
Appel à candidature

Master « Intelligence Artificielle et Cybersécurité » (2026-2027)

Le Doyen de la Faculté des Sciences Appliquées Béni Mellal annonce l'ouverture de la pré-candidature en ligne pour l'accès au Master « Intelligence Artificielle et Cybersécurité » au titre de l'année universitaire 2026-2027 du 21 septembre 2026 au 05 octobre 2026.

Objectifs de la formation :

L'objectif du master " intelligence artificielle et cybersécurité " est de fournir aux étudiants les connaissances nécessaires pour travailler dans les domaines de la data science et de la sécurité des systèmes. Cette formation vise à former des professionnels capables de collecter, analyser et interpréter des données, tout en garantissant la sécurité des systèmes. Voici les principaux objectifs de cette formation :

1. Data Science : Les étudiants acquièrent une compréhension approfondie des principes et des techniques de la science des données. Ils apprennent à collecter, nettoyer, explorer et analyser des données à grande échelle. L'objectif est de développer des compétences en statistiques, en apprentissage automatique, en visualisation des données et en extraction de connaissances à partir de données.
2. Sécurité des systèmes : Les étudiants se familiarisent avec les concepts fondamentaux de la sécurité des systèmes. Ils apprennent à évaluer les vulnérabilités des systèmes, à mettre en place des mesures de protection, à détecter et à prévenir les attaques informatiques. L'objectif est de développer des compétences en gestion des risques, en cryptographie, en sécurité des réseaux et en sécurité des applications.
3. Analyse de données et sécurité : Les étudiants apprennent à appliquer les principes de la data science dans le contexte de la sécurité des systèmes. Ils acquièrent des compétences pour analyser les données de sécurité, détecter les anomalies, identifier les modèles et prévenir les incidents de sécurité. L'objectif est d'utiliser les techniques d'analyse de données pour renforcer la sécurité des systèmes.
4. Gestion de la confidentialité des données : Les étudiants comprennent les enjeux liés à la confidentialité des données dans les systèmes. Ils apprennent les réglementations et les normes relatives à la protection des données, ainsi que les techniques de protection de la vie privée. L'objectif est de développer des compétences pour assurer la conformité réglementaire et mettre en place des pratiques de gestion de la confidentialité.

Compétences à acquérir

- Maîtrise de la programmation avancée en Python.
- Compréhension approfondie de la sécurité des réseaux, du web et des systèmes.
- Expertise en cryptographie avancée et en protection des données.
- Utilisation de techniques avancées de Machine Learning et de Data Mining pour détecter les menaces.
Développement de compétences en Deep Learning avec des outils comme PyTorch, TensorFlow, ...
- Connaissance pratique du Cloud Computing et de la sécurité dans le cloud

Programme de la formation :

Semestre 1	Semestre 2
<ul style="list-style-type: none"> • Programmation avancée en python • Algorithmes évolutionnaires pour l'intelligence artificielle • Réseaux mobiles avancés • Théorie de l'information et codage • Entrepôt de données et informatique décisionnelle • Anglais • Intelligence Artificielle et Innovation 	<ul style="list-style-type: none"> • Machine Learning et data mining • Apprentissage profond • Cloud computing et sécurité • Cryptographie avancée • Optimisation avancée pour le Machine Learning • Culture entrepreneuriale et techniques de communication • Méthodologie de recherche scientifique
Semestre 3	Semestre 4
<ul style="list-style-type: none"> • Apprentissage automatique pour la cybersécurité • Big data pour la cybersécurité • Applications de la blockchain en cybersécurité • Large language models avec retrieval augmented generation • Text mining et social media analysis • Sécurité des réseaux et du web • Apprentissage par renforcement 	<ul style="list-style-type: none"> • Projet de fin d'études (Equivalent à 7 modules disciplinaires)

Débouchés de la formation :

La formation master "intelligence artificielle et cybersécurité" offre aux étudiants un large éventail de débouchés professionnels dans les domaines de l'intelligence artificielle, data science et de la cybersécurité. Voici quelques exemples de débouchés auxquels les étudiants peuvent accéder après l'obtention de leur diplôme :

1. **Data Scientist** : Les étudiants peuvent travailler en tant que data scientists, en utilisant des techniques d'analyse de données pour extraire des informations et des connaissances à partir de grands ensembles de données. Ils peuvent résoudre des problèmes complexes, développer des modèles prédictifs, effectuer des analyses statistiques et présenter des résultats pour aider les entreprises à prendre des décisions éclairées basées sur les données.
2. **Analyste en sécurité des systèmes** : Les étudiants peuvent se spécialiser dans la sécurité des systèmes et travailler en tant qu'analystes en sécurité. Ils peuvent évaluer les vulnérabilités des systèmes, mettre en œuvre des mesures de sécurité, détecter les incidents de sécurité, effectuer des analyses de risques et recommander des solutions pour protéger les données et les systèmes d'information contre les cyberattaques.
3. **Consultant en data science** : Les diplômés peuvent travailler en tant que consultants en data science, fournissant des conseils et des solutions aux entreprises qui cherchent à exploiter leurs données de manière efficace. Ils peuvent aider à la définition de stratégies de data science, à la mise en place d'infrastructures de données, à l'analyse des données et à la création de modèles prédictifs pour améliorer les performances commerciales.
4. **Analyste en veille stratégique** : Les étudiants peuvent utiliser leurs compétences en data science pour travailler en tant qu'analystes en veille stratégique. Ils peuvent collecter et analyser des données provenant de diverses sources pour aider les entreprises à prendre des décisions éclairées, à identifier les tendances du marché, à évaluer la concurrence et à anticiper les évolutions futures.
5. **Chercheur en data science** : Certains diplômés peuvent poursuivre des études supérieures et se lancer dans une carrière de recherche en data science. Ils peuvent contribuer à l'avancement des connaissances en développant de nouvelles méthodes d'analyse de données, en explorant des domaines d'application innovants et en publiant leurs résultats dans des revues scientifiques.
6. **Entrepreneur** : Certains étudiants peuvent choisir de créer leur propre entreprise dans le domaine de la data science et de la sécurité des systèmes d'information. Ils peuvent développer des solutions

logicielles, des outils d'analyse de données, des services de sécurité ou des plateformes de gestion des données pour répondre aux besoins du marché.

Conditions d'accès :

Licence en Informatique

Prérequis pédagogiques :

Formation antérieure dans des domaines tels que l'informatique, les mathématiques, l'ingénierie ou des domaines connexes. Compétences en programmation, notamment dans des langages comme Python. Compréhension fondamentale des concepts de sécurité informatique et d'intelligence artificielle. Prérequis spécifiques pouvant inclure des cours préalables en algorithmique, en réseaux informatiques, en statistiques ou en apprentissage automatique.

Procédure de sélection :

Étude de dossier selon des critères proposés par l'équipe pédagogique : nombre de mentions, nombre d'inscription pour l'obtention du diplôme B+3, adéquation des prérequis avec la filière, résultats académiques dans les matières clés, stages ou projets pertinents.

Effectif prévu : 30 étudiants.

Date importante :

• Du 21/09/2026 au 05/10/2026 :

- Préinscription en ligne, obligatoire, via le site <https://www.fpbm.ma/fsabm/index>. Les candidats doivent scanner et déposer électroniquement leur dossier dans des fichiers "pdf" (*Toute information fausse sera passible d'un rejet*).

Dossier de candidature :

- ✓ Préinscription en ligne (**obligatoire**) à travers le lien : <https://www.fpbm.ma/fsabm/index>
- ✓ Dossier de candidature « version électronique » comportant les pièces suivantes (**tout dossier incomplet sera systématiquement rejeté**):
 1. Demande manuscrite adressée à Monsieur le Doyen de la Faculté des Sciences Appliquées Béni Mellal ;
 2. Curriculum vitae avec photo du candidat ;
 3. Copie de la C.I.N;
 4. Lettre de motivation ;
 5. Copie recto-verso du Baccalauréat, faisant apparaître les différentes inscriptions post baccalauréat ;
 6. Copie du diplôme Bac+2 (ou équivalent) ;
 7. Copie du diplôme Bac+3 (ou équivalent) ;
 8. Copies des relevés de notes obtenues durant tout le cursus Bac+3 (S1, S2, S3, S4, S5, S6 ou première année, deuxième année et troisième année) ;
 9. Tout autre document relatif aux compétences professionnelles du candidat.

Remarques Importantes :

1. Toute préinscription en ligne hors délai sera rejetée.
2. Les candidats n'ayant pas procédé à la préinscription en ligne verront leurs dossiers rejetés.
3. Toute information fausse sera passible d'un rejet.
4. Les dossiers incomplets seront passibles d'un rejet.
5. Les candidats doivent consulter régulièrement le site web de l'établissement (<https://fsabm.usms.ac.ma>) pour être au courant des nouvelles introduites.

Responsable de la formation :

Pr M. Biniz
Département de l'Informatique
Université Sultan Moulay Slimane
Faculté des Sciences Appliquées
B.P. 592, Mghila, Béni-Mellal
Tél. : 05234246 85 ; Fax. 0523424597
<https://fsabm.usms.ac.ma>