

CLO

Durée : 06 Semestres**Crédits :** 180 crédits**Formation :** A distance**PUBLICS CIBLES**

- Étudiants en cybersécurité
- Étudiants en réseaux et télécommunications
- Professionnels en sécurité informatique
- Ingénieurs en systèmes embarqués
- Développeurs d'applications IoT
- Consultants en sécurité des données
- Chercheurs en Internet des Objets
- Spécialistes en infrastructure réseau
- Architectes en sécurité des systèmes
- Administrateurs réseau
- Responsables IT dans les entreprises
- Professionnels de la gestion des risques numériques

DÉBOUCHÉS PROFESSIONNELS

- Directeur des systèmes d'information
- Expert infrastructure
- Architecte des systèmes d'information
- Chef de projet informatique
- Responsable sécurité informatique
- Expert en virtualisation
- Expert en sécurité informatique
- Architecte réseaux
- Consultant en Internet des objets
- Administrateur systèmes et réseaux d'objets
- Expert en transformation numérique
- Expert en régulation de la Blockchain

COÛTS DE LA FORMATION**Frais de dossier (Non affecté de l'Etat) :**

Etudiants ivoiriens : 10 000 FCFA

Etudiants UEMOA : 10 000 FCFA

Etudiants hors UEMOA : 30 000 FCFA

Formation initiale (Affecté de l'Etat) :

Etudiants ivoiriens : 90 000 FCFA

Etudiants UEMOA : 300 000 FCFA

Etudiants hors UEMOA : 500 000 FCFA

Formation continue (Non affecté de l'Etat) :

Etudiants ivoiriens : 300 000 FCFA

Etudiants UEMOA : 300 000 FCFA

Etudiants hors UEMOA : 500 000 FCFA

**DOCTORAT****CYBERSECURITE ET INTERNET DES OBJETS****DESCRIPTION DE LA FORMATION**

Le Doctorat en Cybersecurité et Internet des Objets (IoT) prépare des chercheurs à aborder les défis liés à la sécurité des environnements numériques et des systèmes interconnectés. Cette spécialité se concentre sur la protection des données et des infrastructures contre les menaces informatiques, ainsi que sur la sécurisation des dispositifs IoT. Les étudiants exploreront des problématiques telles que la cryptographie avancée, les protocoles de sécurité, et les techniques de détection des intrusions.

Durant la formation, les étudiants se concentreront sur leur thèse, menant des recherches originales sur les défis contemporains en cybersécurité et IoT. Ils travailleront en collaboration avec des laboratoires ou des entreprises pour développer des solutions innovantes et améliorer les pratiques de sécurité dans les environnements numériques et les réseaux de dispositifs interconnectés.

La formation se termine par la soutenance de la thèse, où les étudiants démontrent leur expertise et leur capacité à proposer des solutions novatrices aux problèmes de sécurité dans les systèmes IoT. Les recherches doivent aboutir à des contributions significatives pour renforcer la sécurité des infrastructures numériques et des objets connectés.

LE MODELE PEDAGOGIQUE

Le modèle pédagogique est conçu selon une approche de pédagogie par résolution de problème permettant à l'apprenant de se former par la méthode « Learning by doing ». L'apprenant mène des projets concrets en appliquant des connaissances, souvent en équipe, tout en définissant objectifs et solutions adaptées. La formation est réalisée à distance avec l'accès aux ressources d'enseignement et d'apprentissage sur les plateformes dédiées. D'autres activités sont également réalisées au travers de webinaires et de travaux d'apprentissages collaboratifs.

Ce dispositif permet à l'apprenant d'étudier autrement, partout et à tout moment. Il permet l'usage du numérique par l'ensemble des acteurs que sont l'Enseignant, l'Apprenant et les Tuteurs.

CONDITIONS D'ACCÈS**Pour les affectés de l'Etat (formation initiale) :**

- Avoir le statut d'affecté de l'Etat à l'UVCI ;
- Être titulaire d'un Master ;
- Avoir un projet de recherche validé ;
- Avoir un financement ou une bourse disponible.

Pour les non affectés de l'Etat (formation continue) :

- Être titulaire d'un Master ou d'un diplôme équivalent ;
- Justifier d'un financement ou d'une bourse de recherche ;
- Avoir un projet de recherche approuvé par un encadrant habilité.

