université), des professeurs agrégés, des professeurs associés et des professionnels du domaine.

Compétences

- Concevoir et développer des solutions matérielles et logicielles de cybersécurité, en particulier en Systèmes embarqués
- Opérer et maintenir des architectures de sécurité de Systèmes d'Information
- Piloter la sécurité d'un Système d'Information
- Collecter et analyser les éléments de preuve suite à un incident de cybersécurité
- Anticiper, gérer et remédier aux incidents et aux crises de cybersécurité
- Auditer et tester la sécurité d'un Système d'Information
- Détecter et analyser les vulnérabilités logicielles et matérielles
- Analyser et prendre en compte les normes et réglementations en vigueur
- Assurer une veille technologique et scientifique sur les menaces et solutions de cybersécurité

Organisation

Ouvert en alternance

Type de contrat : Contrat d'apprentissage.

Ce parcours est exclusivement proposé en apprentissage et alternance.

Admission

Conditions d'admission

La deuxième année de master est accessible sur dossier (et / ou entretien) aux candidats ayant validé la 1## année d'un parcours compatible ou bien via une validation d'études ou d'acquis selon les conditions déterminées par l'université ou la formation.

Public formation continue : Vous relevez de la formation continue :

- si vous reprenez vos études après 2 ans d'interruption d'études
- ou si vous suiviez une formation sous le régime formation continue l'une des 2 années précédentes
- ou si vous êtes salarié, demandeur d'emploi, travailleur indépendant

Si vous n'avez pas le diplôme requis pour intégrer la formation, vous pouvez entreprendre une démarche de validation des acquis personnels et professionnels (VAPP)

Candidature

Vous souhaitez candidater et vous inscrire ? Sachez que la procédure diffère selon le diplôme envisagé, le diplôme obtenu, ou le lieu de résidence pour les étudiants étrangers.

Connaître la procédure qui me concerne et candidater

Pré-requis recommandés

Il est préférable de maitriser un langage de programmation et d'avoir des connaissances de bases en développement logiciel et en réseaux.

Et après

Informations non contractuelles.
Dernière mise à jour le 21 juillet 2026

Notre offre de formation évolue ! Les programmes pour l'année 2027-2028 sont en cours de mise à jour et peuvent encore évoluer. Les programmes de l'année universitaire 2026-2027 restent consultables en cas de besoin.

Secteur(s) d'activité(s)

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 : entreprises spécialisées dans les domaines de la sécurité informatique, PM et grand groupe (sécurité des systèmes d'informations), grands comptes : assurances, banques, grands groupes, agences gouvernementales.

Lieu(x) ville

Grenoble

Campus

Grenoble - Domaine universitaire

Métiers visés

- Ingénieur-consultant en sécurité
- Ingénieur d'études et R&D en sécurité
- Responsable des systèmes d'information
- Responsable système et réseaux
- Responsable sécurité informatique

Infos pratiques

Contacts

Responsable pédagogique

Florent Autréau

florent.autreau@univ-grenoble-alpes.fr

Responsable pédagogique

Laurent Mounier

Laurent.Mounier@univ-grenoble-alpes.fr

Secrétariat de scolarité

Coralie Thomasso

coralie.thomasso@univ-grenoble-alpes.fr

Informations non contractuelles.
Dernière mise à jour le 21 juillet 2026

Notre offre de formation évolue ! Les programmes pour l'année 2027-2028 sont en cours de mise à jour et peuvent encore évoluer. Les programmes de l'année universitaire 2026-2027 restent consultables en cas de besoin.

Programme

Spécificités du programme

Programme en cours de construction - en attente de vote CFVU

Master 2e année

Semestre 9

	Nature	CM	TD	TP	Crédits
UE Ingénierie cryptographique et protocoles	UE	45h		34,5h	6 crédits
UE Architecture de sécurité	UE	42h		37,5h	6 crédits
UE Sécurité des composants et des logiciels	UE	42h		37,5h	6 crédits
UE Informatique légale et aspects législatifs et politiques de la cybersécurité	UE	45h		34,5h	6 crédits
UE Audit et analyse de risques	UE	18h		21h	6 crédits

Semestre 10

	Nature	CM	TD	TP	Crédits
UE Projet de Cybersécurité ou Informatique légale en entreprise	UE				30 crédits

Informations non contractuelles.
Dernière mise à jour le 21 juillet 2026