Notre offre de formation évolue ! Les programmes pour l'année 2027-2028 sont en cours de mise à jour et peuvent évoluer jusqu'au 28 novembre 2026. Les programmes de l'année universitaire 2026-2027 restent consultables en cas de besoin.

SCIENCES, TECHNOLOGIES, SANTÉ, INGÉNIERIE

Parcours Cybersécurité

BUT Réseaux informatiques et télécommunications / Grenoble

Université Grenoble Alpes

Niveau d'étude visé
Bac +3

ECTS
180 crédits

Durée
3 ans

Composante
Institut universitaire de technologie (IUT 1)

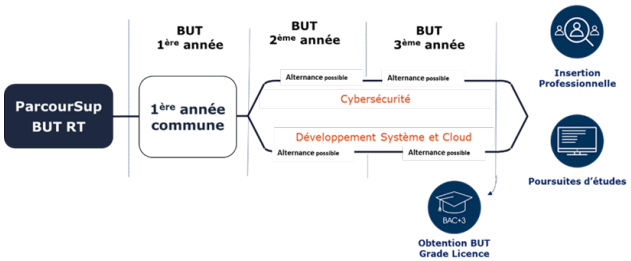
Présentation

Le **BUT R&T** est une formation en 3 ans, reconnue par l'Etat et les entreprises, et basé sur un programme national. Le diplôme valant grade de licence professionnelle universitaire (Bac+3) permet autant une **insertion professionnelle** qu'une **poursuite d'études** (Bac +4/5).

Le BUT R&T forme des spécialistes des technologies de l'information et de la communication pour les besoins des réseaux informatiques et de télécommunication : ils sont au cœur de nombreuses activités en lien avec la vie sociale et économique : télétravail, communications mobiles, réseaux à très haut débit, transport et accès à l'information…

Dès la 2ème année la formation à l'IUT1 offre la possibilité d'une **spécialisation métier** sous la forme d'un parcours **Cybersécurité (CYBER)** :

Le parcours Cybersécurité s'intéresse plus particulièrement à la sécurisation des systèmes d'information d'une entreprise, c'est-à-dire l'ensemble des ressources qui interviennent dans la gestion de ses informations/données. Le diplômé du parcours Cybersécurité est capable d'installer des équipements spécifiques de sécurité, d'administrer un système d'information sécurisé, de le superviser, de détecter et de parer aux attaques informatiques.



En 3 années, la formation assure l'acquisition des **compétences** socles, communes à tous les métiers de réseaux informatiques et télécommunications, à savoir :

- **Administrer** les réseaux et l'internet : l'apprenant est formé pour assurer le bon fonctionnement du réseau d'une entreprise (conception, déploiement, administration) en exploitant des équipements complexes (routeurs, commutateurs...). Il est formé à réagir en cas d'incidents (surveillance, maintenance, résolution de problèmes) et à mettre en place des procédures pour les prévenir.
- **Connecter** les entreprises et les usagers **:** l'apprenant est formé pour intervenir sur les infrastructures de transmission qui permettent l'acheminement des données entre les différents équipements du réseau. Leur installation et leur administration reposent sur de bonnes

Informations non contractuelles.
Dernière mise à jour le 30 juin 2026

IUT1 Grenoble Université Grenoble Alpes

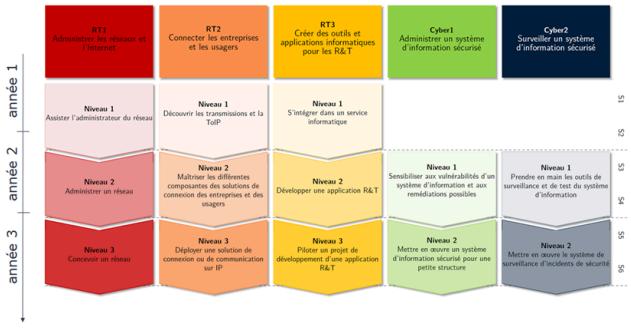
Notre offre de formation évolue ! Les programmes pour l'année 2027-2028 sont en cours de mise à jour et peuvent évoluer jusqu'au 28 novembre 2026. Les programmes de l'année universitaire 2026-2027 restent consultables en cas de besoin.

connaissances dans certains domaines de la physique, du traitement du signal et des communications numériques.

- **Développer** des outils et applications informatiques pour les R&T (**Programmer**) : l'apprenant est formé pour développer des applications spécifiques pour le réseau de son entreprise (par ex. remonter et analyser des informations sur ses équipements). Il peut également intervenir sur les sites Web ou gérer les données de son entreprise.

A partir de la 2ème année, la formation se complète de compétences complémentaires :

- **Sécuriser** un système d'information : l'apprenant est formé pour identifier les éléments essentiels du système d'information de l'entreprise à protéger, d'évaluer les risques associés. Il peut définir une politique de sécurité, en s'appuyant sur le cadre juridique, les normes et les préconisations de différentes autorités. Il peut être amené à installer et configurer des équipements spécifiques pour les besoins de sécurité. Il peut également intervenir dans des actions de prévention et de responsabilisation de ses collaborateurs en entreprise.
- **Surveiller** un système d'information sécurisé : l'apprenant est formé pour intégrer différents outils de surveillance au réseau de son entreprise : ces outils permettent de vérifier que le système d'information reste opérationnel, fiable, sûre et régulièrement mis à jour tout au long de son exploitation. Il intervient également dans la mise en place de procédures, prévues en cas d'incidents (pannes ou attaques) pour en minimiser les impacts sur l'entreprise, incluant les plans de reprise ou de continuité d'activité.



Informations non contractuelles.
Dernière mise à jour le 30 juin 2026

Notre offre de formation évolue ! Les programmes pour l'année 2027-2028 sont en cours de mise à jour et peuvent évoluer jusqu'au 28 novembre 2026. Les programmes de l'année universitaire 2026-2027 restent consultables en cas de besoin.

Programme

Spécificités du programme

Référentiel de compétences

Règlement des études (RDE) 2025-2026

Modalités de Contrôle des Connaissances et des Compétences (MCCC) 2025-2026 :

- **BUT 1ère année MCCC**
- **BUT 2ème année Parcours Cybersécurité (CYBER) :**
  - **Formation initiale (CYBER-FI)**
  - **Alternance (CYBER-ALT)**
- **BUT 3ème année Parcours Cybersécurité (CYBER) :**
  - **Formation initiale (CYBER-FI)**
  - **Alternance (CYBER-ALT)**

Informations non contractuelles.
Dernière mise à jour le 30 juin 2026