

# BUT Réseaux et Télécommunications Parcours Cybersécurité

Financement

Formation professionnelle continue  
Non conventionnée / sans dispositif

Organisme responsable et contact

UNIVERSITE DE PAU ET DES  
PAYS DE L'ADOUR  
**Service Alternance - DFTLV**  
05.59.40.78.88  
alternance@univ-pau.fr

Accès à la formation

Publics visés :  
  
Demandeur d'emploi  
Jeune de moins de 26 ans  
Personne handicapée  
Salarie(e)  
Actif(ve) non salarié(e)

Sélection :  
  
Dossier  
Entretien

Niveau d'entrée requis :  
  
Niveau 4 : Baccalauréat (Niveau 4 européen)

Conditions d'accès :  
  
En 1re année de BUT : Connectez-vous sur le site PARCOURSUP entre mi-janvier et mi-mars Remplissez les informations en ligne La procédure d'admission se déroule de la manière suivante : Étude du dossier complété sur PARCOURSUP (notes de première, de terminale et lettre de motivation) Classement des candidats en fonction de leur dossier scolaire par un jury composé d'enseignants du département. Sont particulièrement regardés : les notes de mathématiques et de physique, les matières technologiques, les appréciations sur la capacité de travail, les appréciations sur le savoir-être du candidat, le projet professionnel du candidat Convocation des candidats à un entretien de motivation Les résultats définitifs sont communiqués fin mai – début juin. En 2e année de BUT : Pour les étudiants ayant validé un bac+2 scientifique (L2, BTS...), une admission est possible en 2e année, après étude du dossier. Les candidatures s'effectuent en ligne sur le site CandIUT.

Prérequis pédagogiques :  
  
En BUT1, sur Parcoursup avec un bac général (options scientifiques recommandées), un bac STI2D, un bac pro cybersécurité, informatique et réseaux, électronique, un titre équivalent Accès direct en 2ème et 3ème année Avec un des diplômes suivants : • BTS (SIO, CIEL/IR, CIEL/ER) • BUT 1 ou 2 (GEII, Info, MMI...) • Bac+2 équivalent • Validation d'Acquis Professionnels Compétences requises : un niveau correct en mathématiques et en physique, une aptitude pour les matières technologiques, une capacité de travail régulier, un esprit logique, méthodique et rigoureux, un attrait pour les manipulations techniques, un niveau raisonnable en anglais est souhaitable et apprécié, un niveau raisonnable en français est souhaitable et apprécié (notes de bac)

Contrat de professionnalisation possible ?  
  
Non

Objectif de la formation

Proposé par l'IUT des Pays de l'Adour, le parcours Cybersécurité (Cyber) forme des professionnels R&T dans l'analyse des risques d'attaques menaçant les systèmes d'informations d'une entreprise (réseaux, serveurs, postes de travail...). Ainsi, il est en mesure de définir la politique de sécurité de l'entreprise visant à fixer le cadre d'utilisation des ressources numériques, à sensibiliser et former les utilisateurs. Il est également en capacité d'appliquer au sein de l'entreprise la loi notamment RGPD et les préconisations de l'État (ANSSI) imposées par le contexte actuel. Ce parcours regroupe l'ensemble des métiers liés à la sécurité des systèmes d'information, de l'installation d'équipements de sécurité à leur surveillance. Le spécialiste en Cybersécurité est capable d'administrer un système d'informations sécurisé, de le superviser, de détecter et de parer aux attaques informatiques. Le BUT Réseaux et Télécommunications s'articule autour de 5 blocs de compétences. 3 d'entre-eux sont des compétences communes à tous les métiers de la filière : - Administrer les réseaux et l'Internet, dans lequel seront abordées toutes les technologies liées à la configuration et à administration des réseaux informatiques, locaux, d'entreprises ou étendus. - Connecter les entreprises et les usagers, permettant d'acquérir toutes les connaissances nécessaires au choix et à la mise en place des infrastructures de communication (cuivre, fibre optique, 4G, 5G, 6G, liaisons satellites,...) et au traitement du signal qu'ils véhiculent, - Créer des outils et applications informatiques pour les R&T, dans laquelle les rudiments de l'administration des systèmes et des services seront dispensés, ainsi que les techniques de programmation d'outils spécialisés. A ces compétences fondamentales s'ajoutent 2 blocs de compétence spécifiques au parcours Cyber : - Administrer un système d'information sécurisé - Surveiller un système d'information sécurisé Ces blocs recouvrent les compétences suivantes : • Effectuer une analyse de risques • Concevoir un système d'information sécurisé • Administrer la sécurité d'un système d'information • Investiguer sur un système d'information corrompu...

...

Contenu et modalités d'organisation

Tronc commun à tous les parcours • Fondamentaux des réseaux • Fondamentaux des télécommunications • Fondamentaux de l'administration système • Fondamentaux de la programmation • Compétences transversales (expression, communication, anglais...) Spécialité parcours Cybersécurité (à partir du BUT 2) • Analyse / gestion de risques • Audits de sécurité : méthodologie EBIOS / norme ISO 27005 • Notions fondamentales de cryptologie • Architectures de réseaux sécurisés (FW, VLANs, VPNs, AAA, 802.1X...) • Sécurité des réseaux sans fils • Administrations système sécurisée • Surveillance de Systèmes d'Informations (SIEM...) • Pentesting • Forensics Situations d'Apprentissage et d'Évaluation (SAÉ) • 600 heures de mise en situation • Projets en groupe, en autonomie à réaliser à court ou moyen terme Le volume horaire global (enseignements et projets tutorés, soit 2600 heures) est distribué de manière homogène sur les 3 années. Les 600 heures de projets tutorés sont réparties sur les 3 années, avec chaque année un minimum de 150 heures. Alternance possible dès la 2ème année, obligatoire en 3e année

Parcours de formation personnalisable ?      Oui      Type de parcours      *Non renseigné*

Validation(s) Visée(s)

BUT spécialité réseaux & télécommunications parcours cybersécurité - Niveau 6 :  
*Licence, licence professionnelle, BUT (Niveau 6 européen)*

Et après ?

Suite de parcours

Métiers de • Correspondant sécurité • Architecte de réseaux sécurisés • Administrateur sécurité des systèmes et réseaux • Analyste SOC.... Poursuite d'études (sous réserve d'admission) : Bac+3 (après BUT 2) : licences pro, Bac+5 : master (après BUT2), écoles d'ingénieurs (après BUT 2 ou 3)

## Calendrier des sessions

Numéro Carif	Dates de formation	Ville	Organisme de formation	Type d'entrée	CPF	Modalités
-----------------	--------------------	-------	------------------------	------------------	-----	-----------

00647990

du 01/09/2026 au  
31/08/2028

Mont-de-  
Marsan (40)

UNIVERSITE DE PAU  
ET DES PAYS DE  
L'ADOUR

Non  
éligible

