

Mastère Avancé

Gestion Sécurisée de l'Information



Mastère Avancé Gestion Sécurisée de l'Information

- » Modalité: en ligne
- » Durée: 2 ans
- » Qualification: TECH Euromed University
- » Accréditation: 120 ECTS
- » Horaire: à votre rythme
- » Examens: en ligne

Accès au site web: www.techtitute.com/fr/informatique/mastere-avance/mastere-avance-gestion-securisee-information

Sommaire

01

Présentation

Page 4

02

Pourquoi étudier à TECH?

Page 8

03

Programme d'études

Page 12

04

Objectifs

Page 32

05

Opportunités de carrière

Page 38

06

Méthodologie d'étude

Page 42

07

Corps Enseignant

Page 52

08

Diplôme

Page 62

01 Présentation

À l'ère du numérique, les activités dans un grand nombre de domaines sont entièrement gérées par l'internet. Les loisirs, le travail et la communication avec les amis et la famille s'appuient de plus en plus sur des outils et des ressources en ligne. D'énormes quantités d'informations sont transférées quotidiennement, qu'il s'agisse de simples données dans les conversations sur les médias sociaux et les applications de messagerie, ou d'informations personnelles et professionnelles sensibles hébergées sur des plateformes bancaires ou commerciales. Ce scénario requiert des spécialistes capables de traiter et de protéger les informations dans différents contextes, en accordant la priorité à leur sécurité. C'est pourquoi TECH a conçu ce programme en génie Logiciel, axé sur la formation de professionnels possédant les compétences nécessaires pour gérer et protéger efficacement l'information, en relevant les défis numériques actuels et en contribuant à créer des environnements technologiques plus sûrs et plus fiables.





“

La protection des données est essentielle face aux menaces constantes. Vous pourriez être le gardien de ces précieuses informations”

Chaque seconde, des milliers de données sont générées, partagées et stockées dans l'environnement numérique. Qu'il s'agisse d'effectuer des paiements en ligne, d'accéder à des services éducatifs, de coordonner des activités commerciales ou de protéger des identités numériques, la technologie est devenue un pilier essentiel qui transforme continuellement notre façon de vivre et de travailler. Ces interactions génèrent et transfèrent des quantités massives de données à chaque instant, qu'il s'agisse d'informations personnelles ou de fichiers sensibles liés aux entreprises et aux institutions. Ce flux constant de données met en évidence la nécessité d'un traitement approprié pour garantir leur sécurité et leur confidentialité.

La gestion et la protection de ces données n'est pas une tâche simple, car elle nécessite une combinaison d'expertises hautement spécialisées dans des domaines tels que la cybersécurité et la gestion de l'information. Ces disciplines, bien que distinctes, doivent être intégrées pour relever les défis complexes de l'environnement numérique actuel. Dans ce contexte, le Mastère Avancé en Gestion Sécurisée de l'Information représente une opportunité unique pour les ingénieurs et les professionnels de l'informatique désireux d'acquérir une vision globale qui leur permettra de maîtriser les deux domaines et de se positionner en tant que leaders dans un secteur en constante croissance.

De nombreuses entreprises et institutions sont confrontées à la nécessité de protéger des données critiques et hautement sensibles, mais manquent d'experts capables d'assurer une gestion, une conservation et une surveillance efficaces de leurs informations numériques. Pour répondre à cette demande, TECH Euromed University a conçu un programme qui combine le meilleur contenu avec une équipe d'enseignants composée de professionnels renommés. Cette approche garantit que les étudiants acquièrent les outils et les connaissances nécessaires pour se démarquer sur le marché du travail et accéder à des postes stratégiques dans des organisations cherchant à renforcer leur sécurité de l'information.

Ce **Mastère Avancé en Gestion Sécurisée de l'Information** contient le programme le plus complet et le plus actualisé du marché. Ses caractéristiques sont les suivantes:

- ♦ Le développement d'études de cas présentées par des experts en Gestion Sécurisée de l'Information
- ♦ Le contenu graphique, schématique et éminemment pratique du programme fournit des informations scientifiques et pratiques sur les disciplines essentielles à la pratique professionnelle
- ♦ Les exercices pratiques où effectuer le processus d'auto-évaluation pour améliorer l'apprentissage
- ♦ Il met l'accent sur les méthodologies innovantes dans la Gestion Sécurisée de l'Information
- ♦ Cours théoriques, questions à l'expert, forums de discussion sur des sujets controversés et travail de réflexion individuel
- ♦ La possibilité d'accéder aux contenus depuis n'importe quel appareil fixe ou portable doté d'une connexion internet



Acquérez les compétences nécessaires pour sécuriser et gérer efficacement les données dans un environnement numérique compétitif"

“

Consolidez vos connaissances théoriques grâce aux nombreuses ressources pratiques incluses dans ce Mastère Avancé en Gestion Sécurisée de l'Information"

Son corps enseignant comprend des professionnels du domaine de la Finance, qui apportent l'expérience de leur travail à ce programme, ainsi que des spécialistes reconnus issus de grandes entreprises et d'universités prestigieuses.

Son contenu multimédia, développé avec les dernières technologies éducatives, permettra au professionnel un apprentissage situé et contextuel, c'est-à-dire un environnement simulé qui fournira un étude immersif programmé pour s'entraîner dans des situations réelles.

La conception de ce programme est axée sur l'Apprentissage par les Problèmes, grâce auquel l'étudiant doit essayer de résoudre les différentes situations de la pratique professionnelle qui se présentent tout au long du programme académique. Pour ce faire, le professionnel aura l'aide d'un système vidéo interactif innovant créé par des experts reconnus.

Découvrez la méthodologie éducative la plus innovante conçue par TECH Euromed University pour garantir un apprentissage immersif et contextualisé.

Accédez à un programme 100% en ligne qui vous permet d'étudier à votre rythme, à tout moment et de n'importe où dans le monde.



02

Pourquoi étudier à TECH?

TECH Euromed University est la plus grande Université Numérique du monde. Avec un catalogue impressionnant de plus de 14 000 programmes universitaires, disponibles en 11 langues, elle est leader en matière d'employabilité, avec un taux de placement de 99%. Elle dispose également d'un vaste corps professoral composé de plus de 6 000 professeurs de renommée internationale.



“

*Étudiez dans la plus grande université
numérique du monde et assurez votre réussite
professionnelle. L'avenir commence chez TECH
Euromed University”*

La meilleure université en ligne selon FORBES

Le prestigieux magazine Forbes, spécialisé dans les affaires et la finance, a désigné TECH Euromed University comme « la meilleure université en ligne du monde ». C'est ce qu'il a récemment déclaré dans un long article de son édition numérique dans lequel il se fait l'écho de la success story de cette institution, "grâce à l'offre académique qu'elle propose, à la sélection de son corps enseignant et à une méthode d'apprentissage innovante visant à former les professionnels du futur".

Un corps professoral international de premier plan

Le corps enseignant de TECH Euromed University est composé de plus de 6 000 professeurs jouissant du plus grand prestige international. Des professeurs, des chercheurs et des cadres supérieurs de multinationales, dont Isaiah Covington, entraîneur de performance des Boston Celtics, Magda Romanska, chercheuse principale au MetaLAB de Harvard, Ignacio Wistumba, président du département de pathologie moléculaire translationnelle au MD Anderson Cancer Center, et D.W. Pine, directeur de la création du magazine TIME, entre autres.

La plus grande université numérique du monde

TECH Euromed University est la plus grande université numérique du monde. Nous sommes le plus grand établissement d'enseignement, avec le meilleur et le plus vaste catalogue d'enseignement numérique, cent pour cent en ligne et couvrant la grande majorité des domaines de la connaissance. Nous proposons le plus grand nombre de diplômes propres, de diplômes officiels de troisième cycle et de premier cycle au monde. Au total, plus de 14 000 diplômes universitaires, dans dix langues différentes, ce qui fait de nous la plus grande institution éducative au monde.



Les programmes d'études les plus complets sur la scène universitaire

TECH Euromed University propose les programmes d'études les plus complets sur la scène universitaire, avec des cursus qui couvrent les concepts fondamentaux et, en même temps, les principales avancées scientifiques dans leurs domaines scientifiques spécifiques. De même, ces programmes sont continuellement mis à jour afin de garantir aux étudiants l'avant-garde académique et les compétences professionnelles les plus demandées. De cette manière, les diplômes de l'université fournissent à ses diplômés un avantage significatif pour propulser leur carrière vers le succès.

Une méthode d'apprentissage unique

TECH est la première université à utiliser *Relearning* dans tous ses diplômes. Il s'agit de la meilleure méthode d'apprentissage en ligne, accréditée par des certifications internationales de qualité de l'enseignement délivrées par des agences éducatives prestigieuses. En outre, ce modèle académique perturbateur est complété par la "Méthode des Cas", configurant ainsi une stratégie d'enseignement en ligne unique. Des ressources pédagogiques innovantes sont également mises en œuvre, notamment des vidéos détaillées, des infographies et des résumés interactifs.

L'université en ligne officielle de la NBA

TECH Euromed University est l'université en ligne officielle de la NBA. Grâce à un accord avec la ligue majeure de basket-ball, elle offre à ses étudiants des programmes universitaires exclusifs, ainsi qu'une grande variété de ressources éducatives axées sur les affaires de la ligue et d'autres domaines de l'industrie du sport. Chaque programme est conçu de manière unique et fait appel à des conférenciers exceptionnels: des professionnels issus du monde du sport qui apportent leur expertise sur les sujets les plus pertinents.

Leaders en matière d'employabilité

TECH Euromed University a réussi à devenir la première université en termes d'employabilité. 99% de ses étudiants trouvent un emploi dans le domaine académique qu'ils ont étudié, un an après avoir terminé l'un des programmes de l'université. Un nombre similaire d'entre eux bénéficient d'une amélioration immédiate de leur carrière. Tout cela grâce à une méthodologie d'étude qui fonde son efficacité sur l'acquisition de compétences pratiques, absolument nécessaires au développement professionnel.



Google Partner Premier

Le géant américain de la TECH Euromed University a décerné à TECH Euromed University le badge Google Partner Premier. Ce prix, qui n'est décerné qu'à 3% des entreprises dans le monde, souligne l'expérience efficace, flexible et adaptée que cette université offre aux étudiants. Cette reconnaissance atteste non seulement de la rigueur, de la performance et de l'investissement maximaux dans les infrastructures numériques de TECH Euromed University, mais place également cette université parmi les entreprises technologiques les plus avant-gardistes au monde.



L'université la mieux évaluée par ses étudiants

Le site d'évaluation Global score a positionné TECH Euromed University comme l'université la mieux notée au monde par ses étudiants. Ce portail d'évaluation, le plus fiable et le plus prestigieux car il vérifie et valide l'authenticité de chaque avis publié, a attribué à TECH Euromed University sa note la plus élevée, 4,9 sur 5, sur la base de plus de 1 000 avis reçus. Ces chiffres placent TECH Euromed University comme la référence internationale absolue en matière d'université.



03

Programme d'études

Le matériel pédagogique qui compose ce Mastère Avancé en Gestion Sécurisée de l'Information a été développé par une équipe d'experts en cybersécurité et en gestion des données. Ainsi, le programme d'études aborde les principales menaces numériques et les méthodologies les plus avancées en matière de protection et de gestion de l'information. Cela permettra aux diplômés d'identifier les risques spécifiques et de développer des solutions efficaces pour assurer la sécurité des données dans divers environnements professionnels. Le programme aborde également les outils les plus innovants du secteur, en promouvant des stratégies visant à protéger les actifs numériques des organisations.




```
function ngSwitchWatchAction(value) {  
  for (i = 0; i < elements.length; ++i) {  
    remove(i);  
  }  
  = 0;  
  for (i = 0; i < scopes.length; ++i) {  
    elements[i];  
    destroy(i);  
    selected;  
    function  
    e(j
```

“

Vous contribuerez à la protection des données sensibles et à la création de systèmes sécurisés qui garantissent la continuité opérationnelle des entreprises et des institutions”

Module 1. L'analyse des données dans l'organisation de l'entreprise

- 1.1. Analyse commerciale
 - 1.1.1. Analyse commerciale
 - 1.1.2. Structuration des données
 - 1.1.3. Phases et éléments
- 1.2. L'analyse des données dans l'entreprise
 - 1.2.1. Tableaux de bord et Kpi's par département
 - 1.2.2. Rapports opérationnels, tactiques et stratégiques
 - 1.2.3. L'analyse des données appliquée à chaque département
 - 1.2.3.1. Marketing et communication
 - 1.2.3.2. Commercial
 - 1.2.3.3. Service à la clientèle
 - 1.2.3.4. Achats
 - 1.2.3.5. Administration
 - 1.2.3.6. RH
 - 1.2.3.7. Production
 - 1.2.3.8. IT
- 1.3. Marketing et communication
 - 1.3.1. Les kpi's à mesurer, applications et avantages
 - 1.3.2. Systèmes de marketing et *data warehouse*
 - 1.3.3. Mise en place d'une structure d'analyse des données dans le domaine du marketing
 - 1.3.4. Plan de marketing et de communication
 - 1.3.5. Stratégies, prévisions et gestion des campagnes
- 1.4. Commercial et ventes
 - 1.4.1. Contributions de l'analyse des données dans le domaine commercial
 - 1.4.2. Besoins du département des Ventes
 - 1.4.3. Étude de marché
- 1.5. Service à la clientèle
 - 1.5.1. Fidélisation
 - 1.5.2. Qualité personnelle et intelligence émotionnelle
 - 1.5.3. Satisfaction des clients

- 1.6. Achats
 - 1.6.1. Analyse de données pour les études de marché
 - 1.6.2. Analyse de données pour les études de concurrence
 - 1.6.3. Autres applications
- 1.7. Administration
 - 1.7.1. Besoins du département d'administration
 - 1.7.2. *Data Warehouse* et analyse des risques financiers
 - 1.7.3. *Data Warehouse* et analyse de risque crédit
- 1.8. Ressources humaines
 - 1.8.1. RH et avantages de l'analyse des données
 - 1.8.2. Outils d'analyse des données dans le département des RH
 - 1.8.3. Application de l'analyse des données dans les RH
- 1.9. Production
 - 1.9.1. Analyse des données dans un service de production
 - 1.9.2. Applications
 - 1.9.3. Bénéfices
- 1.10. IT
 - 1.10.1. Département IT
 - 1.10.2. Analyse des données et transformation numérique
 - 1.10.3. Innovation et productivité

Module 2. Gestion des données, manipulation des données et informations pour la science des données

- 2.1. Statistiques Variables, indices et ratios
 - 2.1.1. Statistiques
 - 2.1.2. Dimensions statistiques
 - 2.1.3. Variables, indices et ratios
- 2.2. Typologie des données
 - 2.2.1. Qualitatif
 - 2.2.2. Quantitatif
 - 2.2.3. Caractérisation et catégories

- 2.3. Connaissance des données issues des mesures
 - 2.3.1. Mesures de centralisation
 - 2.3.2. Mesures de la dispersion
 - 2.3.3. Corrélation
- 2.4. Connaissance des données issues des graphiques
 - 2.4.1. Visualisation selon le type de données
 - 2.4.2. Interprétation des informations graphiques
 - 2.4.3. Personnalisation des graphiques avec R
- 2.5. Probabilités
 - 2.5.1. Probabilités
 - 2.5.2. Fonction de probabilité
 - 2.5.3. Distributions
- 2.6. Collecte des données
 - 2.6.1. Méthodologie de collecte
 - 2.6.2. Outils de collecte
 - 2.6.3. Canaux de collecte
- 2.7. Nettoyage des données
 - 2.7.1. Phases du nettoyage des données
 - 2.7.2. Qualité des données
 - 2.7.3. Manipulation des données (avec R)
- 2.8. Analyse des données. interprétations. évaluation des résultats
 - 2.8.1. Mesures statistiques
 - 2.8.2. Indices de ratios
 - 2.8.3. Extraction de données
- 2.9. Entrepôt de données (*Datawarehouse*)
 - 2.9.1. Éléments
 - 2.9.2. Conception
- 2.10. Disponibilité des données
 - 2.10.1. Accès
 - 2.10.2. Utilité
 - 2.10.3. Sécurité

Module 3. Les dispositifs et Plateformes IoT comme base de la science des données

- 3.1. *Internet of Things*
 - 3.1.1. Internet du futur. *Internet of Things*
 - 3.1.2. Le consortium industrial internet
- 3.2. Architecture de référence
 - 3.2.1. L'Architecture de référence
 - 3.2.2. Couches
 - 3.2.3. Composants
- 3.3. Capteurs et dispositifs IoT
 - 3.3.1. Principaux composants
 - 3.3.2. Capteurs et actionneurs
- 3.4. Communications et protocoles
 - 3.4.1. Protocoles Modèle OSI
 - 3.4.2. Technologie de communication
- 3.5. Plateformes *cloud* pour IoT et IIoT
 - 3.5.1. Plateformes à usage général
 - 3.5.2. Plateformes industrielles
 - 3.5.3. Plateformes Open Source
- 3.6. Gestion des données dans les plateformes IoT
 - 3.6.1. Mécanisme de gestion des données Données ouvertes
 - 3.6.2. Échange et visualisation de données
- 3.7. Sécurité IoT
 - 3.7.1. Exigences de sécurité et domaines de sécurité
 - 3.7.2. Stratégies de sécurité IIoT
- 3.8. Applications IoT
 - 3.8.1. Villes intelligentes
 - 3.8.2. Santé et conditions physiques
 - 3.8.3. Maison intelligente
 - 3.8.4. Autres applications
- 3.9. Applications de IIoT
 - 3.9.1. Fabrication
 - 3.9.2. Transport
 - 3.9.3. Énergie
 - 3.9.4. Agriculture et élevage
 - 3.9.5. Autres secteurs

- 3.10. Industrie 4.0
 - 3.10.1. *IoRT (Internet of Robotics Things)*
 - 3.10.2. Fabrication additive 3D
 - 3.10.3. *Big Data Analytics*

Module 4. Représentation graphique pour l'analyse des données

- 4.1. Analyse exploratoire
 - 4.1.1. Représentation pour l'analyse des données
 - 4.1.2. La valeur de la représentation graphique
 - 4.1.3. Nouveaux paradigmes de la représentation graphique
- 4.2. Optimisation pour la science des données
 - 4.2.1. La Gamme de couleurs et design
 - 4.2.2. La Gestalt dans la représentation graphique
 - 4.2.3. Erreurs à éviter et conseils
- 4.3. Sources des données de base
 - 4.3.1. Pour une représentation de qualité
 - 4.3.2. Pour une représentation de quantité
 - 4.3.3. Pour une représentation de temps
- 4.4. Sources des données de complexes
 - 4.4.1. Fichiers, listes et bases de données
 - 4.4.2. Données ouvertes
 - 4.4.3. Données de génération continue
- 4.5. Types de graphiques
 - 4.5.1. Représentations basiques
 - 4.5.2. Représentation par blocs
 - 4.5.3. Représentation pour l'analyse de la dispersion
 - 4.5.4. Représentations circulaires
 - 4.5.5. Représentations de bulles
 - 4.5.6. Représentations géographiques
- 4.6. Types de visualisation
 - 4.6.1. Comparatives et relationnelles
 - 4.6.2. Distribution
 - 4.6.3. Hiérarchique

- 4.7. Conception de rapports avec représentation graphique
 - 4.7.1. Application des graphiques dans les rapports de marketing
 - 4.7.2. Application des graphiques dans les tableaux de bord et Kpi's
 - 4.7.3. Application des graphiques dans les plans stratégiques
 - 4.7.4. Autres utilisations: science, santé, affaires
- 4.8. Récit graphique
 - 4.8.1. Le récit graphique
 - 4.8.2. Évolution
 - 4.8.3. Utilité
- 4.9. Outils orientés vers la visualisation
 - 4.9.1. Outils avancés
 - 4.9.2. Software en ligne
 - 4.9.3. *Open Source*
- 4.10. Nouvelles technologies de la visualisation données
 - 4.10.1. Systèmes de virtualisation de la réalité
 - 4.10.2. Systèmes d'augmentation et amélioration de la réalité
 - 4.10.3. Systèmes intelligents

Module 5. Outils de science des données

- 5.1. Science des données
 - 5.1.1. La science des données
 - 5.1.2. Outils avancés pour le scientifique des données
- 5.2. Données, informations et connaissances
 - 5.2.1. Données, informations et connaissances
 - 5.2.2. Types de données
 - 5.2.3. Sources des données
- 5.3. Des données aux informations
 - 5.3.1. Analyse des données
 - 5.3.2. Types d'analyse
 - 5.3.3. Extraction d'informations d'un *dataset*
- 5.4. Extraction d'informations par la visualisation
 - 5.4.1. La visualisation comme outils d'analyse
 - 5.4.2. Méthodes de visualisation
 - 5.4.3. Visualisation d'un ensemble de données

- 5.5. Qualité des données
 - 5.5.1. Données de qualités
 - 5.5.2. Nettoyage des données
 - 5.5.3. Prétraitement de base des données
- 5.6. *Dataset*
 - 5.6.1. Enrichissement des données *dataset*
 - 5.6.2. La malédiction de la dimensionnalité
 - 5.6.3. Modification d'un ensemble de données
- 5.7. Déséquilibre
 - 5.7.1. Déséquilibre des classes
 - 5.7.2. Techniques d'atténuation du déséquilibre
 - 5.7.3. Equilibrage d'un *dataset*
- 5.8. Modèles non supervisé
 - 5.8.1. Modèles non supervisé
 - 5.8.2. Méthodes
 - 5.8.3. Classifications avec modèles non supervisé
- 5.9. Modèles supervisés
 - 5.9.1. Modèles supervisé
 - 5.9.2. Méthodes
 - 5.9.3. Classifications avec modèles supervisés
- 5.10. Outils et bonnes pratiques
 - 5.10.1. Bonnes pratiques pour un scientifique des données
 - 5.10.2. Le meilleur modèle
 - 5.10.3. Outils utiles

Module 6. Exploration des données. Selection. prétraitement et transformation

- 6.1. Inférence statistique
 - 6.1.1. Statistiques Descriptives vs. Inférence Statistique
 - 6.1.2. Procédures paramétriques
 - 6.1.3. Procédures non paramétriques
- 6.2. Analyse exploratoire
 - 6.2.1. Analyse descriptive
 - 6.2.2. Visualisation
 - 6.2.3. Préparations des données

- 6.3. Préparations des données
 - 6.3.1. Intégration et nettoyage des données
 - 6.3.2. Normalisation des données
 - 6.3.3. Transformer les attributs
- 6.4. Valeurs manquantes
 - 6.4.1. Traitement des valeurs manquantes
 - 6.4.2. Méthodes d'imputation par maximum de vraisemblance
 - 6.4.3. Imputation des valeurs manquantes à l'aide de l'apprentissage automatique
- 6.5. Bruit dans les données
 - 6.5.1. Classes et attributs de bruit
 - 6.5.2. Filtrage du bruit
 - 6.5.3. L'effet du bruit
- 6.6. La malédiction de la dimensionnalité
 - 6.6.1. *Oversampling*
 - 6.6.2. *Undersampling*
 - 6.6.3. Réduction des données multidimensionnelles
- 6.7. Des attributs continus aux attributs discrets
 - 6.7.1. Données continues ou discrètes
 - 6.7.2. Processus de discrétisation
- 6.8. Les données
 - 6.8.1. Sélection des données
 - 6.8.2. Perspectives et critères de sélections
 - 6.8.3. Méthodes de sélection
- 6.9. Sélection d'instances
 - 6.9.1. Méthodes de sélection des instances
 - 6.9.2. Sélection des prototypes
 - 6.9.3. Méthodes avancées de sélection des instances
- 6.10. Prétraitement des données dans les environnements *Big Data*
 - 6.10.1. *Big Data*
 - 6.10.2. Prétraitement "classique" versus massif
 - 6.10.3. *Données Intelligentes*

Module 7. Prévisibilité et analyse des phénomènes stochastiques

- 7.1. Séries chronologiques
 - 7.1.1. Séries chronologiques
 - 7.1.2. Utilité et applicabilité
 - 7.1.3. Études de cas connexes
- 7.2. Séries chronologiques
 - 7.2.1. Tendance Saisonnalité de ST
 - 7.2.2. Variations typiques
 - 7.2.3. Analyse des résidus
- 7.3. Typologies
 - 7.3.1. Stationnaire
 - 7.3.2. Non stationnaire
 - 7.3.3. Transformations et ajustements
- 7.4. Schémas pour les séries temporelles
 - 7.4.1. Schéma additif (modèle)
 - 7.4.2. Schéma multiplicatif (modèle)
 - 7.4.3. Procédures pour déterminer le type de modèle
- 7.5. Méthodes basiques de *forecast*
 - 7.5.1. Moyenne
 - 7.5.2. *Naïve*
 - 7.5.3. *Naïve* saisonnière
 - 7.5.4. Comparaison des méthodes
- 7.6. Analyse des résidus
 - 7.6.1. Autocorrélation
 - 7.6.2. ACF des résidus
 - 7.6.3. Test de corrélation
- 7.7. Régression dans le contexte des séries temporelles
 - 7.7.1. ANOVA
 - 7.7.2. Principes fondamentaux
 - 7.7.3. Application pratique
- 7.8. Modèles prédictifs de séries chronologiques
 - 7.8.1. ARIMA
 - 7.8.2. Lissage exponentiel

- 7.9. Manipulation et analyse de Séries chronologiques avec R
 - 7.9.1. Préparations des données
 - 7.9.2. Identification des motifs
 - 7.9.3. Analyse du modèle
 - 7.9.4. Prédiction
- 7.10. Analyse graphique combinée avec R
 - 7.10.1. Situations typiques
 - 7.10.2. Application pratique pour la résolution de problèmes simples
 - 7.10.3. Application pratique pour la résolution de problèmes avancés

Module 8. Conception et développement de systèmes intelligents

- 8.1. Prétraitement des données
 - 8.1.1. Prétraitement des données
 - 8.1.2. Transformation des données
 - 8.1.3. Extraction de données
- 8.2. Apprentissage Automatique
 - 8.2.1. Apprentissage supervisé et non supervisé
 - 8.2.2. Apprentissage par renforcement
 - 8.2.3. Autres paradigmes d'apprentissage
- 8.3. Algorithmes de classification
 - 8.3.1. Apprentissage automatique inductif
 - 8.3.2. SVM y KNN
 - 8.3.3. Métriques et scores pour le classement
- 8.4. Algorithmes de Régression
 - 8.4.1. Régression linéaire. régression logistique et modèles non linéaires
 - 8.4.2. Séries chronologiques
 - 8.4.3. Métriques et scores pour le régression
- 8.5. Algorithmes de Regroupement
 - 8.5.1. Techniques de regroupement hiérarchique
 - 8.5.2. Techniques de regroupement partitionnel
 - 8.5.3. Métriques et scores pour le *Clustering*

- 8.6. Techniques de règles d'association
 - 8.6.1. Méthodes d'extraction de règles
 - 8.6.2. Métriques et scores pour les algorithmes de règles d'association
- 8.7. Techniques de classification avancées. Multiclassificateurs
 - 8.7.1. Algorithme de *Bagging*
 - 8.7.2. Classificateur *Random Forests*
 - 8.7.3. *Boosting* pour les arbres de décision
- 8.8. Modèles graphiques probabilistes
 - 8.8.1. Modèles probabilistes
 - 8.8.2. Les réseaux bayésiens. Propriétés, représentation et paramétrage
 - 8.8.3. Autres modèles graphiques probabilistes
- 8.9. Réseaux neuronaux
 - 8.9.1. Apprentissage automatique avec les réseaux de neurones artificiels
 - 8.9.2. Réseaux *feedforward*
- 8.10. Apprentissage profond
 - 8.10.1. Réseaux *feedforward* profond
 - 8.10.2. Réseaux neuronaux convolutifs et modèles de séquences
 - 8.10.3. Outils pour la mise en œuvre de réseaux neuronaux profonds

Module 9. Architectures et systèmes à forte intensité de données

- 9.1. Exigences non fonctionnelles. Piliers des applications big data
 - 9.1.1. Fiabilité
 - 9.1.2. Adaptabilité
 - 9.1.3. Maintenance
- 9.2. Modèles de données
 - 9.2.1. Modèle relationnel
 - 9.2.2. Modèle documentaire
 - 9.2.3. Modèle de données du réseau
- 9.3. Bases de données. Gestion du stockage et de la récupération des données
 - 9.3.1. Indices has
 - 9.3.2. Stockage structuré en log
 - 9.3.3. Arbres B
- 9.4. Formats de codage des données
 - 9.4.1. Formats spécifiques à une langue
 - 9.4.2. Formats standardisés
 - 9.4.3. Formats d'encodage binaire
 - 9.4.4. Flux de données interprocessus
- 9.5. Réplication
 - 9.5.1. Objectifs de la réplication
 - 9.5.2. Modèles de réplication
 - 9.5.3. Problèmes de réplication
- 9.6. Transactions distribuées
 - 9.6.1. Transaction
 - 9.6.2. Protocoles pour les transactions distribuées
 - 9.6.3. Transactions sérialisables
- 9.7. Cloisonnement
 - 9.7.1. Les formes de cloisonnement
 - 9.7.2. Interaction de l'index secondaire et du partitionnement
 - 9.7.3. Rééquilibrage des partitions
- 9.8. Traitement des données *offline*
 - 9.8.1. Traitement par lots
 - 9.8.2. Systèmes de fichiers distribués
 - 9.8.3. *MapReduce*
- 9.9. Traitement des données en temps réel
 - 9.9.1. Types de *broker* de messages
 - 9.9.2. Représentation des bases de données en tant que flux de données
 - 9.9.3. Traitement des flux de données
- 9.10. Applications pratiques dans l'entreprise
 - 9.10.1. Cohérence dans les lectures
 - 9.10.2. Approche holistique des données
 - 9.10.3. Mise à l'échelle d'un service distribué

Module 10. Application pratique de la science des données dans les secteurs d'activité d'entreprise

- 10.1. Secteur sanitaire
 - 10.1.1. Implications de l'IA et de l'analyse des données dans le secteur de la santé
 - 10.1.2. Opportunités et défis
- 10.2. Risques et tendances dans le secteur de la santé
 - 10.2.1. Utilisation dans le secteur de la santé
 - 10.2.2. Risques potentiels liés à l'utilisation de l'IA
- 10.3. Services financiers
 - 10.3.1. Implications de l'IA et de l'analyse des données dans le secteur des services financiers
 - 10.3.2. Utilisation dans les secteurs financiers
 - 10.3.3. Risques potentiels liés à l'utilisation de l'IA
- 10.4. Retail
 - 10.4.1. Implications de l'IA l'analyse des données sont abordées dans le secteur du Retail
 - 10.4.2. Utilisation pendant la vente au détail
 - 10.4.3. Risques potentiels liés à l'utilisation de l'IA
- 10.5. Industrie 4.0
 - 10.5.1. Implications de l'IA et l'analyse des données dans l'Industrie 4.0
 - 10.5.2. Utilisation dans l'Industrie 4.0
- 10.6. Risques et tendances dans l'Industrie 4.0
 - 10.6.1. Risques potentiels liés à l'utilisation de l'IA
- 10.7. Administration publique
 - 10.7.1. Implications de l'IA et de l'analyse des données dans l'administration publique
 - 10.7.2. Utilisation dans l'administration publique
 - 10.7.3. Risques potentiels liés à l'utilisation de l'IA
- 10.8. Éducation
 - 10.8.1. Implications de l'IA et de l'analyse des données dans l'éducation
 - 10.8.2. Risques potentiels liés à l'utilisation de l'IA
- 10.9. Sylviculture et agriculture
 - 10.9.1. Implications de l'IA et de l'analyse des données dans la sylviculture et agriculture
 - 10.9.2. Utilisation dans la sylviculture et agriculture
 - 10.9.3. Risques potentiels liés à l'utilisation de l'IA

- 10.10. Ressources humaines
 - 10.10.1. Implications de l'IA et de l'analyse des données dans la gestion des ressources humaines
 - 10.10.2. Applications pratiques dans le monde des affaires
 - 10.10.3. Risques potentiels liés à l'utilisation de l'IA

Module 11. Cyber intelligence et cybersécurité

- 11.1. Cyber Intelligence
 - 11.1.1. Cyber Intelligence
 - 11.1.1.1. Intelligence
 - 11.1.1.1.1. Cycle de l'intelligence
 - 11.1.1.2. Cyber Intelligence
 - 11.1.1.3. Cyber intelligence et cybersécurité
 - 11.1.2. L'Analyste de l'Intelligence
 - 11.1.2.1. Le rôle de l'analyste du renseignement
 - 11.1.2.2. Biais de l'analyste du renseignement dans l'activité d'évaluation
- 11.2. Cybersécurité
 - 11.2.1. Couches de sécurité
 - 11.2.2. Identification des cybermenaces
 - 11.2.2.1. Menaces extérieures
 - 11.2.2.2. Menaces internes
 - 11.2.3. Actions défavorables
 - 11.2.3.1. Ingénierie sociale
 - 11.2.3.2. Méthodes de communément utilisées
- 11.3. Techniques et outils d'intelligences
 - 11.3.1. OSINT
 - 11.3.2. SOCMINT
 - 11.3.3. HUMINT
 - 11.3.4. Distributions et outils Linux
 - 11.3.5. OWISAM
 - 11.3.6. OWISAP
 - 11.3.7. PTES
 - 11.3.8. OSSTM

- 11.4. Méthodologie d'évaluation
 - 11.4.1. L'analyse de Intelligence
 - 11.4.2. Techniques d'organisation des informations acquises
 - 11.4.3. Fiabilité et crédibilité des sources d'information
 - 11.4.4. Méthodologie d'analyse
 - 11.4.5. Présentation les résultats de l'Intelligence
- 11.5. Audits et documentation
 - 11.5.1. Audit de la sécurité informatique
 - 11.5.2. Documentation et autorisations pour l'audit
 - 11.5.3. Types d'audits
 - 11.5.4. Produits livrables
 - 11.5.4.1. Rapport technique
 - 11.5.4.2. rapport exécutif
- 11.6. Détection sur le web
 - 11.6.1. Utilisation de l'anonymat
 - 11.6.2. Techniques d'anonymat (Proxy, VPN)
 - 11.6.3. Réseaux TOR, Freenet et IP2
- 11.7. Menaces et types de sécurité
 - 11.7.1. Types de menaces
 - 11.7.2. Sécurité physique
 - 11.7.3. Sécurité en réseaux
 - 11.7.4. Sécurité logique
 - 11.7.5. Sécurité sur les applications web
 - 11.7.6. Sécurité des appareils mobiles
- 11.8. Réglementation et *compliance*
 - 11.8.1. Le RGPD
 - 11.8.2. La stratégie nationale de cybersécurité de 2019
 - 11.8.3. Famille ISO 27000
 - 11.8.4. Cadre de cybersécurité du NIST
 - 11.8.5. PIC
 - 11.8.6. ISO 27032
 - 11.8.7. Réglementation *cloud*
 - 11.8.8. SOX
 - 11.8.9. PCI

- 11.9. Analyse et mesure des risques
 - 11.9.1. Portée des risques
 - 11.9.2. Les actifs
 - 11.9.3. Menaces
 - 11.9.4. Vulnérabilités
 - 11.9.5. Évaluation des risques
 - 11.9.6. Traitement du risque
- 11.10. Organismes importants en matière de cybersécurité
 - 11.10.1. NIST
 - 11.10.2. ENISA
 - 11.10.3. INCIBE
 - 11.10.4. OEA
 - 11.10.5. UNASUR-PROSUR

Module 12. Sécurité de l'hôte

- 12.1. Copies de sauvegarde
 - 12.1.1. Stratégies de sauvegarde
 - 12.1.2. Outils pour Windows
 - 12.1.3. Outils pour Linux
 - 12.1.4. Outils pour MacOS
- 12.2. Antivirus utilisateur
 - 12.2.1. Types d'antivirus
 - 12.2.2. Antivirus pour Windows
 - 12.2.3. Antivirus pour Linux
 - 12.2.4. Antivirus pour MacOS
 - 12.2.5. Antivirus pour smartphones
- 12.3. Détecteurs d'intrusion - HIDS
 - 12.3.1. Méthodes de détection des intrusions
 - 12.3.2. *Sagan*
 - 12.3.3. *Aide*
 - 12.3.4. *Rkhunter*

Module 13. Sécurité des réseaux (périmètre)

- 13.1. Systèmes de détection et de prévention des menaces
 - 13.1.1. Cadre général des incidents de sécurité
 - 13.1.2. Les systèmes de défense actuels: *Defense in Depth* et SOC
 - 13.1.3. Architectures de réseau actuelles
 - 13.1.4. Types d'outils de détection et de prévention des incidents
 - 13.1.4.1. Systèmes en réseau
 - 13.1.4.2. Systèmes basés sur Host
 - 13.1.4.3. Systèmes centralisés
 - 13.1.5. Communication et découverte d'instances/*hosts*. conteneurs et *serverless*
- 13.2. *Firewall*
 - 13.2.1. Types de *firewalls*
 - 13.2.2. Attaques et atténuation
 - 13.2.3. *Firewalls* courants du kernel Linux
 - 13.2.3.1. UFW
 - 13.2.3.2. Nftables et iptables
 - 13.2.3.3. *Firewalls*
 - 13.2.4. Systèmes de détection basés sur les journaux du système
 - 13.2.4.1. *TCP Wrappers*
 - 13.2.4.2. *BlockHosts* et *DenyHosts*
 - 13.2.4.3. *Fai2ban*
- 13.3. Systèmes de détection et de prévention des intrusions (IDS/IPS)
 - 13.3.1. Attaques contre les IDS/IPS
 - 13.3.2. Systèmes IDS/IPS
 - 13.3.2.1. *Snort*
 - 13.3.2.2. *Suricata*
- 13.4. *Firewalls* de nouvelle génération (NGFW)
 - 13.4.1. Différences entre les NGFW et les Pare-feu traditionnels
 - 13.4.2. Principales capacités
 - 13.4.3. Solutions commerciales
 - 13.4.4. *Firewalls* pour les services en *Cloud*
 - 13.4.4.1. Architecture *Cloud* VPC
 - 13.4.4.2. *Cloud* ACLs
 - 13.4.4.3. *Security Group*

- 13.5. Proxy
 - 13.5.1. Types de Proxy
 - 13.5.2. Utilisation du Proxy. Avantages et inconvénients
- 13.6. Moteurs antivirus
 - 13.6.1. Contexte général des *malwares* et des IOC
 - 13.6.2. Problèmes de moteur antivirus
- 13.7. Systèmes de protection du courrier
 - 13.7.1. Antispam
 - 13.7.1.1. Liste blanche et liste noire
 - 13.7.1.2. Filtres bayésiens
 - 13.7.2. *Mail Gateway* (MGW)
- 13.8. SIEM
 - 13.8.1. Composants et architecture
 - 13.8.2. Règles de corrélation et cas d'utilisation
 - 13.8.3. Les défis actuels des systèmes SIEM
- 13.9. SOAR
 - 13.9.1. SOAR et SIEM: ennemis ou alliés
 - 13.9.2. L'avenir des systèmes SOAR
- 13.10. Autres systèmes en réseau
 - 13.10.1. WAF
 - 13.10.2. NAC
 - 13.10.3. HoneyPots y HoneyNets
 - 13.10.4. CASB

Module 14. La sécurité sur les smartphones

- 14.1. Le monde de l'appareil mobile
 - 14.1.1. Types de plateformes mobiles
 - 14.1.2. Dispositifs iOS
 - 14.1.3. Dispositifs Android
- 14.2. Gestion de la Sécurité Mobile
 - 14.2.1. Projet de Sécurité Mobile OWASP
 - 14.2.1.1. Les 10 principales Vulnérabilités
 - 14.2.2. Communications, réseaux et modes de connexion

- 14.3. Le dispositif mobile dans l'environnement professionnel
 - 14.3.1. Risques
 - 14.3.2. Politiques de sécurité
 - 14.3.3. Surveillance des dispositifs
 - 14.3.4. Gestion des dispositifs mobiles (MDM)
- 14.4. Vie privée des utilisateurs et sécurité des données
 - 14.4.1. États d'information
 - 14.4.2. Protection des données et confidentialité
 - 14.4.2.1. Permissions
 - 14.4.2.2. Cryptage
 - 14.4.3. Stockage sécurisé des données
 - 14.4.3.1. Stockage sécurisé sur iOS
 - 14.4.3.2. Stockage sécurisé sur Android
 - 14.4.4. Bonnes pratiques en matière de développement d'applications
- 14.5. Vulnérabilités et vecteurs d'attaque
 - 14.5.1. Vulnérabilités
 - 14.5.2. Vecteurs d'attaque
 - 14.5.2.1. *Malware*
 - 14.5.2.2. Exfiltration de données
 - 14.5.2.3. Manipulation des données
- 14.6. Principales menaces
 - 14.6.1. Utilisateur non forcé
 - 14.6.2. *Malware*
 - 14.6.2.1. Types de *Malware*
 - 14.6.3. Ingénierie sociale
 - 14.6.4. Fuite de données
 - 14.6.5. Vol d'informations
 - 14.6.6. Réseaux *Wi-Fi* non sécurisés
 - 14.6.7. Software obsolètes

- 14.6.8. Applications malveillantes
- 14.6.9. Mots de passe non sécurisés
- 14.6.10. Paramètres de sécurité faibles ou inexistants
- 14.6.11. Accès physique
- 14.6.12. Perte ou vol de l'appareil
- 14.6.13. Vol d'identité (intégrité)
- 14.6.14. Cryptographie faible ou brisée
- 14.6.15. Déni de service (DoS)
- 14.7. Attaques majeures
 - 14.7.1. Attaques de *phishing*
 - 14.7.2. Attaques liées aux modes de communication
 - 14.7.3. Attaques de *Smishing*
 - 14.7.4. Attaques de *Cryptojacking*
 - 14.7.5. *Man in the Middle*
- 14.8. *Hacking*
 - 14.8.1. *Rooting et Jailbreaking*
 - 14.8.2. Anatomie d'une attaque mobile
 - 14.8.2.1. Propagation de la menace
 - 14.8.2.2. Installation d'un *malware* sur l'appareil
 - 14.8.2.3. Persistance
 - 14.8.2.4. Exécution du *payload* et extraction de l'information
 - 14.8.3. *Hacking* des appareils iOS: mécanismes et outils
 - 14.8.4. *Hacking* des appareils Android: mécanismes et outils
- 14.9. Tests de pénétration
 - 14.9.1. *iOS PenTesting*
 - 14.9.2. *Android PenTesting*
 - 14.9.3. Outils
- 14.10. Sûreté et sécurité
 - 14.10.1. Paramètres de sécurité
 - 14.10.1.1. Sur les appareils iOS
 - 14.10.1.2. Sur les appareils Android
 - 14.10.2. Mesures de sécurité
 - 14.10.3. Outils de protection

Module 15. Sécurité IoT

- 15.1. Dispositifs
 - 15.1.1. Types de dispositifs
 - 15.1.2. Architectures standardisées
 - 15.1.2.1. ONEM2M
 - 15.1.2.2. IoTWF
 - 15.1.3. Protocoles d'application
 - 15.1.4. Technologies de la connectivité
- 15.2. Dispositifs IoT. Domaines d'application
 - 15.2.1. *SmartHome*
 - 15.2.2. *SmartCity*
 - 15.2.3. Transports
 - 15.2.4. *Wearables*
 - 15.2.5. Secteur de la santé
 - 15.2.6. IIoT
- 15.3. Protocoles de communication
 - 15.3.1. MQTT
 - 15.3.2. LWM2M
 - 15.3.3. OMA-DM
 - 15.3.4. TR-069
- 15.4. *SmartHome*
 - 15.4.1. Domotique
 - 15.4.2. Réseaux
 - 15.4.3. Appareils ménagers
 - 15.4.4. Surveillance et sécurité
- 15.5. *SmartCity*
 - 15.5.1. Éclairage
 - 15.5.2. Météorologie
 - 15.5.3. Sécurité
- 15.6. Transports
 - 15.6.1. Localisation
 - 15.6.2. Effectuer des paiements et obtenir des services
 - 15.6.3. Connectivité

- 15.7. *Wearables*
 - 15.7.1. Vêtements intelligents
 - 15.7.2. Bijoux intelligents
 - 15.7.3. Montres intelligentes
- 15.8. Secteur de la santé
 - 15.8.1. Surveillance de l'exercice et de la fréquence cardiaque
 - 15.8.2. Surveillance des patients et des personnes âgées
 - 15.8.3. Implantable
 - 15.8.4. Robots chirurgicaux
- 15.9. Connectivité
 - 15.9.1. *Wi-Fi/Gateway*
 - 15.9.2. *Bluetooth*
 - 15.9.3. Connectivité embarquée
- 15.10. Titrisation
 - 15.10.1. Réseaux dédiés
 - 15.10.2. Gestionnaire de mots de passe
 - 15.10.3. Utilisation de protocoles cryptés
 - 15.10.4. Conseils d'utilisation

Module 16. *Hacking* éthique

- 16.1. Environnement de travail
 - 16.1.1. Distributions Linux
 - 16.1.1.1. Kali Linux - Offensive Security
 - 16.1.1.2. Parrot OS
 - 16.1.1.3. Ubuntu
 - 16.1.2. Systèmes de virtualisation
 - 16.1.3. *Sandbox*
 - 16.1.4. Déploiement des laboratoires
- 16.2. Méthodologie
 - 16.2.1. OSSTM
 - 16.2.2. OWASP
 - 16.2.3. NIST
 - 16.2.4. PTES
 - 16.2.5. ISSAF

- 16.3. *Footprinting*
 - 16.3.1. Renseignement de source ouverte (OSINT)
 - 16.3.2. Recherche de violations de données et de vulnérabilité
 - 16.3.3. Utilisation d'outils passif
- 16.4. Analyse du réseau
 - 16.4.1. Outils d'analyse
 - 16.4.1.1. Nmap
 - 16.4.1.2. Hping3
 - 16.4.1.3. Autres outils d'analyse
 - 16.4.2. Techniques de balayage
 - 16.4.3. Techniques de contournement des *Firewall* et IDS
 - 16.4.4. *Banner Grabbing*
 - 16.4.5. Diagrammes de réseau
- 16.5. Énumération
 - 16.5.1. Énumération SMTP
 - 16.5.2. Énumération DNS
 - 16.5.3. Énumération de NetBIOS et de samba
 - 16.5.4. Énumération LDAP
 - 16.5.5. Énumération SNMP
 - 16.5.6. Autres techniques d'énumération
- 16.6. Analyse des vulnérabilités
 - 16.6.1. Solutions d'analyse des vulnérabilités
 - 16.6.1.1. Qualys
 - 16.6.1.2. Nessus
 - 16.6.1.3. Nessus
 - 16.6.2. Systèmes d'évaluation des vulnérabilités
 - 16.6.2.1. CVSS
 - 16.6.2.2. CVE
 - 16.6.2.3. NVD
- 16.7. Attaques contre les réseaux *sans fil*
 - 16.7.1. Méthodologie de *hacking* des réseaux sans fil
 - 16.7.1.1. Wi-Fi Discovery
 - 16.7.1.2. Analyse du trafic

- 16.7.1.3. Attaques d' *Aircrack*
 - 16.7.1.3.1. Attaques WEP
 - 16.7.1.3.2. Attaques WPA/WPA2
- 16.7.1.4. Les attaques de *Evil Twin*
- 16.7.1.5. Attaques sur le WPS
- 16.7.1.6. *Jamming*
- 16.7.2. Outils pour la sécurité sans fil
- 16.8. Piratage de serveurs web
 - 16.8.1. *Cross site Scripting*
 - 16.8.2. CSRF
 - 16.8.3. *Session Hijacking*
 - 16.8.4. *SQLinjection*
- 16.9. Exploitation des vulnérabilités
 - 16.9.1. Utilisation d' *exploits* connus
 - 16.9.2. Utilisation des *metasploit*
 - 16.9.3. Utilisation des *Malware*
 - 16.9.3.1. Définition et champ d'application
 - 16.9.3.2. Génération de *malware*
 - 16.9.3.3. Bypass des solutions anti-virus
- 16.10. Persistance
 - 16.10.1. Installation de rootkits
 - 16.10.2. Utilisation de ncat
 - 16.10.3. Utilisation de tâches planifiées pour les backdoors
 - 16.10.4. Création d'utilisateurs
 - 16.10.5. Détection HIDS

Module 17. Ingénierie inverse

- 17.1. Compilateurs
 - 17.1.1. Types de code
 - 17.1.2. Les phases d'un compilateur
 - 17.1.3. Table des symboles
 - 17.1.4. Gestionnaire d'erreurs
 - 17.1.5. Compilateur GCC
- 17.2. Types d'analyse de compilateur
 - 17.2.1. Analyse lexicale
 - 17.2.1.1. Terminologie
 - 17.2.1.2. Composante lexicale
 - 17.2.1.3. Analyseur Lexical LEX
 - 17.2.2. Analyse syntaxique
 - 17.2.2.1. Grammaires sans contexte
 - 17.2.2.2. Types d'analyse syntaxique
 - 17.2.2.2.1. Analyse syntaxique descendante
 - 17.2.2.2.2. Analyse ascendante
 - 17.2.2.3. Arbres syntaxiques et dérivations
 - 17.2.2.4. Types d'analyseurs syntaxiques
 - 17.2.2.4.1. Analyseurs LR(*Left To Right*)
 - 17.2.2.4.2. Analyseurs LALR
 - 17.2.3. Analyse sémantique
 - 17.2.3.1. Grammaires d'attributs
 - 17.2.3.2. S-Attributs
 - 17.2.3.3. L-attributs
- 17.3. Structures de données de l'assemblage
 - 17.3.1. Variables
 - 17.3.2. Tableaux
 - 17.3.3. Pointeurs
 - 17.3.4. Structures
 - 17.3.5. Objets
- 17.4. Structures du code d'assemblage
 - 17.4.1. Structures de sélection
 - 17.4.1.1. If. else if. Else
 - 17.4.1.2. Switch
 - 17.4.2. Structures d'itération
 - 17.4.2.1. For
 - 17.4.2.2. While
 - 17.4.2.3. Utilisation du break
 - 17.4.3. Fonctions

- 17.5. Architecture Hardware x86
 - 17.5.1. Architecture de processeur x86
 - 17.5.2. Structures de données x86
 - 17.5.3. Structures de code x86
- 17.6. Architecture Hardware ARM
 - 17.6.1. Architecture du processeur ARM
 - 17.6.2. Structures de données ARM
 - 17.6.3. Structures de code ARM
- 17.7. Analyse du code statique
 - 17.7.1. Démonteurs
 - 17.7.2. IDA
 - 17.7.3. Reconstructeurs de code
- 17.8. Analyse dynamique du code
 - 17.8.1. Analyse comportementale
 - 17.8.1.1. Communications
 - 17.8.1.2. Suivi
 - 17.8.2. Débogueurs de code Linux
 - 17.8.3. Débogueurs de code sous Windows
- 17.9. *Sandbox*
 - 17.9.1. Architecture d'un *Sandbox*
 - 17.9.2. Évasion du *Sandbox*
 - 17.9.3. Techniques de détection
 - 17.9.4. Techniques d'évasion
 - 17.9.5. Contre-mesures
 - 17.9.6. *Sandbox* sur Linux
 - 17.9.7. *Sandbox* sur Windows
 - 17.9.8. *Sandbox* sur MacOS
 - 17.9.9. *Sandbox* sur Android
- 17.10. Analyse des malware
 - 17.10.1. Méthodes d'analyse des *malware*
 - 17.10.2. Techniques d'obscurcissement des *malware*
 - 17.10.2.1. Obfuscation des exécutables
 - 17.10.2.2. Restriction des environnements d'exécution
 - 17.10.3. Outils d'analyse des *malware*

Module 18. Développement sécurisé

- 18.1. Développement sécurisé
 - 18.1.1. Qualité, fonctionnalité et sécurité
 - 18.1.2. Confidentialité, intégrité et disponibilité
 - 18.1.3. Cycle de vie du développement du Software
- 18.2. Phase des Prérequis
 - 18.2.1. Gestion de l'authentification
 - 18.2.2. Contrôle des rôles et des privilèges
 - 18.2.3. Exigences axées sur le risque
 - 18.2.4. Approbation des privilèges
- 18.3. Phase d'analyse et de conception
 - 18.3.1. Accès aux composants et administration du système
 - 18.3.2. Pistes d'audit
 - 18.3.3. Gestion des sessions
 - 18.3.4. Données historiques
 - 18.3.5. Traitement approprié des erreurs
 - 18.3.6. Séparation des fonctions
- 18.4. Phase de mise en œuvre et de codification
 - 18.4.1. Sécuriser l'environnement de développement
 - 18.4.2. Élaboration de la documentation technique
 - 18.4.3. Codage sécurisé
 - 18.4.4. Communications sécurisées
- 18.5. Bonnes pratiques de codage sécurisé
 - 18.5.1. Validation des données d'entrée
 - 18.5.2. Cryptage des données de sortie
 - 18.5.3. Style de programmation
 - 18.5.4. Traitement du journal des modifications
 - 18.5.5. Pratiques cryptographiques
 - 18.5.6. Gestion des erreurs et des journaux
 - 18.5.7. Gestion des fichiers
 - 18.5.8. Gestion de la mémoire
 - 18.5.9. Standardisation et réutilisation des fonctions de sécurité

- 18.6. Préparation du serveur et *Hardening*
 - 18.6.1. Gestion des utilisateurs, des groupes et des rôles sur le serveur
 - 18.6.2. Installation du logiciel
 - 18.6.3. *Hardening* du serveur
 - 18.6.4. Configuration robuste de l'environnement de l'application
- 18.7. Préparation de la BBDD et *Hardening*
 - 18.7.1. Optimisation de la BBDD
 - 18.7.2. Création d'un utilisateur propre pour l'application
 - 18.7.3. Attribution des privilèges nécessaires à l'utilisateur
 - 18.7.4. *Hardening* de la BBDD
- 18.8. Phase de test
 - 18.8.1. Contrôle de la qualité des contrôles de sécurité
 - 18.8.2. Inspection progressive du code
 - 18.8.3. Contrôle de la gestion de la configuration
 - 18.8.4. Tests boîte noire
- 18.9. Préparer la transition vers la production
 - 18.9.1. Effectuer le contrôle des changements
 - 18.9.2. Effectuer la procédure de changement de production
 - 18.9.3. Exécuter la procédure de *rollback*
 - 18.9.4. Essais de pré-production
- 18.10. Phase de maintenance
 - 18.10.1. Assurance basée sur le risque
 - 18.10.2. Test de maintenance de la sécurité de la boîte blanche
 - 18.10.3. Tests de maintenance de la sécurité en boîte noire

Module 19. Analyse médico-légale

- 19.1.3. Méthodes de validation des données acquises
 - 19.1.3.1. Méthodes pour Linux
 - 19.1.3.2. Méthodes pour Windows
- 19.2. Évaluation et défaite des techniques anti-forensic
 - 19.2.1. Objectifs des techniques médico-légales
 - 19.2.2. Effacement des données
 - 19.2.2.1. Effacement des données et des fichiers
 - 19.2.2.2. Récupération de fichiers
 - 19.2.2.3. Récupération de partitions supprimées
 - 19.2.3. Protection par mot de passe
 - 19.2.4. Stéganographie
 - 19.2.5. Effacement sécurisé des dispositifs
 - 19.2.6. Cryptage
- 19.3. Analyse Forensique des systèmes d'exploitation
 - 19.3.1. Analyse légale de Windows
 - 19.3.2. Analyse légale de Linux
 - 19.3.3. Analyse légale de Mac
- 19.4. Analyse Forensique des réseaux
 - 19.4.1. Analyse des logs
 - 19.4.2. Corrélation des données
 - 19.4.3. Enquête sur le réseau
 - 19.4.4. Étapes à suivre pour l'analyse criminelle du réseau
- 19.5. Analyse légale Web
 - 19.5.1. Enquête sur les attaques sur Internet
 - 19.5.2. Détection des attaques
 - 19.5.3. Localisation de l'adresse IP
- 19.6. Analyse légale des bases de données
 - 19.6.1. Analyse légale de MSSQL
 - 19.6.2. Analyse légale de MySQL
 - 19.6.3. Analyse légale de PostgreSQL
 - 19.6.4. Analyse légale de MongoDB
- 19.7. Analyse médico-légale sur le *Cloud*
 - 19.7.1. Types de délits sur le *Cloud*
 - 19.7.1.1. *Cloud* comme sujet

- 19.7.1.2. *cloud* comme objet
 - 19.7.1.3. *cloud* comme outil
- 19.7.2. Les défis médico-légaux sur le *Cloud*
- 19.7.3. Recherche sur les services de stockage dans le *Cloud*
- 19.7.4. Outils d'analyse médico-légale pour le *Cloud*
- 19.8. Enquêtes sur les crimes par courriel
 - 19.8.1. Systèmes de courrier
 - 19.8.1.1. Clients de messagerie
 - 19.8.1.2. Serveur de messagerie
 - 19.8.1.3. Serveur SMTP
 - 19.8.1.4. Serveur POP3
 - 19.8.1.5. Serveur IMAP4
 - 19.8.2. Délits de courrier
 - 19.8.3. Message de courrier
 - 19.8.3.1. En-têtes standard
 - 19.8.3.2. En-têtes étendus
 - 19.8.4. Étapes de l'enquête sur ces crimes
 - 19.8.5. Outils d'analyse des e-mails
- 19.9. Analyse légale des mobiles
 - 19.9.1. Réseaux cellulaires
 - 19.9.1.1. Types de réseaux
 - 19.9.1.2. Contenu du CDR
 - 19.9.2. *Subscriber Identity Module* (SIM)
 - 19.9.3. Acquisition logique
 - 19.9.4. Acquisition physique
 - 19.9.5. Acquisition du système de fichiers
- 19.10. Rédaction et soumission de Rapports Forensiques
 - 19.10.1. Aspects importants d'un rapport forensique
 - 19.10.2. Classification et types de rapports
 - 19.10.3. Guide pour la rédaction d'un rapport
 - 19.10.4. Présentation du rapport
 - 19.10.4.1. Préparation préalable au témoignage
 - 19.10.4.2. Dépôt
 - 19.10.4.3. Traiter avec les médias

Module 20. Défis actuels et futurs en matière de sécurité informatique

- 20.1. Technologie *blockchain*
 - 20.1.1. Domaines d'application
 - 20.1.2. Garantie de confidentialité
 - 20.1.3. Garantie de non-répudiation
- 20.2. La monnaie numérique
 - 20.2.1. Bitcoins
 - 20.2.2. Cryptocurrencies
 - 20.2.3. Extraction de crypto-monnaies
 - 20.2.4. Les systèmes pyramidaux
 - 20.2.5. Autres crimes et problèmes potentiels
- 20.3. *Deepfake*
 - 20.3.1. Impact des médias
 - 20.3.2. Dangers pour la société
 - 20.3.3. Mécanismes de détection
- 20.4. L'avenir de l'intelligence artificielle
 - 20.4.1. Intelligence artificielle et informatique cognitive
 - 20.4.2. Utilisations pour simplifier le service à la clientèle
- 20.5. Vie privée numérique
 - 20.5.1. Valeur des données sur le réseau
 - 20.5.2. Utilisation des données sur le réseau
 - 20.5.3. Vie privée et gestion de l'identité numérique
- 20.6. Cyberconflits, cybercriminels et cyberattaques
 - 20.6.1. Impact de la cybersécurité sur les conflits internationaux
 - 20.6.2. Conséquences des cyberattaques sur la population générale
 - 20.6.3. Types de cybercriminels. Mesures de protection
- 20.7. Télétravail
 - 20.7.1. La révolution du télétravail pendant et après la Covid19
 - 20.7.2. Goulets d'étranglement dans l'accès
 - 20.7.3. Variation de la surface d'attaque
 - 20.7.4. Besoins des travailleurs

- 20.8. Technologies *wireless* émergentes
 - 20.8.1. WPA3
 - 20.8.2. 5G
 - 20.8.3. Ondes millimétriques
 - 20.8.4. Tendance *Get Smart* au lieu de *Get more*
- 20.9. L'adressage futur dans les réseaux
 - 20.9.1. Problèmes actuels de l'adressage IP
 - 20.9.2. IPv6
 - 20.9.3. IPv4+
 - 20.9.4. Avantages d'IPv4+ par rapport à IPv4
 - 20.9.5. Avantages d'IPv6 par rapport à IPv4
- 20.10. Le défi de la sensibilisation de la population à l'éducation précoce et continue
 - 20.10.1. Stratégies gouvernementales actuelles
 - 20.10.2. Résistance de la population à l'apprentissage
 - 20.10.3. Des plans de formation à adopter par les entreprises

“ Vous apprendrez à travers des cas réels conçus dans des environnements d'apprentissage simulés qui reflètent les défis actuels en matière de gestion des données et de cybersécurité ”

04 Objectifs

L'objectif principal du Mastère Avancé en Gestion Sécurisée de l'Information est de fournir aux étudiants d'excellentes connaissances dans deux domaines fondamentaux et complémentaires de l'informatique et de l'ingénierie: la gestion des données dans les environnements numériques et la cybersécurité. Ce programme combine les deux disciplines pour former des professionnels à la mise en œuvre de solutions avancées, leur permettant de faire face aux défis du travail avec les outils nécessaires pour gérer et protéger les informations sensibles dans leurs organisations.



“

Transformez votre carrière avec ce Mastère Avancé innovant, conçu pour marquer un avant et un après dans votre spécialisation en gestion des données et cybersécurité”



Objectifs généraux

- ♦ Développe des compétences avancées en matière d'analyse de données et de cybersécurité afin d'optimiser les processus opérationnels à l'aide d'outils et de techniques innovants
- ♦ Met en œuvre des stratégies de sécurité efficaces pour prévenir les menaces numériques pesant sur les systèmes, les réseaux et les appareils mobiles
- ♦ Résout les problèmes de cybersécurité par l'audit, la rétro-ingénierie et la criminalistique fondée sur des preuves
- ♦ Anticipe les tendances technologiques en appliquant des solutions de rupture qui protègent les actifs numériques et les systèmes avancés



Dirigez la gestion des données et la cybersécurité dans l'environnement numérique avec ce programme de spécialisation"





Objectifs spécifiques

Module 1. L'analyse des données dans l'organisation de l'entreprise

- ♦ Développer des compétences dans l'utilisation des techniques d'analyse des données
- ♦ Générer des informations précieuses qui orientent la prise de décision stratégique dans les organisations commerciales, en améliorant l'efficacité et la compétitivité

Module 2. Gestion des données et des informations, manipulation des données et informations pour la Science des Données

- ♦ Former à la gestion et à la manipulation efficaces de grands volumes de données
- ♦ Appliquer des méthodologies et des outils pour structurer, nettoyer et transformer les données en informations utiles pour les projets de science des données

Module 3. Dispositifs et plateformes IoT comme base de la Science des Données

- ♦ Fournir les connaissances nécessaires sur les plateformes et les dispositifs de l'Internet des Objets et leur intégration dans la science des données
- ♦ Approfondir la capture, le traitement et l'analyse des données en temps réel

Module 4. Représentation graphique pour l'analyse des données

- ♦ Représenter les données sous forme graphique à l'aide d'outils et de techniques de visualisation avancés
- ♦ Faciliter la compréhension des modèles, des tendances et des relations au sein de grands ensembles de données

Module 5. Outils de science des données

- ♦ Former à l'utilisation d'outils et de logiciels spécifiques à la science des données, tels que Python
- ♦ Approfondir la collecte, l'analyse et la présentation des données dans une variété de contextes professionnels

Module 6. Extraction de données. Sélection, prétraitement et transformation

- ♦ Fournir les connaissances et les compétences nécessaires pour appliquer les techniques d'exploration de données
- ♦ Analyser la sélection, le prétraitement et la transformation des données afin d'extraire des modèles et des tendances significatifs

Module 7. Prévisibilité et analyse des phénomènes stochastiques

- ♦ Développer des compétences en matière de modélisation et d'analyse des phénomènes stochastiques
- ♦ Utiliser des méthodes statistiques avancées pour prédire le comportement et les tendances dans des environnements incertains et dynamiques

Module 8. Conception et développement de systèmes intelligents

- ♦ Se former à la conception et au développement de systèmes intelligents, en intégrant des techniques d'apprentissage automatique et d'intelligence artificielle
- ♦ Créer des solutions automatisées qui résolvent efficacement des problèmes complexes

Module 9. Systèmes et architectures à forte intensité de données

- ♦ Fournir des connaissances sur la création d'architectures de systèmes capables de traiter efficacement de grands volumes de données
- ♦ Utiliser des technologies avancées telles que les bases de données distribuées et le traitement parallèle

Module 10. Application pratique de la science des données dans les secteurs d'activité

- ♦ Développer la capacité à appliquer les pratiques de la science des données dans divers secteurs d'activité
- ♦ Intégrer les connaissances acquises pour améliorer la prise de décision, l'optimisation des processus et l'innovation dans l'entreprise



Module 11. Cyber intelligence et cybersécurité

- ♦ Fournir les connaissances et les compétences nécessaires pour appliquer les techniques de cyberespionnage et de cybersécurité
- ♦ Protéger les systèmes et les réseaux de l'entreprise contre les cybermenaces et garantir l'intégrité des données

Module 12. Sécurité de l'Hôte

- ♦ Former à la mise en œuvre des mesures de sécurité sur les systèmes hôtes
- ♦ Assurer la protection des serveurs et des applications critiques par l'utilisation d'outils de sécurité informatique et de bonnes pratiques

Module 13. Sécurité des réseaux (périmètre)

- ♦ Fournir des connaissances sur la protection des réseaux et des systèmes informatiques au niveau du périmètre
- ♦ Gérer les pare-feux, les VPN et d'autres outils pour assurer la sécurité de l'infrastructure du réseau de l'entreprise

Module 14. La sécurité sur les smartphones

- ♦ Développer des compétences pour assurer la sécurité des appareils mobiles
- ♦ Comprendre les vulnérabilités courantes et appliquer des mesures préventives pour protéger les informations et les applications sur les smartphones

Module 15. Sécurité IoT

- ♦ Fournir les connaissances nécessaires pour mettre en œuvre des solutions de sécurité pour les dispositifs IoT
- ♦ Protéger les réseaux et les systèmes interconnectant les dispositifs et assurer la confidentialité et l'intégrité des données générées

Module 16. Piratage éthique

- ♦ Former aux pratiques de hacking éthique, enseigner comment effectuer des tests de pénétration contrôlés
- ♦ Identifier les vulnérabilités des systèmes informatiques afin d'améliorer la sécurité avant qu'elles ne soient exploitées par des attaquants

Module 17. Ingénierie inverse

- ♦ Fournir une connaissance des techniques de rétro-ingénierie, permettant d'analyser et de comprendre le fonctionnement des logiciels et du hardware
- ♦ Détecter les failles de sécurité ou améliorer la fonctionnalité des systèmes existants

Module 18. Développement sécurisé

- ♦ Former au développement sécurisé de logiciels, en enseignant les bonnes pratiques de codage et de sécurité pendant le cycle de vie du logiciel
- ♦ Être capable de prévenir les vulnérabilités et de protéger les systèmes informatiques contre les attaques

Module 19. Analyse médico-légale

- ♦ Développer les compétences nécessaires pour mener des enquêtes de police scientifique numérique
- ♦ Utiliser des outils et des techniques avancés pour récupérer, analyser et préserver les preuves électroniques lors d'incidents de sécurité informatique

Module 20. Défis actuels et futurs en matière de sécurité informatique

- ♦ Explorer les défis actuels et futurs dans le domaine de la sécurité informatique, en analysant les menaces émergentes et les nouvelles technologies de protection
- ♦ Examiner les stratégies visant à atténuer les risques dans un environnement technologique en constante évolution

05

Opportunités de carrière

À l'issue de ce Mastère Avancé en Gestion Sécurisée de l'Information, les professionnels auront acquis une solide compréhension des stratégies les plus avancées en matière de cybersécurité et de gestion des données numériques. Les diplômés seront préparés à concevoir et à mettre en œuvre des solutions qui garantissent la protection des informations sensibles et optimisent les processus d'analyse et de prise de décision dans les environnements professionnels. Ils amélioreront ainsi leurs perspectives d'emploi et occuperont des fonctions spécialisées en tant qu'analystes en cybersécurité, consultants en intelligence ou gestionnaires de données critiques.



“

*Vous assurerez la sécurité des actifs numériques
et jouerez un rôle clé dans la transformation
numérique des organisations”*

Profil des diplômés

Les diplômés du Mastère Avancé en Gestion Sécurisée de l'Information seront des professionnels hautement qualifiés pour gérer et protéger les informations dans les environnements numériques. Ils posséderont des connaissances avancées dans des domaines tels que la cybersécurité, l'intelligence numérique et l'analyse de données, ainsi que des compétences pratiques dans la conception et la mise en œuvre de stratégies de défense contre les menaces. Leur profil combine des connaissances techniques approfondies et des compétences stratégiques qui leur permettront de diriger des projets dans des secteurs d'activité clés.

Vous deviendrez un leader en matière de protection des données et de cybersécurité, en collaborant avec les entreprises pour relever les défis de l'environnement numérique.

- ♦ **Gestion de la sécurité:** Développer la capacité à identifier les risques, à mettre en œuvre des stratégies de défense multicouches et à garantir la confidentialité, l'intégrité et la disponibilité des données
- ♦ **Analyse critique et résolution de problèmes:** Vous appliquerez des techniques avancées pour évaluer les systèmes, détecter les vulnérabilités et concevoir des solutions adaptées à différents environnements technologiques
- ♦ **Compétences techniques et numériques:** Vous manierez des outils avancés pour l'analyse des données, la cybersécurité et les systèmes de renseignement, ce qui vous permettra de mener des projets d'innovation technologique
- ♦ **Réflexion stratégique:** Vous concevrez des politiques de sécurité et des stratégies commerciales qui répondent aux exigences actuelles et futures de l'environnement numérique
- ♦ **Collaboration interdisciplinaire:** Vous travaillerez avec des équipes multidisciplinaires pour relever des défis complexes et assurer la sécurité sur les réseaux, les plateformes IoT et les appareils mobiles



À l'issue de ce Mastère Avancé, vous serez en mesure d'utiliser vos connaissances et vos compétences pour occuper les postes suivants:

1. **Directeur de la Cybersécurité:** Responsable de la coordination des équipes et de la conception des stratégies de protection des actifs numériques dans les grandes organisations
2. **Analyste de Données:** Concepteur de systèmes d'analyse prédictive et de visualisation pour optimiser la prise de décision
3. **Consultant en Intelligence Numérique:** Conseiller spécialisé dans l'offre de solutions avancées basées sur l'intelligence et l'analyse des risques
4. **Spécialiste de l'IoT et de la Sécurité:** Concepteur de mesures de protection pour les appareils connectés et les environnements industriels
5. **Hacker Éthique:** Évaluateur de vulnérabilités qui corrige les failles des systèmes d'entreprise pour prévenir les cyberattaques
6. **Auditeur de Sécurité:** Inspecteur réalisant des audits et des analyses médico-légales pour assurer la conformité réglementaire
7. **Gestionnaire de Données d'Entreprise:** Administrateur chargé de concevoir et de gérer des systèmes de stockage et d'analyse afin d'améliorer l'efficacité opérationnelle

“

En suivant ce programme, vous vous distinguerez en tant que spécialiste dans les domaines les plus demandés de l'environnement numérique”

06

Méthodologie d'étude

TECH Euromed University est la première au monde à combiner la méthodologie des **case studies** avec **Relearning**, un système d'apprentissage 100% en ligne basé sur la répétition guidée.

Cette stratégie d'enseignement innovante est conçue pour offrir aux professionnels la possibilité d'actualiser leurs connaissances et de développer leurs compétences de manière intensive et rigoureuse. Un modèle d'apprentissage qui place l'étudiant au centre du processus académique et lui donne le rôle principal, en s'adaptant à ses besoins et en laissant de côté les méthodologies plus conventionnelles.



“

*TECH Euromed University vous prépare
à relever de nouveaux défis dans des
environnements incertains et à réussir
votre carrière”*

L'étudiant: la priorité de tous les programmes de TECH Euromed University

Dans la méthodologie d'étude de TECH Euromed University, l'étudiant est le protagoniste absolu.

Les outils pédagogiques de chaque programme ont été sélectionnés en tenant compte des exigences de temps, de disponibilité et de rigueur académique que demandent les étudiants d'aujourd'hui et les emplois les plus compétitifs du marché.

Avec le modèle éducatif asynchrone de TECH Euromed University, c'est l'étudiant qui choisit le temps qu'il consacre à l'étude, la manière dont il décide d'établir ses routines et tout cela dans le confort de l'appareil électronique de son choix. L'étudiant n'a pas besoin d'assister à des cours en direct, auxquels il ne peut souvent pas assister. Les activités d'apprentissage se dérouleront à votre convenance. Vous pouvez toujours décider quand et où étudier.

“

À TECH Euromed University, vous n'aurez PAS de cours en direct (auxquelles vous ne pourrez jamais assister)”



Les programmes d'études les plus complets au niveau international

TECH Euromed University se caractérise par l'offre des itinéraires académiques les plus complets dans l'environnement universitaire. Cette exhaustivité est obtenue grâce à la création de programmes d'études qui couvrent non seulement les connaissances essentielles, mais aussi les dernières innovations dans chaque domaine.

Grâce à une mise à jour constante, ces programmes permettent aux étudiants de suivre les évolutions du marché et d'acquérir les compétences les plus appréciées par les employeurs. Ainsi, les diplômés de TECH Euromed University reçoivent une préparation complète qui leur donne un avantage concurrentiel significatif pour progresser dans leur carrière.

De plus, ils peuvent le faire à partir de n'importe quel appareil, PC, tablette ou smartphone.

“

Le modèle de TECH Euromed University est asynchrone, de sorte que vous pouvez étudier sur votre PC, votre tablette ou votre smartphone où vous voulez, quand vous voulez et aussi longtemps que vous le voulez”

Case studies ou Méthode des cas

La méthode des cas est le système d'apprentissage le plus utilisé par les meilleures écoles de commerce du monde. Développée en 1912 pour que les étudiants en Droit n'apprennent pas seulement le droit sur la base d'un contenu théorique, sa fonction était également de leur présenter des situations réelles et complexes. De cette manière, ils pouvaient prendre des décisions en connaissance de cause et porter des jugements de valeur sur la manière de les résoudre. Elle a été établie comme méthode d'enseignement standard à Harvard en 1924.

Avec ce modèle d'enseignement, ce sont les étudiants eux-mêmes qui construisent leurs compétences professionnelles grâce à des stratégies telles que *Learning by doing* ou le *Design Thinking*, utilisées par d'autres institutions renommées telles que Yale ou Stanford.

Cette méthode orientée vers l'action sera appliquée tout au long du parcours académique de l'étudiant avec TECH Euromed University. Vous serez ainsi confronté à de multiples situations de la vie réelle et devrez intégrer des connaissances, faire des recherches, argumenter et défendre vos idées et vos décisions. Il s'agissait de répondre à la question de savoir comment ils agiraient lorsqu'ils seraient confrontés à des événements spécifiques complexes dans le cadre de leur travail quotidien.



Méthode Relearning

À TECH Euromed University, les *case studies* sont complétées par la meilleure méthode d'enseignement 100% en ligne: le *Relearning*.

Cette méthode s'écarte des techniques d'enseignement traditionnelles pour placer l'apprenant au centre de l'équation, en lui fournissant le meilleur contenu sous différents formats. De cette façon, il est en mesure de revoir et de répéter les concepts clés de chaque matière et d'apprendre à les appliquer dans un environnement réel.

Dans le même ordre d'idées, et selon de multiples recherches scientifiques, la répétition est le meilleur moyen d'apprendre. C'est pourquoi TECH Euromed University propose entre 8 et 16 répétitions de chaque concept clé au sein d'une même leçon, présentées d'une manière différente, afin de garantir que les connaissances sont pleinement intégrées au cours du processus d'étude.

Le Relearning vous permettra d'apprendre plus facilement et de manière plus productive tout en développant un esprit critique, en défendant des arguments et en contrastant des opinions: une équation directe vers le succès.



Un Campus Virtuel 100% en ligne avec les meilleures ressources didactiques

Pour appliquer efficacement sa méthodologie, TECH Euromed University se concentre à fournir aux diplômés du matériel pédagogique sous différents formats: textes, vidéos interactives, illustrations et cartes de connaissances, entre autres. Tous ces supports sont conçus par des enseignants qualifiés qui axent leur travail sur la combinaison de cas réels avec la résolution de situations complexes par la simulation, l'étude de contextes appliqués à chaque carrière professionnelle et l'apprentissage basé sur la répétition, par le biais d'audios, de présentations, d'animations, d'images, etc.

Les dernières données scientifiques dans le domaine des Neurosciences soulignent l'importance de prendre en compte le lieu et le contexte d'accès au contenu avant d'entamer un nouveau processus d'apprentissage. La possibilité d'ajuster ces variables de manière personnalisée aide les gens à se souvenir et à stocker les connaissances dans l'hippocampe pour une rétention à long terme. Il s'agit d'un modèle intitulé *Neurocognitive context-dependent e-learning* qui est sciemment appliqué dans le cadre de ce diplôme d'université.

D'autre part, toujours dans le but de favoriser au maximum les contacts entre mentors et mentorés, un large éventail de possibilités de communication est offert, en temps réel et en différé (messagerie interne, forums de discussion, service téléphonique, contact par courrier électronique avec le secrétariat technique, chat et vidéoconférence).

De même, ce Campus Virtuel très complet permettra aux étudiants TECH Euromed University d'organiser leurs horaires d'études en fonction de leurs disponibilités personnelles ou de leurs obligations professionnelles. De cette manière, ils auront un contrôle global des contenus académiques et de leurs outils didactiques, mis en fonction de leur mise à jour professionnelle accélérée.



Le mode d'étude en ligne de ce programme vous permettra d'organiser votre temps et votre rythme d'apprentissage, en l'adaptant à votre emploi du temps"

L'efficacité de la méthode est justifiée par quatre acquis fondamentaux:

1. Les étudiants qui suivent cette méthode parviennent non seulement à assimiler les concepts, mais aussi à développer leur capacité mentale au moyen d'exercices pour évaluer des situations réelles et appliquer leurs connaissances.
2. L'apprentissage est solidement traduit en compétences pratiques ce qui permet à l'étudiant de mieux s'intégrer dans le monde réel.
3. L'assimilation des idées et des concepts est rendue plus facile et plus efficace, grâce à l'utilisation de situations issues de la réalité.
4. Le sentiment d'efficacité de l'effort investi devient un stimulus très important pour les étudiants, qui se traduit par un plus grand intérêt pour l'apprentissage et une augmentation du temps passé à travailler sur le cours.

La méthodologie universitaire la mieux évaluée par ses étudiants

Les résultats de ce modèle académique innovant sont visibles dans les niveaux de satisfaction générale des diplômés de TECH Euromed University.

L'évaluation par les étudiants de la qualité de l'enseignement, de la qualité du matériel, de la structure et des objectifs des cours est excellente. Sans surprise, l'institution est devenue l'université la mieux évaluée par ses étudiants sur la plateforme d'évaluation Global Score, avec une note de 4,9 sur 5.

Accédez aux contenus de l'étude depuis n'importe quel appareil disposant d'une connexion Internet (ordinateur, tablette, smartphone) grâce au fait que TECH Euromed University est à la pointe de la technologie et de l'enseignement.

Vous pourrez apprendre grâce aux avantages offerts par les environnements d'apprentissage simulés et à l'approche de l'apprentissage par observation: le Learning from an expert.



Ainsi, le meilleur matériel pédagogique, minutieusement préparé, sera disponible dans le cadre de ce programme:



Matériel didactique

Tous les contenus didactiques sont créés par les spécialistes qui enseignent les cours. Ils ont été conçus en exclusivité pour le programme afin que le développement didactique soit vraiment spécifique et concret.

Ces contenus sont ensuite appliqués au format audiovisuel afin de mettre en place notre mode de travail en ligne, avec les dernières techniques qui nous permettent de vous offrir une grande qualité dans chacune des pièces que nous mettrons à votre service.



Pratique des aptitudes et des compétences

Vous effectuerez des activités visant à développer des compétences et des aptitudes spécifiques dans chaque domaine. Pratiques et dynamiques permettant d'acquérir et de développer les compétences et les capacités qu'un spécialiste doit acquérir dans le cadre de la mondialisation dans laquelle nous vivons.



Résumés interactifs

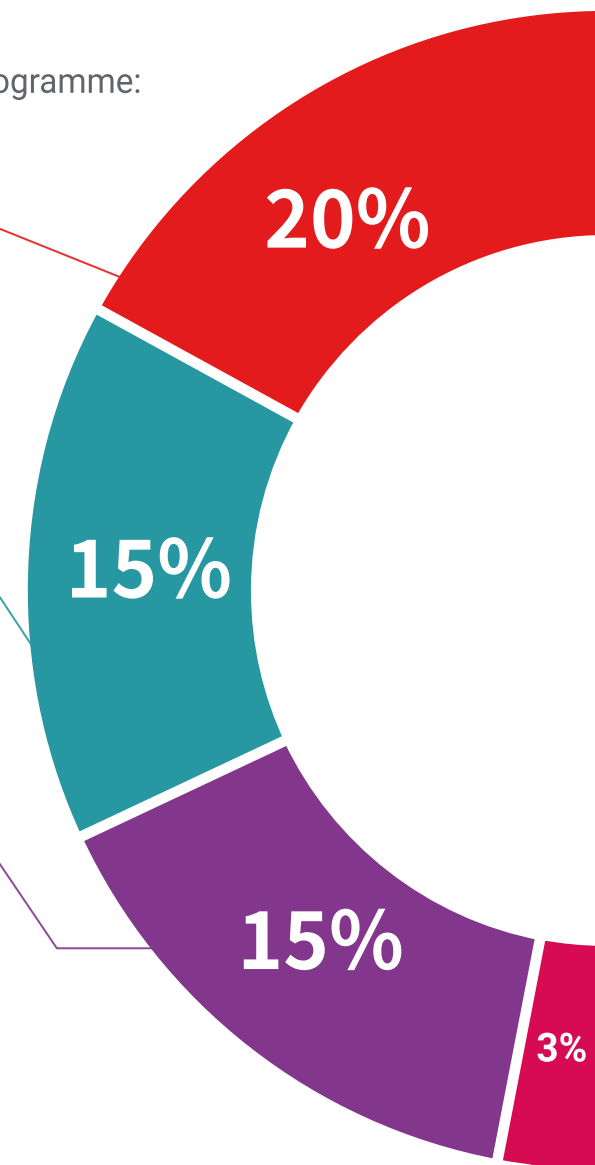
Nous présentons les contenus de manière attrayante et dynamique dans des dossiers multimédias qui incluent de l'audio, des vidéos, des images, des diagrammes et des cartes conceptuelles afin de consolider les connaissances.

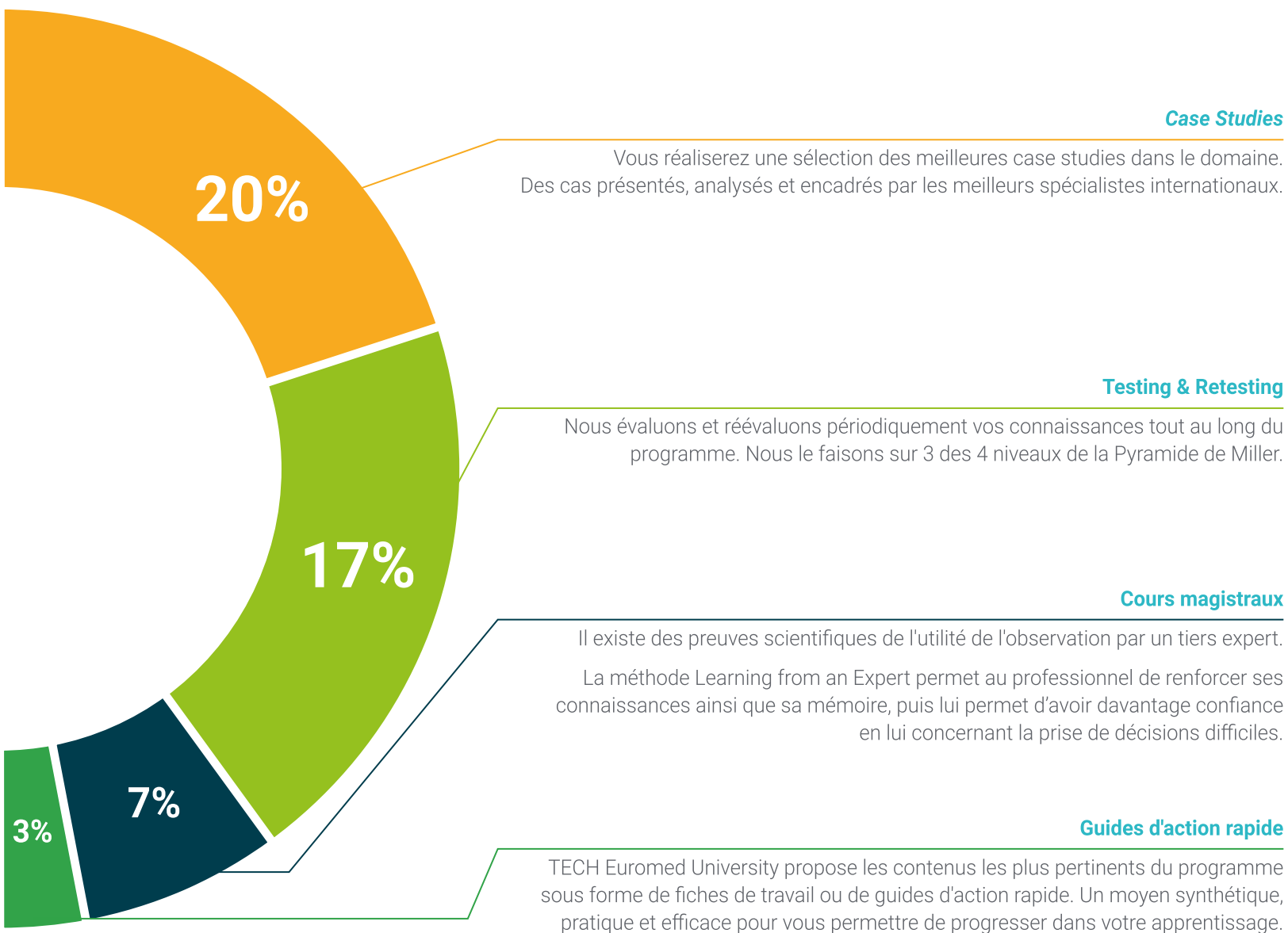
Ce système éducatif unique de présentation de contenu multimédia a été récompensé par Microsoft en tant que «European Success Story».



Lectures complémentaires

Articles récents, documents de consensus, guides internationaux, etc... Dans notre bibliothèque virtuelle, vous aurez accès à tout ce dont vous avez besoin pour compléter votre formation.





07

Corps Enseignant

Ce diplôme est enseigné par des professionnels de premier plan dans le domaine de la cybersécurité et de la gestion des données numériques. Leur expérience garantit aux étudiants un contenu complet et actualisé, directement applicable à leur carrière. Ainsi, les enseignants de ce Mastère Avancé en Gestion Sécurisée de l'Information partagent leurs connaissances, formant des spécialistes hautement qualifiés qui sont recherchés par les grandes entreprises internationales.





“

*Réussissez avec les meilleurs et acquérez
les connaissances et les compétences clés
pour diriger la gestion des données et la
cybersécurité dans l'environnement numérique"*

Directeur International Invité

Le Docteur Frédéric Lemieux est internationalement reconnu comme un expert innovant et un leader inspirant dans les domaines du **Renseignement**, de la **Sécurité Nationale**, de la **Sécurité Intérieure**, de la **Cybersécurité** et des **Technologies Disruptives**. Son dévouement constant et ses contributions pertinentes à la Recherche et à l'Éducation font de lui une figure clé de la promotion de la sécurité et de la compréhension des technologies émergentes d'aujourd'hui. Au cours de sa carrière professionnelle, il a conceptualisé et dirigé des programmes académiques de pointe dans plusieurs institutions renommées, telles que l'Université de Montréal, l'Université George Washington et l'Université de Georgetown.

Tout au long de son parcours, il a publié de nombreux ouvrages très pertinents, tous liés au **renseignement criminel**, au **maintien de l'ordre**, aux **cybermenaces** et à la **sécurité internationale**. Il a également contribué de manière significative au domaine de la Cybersécurité en publiant de nombreux articles dans des revues universitaires, qui traitent de la lutte contre la criminalité lors de catastrophes majeures, de la lutte contre le terrorisme, des agences de renseignement et de la coopération policière. En outre, il a participé en tant que panéliste et orateur principal à diverses conférences nationales et internationales, s'imposant ainsi comme un universitaire et un praticien de premier plan.

Le Docteur Lemieux a occupé des fonctions éditoriales et d'évaluation dans diverses organisations universitaires, privées et gouvernementales, ce qui témoigne de son influence et de son engagement en faveur de l'excellence dans son domaine d'expertise. Ainsi, sa prestigieuse carrière universitaire l'a amené à être Professeur de Pratiques et Directeur de la Faculté des programmes MPS en **Intelligence Appliquée**, **Gestion des Risques de Cybersécurité**, **Gestion de la Technologie** et **Gestion des Technologies de l'Information**, à l'Université de Georgetown.



Dr Lemieux, Frederic

- Directeur du Master en Cybersecurity Risk Management à l'Université de Georgetown, Washington, États-Unis
- Directeur du Master en Technology Management à l'Université de Georgetown
- Directeur du Master en Applied Intelligence à l'Université de Georgetown
- Professeur de Stages Pratiques à l'Université de Georgetown
- Doctorat en Criminologie de la School of Criminology de l'Université de Montréal
- Licence en Sociologie et Minor Degree en Psychologie de l'Université de Laval
- Membre de: New Program Roundtable Committee, Université de Georgetown

“

Grâce à TECH, vous pourrez apprendre avec les meilleurs professionnels du monde"

Direction



Dr Peralta Martín-Palomino, Arturo

- CEO et CTO de Prometeus Global Solutions
- CTO chez Korporate Technologies
- CTO de AI Shepherds GmbH
- Consultant et Conseiller Stratégique auprès d'Alliance Medical
- Directeur de la Conception et du Développement chez DocPath
- Doctorat en Ingénierie Informatique de l'Université de Castille-La Manche
- Doctorat en Économie, Commerce et Finances de l'Université Camilo José Cela
- Doctorat en Psychologie de l'Université de Castille -La Manche
- Master en Executive MBA de l'Université Isabel I
- Master en Gestion Commerciale et Marketing de l'Université Isabel I
- Master en Big Data par Formation Hadoop
- Master en Technologies Avancées de l'Information de l' Université de Castille La Manche
- Membre du Groupe de Recherche SMILE



Mme Fernández Sapena, Sonia

- Formatrice en Sécurité Informatique et Piratage Éthique au Centre de Référence Nationale pour l'Informatique et les Télécommunications à Getafe à Madrid
- Instructrice agréée E-Council
- Formatrice dans les certifications suivantes: EXIN Ethical Hacking Foundation et EXIN Cyber & IT Security Foundation. Madrid
- Formatrice experte accréditée par la CAM pour les certificats professionnels suivants: Sécurité Informatique (IFCT0190), Gestion des Réseaux de Voix et de données (IFCM0310), Administration des Réseaux départementaux (IFCT0410), Gestion des Alarmes de réseaux de télécommunications (IFCM0410), Opérateur de Réseaux de voix et données (IFCM0110), et Administration des services internet (IFCT0509)
- Collaboratrice externe CSO/SSA (*Chief Security Officer/Senior Security Architect*) à l'Université des Iles Baléares
- Ingénieure en Informatique de l'Université d'Alcalá de Henares de Madrid
- Master en DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Technologies. E-Council

Professeurs

M. Montoro Montarroso, Andrés

- ♦ Chercheur dans le groupe SMILe de l' Université de Castille La Manche
- ♦ Chercheur à l'Université de Grenade
- ♦ Data Scientist chez Prometeus Global Solutions
- ♦ Vice-président et Software Developer chez CireBits
- ♦ Doctorat en Technologies Avancées de l'Information de l'Université de Castille La Manche
- ♦ Diplôme d'Ingénieur en Informatique de l'Université de Castilla-La Mancha
- ♦ Master en science des données et ingénierie informatique de l'Université de Grenade
- ♦ Professeur invité dans le domaine des Systèmes Fondés sur la Connaissance de l'École Supérieure d'Informatique de Ciudad Real, donnant la conférence: *Techniques Avancées d'Intelligence Artificielle: Recherche et analyse des radicaux potentiels sur les Médias Sociaux*
- ♦ Professeur invité dans la matière d'Exploration de Données de l'École Supérieure d'Informatique de Ciudad Real, donnant la conférence: *Applications de Traitement du Langage Naturel: Logique floue l'analyse des messages sur les réseaux sociaux*
- ♦ Intervenant au Séminaire sur la Prévention de la Corruption dans les Administrations Publiques et Intelligence Artificielle à la Faculté des Sciences Juridiques et Sociales de Tolède, donnant la conférence: *Techniques d'Intelligence Artificielle*
- ♦ Intervenant au premier Séminaire International sur le Droit Administratif et l'Intelligence artificielle (DAIA). Organisé par le Centre d'Études Européennes Luis Ortega Álvarez et l'Institut de Recerca TransJus. Conférence intitulée *Analyse des Sentiments pour la prévention des messages de haine sur les réseaux sociaux*

M. Peris Morillo, Luis Javier

- ♦ Senior Technical Lead et Delivery Lead Support chez HCL Technologies
- ♦ Rédacteur technique chez Baelung
- ♦ Agile Coach et directeur des Opérations chez Mirai Advisory

- ♦ Développeur, Team Lead, Scrum Master, Agile Coach, Product Manager chez DocPath
- ♦ Technologue chez ARCO
- ♦ Diplôme d'Ingénieur Supérieur en Informatique de l'Université de Castille-La Manche
- ♦ Diplôme Supérieur en Gestion de Projets de la CEOE

Mme Fernández Meléndez, Galina

- ♦ Spécialiste en Big Data
- ♦ Analyste de Données chez Aresi Gestión de Fincas
- ♦ Analyste de Données chez ADN Mobile Solution
- ♦ Licence en Administration des Affaires de l'Université Bicentenario de Aragua Caracas, Venezuela
- ♦ Diplôme en Planification et Finances Publiques de l'École de Planification du Venezuela
- ♦ Master en Analyse des Données et Intelligence Économique de l'Université d'Oviedo
- ♦ MBA en Administration et Direction des Entreprises de l'École de Commerce Européenne de Barcelone
- ♦ Master en Big Data et Business Intelligence de l'École de Commerce Européenne de Barcelone

Mme Pedrajas Parabá, María Elena

- ♦ New Technologies and Digital Transformation Consultant chez Management Solutions
- ♦ Chercheuse au Département d' Informatique et d' Analyse Numérique de l' Université de Cordoue
- ♦ Chercheuse au Centre Singulier de Recherche en Technologies Intelligentes à Saint-Jacques de Compostelle
- ♦ Licence en Génie Informatique de l'Université de Cordoue
- ♦ Master en science des données et ingénierie informatique de l'Université de Grenade
- ♦ Master en Conseil en Affaires de l'Université Pontificiale Comillas

Mme Martínez Cerrato, Yésica

- ♦ Responsable des Formations Techniques chez Securitas Security Espagne
- ♦ Spécialiste en Éducation, affaires et Marketing
- ♦ *Product Manager* en Sécurité Électronique chez Securitas Seguridad España
- ♦ Analyste en Intelligence Économique chez Ricopia Technologies
- ♦ Technicienne Informatique et Responsable des Salles informatiques de l'OTEC à l'Université d'Alcalá de Henares
- ♦ Collaboratrice de l'Association ASALUMA
- ♦ Diplôme d'Ingénieur en Électronique des Communications de l'École Polytechnique Supérieure de l'Université d'Alcalá de Henares

M. Fondón Alcalde, Rubén

- ♦ Analyste EMEA d'Amazon Web Services
- ♦ Analyste Commercial en Gestion de la Valeur Client chez Vodafone Espagne
- ♦ Responsable de l'Intégration des Services chez Entelgy pour Telefónica Global Solutions
- ♦ Responsable du compte Clone Server Online chez EDM Electronics
- ♦ Responsable de la Mise en œuvre des Services Internationaux chez Vodafone Global Enterprise
- ♦ Consultant en Solutions pour l'Espagne et le Portugal chez Telvent Global Services
- ♦ Analyste Commercial pour l'Europe du Sud chez Vodafone Global Enterprise
- ♦ Ingénieur en télécommunications de l'Université européenne de Madrid
- ♦ Master en Big Data et analyse de l'Université internationale de Valence

M. Díaz Díaz-Chirón, Tobías

- ♦ Chercheur dans le Laboratoire ArCO de l' Université de Castille (La Manche)
- ♦ Consultant chez Blue Telecom
- ♦ Freelance principalement dédié au secteur des télécommunications, spécialisé dans les réseaux 4G/5G
- ♦ OpenStack: déploiement et administration
- ♦ Ingénieur Supérieur en Informatique de l' Université de Castille La Manche
- ♦ Spécialisation en Architecture et réseaux informatiques
- ♦ Enseignant associé à l'Université de Castille- La Manche
- ♦ Conférencier dans le cours Sepecam sur l'administration des réseaux

M. Tato Sánchez, Rafael

- ♦ Directeur Technique chez Indra Sistemas SA
- ♦ Ingénieur Systèmes chez ENA TRÁFICO SAU
- ♦ Master en Industrie 4.0 de l'Université sur Internet
- ♦ Master en Génie Industriel de l'Université Européenne
- ♦ Diplôme d'Ingénieur en Électronique Industrielle et Automatique de l'Université Européenne
- ♦ Ingénieur Technique Industriel de l'Université Polytechnique de Madrid

Mme Marcos Sbarbaro, Victoria Alicia

- ◆ Développeuse d'applications mobiles natives Android chez B60. UK
- ◆ Analyste Programmeuse pour la Gestion, la Coordination et la Documentation d'un Environnement Virtualisé d'Alarme de Sécurité
- ◆ Analyste Programmeuse d'Applications Java pour les guichets automatiques bancaires
- ◆ Professionnelle du Développement de *Software* pour une Application de Validation de Signature et de Gestion de Documents
- ◆ Technicienne des Systèmes pour la Migration des Équipements et pour la Gestion, la Maintenance et la Formation des PDA Mobiles
- ◆ Ingénieure Technique en Systèmes Informatiques de l'Université Ouverte de Catalogne
- ◆ Master en Sécurité Informatique et Hacking Éthique Officiel de EC- Council et CompTIA de l'École Professionnelle des Nouvelles Technologies CICE

M. Catalá Barba, José Francisco

- ◆ Technicien en Électronique Expert en Cybersécurité
- ◆ Développeur d'Applications pour Dispositifs Mobiles
- ◆ Technicien en Électronique dans L'Encadrement Intermédiaire au sein du Ministère Espagnol de la Défense
- ◆ Technicien en Électronique à l'Usine Ford Sita à Valence

M. Armero Fernández, Rafael

- ◆ Business Intelligence Consultant chez SDG Group
- ◆ Digital Engineer chez MI-GSO
- ◆ Logistic Engineer chez Torrecid SA
- ◆ Quality Intern chez INDRA
- ◆ Diplôme en Ingénierie Aérospatiale de l'Université Polytechnique de Valence
- ◆ Master en Développement Professionnel 4.0 de l'Université d'Alcalá



M. Peralta Alonso, Jon

- ♦ Consultant Senior de Protection des Données et Cybersécurité à Altia
- ♦ Avocat / Conseiller Juridique chez Arriaga Asociés Conseil Juridique et Économique, S.L
- ♦ Conseiller juridique / Stagiaire dans un Cabinet Professionnel: Oscar Padura
- ♦ Diplôme en Droit de l'Université Publique du Pays Basque
- ♦ Master en Délégué de Protection des Données de l'EIS Innovative School
- ♦ Master en Pratique Juridique de l'Université Publique du Pays Basque
- ♦ Master Spécialiste en Pratique du Contentieux Civil de l'Université Internationale Isabel I de Castille et León
- ♦ Professeur du Master en Protection des Données Personnelles, Cybersécurité et Droit des TIC

M. Redondo, Jesús Serrano

- ♦ Développeur Web et Technicien en Cybersécurité
- ♦ Développeur Web à Roams, Palencia
- ♦ Développeur FrontEnd chez Telefónica, Madrid
- ♦ Développeur FrontEnd chez Best Pro Consulting SL, Madrid
- ♦ Installateur d'Équipements et de Services de Télécommunications chez Groupe Zener, Castille et León
- ♦ Installateur d'Équipements et de Services de Télécommunications chez Lican Comunicaciones SL, Castille et León
- ♦ Certificat en Sécurité Informatique, CFTIC Getafe, Madrid
- ♦ Technicien Supérieur en Télécommunications et Systèmes Informatiques de l'IES Trinidad Arroyo, Palencia
- ♦ Technicien Supérieur en Installations Electrotechniques MT et BT de l'IES Trinidad Arroyo, Palencia
- ♦ Formation en Ingénierie Inverse, Sténographie et Cryptage de Incibe Hacker Academy

M. Jiménez Ramos, Álvaro

- ♦ Analyste en Cybersécurité
- ♦ Analyste Principal de la Sécurité à The Workshop
- ♦ Analyste en Cybersécurité L1 chez Axians
- ♦ Analyste en Cybersécurité L2 chez Axians
- ♦ Analyste en Cybersécurité chez SACYR S.A
- ♦ Diplôme d'Ingénieur en Télématique de l'Université Polytechnique de Madrid
- ♦ Master en Cybersécurité et Hacking Éthique du CICE
- ♦ Cours Avancé en Cybersécurité de la Formation Deusto



Profitez de l'occasion pour vous informer sur les derniers développements dans ce domaine afin de les appliquer à votre pratique quotidienne"

08 Diplôme

Le Mastère Avancé en Gestion Sécurisée de l'Information garantit, outre la formation la plus rigoureuse et la plus actualisée, l'accès à un diplôme de Mastère Avancé délivré par TECH Euromed University.



“

Terminez ce programme avec succès et obtenez votre diplôme universitaire sans avoir à vous déplacer ou à passer par des procédures fastidieuses”

Le programme du **Mastère Avancé en Gestion Sécurisée de l'Information** est le programme le plus complet sur la scène académique actuelle. Après avoir obtenu leur diplôme, les étudiants recevront un diplôme d'université délivré par TECH Global University et un autre par Université Euromed de Fès.

Ces diplômes de formation continue et d'actualisation professionnelle de TECH Global University et d'Université Euromed de Fès garantissent l'acquisition de compétences dans le domaine de la connaissance, en accordant une grande valeur curriculaire à l'étudiant qui réussit les évaluations et accrédite le programme après l'avoir suivi dans son intégralité.

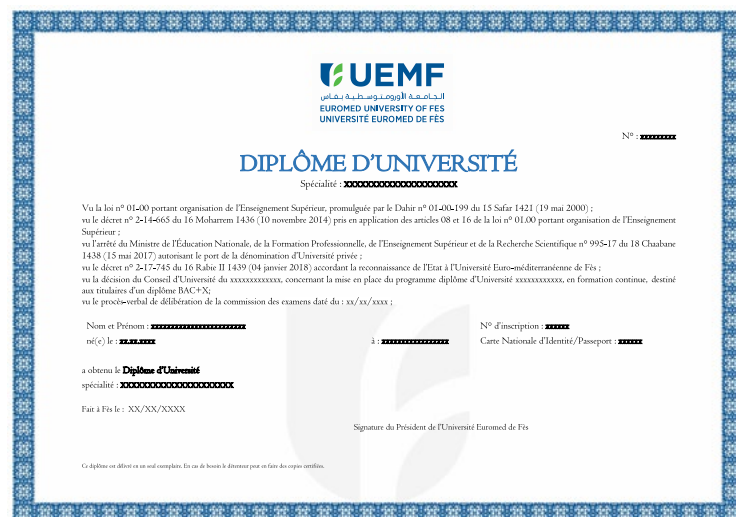
Ce double certificat, de la part de deux institutions universitaires de premier plan, représente une double récompense pour une formation complète et de qualité, assurant à l'étudiant l'obtention d'une certification reconnue au niveau national et international. Ce mérite académique vous positionnera comme un professionnel hautement qualifié, prêt à relever les défis et à répondre aux exigences de votre secteur professionnel.

Diplôme: Mastère Avancé en Gestion Sécurisée de l'Information

Modalité: en ligne

Durée: 2 ans

Accréditation: 120 ECTS



*Si l'étudiant souhaite que son diplôme version papier possède l'Apostille de La Haye, TECH Euromed University fera les démarches nécessaires pour son obtention moyennant un coût supplémentaire.



Mastère Avancé Gestion Sécurisée de l'Information

- » Modalité: en ligne
- » Durée: 2 ans
- » Qualification: TECH Euromed University
- » Accréditation: 120 ECTS
- » Horaire: à votre rythme
- » Examens: en ligne

Mastère Avancé

Gestion Sécurisée de l'Information

