

Mastère Avancé

Science Informatique, Cybersécurité
et Analytique de Données





Mastère Avancé

Science Informatique,
Cybersécurité et
Analytique de Données

- » Modalité: en ligne
- » Durée: 2 ans
- » Qualification: TECH Université Technologique
- » Intensité: 16h/semaine
- » Horaire: à votre rythme
- » Examens: en ligne

Accès au site web: www.techtitute.com/fr/informatique/mastere-avance/mastere-avance-science-informatique-cybersecurite-analytique-donnees

Sommaire

01

Présentation

page 4

02

Objectifs

page 8

03

Compétences

page 20

04

Direction de la formation

page 24

05

Structure et contenu

page 32

06

Méthodologie

page 60

07

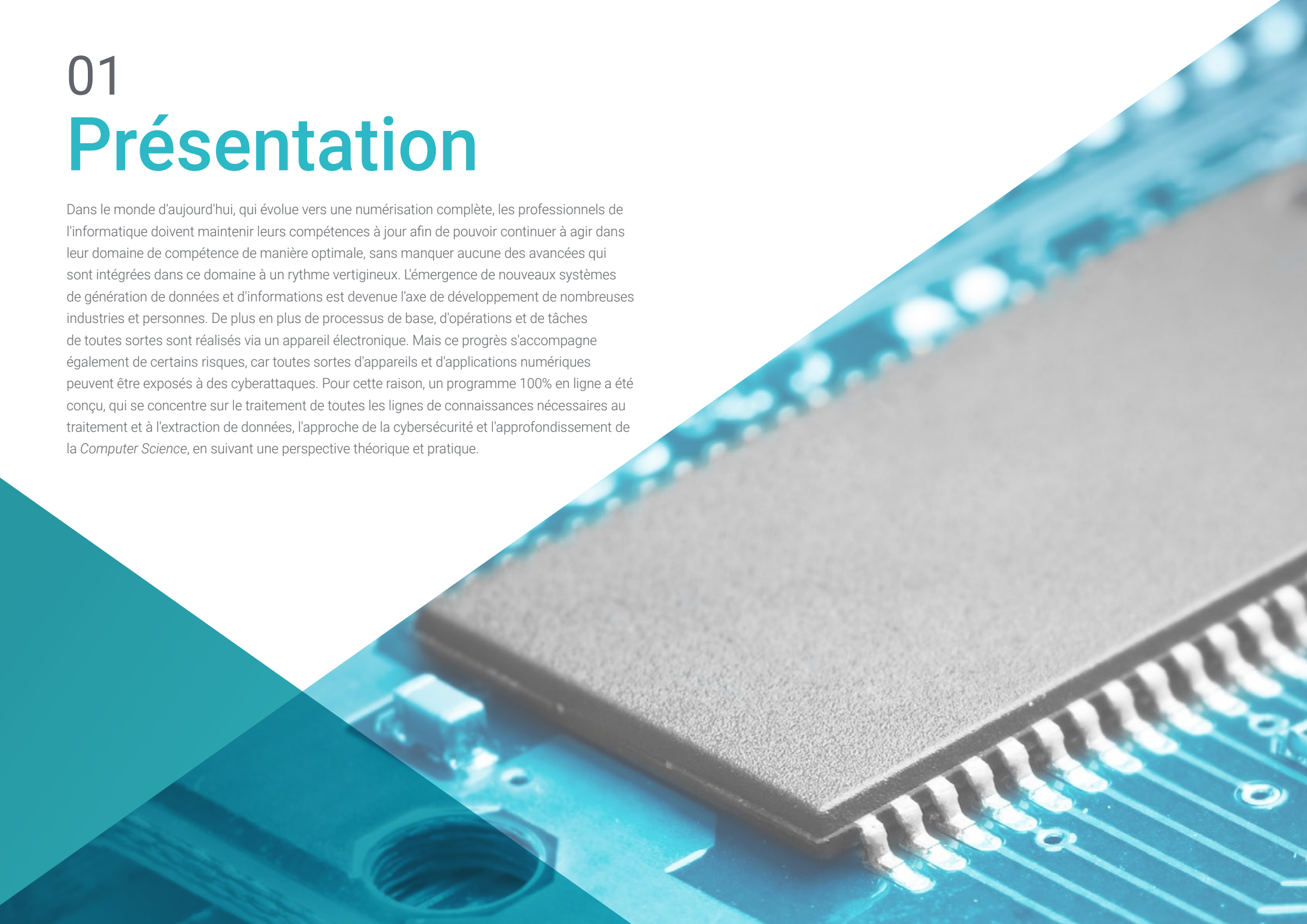
Diplôme

page 68

01

Présentation

Dans le monde d'aujourd'hui, qui évolue vers une numérisation complète, les professionnels de l'informatique doivent maintenir leurs compétences à jour afin de pouvoir continuer à agir dans leur domaine de compétence de manière optimale, sans manquer aucune des avancées qui sont intégrées dans ce domaine à un rythme vertigineux. L'émergence de nouveaux systèmes de génération de données et d'informations est devenue l'axe de développement de nombreuses industries et personnes. De plus en plus de processus de base, d'opérations et de tâches de toutes sortes sont réalisés via un appareil électronique. Mais ce progrès s'accompagne également de certains risques, car toutes sortes d'appareils et d'applications numériques peuvent être exposés à des cyberattaques. Pour cette raison, un programme 100% en ligne a été conçu, qui se concentre sur le traitement de toutes les lignes de connaissances nécessaires au traitement et à l'extraction de données, l'approche de la cybersécurité et l'approfondissement de la *Computer Science*, en suivant une perspective théorique et pratique.



“

Devenez un expert en matière de Cybersécurité en maîtrisant la Science Informatique et l'Analyse des Données, améliorant ainsi considérablement votre employabilité dans un secteur de plus en plus dynamique"

Sous l'impulsion des progrès constants de l'informatique, non seulement la technologie a connu de grandes améliorations, mais aussi les outils numériques mêmes avec lesquels de nombreuses tâches sont effectuées aujourd'hui. Le revers de la médaille est que ces progrès ont également entraîné une augmentation des vulnérabilités informatiques. C'est pourquoi de plus en plus d'entreprises recherchent des professionnels spécialisés dans la cybersécurité, capables de leur fournir une protection adéquate contre tous les types d'attaques informatiques.

Ce programme vous permettra d'approfondir des aspects tels que la sécurité dans le développement et la conception de systèmes, les meilleures techniques cryptographiques ou la sécurité dans les environnements de *Cloud Computing*. Ce programme se concentre également sur les principes fondamentaux de la programmation et de la structure des données, des algorithmes et de la complexité, ainsi que sur la conception avancée d'algorithmes, la programmation avancée, les processeurs de langage et l'infographie, entre autres aspects. Le tout, avec de nombreuses ressources pédagogiques multimédias, dispensé par le corps enseignant le plus prestigieux et le plus spécialisé dans le domaine.

D'autre part, ce diplôme aborde, d'un point de vue technique et commercial, la science des données, en offrant toutes les connaissances nécessaires pour extraire le savoir qui s'y cache. Les informaticiens pourront ainsi analyser en détail les différents algorithmes, les plateformes et les outils les plus récents pour l'exploration, la visualisation, la manipulation, le traitement et l'analyse des données. Tous ces éléments, complétés par le développement de compétences commerciales, sont nécessaires pour atteindre un profil de niveau exécutif capable de prendre des décisions clés dans une entreprise.

Ainsi, cette formation fournit au professionnel les outils et les compétences spécifiques pour développer avec succès son activité professionnelle dans le vaste environnement de l'informatique. En travaillant sur des compétences clés telles que la connaissance de la réalité et de la pratique quotidienne dans différents domaines informatiques et en développant la responsabilité dans le suivi et la supervision de leur travail, ainsi que des compétences spécifiques dans chaque domaine.

Grâce à ce diplôme, les informaticiens pourront se spécialiser dans l'informatique, la cybersécurité et l'analyse des données, ce qui en fait l'occasion idéale d'améliorer leur carrière professionnelle. Tout cela sera tangible grâce à un programme 100% en ligne, qui s'adapte aux besoins quotidiens des professionnels, il suffira donc de disposer d'un appareil avec une connexion internet pour commencer à travailler pour un profil professionnel complet avec une projection internationale.

Ce **Mastère Avancé en Science Informatique, Cybersécurité et Analytique de Données** contient le programme académique le plus complet et le plus actuel du marché. Les principales caractéristiques sont les suivantes:

- ◆ Le développement d'études de cas présentées par des experts en informatique
- ◆ Les contenus graphiques, schématiques et éminemment pratiques avec lesquels ils sont conçus, rassemblent des informations scientifiques et pratiques sur les disciplines indispensables à la pratique professionnelle
- ◆ Les exercices pratiques où le processus d'auto-évaluation peut être réalisé afin d'améliorer l'apprentissage
- ◆ Son accent particulier sur les méthodologies innovantes en matière de Cybersécurité et Analyse des Données
- ◆ Les 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



De manière simple et confortable, acquérir les connaissances nécessaires en Sciences Informatique, Cybersécurité et Analyse de Données pour réaliser une programmation informatique de qualité"

“ *TECH met à votre service un support didactique large et clair, qui intègre tous les sujets d'intérêt actuels, afin que vous puissiez continuer à progresser en informatique*”

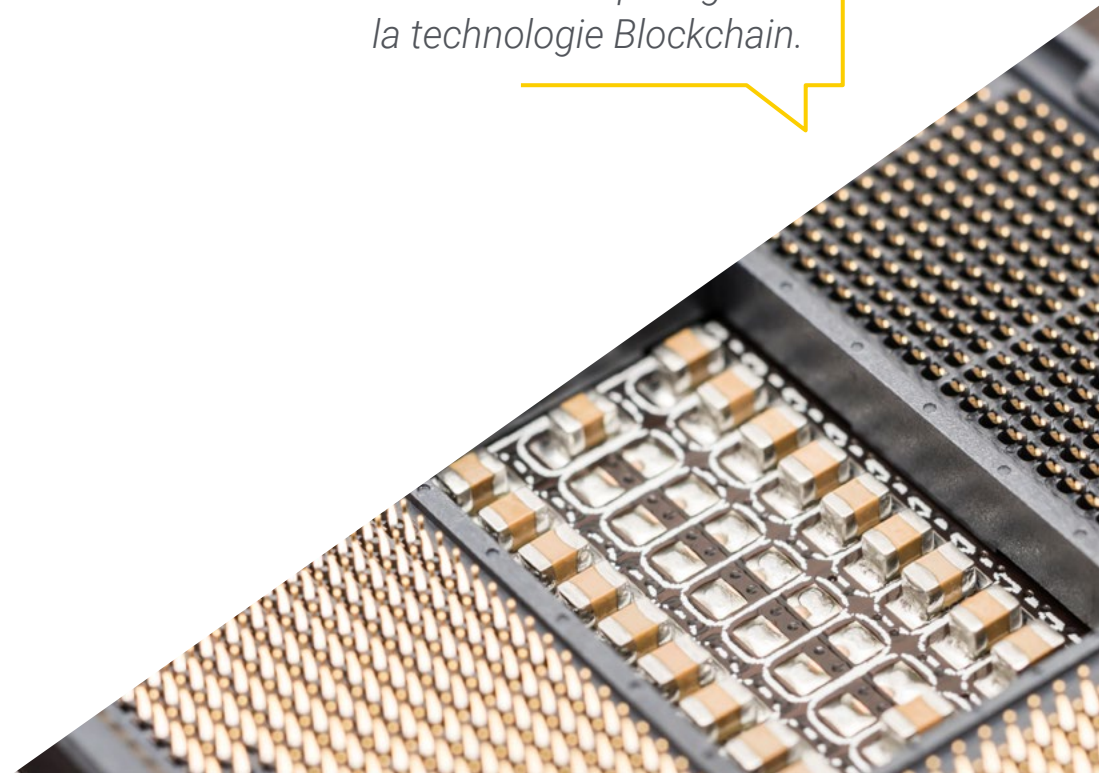
Son corps enseignant comprend des professionnels du domaine de la informatique, qui apportent l'expérience de leur travail à ce programme, ainsi que des spécialistes reconnus issus de grandes entreprises et d'universités prestigieuses.

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 basée sur l'apprentissage par Problèmes. Ainsi l'apprenant devra essayer de résoudre les différentes situations de pratique professionnelle qui se présentent à lui tout au long du Mastère Avancé. Pour ce faire, le professionnel aura l'aide d'un système vidéo interactif innovant créé par des experts reconnus.

Renforcez votre carrière en déterminant la création de tableaux de bord et de KPI en fonction du département dans lequel vous travaillez.

Apprenez, de première main, les meilleures techniques de sécurité appliquées aux environnements de Cloud Computing ou à la technologie Blockchain.



02 Objectifs

Le Mastère Avancé en Science Informatique, Cybersécurité et Analytique de Données a été créé spécifiquement pour l'informaticien qui cherche à progresser dans ce domaine rapidement et avec une réelle qualité. C'est pourquoi un programme a été organisé sur la base d'objectifs réalistes et à forte valeur ajoutée qui vous propulseront à un autre niveau de travail dans ce domaine. Le professionnel se concentrera sur l'étude des différentes techniques, technologies et phases nécessaires à l'informatique, dans une perspective disruptive, complète et actualisée.





“

TECH vous offre une qualification de haute qualité qui vous permettra d'intervenir avec solvabilité dans l'informatique, en garantissant la sécurité de votre entreprise"



Objectifs généraux

- ◆ Être à jour sur le plan scientifique et technologique, ainsi que se préparer à la pratique professionnelle de l'informatique et des langues de manière transversale et polyvalente, adaptée aux nouvelles technologies et aux innovations dans ce domaine
- ◆ Générer des connaissances spécialisées sur un système d'information, les types et les aspects de sécurité qui doivent être pris en compte
- ◆ Identifier les vulnérabilités d'un système d'information
- ◆ Développer les réglementations légales et la typification de la criminalité en s'attaquant à un système d'information
- ◆ Évaluer les différents modèles d'architecture de sécurité afin d'établir le modèle le plus approprié pour l'organisation
- ◆ Identifier les cadres réglementaires d'application et leurs bases réglementaires
- ◆ Analyser la structure organisationnelle et fonctionnelle d'un secteur de sécurité de l'information (le bureau du CISO)
- ◆ Analyser et développer le concept de risque, d'incertitude dans l'environnement dans lequel nous vivons
- ◆ Examiner le modèle de gestion des risques basé sur la norme ISO 31.000
- ◆ Examiner la science de la cryptologie et la relation avec ses branches: cryptographie, cryptanalyse, stéganographie et stégoanalyse
- ◆ Analyser les types de cryptographie en fonction du type d'algorithme et en fonction de son utilisation
- ◆ Examiner les certificats numériques
- ◆ Examiner l'infrastructure à clé publique (ICP)
- ◆ Développer le concept de gestion de l'identité
- ◆ Identifier les méthodes d'authentification
- ◆ Générer des connaissances spécialisées sur l'écosystème de la sécurité informatique
- ◆ Évaluer les connaissances en matière de cybersécurité
- ◆ Identifier les domaines de sécurité dans le *Cloud*
- ◆ Analyser les services et les outils dans chacun des domaines de sécurité
- ◆ Développer les spécifications de sécurité de chaque technologie LPWAN
- ◆ Analyse comparative de la sécurité des technologies LPWAN
- ◆ Analyser les avantages de l'application des techniques d'analyse des données dans chaque département de l'entreprise
- ◆ Développer les bases de la connaissance des besoins et des applications de chaque département
- ◆ Générer des connaissances spécialisées pour sélectionner le bon outil
- ◆ Proposer des techniques et des objectifs pour être le plus productif possible selon le département



Objectifs spécifiques

Module 1. Fondamentaux de la Programmation

- ◆ Comprendre la structure de base d'un ordinateur, les logiciels et les langages de programmation à usage général
- ◆ Apprenez à concevoir et à interpréter des algorithmes, qui constituent la base nécessaire au développement de logiciels
- ◆ Comprendre les éléments essentiels d'un programme informatique, tels que les différents types de données, les opérateurs, les expressions, les instructions, les instructions d'entrée/sortie et de contrôle
- ◆ Comprendre les différentes structures de données disponibles dans les langages de programmation polyvalents, tant statiques que dynamiques, et acquérir les connaissances essentielles pour la manipulation des fichiers
- ◆ Connaître les différentes techniques de test des programmes informatiques et l'importance de générer une bonne documentation en même temps qu'un bon code source
- ◆ Apprendre les bases du langage de programmation C++, l'un des langages de programmation les plus utilisés dans le monde

Module 2. Structure de Données

- ◆ Apprendre les bases de la programmation en langage C++, notamment les classes, les variables, les expressions conditionnelles et les objets
- ◆ Comprendre les types de données abstraits, les types de structures de données linéaires, les structures de données hiérarchiques simples et complexes et leur mise en œuvre en C++
- ◆ Comprendre le fonctionnement des structures de données avancées autres que les structures habituelles
- ◆ Comprendre la théorie et la pratique liées à l'utilisation des tas et des files d'attente prioritaires
- ◆ Apprenez comment les tables de *Hash*, en tant que types de données et fonctions abstraites
- ◆ Comprendre la théorie des graphes, ainsi que les algorithmes et concepts avancés relatifs aux graphes

Module 3. Algorithme et complexité

- ◆ Apprendre les principales stratégies de conception d'algorithmes, ainsi que les différentes méthodes et mesures pour le calcul des algorithmes
- ◆ Apprendre les principaux algorithmes de tri utilisés dans le développement de logiciels
- ◆ Comprendre le fonctionnement des différents algorithmes avec les arbres, les *Heaps* et les Graphes
- ◆ Comprendre le fonctionnement des algorithmes *Greedy*, leur stratégie et des exemples de leur utilisation dans les principaux problèmes connus Nous apprendrons également l'utilisation des algorithmes *Greedy* sur les Graphes
- ◆ Nous apprendrons les principales stratégies de recherche de chemin minimum, avec l'approche des problèmes essentiels du domaine et des algorithmes pour leur résolution
- ◆ Comprendre la technique du *Backtracking* et ses principales utilisations, ainsi que d'autres techniques alternatives

Module 4. Conception avancés d'algorithmes

- ◆ Approfondissez la conception avancée d'algorithmes, en analysant les algorithmes récursifs et de division et de conquête, ainsi qu'en effectuant des analyses amorties
- ◆ Comprendre les concepts de la programmation dynamique et les algorithmes pour les problèmes de NP
- ◆ Comprendre le fonctionnement de l'optimisation combinatoire, ainsi que les différents algorithmes de randomisation et les algorithmes parallèles
- ◆ Connaître et comprendre le fonctionnement des différentes méthodes de recherche locale et de recherche de candidats
- ◆ Apprendre les mécanismes de la vérification formelle des programmes et de la vérification itérative des programmes, y compris la logique du premier ordre et le système formel de Hoare
- ◆ Apprendre le fonctionnement de certaines des principales méthodes numériques telles que la méthode de bisection, la méthode de Newton - Raphson et la méthode de la sécante

Module 5. Programmation avancée

- ◆ Approfondir les connaissances en programmation, notamment en ce qui concerne la programmation orientée objet, et les différents types de relations entre les classes existantes
- ◆ Connaître les différents patrons de conception pour les problèmes Orientés Objets
- ◆ Découvrez la programmation événementielle et le développement d' *Interfaces* d'utilisateur avec Qt
- ◆ Acquérir les connaissances essentielles de la programmation concurrente, des processus et des threads
- ◆ Apprendre à gérer l'utilisation des threads et de la synchronisation, ainsi que la résolution des problèmes courants de la programmation concurrente
- ◆ Comprendre l'importance de la documentation et des tests dans le développement de Software

Module 6. Informatique théorique

- ◆ Comprendre les concepts mathématiques théoriques essentiels de l'informatique, tels que la logique propositionnelle, la théorie des ensembles et les ensembles numériques et non numériques
- ◆ Comprendre les concepts de langages formels et de grammaires, ainsi que les machines de Turing dans leurs différentes variantes
- ◆ Apprendre les différents types de problèmes indécidables et insolubles, y compris leurs différentes variantes et approximations
- ◆ Comprendre le fonctionnement de différents types de langages basés sur la randomisation et d'autres types de classes et de grammaires
- ◆ Comprendre d'autres systèmes informatiques avancés tels que l'informatique membranaire, l'informatique ADN et l'informatique quantique

Module 7. Théorie des automates et des langages formels

- ◆ Comprendre la théorie des automates et des langages formels, en apprenant les concepts d'alphabets, de chaînes de caractères et de langages, ainsi que la manière d'effectuer des preuves formelles
- ◆ Apprendre les différents types d'automates finis, déterministes et non-déterministes
- ◆ Apprendre les concepts de base et avancés liés aux langages et aux expressions régulières, ainsi que l'application du lemme de pompage et la fermeture des langages réguliers
- ◆ Comprendre les grammaires indépendantes du contexte, ainsi que le fonctionnement des automates à pile
- ◆ Approfondir la compréhension des formes normales, du lemme de pompage des grammaires indépendantes du contexte et des propriétés des langues indépendantes du contexte

Module 8. Processeurs de langue

- ◆ Introduire les concepts liés au processus de compilation et les différents types d'analyse: lexicale, syntaxique et sémantique
- ◆ Connaître le fonctionnement d'un analyseur lexical, sa mise en œuvre et la récupération des erreurs
- ◆ Approfondir la connaissance de l'analyse syntaxique, à la fois descendante et ascendante, mais en mettant l'accent sur les différents types d'analyseurs syntaxiques ascendants
- ◆ Comprendre le fonctionnement des analyseurs sémantiques, la tradition syntaxique, la table des symboles et les différents types d'analyseurs
- ◆ Apprendre les différents mécanismes de génération de code, tant dans les environnements d'exécution que pour la génération de code intermédiaire
- ◆ Poser les bases de l'optimisation du code, notamment la réorganisation des expressions et l'optimisation des boucles

Module 9. Informatique graphique et visualisation

- ◆ Introduire les concepts essentiels de l'infographie et de la visualisation par ordinateur, tels que la théorie de la couleur et ses modèles et les propriétés de la lumière
- ◆ Comprendre le fonctionnement des primitives de sortie et leurs algorithmes, tant pour le dessin de lignes que pour le dessin de cercles et de remplissages
- ◆ Approfondir l'étude des différentes transformations, tant en 2D qu'en 3D, et de leurs systèmes de coordonnées et de visualisation par ordinateur
- ◆ Apprendre à faire des projections et des coupes en 3D, ainsi que l'élimination des surfaces cachées
- ◆ Apprendre la théorie liée à l'interpolation et aux courbes paramétriques, ainsi que les courbes de Bézier et les *B-Splines*

Module 10. Informatique bio-inspirée

- ◆ Introduire le concept de calcul bio-inspiré, ainsi que comprendre le fonctionnement des différents types d'algorithmes d'adaptation sociale et d'algorithmes génétiques
- ◆ Étudier en profondeur les différents modèles de calcul évolutif, en connaissant leurs stratégies, leur programmation, leurs algorithmes et les modèles basés sur l'estimation de la distribution
- ◆ Comprendre les principales stratégies d'exploration-exploitation de l'espace pour les algorithmes génétiques
- ◆ Comprendre le fonctionnement de la programmation évolutionnaire appliquée aux problèmes d'apprentissage et aux problèmes multi-objectifs
- ◆ Apprenez les concepts essentiels liés aux réseaux neuronaux et comprenez le fonctionnement de cas d'utilisation réels appliqués à des domaines aussi divers que la recherche médicale, l'économie et la vision artificielle

Module 11. Sécurité dans la conception et le développement des systèmes

- ◆ Évaluer la sécurité d'un système d'information dans toutes ses composantes et couches
- ◆ Identifier les types actuels de menaces pour la sécurité et leurs tendances
- ◆ Établir des directives de sécurité en définissant politiques et plans de sécurité et d'urgence
- ◆ Analyser les stratégies et les outils permettant de garantir l'intégrité et la sécurité des systèmes d'information
- ◆ Appliquer des techniques et des outils spécifiques pour chaque type d'attaque ou de vulnérabilité de sécurité
- ◆ Protéger les informations sensibles stockées dans le système d'information
- ◆ Disposer du cadre juridique et de la typologie du crime, en complétant la vision par la typologie du délinquant et de sa victime

Module 12. Architectures et modèles de sécurité de l'information

- ◆ Aligner le Plan Directeur de Sécurité sur les objectifs stratégiques de l'organisation
- ◆ Établir un cadre permanent de gestion des risques faisant partie intégrante du plan directeur de sécurité
- ◆ Déterminer les indicateurs appropriés pour le suivi de la mise en œuvre du SGSI
- ◆ Établir une stratégie de sécurité basée sur des politiques
- ◆ Analyser les objectifs et les procédures associés au plan de sensibilisation des employés, des fournisseurs et des partenaires
- ◆ Identifier, dans le cadre réglementaire, les règlements, les certifications et les lois applicables dans chaque organisation
- ◆ Développer les éléments clés requis par la norme ISO 27001:2013
- ◆ Mettre en œuvre un modèle de gestion de la confidentialité conforme au règlement européen GDPR/RGPD



Module 13. Gestion de la sécurité IT

- ◆ Identifier les différentes structures que peut avoir un secteur de sécurité de l'information
- ◆ Développez un modèle de sécurité basé sur trois lignes de défense
- ◆ Présenter les différents comités périodiques et extraordinaires dans lesquels le domaine de la cybersécurité intervient
- ◆ Spécifier les outils technologiques qui soutiennent les principales fonctions de l'équipe des opérations de sécurité (SOT)
- ◆ Évaluer les mesures de contrôle de la vulnérabilité appropriées à chaque scénario
- ◆ Développer le cadre des opérations de sécurité sur la base du NIST CSF
- ◆ Préciser la portée des différents types de contrôles (*Red Team, Pentesting, Bug Bounty, etc.*)
- ◆ Proposer les activités à mener après un incident de sécurité
- ◆ Mettre en place un centre de commandement de la sécurité de l'information englobant tous les acteurs concernés (autorités, clients, fournisseurs, etc.)

Module 14. Analyse des risques et environnement de la sécurité informatique

- ◆ Examiner, avec une vision holistique, l'environnement dans lequel nous opérons
- ◆ Identifier les principaux risques et opportunités qui peuvent affecter la réalisation de nos objectifs. de nos objectifs
- ◆ Analyser les risques sur la base des meilleures pratiques dont nous disposons
- ◆ Évaluer l'impact potentiel de ces risques et opportunités
- ◆ Développer des techniques pour traiter les risques et les opportunités de manière à maximiser la contribution à la valeur
- ◆ Examiner en profondeur les différentes techniques de transfert de risque, ainsi que la valeur
- ◆ Examiner en profondeur les différentes techniques de transfert de risques et de valeurs

- ♦ Examiner les résultats pour proposer des améliorations continues de la gestion des projets et des processus sur la base de modèles de gestion axés sur les risques ou les *Risk-Driven*
- ♦ Innover et transformer des données générales en informations pertinentes pour la prise de décision fondée sur le risque

Module 15. Cryptographie en informatique

- ♦ Compiler les opérations fondamentales (XOR, grands nombres, substitution et transposition) et les différents composants (fonctions *One-Way*, *Hash*, générateurs de nombres aléatoires)
- ♦ Analyser les techniques cryptographiques
- ♦ Développer différents algorithmes cryptographiques
- ♦ Démontrer l'utilisation des signatures numériques et leur application dans les certificats numériques
- ♦ Évaluer les systèmes de gestion des clés et l'importance de la longueur des clés cryptographiques
- ♦ Examiner les algorithmes de dérivation de clés
- ♦ Analyser le cycle de vie des clés
- ♦ Évaluer les modes de chiffrement par blocs et de chiffrement par flux
- ♦ Déterminer les générateurs de nombres pseudo-aléatoires
- ♦ Développer des cas réels d'applications cryptographiques, comme Kerberos, PGP ou les cartes à puce
- ♦ Examinez les associations et organismes connexes, tels que l'ISO, le NIST ou le NCSC
- ♦ Déterminer les défis de la cryptographie de l'informatique quantique

Module 16. Gestion des identités et des accès dans la sécurité informatique

- ♦ Développer le concept d'identité numérique
- ♦ Évaluation du contrôle de l'accès physique aux informations
- ♦ Principes fondamentaux de l'authentification biométrique et de l'authentification MFA
- ♦ Évaluer les attaques contre la confidentialité des informations
- ♦ Analyser la fédération d'identité
- ♦ Établir un contrôle d'accès au réseau

Module 17. Sécurité des communications et de l'exploitation du software

- ♦ Développer des connaissances spécialisées en matière de sécurité physique et logique
- ♦ Démontrer une connaissance des communications et des réseaux
- ♦ Identifier les principales attaques malveillantes
- ♦ Établir un cadre de développement sécurisé
- ♦ Démontrer une compréhension des principales réglementations relatives aux systèmes de gestion de la sécurité de l'information
- ♦ Démontrer le bien-fondé de l'exploitation d'un centre opérationnel de cybersécurité
- ♦ Démontrer l'importance des pratiques de cyber-sécurité pour les catastrophes organisationnelles

Module 18. Sécurité des Environnements *cloud*

- ♦ Identifier les risques liés au déploiement d'une infrastructure de *Cloud* publique
- ♦ Définir les exigences de sécurité
- ♦ Élaborer un plan de sécurité pour un déploiement dans le *Cloud*
- ♦ Identifier les services *Cloud* à déployer pour l'exécution d'un plan de sécurité
- ♦ Déterminer les exigences opérationnelles des mécanismes de prévention
- ♦ Établir des lignes directrices pour un système *Logging* et de suivi
- ♦ Proposer des actions de réponse aux incidents

Module 19. Sécurité des communications des dispositifs IoT

- ◆ Présenter l'architecture IoT simplifiée
- ◆ Expliquer les différences entre les technologies de connectivité généralistes et les technologies de connectivité IoT
- ◆ Établir le concept du triangle de fer de la connectivité IoT
- ◆ Analyser les spécifications de sécurité de la technologie LoRaWAN, de la technologie NB-IoT et de la technologie WiSUN
- ◆ Justifier le choix de la technologie IoT appropriée pour chaque projet

Module 20. Plan de continuité des activités associé à la sécurité

- ◆ Présenter les éléments clés de chaque phase et analyser les caractéristiques du plan de continuité des activités (PCA). Plan de continuité des activités (PCA)
- ◆ Justifier la nécessité d'un plan de continuité des activités
- ◆ Déterminer les cartes de réussite et de risque de chaque phase du plan de Continuité des Activités
- ◆ Préciser comment établir un plan d'action pour la mise en œuvre
- ◆ Évaluer l'exhaustivité d'un plan de continuité des activités (PCA)
- ◆ Développer le plan pour une mise en œuvre réussie d'un plan de continuité des activités

Module 21. Analytique des données dans l'organisation de l'entreprise

- ◆ Développer des compétences analytiques pour prendre des décisions de qualité
- ◆ Examiner les campagnes de marketing et de communication efficaces
- ◆ Déterminer la création de tableaux de bord et de KPI's en fonction du département
- ◆ Générer des connaissances spécialisées pour développer des analyses prédictives
- ◆ Proposer des plans d'affaires et de fidélisation sur la base d'études de marché
- ◆ Développer la capacité d'écouter le client
- ◆ Appliquer des connaissances statistiques, quantitatives et techniques dans des situations réelles

Module 22. Gestion et manipulation de Données et d'Informations pour la Science de Données

- ◆ Effectuer une analyse de Données
- ◆ Unifier des données diverses: assurer la cohérence des informations
- ◆ Produire des informations pertinentes et efficaces pour la prise de décision
- ◆ Déterminer les meilleures pratiques pour la gestion de données en fonction de leur typologie et de leurs utilisations
- ◆ Développer des politiques d'accès et de réutilisation des données
- ◆ Assurer la sécurité et la disponibilité, l'intégrité et la confidentialité des informations
- ◆ Examiner les outils de gestion des données langages de programmation

Module 23. Dispositifs et plateformes IoT comme base de la science des données

- ◆ Identifier ce qu'est l'IoT (*Internet of Things*) et l'IIoT (*Industrial Internet of Things*)
- ◆ Examiner le Consortium d'Internet industriel
- ◆ Analyser ce qu'est l'architecture de référence de l'IoT
- ◆ Aborder les capteurs et dispositifs IoT et leur classification
- ◆ Identifier les protocoles et technologies de communication utilisés dans l'IoT
- ◆ Examiner les différentes plateformes de *Cloud* dans l'IdO : usage général, industriel, open source
- ◆ Développer des mécanismes d'échange de données
- ◆ Établir des exigences et des stratégies de sécurité
- ◆ Présenter les différents domaines d'application IoT et IIoT

Module 24. Représentation graphique pour l'analyse de Données

- ◆ Générer des connaissances spécialisées de l'analyse des données
- ◆ Examiner les différents types de données groupées
- ◆ Établir les représentations graphiques les plus couramment utilisées dans différents domaines
- ◆ Déterminer les principes de conception de la visualisation des données
- ◆ Présenter la narration graphique comme un outil
- ◆ Analyser les différents outils logiciels pour la création de graphiques et l'analyse exploratoire des données

Module 25. Outils de science de Données

- ◆ Développer des compétences pour convertir les données en informations dont on peut extraire des connaissances
- ◆ Déterminer les principales caractéristiques d'un *dataset*, sa structure, ses composants et les implications de sa distribution dans la modélisation
- ◆ Fonder la prise de décision en effectuant une analyse préalable approfondie des données
- ◆ Développer des compétences pour résoudre des études de cas en utilisant des techniques de science des données
- ◆ Établir les outils et méthodes généraux les plus appropriés pour modéliser chaque *Dataset* en fonction du prétraitement effectué
- ◆ Évaluer les résultats de manière analytique, en comprenant l'impact de la stratégie choisie sur différents paramètres
- ◆ Démontrer une capacité critique des résultats obtenus après application de méthodes de prétraitement ou de modélisation

Module 26. Extraction de Données; Sélection, pré-traitement et transformation

- ◆ Acquérir des connaissances spécialisées sur les conditions statistiques préalables à toute analyse et évaluation des données
- ◆ Développer les compétences nécessaires à l'identification, la préparation et la transformation des données
- ◆ Évaluer les différentes méthodologies présentées et identifier les avantages et les inconvénients
- ◆ Examiner les problèmes dans les environnements de données de haute dimension
- ◆ Développer l'implémentation des algorithmes utilisés pour le prétraitement des données
- ◆ Démontrer la capacité d'interpréter des visualisations de données pour une analyse descriptive
- ◆ Développer une connaissance avancée des différentes techniques de préparation des données existantes pour le nettoyage, la normalisation et la transformation des données

Module 27. Prédicibilité et analyse des phénomènes stochastiques

- ◆ Analyser les séries chronologiques
- ◆ Développer la formulation et les propriétés de base des modèles de séries temporelles univariées
- ◆ Examiner la méthodologie de modélisation et de prédiction des séries en temps réel
- ◆ Déterminer les modèles univariés incluant les valeurs aberrantes
- ◆ Appliquer des modèles de régression dynamique et appliquer la méthodologie de construction de tels modèles à partir de séries observées
- ◆ Aborder l'analyse spectrale des séries temporelles univariées, ainsi que les aspects fondamentaux liés à l'inférence basée sur les périodogrammes et son interprétation
- ◆ Estimer la probabilité et la tendance d'une série chronologique pour un horizon temporel donné

Module 28. Conception et développement de systèmes intelligents

- ◆ Analyser le passage de l'information à la connaissance
- ◆ Développer les différents types de techniques d'apprentissage automatique
- ◆ Examen des métriques et des scores pour quantifier la qualité des modèles
- ◆ Mettre en œuvre les différents algorithmes d'apprentissage automatique
- ◆ Identifier les modèles de raisonnement probabiliste
- ◆ Poser les bases de l'apprentissage profond
- ◆ Démontrer les compétences acquises pour comprendre les différents algorithmes d'apprentissage automatique

Module 29. Architectures et systèmes à forte intensité de données

- ◆ Déterminer les exigences des systèmes d'utilisation des données de masse
- ◆ Examiner différents modèles de données et analyser les bases de données
- ◆ Analyser les fonctionnalités clés des systèmes distribués et leur importance dans différents types de systèmes
- ◆ Évaluer quelles applications largement répandues utilisent les principes fondamentaux des systèmes distribués pour concevoir leurs systèmes
- ◆ Analyser comment les bases de données stockent et récupèrent les informations
- ◆ Identifier les différents modèles de réplication et les problèmes associés
- ◆ Développer des moyens de partitionnement et de transactions distribuées
- ◆ Identifier les systèmes par lots et les systèmes en temps (quasi) réel

Module 30. Application pratique de la science des données dans les secteurs d'activité

- ◆ Analyser l'état de l'art de l'intelligence artificielle (IA) et de l'analyse des données
- ◆ Développer une connaissance spécialisée des technologies les plus utilisées
- ◆ Favoriser une meilleure compréhension de la technologie grâce à des cas d'utilisation
- ◆ Analyser les stratégies choisies pour sélectionner les meilleures technologies à mettre en œuvre
- ◆ Déterminer les domaines d'application
- ◆ Examiner les risques réels et potentiels de la technologie appliquée
- ◆ Proposer des avantages dérivés de l'utilisation
- ◆ Identifier les tendances futures dans des secteurs spécifiques



Atteignez l'excellence en suivant un programme qui vous permettra de générer des connaissances spécialisées dans la Science Informatique, Cybersécurité et l'Analyse des données"

03

Compétences

Après avoir passé les évaluations de ce programme, l'informaticien aura acquis les compétences nécessaires pour comprendre les principes fondamentaux de l'informatique avec la capacité de travailler avec des langages de programmation et des données. Ils pourront ainsi aspirer à une amélioration de leur travail quotidien dans ce domaine de spécialisation, qui devient une occasion d'offrir des connaissances précieuses lors de la prise de décisions qui affectent le fonctionnement des départements d'une entreprise.



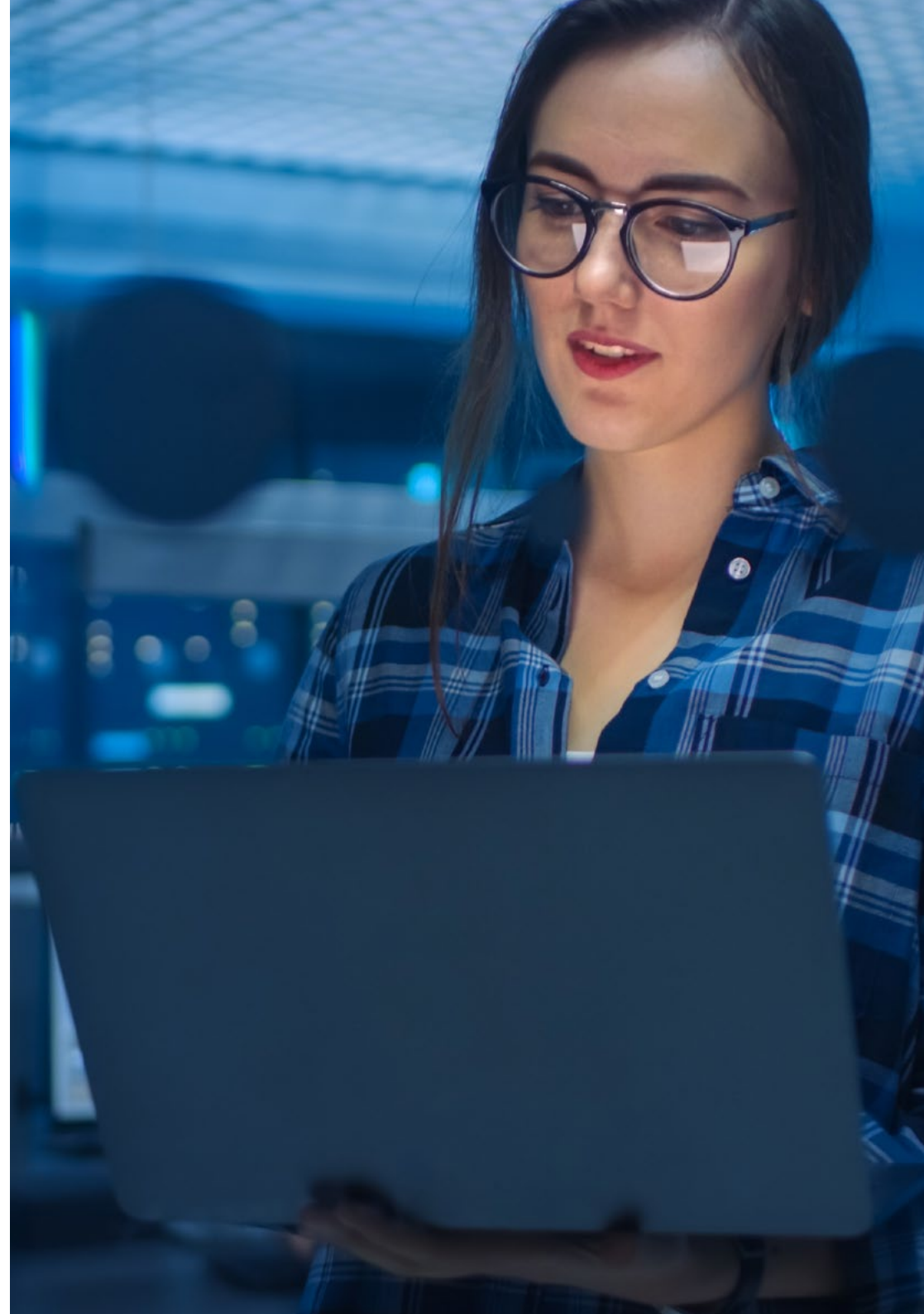
“

Obtenez les compétences nécessaires pour porter votre profession au plus haut niveau, grâce à ce Mastère Avancé qui vous permettra de vous mettre à jour et de vous adapter au nouvel environnement informatique”



Compétences générales

- ◆ Réaliser correctement des travaux liés aux ordinateurs et au langage informatique
- ◆ Appliquer les mesures de sécurité les plus appropriées en fonction des menaces
- ◆ Déterminer la politique et le plan de sécurité dans le système d'information d'une entreprise, achever la conception et la mise en œuvre du plan d'urgence
- ◆ Établir un programme d'audits pour couvrir les besoins d'auto-évaluation de l'organisation en matière de cybersécurité
- ◆ Développer un programme d'analyse et de surveillance des vulnérabilités et un plan de réponse aux incidents de cybersécurité
- ◆ Maximiser les opportunités présentées et éliminer l'exposition à tous les risques potentiels par la conception
- ◆ Compiler les systèmes de gestion des clés
- ◆ Évaluer la sécurité de l'information d'une entreprise
- ◆ Analyser les systèmes d'accès à l'information
- ◆ Développer les meilleures pratiques en matière de développement sécurisé
- ◆ Présenter les risques pour les entreprises de ne pas avoir mis en place un environnement de sécurité informatique
- ◆ Développer une perspective technique et commerciale de l'analyse des données
- ◆ Comprendre les algorithmes, les plateformes et les outils les plus courants pour l'exploration, la visualisation, la manipulation, le traitement et l'analyse des données
- ◆ Mettre en œuvre une vision d'entreprise nécessaire à la valorisation comme élément clé de la prise de décision
- ◆ Être capable d'aborder les problèmes spécifiques à l'analyse des données





Compétences spécifiques

- ◆ Concevoir des algorithmes pour développer des programmes informatiques et appliquer le langage de programmation
- ◆ Comprendre et utiliser la structure des données informatiques
- ◆ Utiliser les algorithmes nécessaires à la résolution de problèmes informatiques
- ◆ Avoir une compréhension approfondie de la conception d'algorithmes avancés et des méthodes de recherche
- ◆ Effectuer des tâches de programmation informatique
- ◆ Comprendre et appliquer la théorie qui sous-tend l'informatique, comme les mathématiques
- ◆ Connaître la théorie des automates et appliquer le langage informatique
- ◆ Connaître les fondements théoriques des langages de programmation et les techniques de traitement lexical, syntaxique et sémantique associées
- ◆ Comprendre les concepts de base des mathématiques et de la complexité computationnelle afin de les appliquer à la résolution de problèmes informatiques
- ◆ Connaître et appliquer les principes fondamentaux du calcul pour réaliser de nouveaux développements informatiques
- ◆ Développez un Systèmes de Gestion de Sécurité de l'Information (SGSI)
- ◆ Identifier les éléments clés qui composent un SMSI
- ◆ Appliquer la méthodologie MAGERIT pour faire évoluer le modèle et le faire progresser
- ◆ Concevoir de nouvelles méthodologies de gestion des risques basées sur le concept de *agile*Risk Management
- ◆ Identifier, analyser, évaluer et traiter les risques auxquels le professionnel est confronté dans une nouvelle perspective commerciale fondée sur un modèle *Risk-Driven* qui permet non seulement de survivre dans son propre environnement, mais aussi de stimuler sa propre contribution à la valeur
- ◆ Examiner le processus de conception d'une stratégie de sécurité lors du déploiement de services de *Cloud*d'entreprise
- ◆ Évaluer les différences dans les implémentations spécifiques des différents fournisseurs de *Cloud* publics
- ◆ Évaluer les options de connectivité IoT pour répondre à un projet, en mettant l'accent sur les technologies LPWAN
- ◆ Présenter les spécifications de base des principales technologies LPWAN pour l'IoT
- ◆ Se spécialiser en *Data Science* d'un point de vue technique et commercial
- ◆ Visualiser les données de la manière la plus appropriée pour favoriser leur partage et leur compréhension par différents profils
- ◆ Aborder les domaines fonctionnels fondamentaux de l'organisation où la science des données peut apporter une plus grande valeur
- ◆ Développer le cycle de vie des données, sa typologie et les technologies et phases nécessaires à sa gestion
- ◆ Traiter et manipuler les données à l'aide de langages et de bibliothèques spécifiques
- ◆ Développer des connaissances avancées dans les techniques fondamentales d'exploration de données pour la sélection, le prétraitement et la transformation des données
- ◆ Se spécialiser dans les principaux algorithmes de *Machine Learning* pour extraire les connaissances cachées des données
- ◆ Acquérir des connaissances spécialisées dans les architectures et systèmes logiciels nécessaires à l'utilisation intensive des données
- ◆ Déterminer comment l'IoT peut être une source de génération de données et d'informations clés sur lesquelles appliquer la science des données pour l'extraction de connaissances
- ◆ Analysez les différentes façons d'appliquer la science des données dans différents secteurs ou verticaux en vous inspirant d'exemples réels

04

Direction de la formation

Aborder avec succès le domaine de la Science Informatique, de la Cybersécurité et de l'Analyse des Données nécessite une étude approfondie complète et détaillée. Pour cette raison, TECH a réuni les meilleurs enseignants spécialisés dans chaque domaine. Ainsi, l'informaticien est accompagné par des professionnels de renom qui lui offrent leurs nombreuses années d'expérience et de formation. De cette manière, les informaticiens sont assurés de recevoir des connaissances actuelles et spécifiques d'un secteur en plein essor au niveau international.



“

Vous bénéficierez des conseils et de l'encadrement d'un corps enseignant au fait des dernières évolutions en matière de Cybersécurité et Analyse de Données”

Direction



M. Olalla Bonal, Martin

- ♦ Spécialiste technique de la *Blockchain* chez IBM SPGI
- ♦ Spécialiste des ventes techniques de *Blockchain*. IBM
- ♦ Directeur d'Architecture. *Blocknitive*
- ♦ Technicien en Électronique Numérique
- ♦ *Blockchain Architect -IT Infrastructure Architect* - Chef de projet IT. Domaines d'activité : Software, Infrastructure, Télécommunications



Dr Peralta Martin-Palomino, Arturo

- ♦ PDG et directeur technique chez Prometeus Global Solutions
- ♦ Directeur technique chez Korporate Technologies
- ♦ Directeur technique chez AI Shephers GmbH
- ♦ Doctorat en ingénierie informatique à l'Université de Castilla la Mancha
- ♦ Doctorat en économie, commerce et finances de l'université Camilo José Cela. Prix du doctorat extraordinaire
- ♦ Docteur en psychologie de l'Université de Castilla la Mancha
- ♦ Master en Technologies de l'information Avancées de l'Université de Castilla La Mancha
- ♦ Master MBA+E (Master en administration des affaires et ingénierie organisationnelle) de l'Université de Castilla la Mancha
- ♦ Professeur associé, enseignant en Licence et en Master d'ingénierie Informatique à l'Université de Castilla la Mancha
- ♦ Professeur du Mastère en Big Data et Data Science à l'Université Internationale de Valence
- ♦ Professeur du Master en Industrie 4.0 et du Master en Design Industriel et Développement de produit
- ♦ Membre du groupe de recherche SMILe à l'Université de Castilla la Mancha

Professeurs

M. Tobal Redondo, Javier

- ◆ Responsable du Programme d'Innovation Applicative chez HUAWEI
- ◆ Responsable de la Sécurité de l'Information, Division des Moyens de Paiement. Amadeus IT Group
- ◆ Chef de la Sécurité de l' Information FINTONIC, Services Financiers
- ◆ Ingénieur de Services et Architecte dans le Domaine de la Planification et de l'Architecture des Services et de
- ◆ sécurité chez Amena / Orange Espagne
- ◆ Diplôme en Informatique de l'Université de Deusto (Bilbao, Espagne)
- ◆ Diplôme d'études supérieures en Informatique Industrielle. École de l' Ingénierie Industrielle. Bilbao

M. Gonzalo Alonso, Félix

- ◆ Directeur général et fondateur. Smart REM Solutions
- ◆ Associé fondateur et responsable de l'ingénierie des risques et de l'innovation Dynargy
- ◆ Directeur général et associé fondateur Risknova (Bureau d'experts spécialisés en technologie)
- ◆ Diplôme d'ingénieur en organisation industrielle de l'Universidad Pontificia de Comillas ICAI
- ◆ Diplômé en ingénierie technique industrielle, spécialisé en électronique industrielle, Universidad Pontificia de Comillas ICAI
- ◆ Master en gestion des assurances de l'ICEA (Institut pour la collaboration entre les compagnies d'assurances)

M. Sevillano Izquierdo, Javier

- ◆ Global Cyber Security Architect chez Vodafone Espagne
- ◆ Chief Technology Security Office (CTSO) chez Vodafone Espagne
- ◆ Responsable Sécurité Technologique chez Bankia
- ◆ Responsable Sécurité Technologique à Caja Madrid
- ◆ Manager de Sécurité à Système 4B
- ◆ SEINCA - Analyste principal
- ◆ Technicien supérieur en informatique de gestion à l'Instituto Cibernos

M. Entrenas, Alejandro

- ◆ Entelgy Innotec
- ◆ Diplôme d'ingénieur technique en systèmes informatiques de l'université de Cordoba
- ◆ Master en gestion de la sécurité de l'information de l'Université polytechnique de Madrid

M. Nogales Avila, Javier

- ◆ Enterprise Cloud and sourcing senior consultant. Quint
- ◆ Cloud and Technology Consultant. Indra
- ◆ Associate Technology Consultant. Accenture
- ◆ Diplômé de l'Université de Jaén et de l'Université de Technologie et d'Économie de Budapest (BME)
- ◆ Diplôme d'ingénieur en Gestion Industrielle

M. Gómez Rodríguez, Antonio

- ◆ Ingénieur en solutions Cloud chez Oracle
- ◆ Directeur de projet chez Sopra Group
- ◆ Directeur de Projets chez Everis
- ◆ Chef de Projets à l'Entreprise Publique pour la Gestion des Programmes Culturels du Ministère de la Culture d'Andalousie
- ◆ Analyste des Systèmes d'Information chez Sopra Group
- ◆ Diplôme d'ingénieur en télécommunications de l'Université polytechnique de Catalogne
- ◆ Diplômé de troisième cycle en Technologies et Systèmes d'Information de l'Institut Catalan de Technologie
- ◆ *E-Business* Master de l'Ecole de Commerce de La Salle

M. del Valle Arias, Jorge

- ◆ Directeur de la division IoT chez Diode Espagne
- ◆ Smart Cities Business Growth Manager Spain en Itron Inc.
- ◆ Consultant IoT
- ◆ Sales Manager IoT & Celular en Aicox Soluciones
- ◆ Fondateur et PDG de Sensor Intelligence
- ◆ Directeur des Opérations chez Codium Networks
- ◆ Chef du secteur électronique chez Aitemin
- ◆ Ingénieur en Télécommunications de l'Université Polytechnique de Madrid
- ◆ Executive MBA de l'International Graduate School de La Salle à Madrid

M. Fernandez, Juan Luis

- ◆ Ingénieur en informatique
- ◆ Professeur Associé en DevOps et Blockchain à l'UNIR
- ◆ Directeur de Blockchain DevOps chez Alastria
- ◆ Directeur du développement des applications mobiles Tinkerlink chez Cronos Telecom
- ◆ Directeur informatique à la Banque Santander
- ◆ Directeur de la Technologie de Gestion des Services Informatiques à la Barclays Bank Espagne
- ◆ Diplôme d'ingénieur en informatique de l'Université Nationale d'Éducation à Distance (UNED)

Mme Jurado Jabonero, Lorena

- ◆ Responsable de la sécurité de l'information (CISO) au Groupe Pascual
- ◆ Diplômé en Ingénierie informatique de l'Université Alfonso X El Sabio
- ◆ Ingénieur Technique en Informatique de gestion de l'Université Polytechnique de Madrid
- ◆ Connaissances: ISO 27001, ISO 27701, ISO 22301, ISO 20000, RGPD/LOPDGDD, NIST CSF, CSA, ITIL, PCI, etc.

M. Armero Fernandez, Rafael

- ◆ Business Intelligence Consultant fr SDG Group
- ◆ Digital Engineer en Mi-GSO
- ◆ Logistic Engineer chez Torrecid S.A.
- ◆ Quality Intern chez INDRA
- ◆ Diplôme en Ingénierie Aérospatiale à l'Université Polytechnique de Valence
- ◆ Master en Médecine Development4,0 de l'Université de Alcalá de Henares

Dr Peris Morillo, Luis Javier

- ◆ Responsable Technique chez Capitole Consulting. Dirige une équipe chez Inditex dans l'unité logistique de sa plateforme ouverte
- ◆ Responsable technique principal et responsable de la livraison du support chez HCL
- ◆ Coach Agile et directeur des opérations chez Mirai Advisory
- ◆ Membre du comité de pilotage en tant que Directeur des Opérations
- ◆ Développeur, chef d'équipe, Scrum Master, coach Agile, chef de produit chez DocPath
- ◆ Diplôme d'ingénieur en informatique de l'ESI de Ciudad Real (UCLM)
- ◆ Postgraduate en Gestion de projet par la CEOE - Confédération Espagnole des Organisations d'entreprises
- ◆ +50 MOOC suivis, enseignés par des universités de renom telles que l'Université de Stanford, l'Université du Michigan, l'Université de Yonsei l'Université Polytechnique de Madrid, etc.
- ◆ Plusieurs certifications, dont certaines des plus notables ou récentes sont Azure Fundamentals

Mme Pedrajas Parabas, Elena

- ◆ Analyste Commercial chez Management Solutions à Madrid
- ◆ Chercheuse au Département d'informatique et d'Analyse Numérique de l'Université de Cordoba
- ◆ Chercheuse au Centre Singulier de Recherche en Technologies Intelligentes à Santiago de Compostela
- ◆ Licence en Ingénierie Informatique Master en Science des Données et Ingénierie Informatique

M. Montoro Montarroso, Andrés

- ◆ Chercheur en le groupe SMILe à l'Université de Castilla-La Mancha
- ◆ Scientifique de chez Prometheus Global Solutions
- ◆ Doctorat en ingénierie informatique à 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 Basés sur la Connaissance à l'école Supérieure d'informatique de Ciudad Real, donnant la conférence: "Techniques avancées d'intelligence artificielle: Recherche et analyse de radicaux potentiels dans les médias sociaux"
- ◆ Conférencier invité dans le domaine du Data Mining à l'école Supérieur Informatique de Ciudad Real, donnant la conférence: "Applications du traitement du langage naturel: Fuzzy Logic to the analysis of messages in social networks"
- ◆ Conférencier au Séminaire sur la prévention de la corruption dans les administrations publiques et l'intelligence artificielle. Faculté des sciences juridiques et sociales de Tolède Conférence intitulée "Techniques d'intelligence artificielle". Conférencier au premier séminaire international sur le droit administratif et l'intelligence artificielle (DAIA). Organisé par le Centre d'études européennes Luis Ortega Alvarez et l'Institut de recherche TransJus. Conférence intitulée "Sentiment Analysis for the prevention of hate messages on social networks"

M. Fondon Alcalde, Rubén

- ◆ Business Analyst pour le segment des PME chez Vodafone Espagne
- ◆ Business Analyst pour l'Europe du Sud chez Vodafone Global Enterprise
- ◆ Consultant senior en processus chez Unisys pour Telefónica Global Solutions
- ◆ Responsable de l'intégration des services chez Entelgy pour Telefónica Global Solutions
- ◆ Diplômé en Ingénierie de Télécommunications de l'Université Européenne de Madrid.
- ◆ Master en *Big Data* et Analytique par l'Université Internationale de Valence

Mme Fernandez Meléndez, Galina

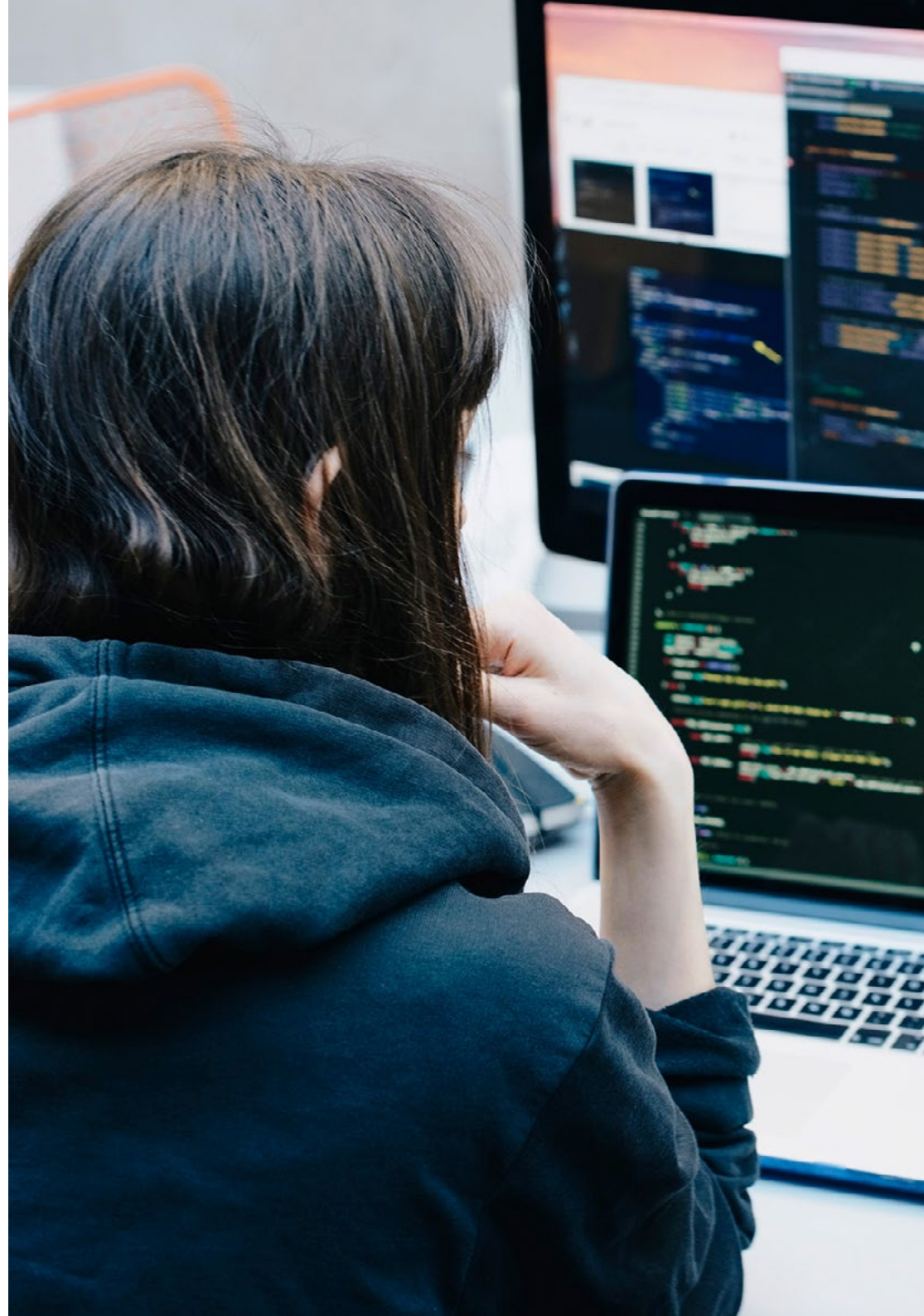
- ◆ Analyste de données chez ADN Mobile Solution
- ◆ Processus ETL, data mining, analyse et visualisation des données, établissement d'indicateurs clés de performance, conception et mise en œuvre de tableaux de bord, contrôle de gestion. Développement R, gestion SQL, entre autres
- ◆ Détermination de modèles, modèles prédictifs, apprentissage automatique
- ◆ Diplôme en administration des affaires. Université bicentenaire d'Aragua-Caracas
- ◆ Diplôme en planification et finances publiques. École vénézuélienne Planification - École des finances
- ◆ Master en Analyse des Données et en Intelligence Économique Université d'Oviedo
- ◆ MBA en Administration et Gestion des Affaires. (École européenne de commerce de Barcelone)
- ◆ Master en Big Data et Business Intelligence (École Européenne de Barcelona)

Dr Diaz Diaz-Chiron, Tobias

- ◆ Chercheur au laboratoire ArCO de l'Université de Castilla-La Mancha, un groupe dédié aux projets liés aux architectures et réseaux informatiques
- ◆ Consultant chez Blue Telecom, une société dédiée au secteur des télécommunications
- ◆ Diplôme en Ingénierie Supérieur en Informatique à l'Université de Castilla - la Mancha

Mme Martinez Cerrato, Yésica

- ◆ Technicien en produits de sécurité électronique chez Securitas Seguridad España
- ◆ Analyste en Intelligence chez Ricopia Technologies
- ◆ Responsable de la formation des nouvelles recrues aux logiciels de gestion d'entreprise (CRM, ERP, INTRANET.), aux produits et aux procédures de Ricopia Technologies (Alcalá de Henares)
- ◆ Responsable de Formation formation des nouveaux stagiaires incorporés aux classes d'informatique à l'Université d'Alcala





- ◆ Chef de projet dans le domaine de l'intégration des grands comptes chez Correos y Telégrafos (Madrid)
- ◆ Professeur de cours d'informatique à l'association ASALUMA
- ◆ Technicien en Informatique - Responsable salles informatiques de l'OTEC à l'Université d'Alcala
- ◆ Licence en Ingénierie de Communications Electroniques de l'Ecole Polytechnique de l'Université d'Alcala
- ◆ Bourse de spécialisation en tant que Technicien Informatique en OTEC de l'Université d'Alcala

M. Tato Sanchez, Rafael

- ◆ Gestion de projet. INDRA SISTEMAS S.A
- ◆ Responsable technique. INDRA SISTEMAS S.A
- ◆ Ingénieur système. ENA TRÁFICO S.A.U.
- ◆ IFCD048PO: Méthodologie de gestion et développement de projets de software avec SCRUM
- ◆ Coursera: Machine learning
- ◆ Apprentissage automatique Deep Learning A-Z. Réseaux neuronaux artificiels pratiques
- ◆ Coursera: IBM: Principes fondamentaux de la science des données évolutives
- ◆ Coursera: IBM: L'IA appliquée avec l'apprentissage profond
- ◆ Coursera: IBM: Apprentissage automatique avancé et traitement du signal
- ◆ Diplôme d'ingénieur en électronique industrielle et automatisation de l'Université européenne de Madrid
- ◆ Master en Ingénierie de l'Université Européenne de Madrid
- ◆ Master en Industrie 4.0 de l'Université Internationale de La Rioja (UNIR)
- ◆ Certification professionnelle. SSCE0110 : Enseignement pour la formation professionnelle à l'emploi

05

Structure et contenu

Ce Mastère Avancé regroupe une série de modules spécialisés qui permettront à l'informaticien d'approfondir des aspects tels que l'identification numérique, les systèmes de contrôle d'accès, l'architecture de la sécurité de l'information, la structure du domaine de la sécurité, les systèmes de gestion de la sécurité de l'information dans l'exploitation des communications et des logiciels ou l'élaboration du plan de continuité des activités associé à la sécurité. Dans le même temps, les techniques les plus complètes et les plus récentes de traitement des données et d'extraction des connaissances sont abordées d'un point de vue théorique et pratique.



“

Tous les domaines d'intérêt que vous devez maîtriser pour travailler avec succès dans l'informatique, compilés dans un syllabus de qualité supérieure"

Module 1. Fondamentaux de la programmation

- 1.1. Introduction à la Programmation
 - 1.1.1. Structure de base d'un ordinateur
 - 1.1.2. Software
 - 1.1.3. Langages de programmation
 - 1.1.4. Cycle de vie de l'application informatique
- 1.2. Conception de l'algorithmes
 - 1.2.1. La résolution de problèmes
 - 1.2.2. Techniques descriptives
 - 1.2.3. Éléments et structure d'un algorithmes
- 1.3. Éléments d'un programme
 - 1.3.1. Origine et caractéristiques du langage C++
 - 1.3.2. L'environnement de développement
 - 1.3.3. Concept du programme
 - 1.3.4. Types de données fondamentales
 - 1.3.5. Opérateurs
 - 1.3.6. Expressions
 - 1.3.7. Phrases
 - 1.3.8. Entrée et sortie de données
- 1.4. Déclarations de contrôle
 - 1.4.1. Phrases
 - 1.4.2. Branches
 - 1.4.3. Boucles
- 1.5. Abstraction et modularité: Fonction
 - 1.5.1. Conception modulaire
 - 1.5.2. Concept de fonction et d'utilité
 - 1.5.3. Définition d'une fonction
 - 1.5.4. Flux d'exécution dans l'appel d'une fonction
 - 1.5.5. Prototypes d'une fonction
 - 1.5.6. Retour des résultats
 - 1.5.7. Appel d'une fonction: Paramètres
 - 1.5.8. Passage de paramètres par référence et par valeur
 - 1.5.9. Identifiant du champ d'application
- 1.6. Structures de données statiques
 - 1.6.1. *Arrays*
 - 1.6.2. Tableaux Polyèdres
 - 1.6.3. Recherche et tri
 - 1.6.4. Cordes. Fonctions d'E/S pour les chaînes de caractères
 - 1.6.5. Structures Unions
 - 1.6.6. Nouveaux types de données
- 1.7. Structures de données dynamiques: Pointeurs
 - 1.7.1. Concept. Définition du pointeur
 - 1.7.2. Opérateurs et opérations avec des pointeurs
 - 1.7.3. *Arrays* de pointeurs
 - 1.7.4. Pointeurs et *Arrays*
 - 1.7.5. Pointeurs vers les cordes
 - 1.7.6. Pointeurs vers les structures
 - 1.7.7. Indirectivité multiple
 - 1.7.8. Pointeurs vers les fonctions
 - 1.7.9. Passage de fonctions, de structures et *Arrays* comme paramètres de fonctions
- 1.8. Fichiers
 - 1.8.1. Concepts de base
 - 1.8.2. Opérations sur les fichiers
 - 1.8.3. Types de fichiers
 - 1.8.4. Organisation des fichiers
 - 1.8.5. Introduction aux fichiers C++
 - 1.8.6. Traitement des fichiers
- 1.9. Récursion
 - 1.9.1. Définition de la récursion
 - 1.9.2. Types de récursions
 - 1.9.3. Avantages et inconvénients
 - 1.9.4. Considérations
 - 1.9.5. Conversion récursive-iterative
 - 1.9.6. La pile de récursion

- 1.10. Tests et documentation
 - 1.10.1. Test du programme
 - 1.10.2. Test boîte blanche
 - 1.10.3. Test de la boîte noire
 - 1.10.4. Outils de test
 - 1.10.5. Documentation de programmes

Module 2. Structure de données

- 2.1. Introduction à la programmation C++
 - 2.1.1. Classes, constructeurs, méthodes et attributs
 - 2.1.2. Variables
 - 2.1.3. Expressions conditionnelles et boucles
 - 2.1.4. Objets
- 2.2. Types abstraits de données (TAD)
 - 2.2.1. Types de Données
 - 2.2.2. Structures de base et TADs
 - 2.2.3. Vecteurs et *Arrays*
- 2.3. Structures de données linéaires
 - 2.3.1. TAD liste. Définition
 - 2.3.2. Listes liées et listes doublement liées
 - 2.3.3. Listes ordonnées
 - 2.3.4. Listes en C++
 - 2.3.5. TAD Pile
 - 2.3.6. TAD Queue
 - 2.3.7. Pile et Queue en C++
- 2.4. Structures de données hiérarchiques
 - 2.4.1. TAD Arbre
 - 2.4.2. Chemins d'accès
 - 2.4.3. Arbres n-aires
 - 2.4.4. Arbres binaires
 - 2.4.5. Arbres binaires de recherche
- 2.5. Structures de données hiérarchiques: arbres complexes
 - 2.5.1. Arbres parfaitement équilibrés ou de hauteur minimale
 - 2.5.2. Arbres à trajets multiples
 - 2.5.3. Références bibliographiques
- 2.6. Monticules prioritaires et queue prioritaire
 - 2.6.1. TAD Monticules
 - 2.6.2. TAD Queue prioritaire
- 2.7. Tables *Hash*
 - 2.7.1. TAD Table *Hash*
 - 2.7.2. Fonctions de *Hash*
 - 2.7.3. Fonction *Hash* dans les tables de *Hash*
 - 2.7.4. Redispersion
 - 2.7.5. Tables *Hash* ouverts
- 2.8. Réseaux
 - 2.8.1. Réseau TAD
 - 2.8.2. Types de Réseaux
 - 2.8.3. Représentation graphique et opérations de base
 - 2.8.4. Design de Réseaux
- 2.9. Algorithmes graphiques et concepts graphiques avancés
 - 2.9.1. Problèmes de graphiques
 - 2.9.2. Algorithmes de parcours
 - 2.9.3. Algorithmes de parcours ou de recherche
 - 2.9.4. Autres algorithmes
- 2.10. Autres structures de Données
 - 2.10.1. Conjonctifs
 - 2.10.2. *Arrays* parallèles
 - 2.10.3. Tables des symboles
 - 2.10.4. *Essais*

Module 3. Algorithme et complexité

- 3.1. Introduction aux stratégies de conception d'algorithmes
 - 3.1.1. Récursion
 - 3.1.2. Diviser pour mieux régner
 - 3.1.3. Autres stratégies
- 3.2. Efficacité et analyse des algorithmes
 - 3.2.1. Mesures d'efficacité
 - 3.2.2. Mesurer la taille de l'entrée
 - 3.2.3. Mesurer le temps d'exécution
 - 3.2.4. Cas le plus défavorable, le meilleur et le moyen
 - 3.2.5. Notation asymptotique
 - 3.2.6. Critères d'analyse mathématique pour les algorithmes non récursifs
 - 3.2.7. Analyse mathématique des algorithmes récursifs
 - 3.2.8. Analyse empirique des algorithmes
- 3.3. Algorithmes de tri
 - 3.3.1. Concept de tri
 - 3.3.2. Classement de la bulle
 - 3.3.3. Classement par sélection
 - 3.3.4. Classement par insertion
 - 3.3.5. Triage par fusion (*Merge Sort*)
 - 3.3.6. Classement Rapide (*Quicksort*)
- 3.4. Algorithmes avec des arbres
 - 3.4.1. Concept d'arbre
 - 3.4.2. Arbres binaires
 - 3.4.3. Chemins d'arbres
 - 3.4.4. Représentation des expressions
 - 3.4.5. Arbres binaires ordonnés
 - 3.4.6. Arbres binaires équilibrés
- 3.5. Algorithmes avec *Heaps*
 - 3.5.1. Les *Heaps*
 - 3.5.2. L'Algorithme *Heapsort*
 - 3.5.3. Les files d'attente prioritaires



- 3.6. Algorithmes avec graphiques
 - 3.6.1. Représentation
 - 3.6.2. Traversée en largeur
 - 3.6.3. Déplacement en profondeur
 - 3.6.4. Classement topologique
- 3.7. Algorithmes *Greedy*
 - 3.7.1. La stratégie *Greedy*
 - 3.7.2. Éléments de la stratégie *Greedy*
 - 3.7.3. Changement de monnaie
 - 3.7.4. Problème du voyageur
 - 3.7.5. Problème de sac à dos
- 3.8. Recherche de chemin minimal
 - 3.8.1. Le problème du chemin minimal
 - 3.8.2. Arcs et cycles négatifs
 - 3.8.3. Algorithme de Dijkstra
- 3.9. Algorithmes *Greedy* sur les graphes
 - 3.9.1. L'arbre à couverture minimale
 - 3.9.2. L'algorithme de Prim
 - 3.9.3. L'algorithme de Kruskal
 - 3.9.4. Analyse de la complexité
- 3.10. *Backtracking*
 - 3.10.1. Le *Backtracking*
 - 3.10.2. Techniques alternatives

Module 4. Conception avancés d'algorithmes

- 4.1. Analyse des algorithmes récursifs et de division et conquête
 - 4.1.1. Poser et résoudre des équations de récursion homogènes et non-homogènes
 - 4.1.2. Aperçu de la stratégie "diviser pour régner"
- 4.2. Analyse amortie
 - 4.2.1. L'analyse des agrégats
 - 4.2.2. La méthode de comptabilisation
 - 4.2.3. La méthode du potentiel

- 4.3. Programmation dynamique et algorithmes pour les problèmes NP
 - 4.3.1. Caractéristiques de la programmation dynamique
 - 4.3.2. Backtracking: retour en arrière
 - 4.3.3. Branchements et élagage
- 4.4. Optimisation combinatoire
 - 4.4.1. Représentation du problème
 - 4.4.2. Optimisation 1D
- 4.5. Algorithmes de randomisation
 - 4.5.1. Exemples d'algorithmes de randomisation
 - 4.5.2. Le théorème de Buffon
 - 4.5.3. Algorithmes de Monte Carlo
 - 4.5.4. Algorithme de Las Vegas
- 4.6. Recherche locale et recherche de candidats
 - 4.6.1. *Garcient Ascent*
 - 4.6.2. *Hill Climbing*
 - 4.6.3. *Simulated Annealing*
 - 4.6.4. *Tabu search*
 - 4.6.5. Recherche de candidats
- 4.7. Vérification formelle des programmes
 - 4.7.1. Spécification d'abstractions fonctionnelles
 - 4.7.2. Le langage de la logique du premier ordre
 - 4.7.3. Le système formel de Hoare
- 4.8. Vérification des programmes itératifs
 - 4.8.1. Règles du système formel de Hoare
 - 4.8.2. Concept d'itérations invariantes
- 4.9. Méthodes numériques
 - 4.9.1. La méthode de bisection
 - 4.9.2. La méthode Newton - Raphson
 - 4.9.3. La méthode sécante

- 4.10. Algorithmes parallèles
 - 4.10.1. Opérations binaires parallèles
 - 4.10.2. Opérations parallèles avec les réseaux
 - 4.10.3. Le parallélisme dans diviser pour mieux régner
 - 4.10.4. Le parallélisme dans la programmation dynamique

Module 5. Programmation avancée

- 5.1. Introduction à la programmation orientée objet
 - 5.1.1. Introduction à la programmation orientée objet
 - 5.1.2. Conception des cours
 - 5.1.3. Introduction à UML pour les problèmes de modélisation
- 5.2. Relations entre les cours
 - 5.2.1. Abstraction et héritage
 - 5.2.2. Concepts d'héritage avancés
 - 5.2.3. Polymorphismes
 - 5.2.4. Composition et agrégation
- 5.3. Introduction aux patrons de conception pour les problèmes orientés objet
 - 5.3.1. Quels sont les modèles de conception?
 - 5.3.2. Modèle *Factory*
 - 5.3.4. Modèle *Singleton*
 - 5.3.5. Modèle *Observer*
 - 5.3.6. Modèle *Composite*
- 5.4. Exceptions
 - 5.4.1. Quelles sont les exceptions?
 - 5.4.2. Capture et traitement des exceptions
 - 5.4.3. Lancement d'exceptions
 - 5.4.4. Création d'exceptions
- 5.5. Interfaces d'utilisateurs
 - 5.5.1. Introduction à Qt
 - 5.5.2. Positionnement
 - 5.5.3. Quels sont les événements?
 - 5.5.4. Événements: définition et saisie
 - 5.5.5. Développement d'interfaces d'utilisateur

- 5.6. Introduction à la programmation concurrente
 - 5.6.1. Introduction à la programmation concurrente
 - 5.6.2. Le concept de processus et de fil
 - 5.6.3. Interaction entre processus ou fils
 - 5.6.4. Les fils en C++
 - 5.6.5. Avantages et inconvénients de la programmation concurrente
- 5.7. Gestion et synchronisation des fils
 - 5.7.1. Cycle de vie d'un fil
 - 5.7.2. La Classe *Thread*
 - 5.7.3. Planification du fil
 - 5.7.4. Groupes de fils
 - 5.7.5. Fils de type Daemon
 - 5.7.6. Synchronisation
 - 5.7.7. Mécanismes de verrouillage
 - 5.7.8. Mécanismes de communication
 - 5.7.9. Moniteurs
- 5.8. Problèmes courants en programmation concurrente
 - 5.8.1. Le problème du consommateur et du producteur
 - 5.8.2. Le problème des lecteurs et des écrivains
 - 5.8.3. Le problème du souper des philosophes
- 5.9. Documentation et test des logiciels
 - 5.9.1. Pourquoi la documentation des logiciels est-elle importante?
 - 5.9.2. Documentation sur la conception
 - 5.9.3. Utilisation des outils de documentation
- 5.10. Tests du Software
 - 5.10.1. Introduction aux tests logiciels
 - 5.10.2. Types de tests
 - 5.10.3. Tests unitaires
 - 5.10.4. Test d'intégration
 - 5.10.5. Test de validation
 - 5.10.6. Test du système

Module 6. Informatique théorique

- 6.1. Concepts mathématiques utilisés
 - 6.1.1. Introduction à la logique propositionnelle
 - 6.1.2. Théorie des relations
 - 6.1.3. Ensembles numérables et non numérables
- 6.2. Langages et grammaires formels et introduction aux machines de Turing
 - 6.2.1. Langages formels et grammaires
 - 6.2.2. Problème de décision
 - 6.2.3. La machine de Turing
- 6.3. Extensions aux machines de Turing, machines de Turing contraintes et ordinateurs
 - 6.3.1. Techniques de programmation pour les machines de Turing
 - 6.3.2. Extensions pour les machines de Turing
 - 6.3.3. Machines de Turing contraintes
 - 6.3.4. Machines de Turing et ordinateurs
- 6.4. Indécision
 - 6.4.1. Langage non récursivement énumérable
 - 6.4.2. Un problème indécidable récursivement énumérable
- 6.5. Autres problèmes indécidables
 - 6.5.1. Problèmes indécidables pour les machines de Turing
 - 6.5.2. Problème de la correspondance postale (PCP)
- 6.6. Problèmes insolubles
 - 6.6.1. Les classes P et NP
 - 6.6.2. Un problème NP-complet
 - 6.6.3. Problème de satisfiabilité restreinte
 - 6.6.4. Autres problèmes NP-complets
- 6.7. Problèmes de co-NP et de PS
 - 6.7.1. Complémentaire aux langages NP
 - 6.7.2. Problèmes solubles dans l'espace polynomial
 - 6.7.3. Problèmes PS complets
- 6.8. Classes de langages basés sur la randomisation
 - 6.8.1. Modèle MT avec randomisation
 - 6.8.2. Les classes RP et ZPP
 - 6.8.3. Test de primauté
 - 6.8.4. Complexité du test de primauté

- 6.9. Autres classes et grammaires
 - 6.9.1. Automates finis probabilistes
 - 6.9.2. Automates cellulaires
 - 6.9.3. Cellules *McCulloch* et Pitts
 - 6.9.4. Grammaires de Lindenmayer
- 6.10. Systèmes informatiques avancés
 - 6.10.1. Informatique membranaire: systèmes P
 - 6.10.2. Informatique ADN
 - 6.10.3. L'informatique quantique

Module 7. Théorie des automates et des langages formels

- 7.1. Introduction à la théorie des automates
 - 7.1.1. Pourquoi étudier la théorie des automates?
 - 7.1.2. Introduction aux preuves formelles
 - 7.1.3. Autres formes de preuve
 - 7.1.4. Induction mathématique
 - 7.1.5. Alphabets, chaînes de caractères et langages
- 7.2. Automates finis déterministes
 - 7.2.1. Introduction aux automates finis
 - 7.2.2. Automates finis déterministes
- 7.3. Automates finis non déterministes
 - 7.3.1. Automates finis non déterministes
 - 7.3.2. Équivalence entre AFD et AFND
 - 7.3.3. Automates finis avec transitions
- 7.4. Langues et expressions régulières (I)
 - 7.4.1. Langages et expressions régulières
 - 7.4.2. Automates finis et expressions régulières
- 7.5. Langages et expressions régulières (II)
 - 7.5.1. Conversion des expressions régulières en automates
 - 7.5.2. Applications des expressions régulières
 - 7.5.3. Algèbre des expressions régulières
- 7.6. Lemme de pompage et fermeture des langages réguliers
 - 7.6.1. Lemme de pompage
 - 7.6.2. Propriétés de fermeture des langages réguliers

- 7.7. Équivalence et minimisation des automates
 - 7.7.1. Équivalence AF
 - 7.7.2. Minimisation AF
- 7.8. Grammaires indépendantes du contexte (CIG)
 - 7.8.1. Grammaires indépendantes du contexte
 - 7.8.2. Arbres de dérivation
 - 7.8.3. Applications des GIC
 - 7.8.4. Ambiguïté dans les grammaires et les langages
- 7.9. Automates à pile et GICs
 - 7.9.1. Définition de Stack Automata
 - 7.9.2. Langues acceptées par un automate empilé
 - 7.9.3. Équivalence entre les automates à pile et les GIC
 - 7.9.4. Automates empilés déterministes
- 7.10. Formes normales, lemme de pompage des GIC et propriétés des LIC
 - 7.10.1. Formes normales des GIC
 - 7.10.2. Lemme de pompage
 - 7.10.3. Propriétés de fermeture des langages
 - 7.10.4. Propriétés de décision des LIC

Module 8. Processeurs de langue

- 8.1. Introduction au processus de compilation
 - 8.1.1. Compilation et interprétation
 - 8.1.2. Environnement d'exécution du compilateur
 - 8.1.3. Processus d'Analyse
 - 8.1.4. Processus de synthèse
- 8.2. Analyseur lexical
 - 8.2.1. Qu'est-ce qu'un analyseur lexical?
 - 8.2.2. Implémentation de l'analyseur lexical
 - 8.2.3. Actions sémantiques
 - 8.2.4. Récupération des erreurs
 - 8.2.5. Questions de mise en œuvre

- 8.3. Analyse syntaxique
 - 8.3.1. Qu'est-ce qu'un analyseur syntaxiques?
 - 8.3.2. Concepts préliminaires
 - 8.3.3. Analyseurs syntaxiques descendants
 - 8.3.4. Analyseurs ascendants
- 8.4. Analyse syntaxique descendante et ascendante
 - 8.4.1. Analyseur LL (1)
 - 8.4.2. Analyseur syntaxique LR (0)
 - 8.4.3. Exemple d'analyseur
- 8.5. Analyse ascendante avancée
 - 8.5.1. Analyseurs SLR
 - 8.5.2. Analyseur LR (1)
 - 8.5.3. Analyseur LR (k)
 - 8.5.4. Analyseurs LALR
- 8.6. Analyse sémantique (I)
 - 8.6.1. Traduction axée sur la syntaxe
 - 8.6.2. Table des symboles
- 8.7. Analyse sémantique (II)
 - 8.7.1. Vérification du type
 - 8.7.2. Le sous-système des types
 - 8.7.3. Équivalence des types et conversions
- 8.8. Génération de code et environnement d'exécution
 - 8.8.1. Aspects de la conception
 - 8.8.2. Environnement d'exécution
 - 8.8.3. Organisation de la mémoire
 - 8.8.4. Attribution de la mémoire
- 8.9. Génération de code intermédiaire
 - 8.9.1. Traduction axée sur la synthèse
 - 8.9.2. Représentations intermédiaires
 - 8.9.3. Exemples de traductions

- 8.10. Optimisation du code
 - 8.10.1. Allocation des registres
 - 8.10.2. Élimination des attributions mortes
 - 8.10.3. Exécution au moment de la compilation
 - 8.10.4. Réorganisation des expressions
 - 8.10.5. Optimisation des boucles

Module 9. Informatique graphique et visualisation

- 9.1. Théorie des couleurs
 - 9.1.1. Propriétés de la lumière
 - 9.1.2. Modèles de couleur
 - 9.1.3. La norme CIE
 - 9.1.4. *Profiling*
- 9.2. Primitives de sortie
 - 9.2.1. Le pilote vidéo
 - 9.2.2. Algorithmes de dessin au trait
 - 9.2.3. Algorithmes de dessin de cercle
 - 9.2.4. Algorithmes de remplissage
- 9.3. Transformations 2D et systèmes de coordonnées 2D et découpage 2D
 - 9.3.1. Transformations géométriques de base
 - 9.3.2. Coordonnées homogènes
 - 9.3.3. Transformation inverse
 - 9.3.4. Composition des transformations
 - 9.3.5. Autres transformations
 - 9.3.6. Coordonner le changement
 - 9.3.7. Systèmes de coordonnées 2D
 - 9.3.8. Changement de coordonnées
 - 9.3.9. Normalisation
 - 9.3.10. Algorithmes d'écritage
- 9.4. Transformations 3D
 - 9.4.1. Translation
 - 9.4.2. Rotation
 - 9.4.3. Mise à l'échelle
 - 9.4.4. Réflexion
 - 9.4.5. Cisaillement

- 9.5. Affichage et modification des coordonnées 3D
 - 9.5.1. Systèmes de coordonnées 3D
 - 9.5.2. Visualisation
 - 9.5.3. Changement de coordonnées
 - 9.5.4. Projection et normalisation
- 9.6. Projection et détournage 3D
 - 9.6.1. Projection orthogonale
 - 9.6.2. Projection Parallèles oblique
 - 9.6.3. Projection en perspective
 - 9.6.4. Algorithmes d'écrêtage 3D
- 9.7. Élimination des surfaces cachées
 - 9.7.1. *Back-Face Removal*
 - 9.7.2. *Z-Buffer*
 - 9.7.3. Algorithme du peintre
 - 9.7.4. Algorithme de Warnock
 - 9.7.5. Détection de lignes cachées
- 9.8. Interpolation et courbes paramétriques
 - 9.8.1. Interpolation et approximation polynomiale
 - 9.8.2. Représentation paramétrique
 - 9.8.3. Polynôme de Lagrange
 - 9.8.4. *Splines* cubiques naturelles
 - 9.8.5. Fonctions de base
 - 9.8.6. Représentation matricielle
- 9.9. Courbes de Bézier
 - 9.9.1. Construction algébrique
 - 9.9.2. Forme matricielle
 - 9.9.3. Composition
 - 9.9.4. Construction géométrique
 - 9.9.5. Algorithme de dessin



- 9.10. *B-Splines*
 - 9.10.1. Le problème du contrôle local
 - 9.10.2. B-splines cubiques uniformes
 - 9.10.3. Fonctions de base et points de contrôle
 - 9.10.4. Dérivée par rapport à l'origine et multiplicité
 - 9.10.5. Représentation matricielle
 - 9.10.6. B-splines non uniformes

Module 10. Informatique bio-inspirée

- 10.1. Introduction au calcul bio-inspiré
 - 10.1.1. Introduction au calcul bio-inspiré
- 10.2. Algorithmes d'adaptation sociale
 - 10.2.1. Calcul bio-inspiré basé sur les colonies de fourmis
 - 10.2.2. Variantes des algorithmes de colonies de fourmis
 - 10.2.3. Informatique en nuage de particules
- 10.3. Algorithmes génétiques
 - 10.3.1. Structure générale
 - 10.3.2. Mise en œuvre des principaux opérateurs
- 10.4. Stratégies spatiales d'exploration-exploitation pour les algorithmes génétiques
 - 10.4.1. Algorithme CHC
 - 10.4.2. Problèmes multimodaux
- 10.5. Modèles de calcul évolutif (I)
 - 10.5.1. Stratégies évolutives
 - 10.5.2. Programmation évolutive
 - 10.5.3. Algorithmes basés sur l'évolution différentielle
- 10.6. Modèles de calcul évolutif (II)
 - 10.6.1. Modèles évolutifs basés sur l'estimation des distributions (EDA)
 - 10.6.2. Programmation génétique
- 10.7. La programmation évolutive appliquée aux problèmes d'apprentissage
 - 10.7.1. Apprentissage basé sur des règles
 - 10.7.2. Méthodes évolutionnistes dans les problèmes de sélection d'instances
- 10.8. Problèmes multi-objectifs
 - 10.8.1. Concept de dominance
 - 10.8.2. Application des algorithmes évolutionnaires aux problèmes multi-objectifs

- 10.9. Réseaux neuronaux (I)
 - 10.9.1. Introduction aux réseaux neuronaux
 - 10.9.2. Exemple pratique avec les réseaux neuronaux
- 10.10. Réseaux neuronaux (II)
 - 10.10.1. Cas d'utilisation des réseaux neuronaux dans la recherche médicale
 - 10.10.2. Cas d'utilisation des réseaux neuronaux en économie
 - 10.10.3. Cas d'utilisation des réseaux neuronaux en vision industrielle

Module 11. Sécurité dans la conception et le développement des systèmes

- 11.1. Systèmes d'information
 - 11.1.1. Domaines de systèmes d'information
 - 11.1.2. Composants de systèmes d'information
 - 11.1.3. Activités de systèmes d'information
 - 11.1.4. Cycle de vie de systèmes d'information
 - 11.1.5. Ressources de systèmes d'information
- 11.2. Systèmes d'information. Typologie
 - 11.2.1. Types des systèmes d'information
 - 11.2.1.1. Entreprise
 - 11.2.1.2. Stratégiques
 - 11.2.1.3. Selon le champ d'application
 - 11.2.1.4. Spécifiques
 - 11.2.2. Systèmes d'information. Exemples concrets
 - 11.2.3. Évolution des systèmes d'information: étapes
 - 11.2.4. Méthodologies des systèmes d'information
- 11.3. Sécurité des systèmes d'information. Implications légales
 - 11.3.1. Accès aux Données
 - 11.3.2. Menaces pour la sécurité: vulnérabilités
 - 11.3.3. Implications juridiques: infractions pénales
 - 11.3.4. Procédures de maintenance des systèmes d'information
- 11.4. Sécurité des systèmes d'information. Protocole de sécurité
 - 11.4.1. Sécurité de systèmes d'information
 - 11.4.1.1. Intégration
 - 11.4.1.2. Confidentialité
 - 11.4.1.3. Disponibilité
 - 11.4.1.4. Authentification
 - 11.4.2. Services de sécurité
 - 11.4.3. Protocoles de sécurité de l'information. Typologie
 - 11.4.4. Sensibilité de systèmes d'information
- 11.5. Sécurité des systèmes d'information Mesures et systèmes de contrôle d'accès
 - 11.5.1. Mesures de sécurité
 - 11.5.2. Type de mesures de sécurité
 - 11.5.2.1. Prévention
 - 11.5.2.2. Détection
 - 11.5.2.3. Correction
 - 11.5.3. Systèmes de contrôle de Accès Typologie
 - 11.5.4. Cryptographie
- 11.6. Sécurité des réseaux et de l'internet
 - 11.6.1. *Firewalls*
 - 11.6.2. Identification numérique
 - 11.6.3. Virus et vers
 - 11.6.4. *Hacking*
 - 11.6.5. Exemples et cas réels
- 11.7. Délits informatiques
 - 11.7.1. Délit informatique
 - 11.7.2. Délits informatiques Typologie
 - 11.7.3. Délit informatique Attaque. Typologies
 - 11.7.4. Le cas de la réalité virtuelle
 - 11.7.5. Profils des délinquants et des victimes. Qualification pénale de l'infraction
 - 11.7.6. Délits informatiques Exemples et cas réels

- 11.8. Plan de sécurité d'un système d'information
 - 11.8.1. Plan de sécurité. Objectifs
 - 11.8.2. Plan de sécurité. Planification
 - 11.8.3. Plan de risques. Analyse
 - 11.8.4. Politique de sécurité. Mise en œuvre dans l'organisation
 - 11.8.5. Plan de sécurité. Mise en œuvre dans l'organisation
 - 11.8.6. Procédures de sécurité. Types
 - 11.8.7. Plan de sécurité. Exemples
- 11.9. Plan d'urgence
 - 11.9.1. Plan d'urgence. Fonctions
 - 11.9.2. Plan d'urgence: éléments et objectifs
 - 11.9.3. Plans des imprévu dans l'organisation. Mise en œuvre
 - 11.9.4. Plans d'intervention. Exemples
- 11.10. Gouvernance de la sécurité de systèmes d'information
 - 11.10.1. Réglementation juridique
 - 11.10.2. Normes
 - 11.10.3. Certifications
 - 11.10.4. Technologies

Module 12. Architectures et modèles de sécurité de l'information

- 12.1. Architecture de sécurité de l'information
 - 12.1.1. SGSI/PDS
 - 12.1.2. Alignement stratégique
 - 12.1.3. Gestion des risques
 - 12.1.4. Mesure de la performance
- 12.2. Modèles de sécurité de l'information
 - 12.2.1. Modèles de sécurités basé sur des politiques
 - 12.2.2. Basés sur des politiques, les modèles de sécurité
 - 12.2.3. Basés sur des outils de protection
- 12.3. Modèle de sécurité. Principaux éléments
 - 12.3.1. Identification des risques
 - 12.3.2. Définition des contrôles
 - 12.3.3. Évaluation continue des niveaux de risque
 - 12.3.4. Plan de sensibilisation des employés, fournisseurs, partenaires, etc.
- 12.4. Processus de gestion des risques
 - 12.4.1. Identification des actifs
 - 12.4.2. Identification des menaces
 - 12.4.3. Évaluation des risques
 - 12.4.4. Priorité des contrôles
 - 12.4.5. Réévaluation et risque résiduel
- 12.5. Processus d'entreprise et sécurité de l'information
 - 12.5.1. Processus d'activité
 - 12.5.2. Évaluation des risques sur la base de paramètres commerciaux
 - 12.5.3. Analyse de l'impact des activités
 - 12.5.4. Les opérations d'entreprise et sécurité de l'information
- 12.6. Processus d'amélioration continue
 - 12.6.1. Le cycle de Deming
 - 12.6.1.1. Planification
 - 12.6.1.2. Faire
 - 12.6.1.3. Vérifier
 - 12.6.1.4. Agir
- 12.7. Architectures de sécurité
 - 12.7.1. Sélection et homogénéisation des technologies
 - 12.7.2. Gestion de l'identité. Authentification
 - 12.7.3. Gestion de l'accès. Autorisation
 - 12.7.4. Sécurité de l'infrastructure des réseaux
 - 12.7.5. Technologies et solutions de cryptage
 - 12.7.6. Sécurité des dispositifs terminaux (EDR)
- 12.8. Le cadre réglementaire
 - 12.8.1. Réglementations sectorielles
 - 12.8.2. Certifications
 - 12.8.3. Législation
- 12.9. La norme ISO 27001
 - 12.9.1. Mise en œuvre
 - 12.9.2. Certification
 - 12.9.3. Contrôles et tests de pénétration
 - 12.9.4. Gestion continue des risques
 - 12.9.5. classification des informations

- 12.10. Législation sur la protection de la vie privée. RGPD (GDPR)
 - 12.10.1. Portée du Règlement Général sur la Protection des Données (RGPD)
 - 12.10.2. Données personnelles
 - 12.10.3. Rôles dans le traitement des données personnelles
 - 12.10.4. Droits d'ARCO
 - 12.10.5. Le DPD. Fonctions

Module 13. Gestion de la sécurité IT

- 13.1. Gestion de la sécurité
 - 13.1.1. Opérations de sécurité
 - 13.1.2. Aspect juridique et réglementaire
 - 13.1.3. Soutien aux entreprises
 - 13.1.4. Gestion des risques
 - 13.1.5. Gestion des identités et des accès
- 13.2. Structure de la zone de sécurité. Le bureau du CISO
 - 13.2.1. Structure organisationnelle Position du CISO dans la structure
 - 13.2.2. Les lignes de défense
 - 13.2.3. Organigramme du bureau du CISO
 - 13.2.4. Gestion du budget
- 13.3. Gouvernance de la sécurité
 - 13.3.1. Comité de sécurité
 - 13.3.2. Comité de suivi des risques
 - 13.3.3. Comité de contrôle
 - 13.3.4. Comité de crise
- 13.4. Gouvernance de la sécurité. Fonctions
 - 13.4.1. Politiques et normes
 - 13.4.2. Plan directeur de sécurité
 - 13.4.3. Tableaux de bord
 - 13.4.4. Sensibilisation et formation
 - 13.4.5. Sécurité de la chaîne d'approvisionnement
- 13.5. Opérations de sécurité
 - 13.5.1. Gestion des identités et des accès
 - 13.5.2. Configuration des règles de sécurité du réseau. *Firewalls*
 - 13.5.3. Gestion de la plateforme IDS/IPS
 - 13.5.4. Analyse de vulnérabilité
- 13.6. Cadre de Cybersécurité. NIST CSF
 - 13.6.1. Méthodologie NIST
 - 13.6.1.1. Identifier
 - 13.6.1.2. Protéger
 - 13.6.1.3. Détecter
 - 13.6.1.4. Répondre
 - 13.6.1.5. Récupérer
- 13.7. Centre des opérations de sécurité (SOC). Fonctions
 - 13.7.1. Protection. *Red Team, Pentesting, Threat Intelligence*
 - 13.7.2. Détection. *SIEM, User Behavior Analytics, Fraud Prevention*
 - 13.7.3. Réponse
- 13.8. Contrôles de sécurité
 - 13.8.1. Tests d'intrusion
 - 13.8.2. Exercices de *red team*
 - 13.8.3. Contrôles du code source. Développement sécurisé
 - 13.8.4. Sécurité des composants (*software supply chain*)
 - 13.8.5. Analyse médico-légale
- 13.9. Réponse aux incidents
 - 13.9.1. Préparation
 - 13.9.2. Détection, analyse et rapports
 - 13.9.3. Confinement, éradication et récupération
 - 13.9.4. Activité après l'incident
 - 13.9.4.1. Conservation des preuves
 - 13.9.4.2. Analyse médico-légale
 - 13.9.4.3. Gestion des lacunes
 - 13.9.5. Lignes directrices officielles pour la gestion des cyberincidents
- 13.10. Gestion des vulnérabilités
 - 13.10.1. Analyse de vulnérabilité
 - 13.10.2. Évaluation de vulnérabilité
 - 13.10.3. Base des systèmes
 - 13.10.4. Les vulnérabilités de type "zero-day" *Zero-Day*

Module 14. Analyse des risques et environnement de la sécurité informatique

- 14.1. Analyse de l'entourage
 - 14.1.1. Analyse de la situation extérieure
 - 14.1.1.1. Environnement VUCA
 - 14.1.1.1.1. Volatile
 - 14.1.1.1.2. Incertain
 - 14.1.1.1.3. complexe
 - 14.1.1.1.4. Ambiguës
 - 14.1.1.2. Environnement BANI
 - 14.1.1.2.1. Fragile
 - 14.1.1.2.2. Anxieux
 - 14.1.1.2.3. Non-linéaire
 - 14.1.1.2.4. Incompréhensible
 - 14.1.2. Analyse de l'environnement général PESTEL
 - 14.1.2.1. Politique
 - 14.1.2.2. Économique
 - 14.1.2.3. Social
 - 14.1.2.4. Technologique
 - 14.1.2.5. Écologique/Environnemental
 - 14.1.2.6. Legal
 - 14.1.3. Analyse de la situation interne. SWOT
 - 14.1.3.1. Objectifs
 - 14.1.3.2. Menaces
 - 14.1.3.3. Opportunités
 - 14.1.3.4. Points forts
- 14.2. Risque et incertitude
 - 14.2.1. Risque
 - 14.2.2. Gestion des risques
 - 14.2.3. Normes de gestion des risques
- 14.3. Lignes directrices pour le management du risque ISO 31.000:2018
 - 14.3.1. Objet
 - 14.3.2. Principes
 - 14.3.3. Cadre de référence
 - 14.3.4. Processus
- 14.4. Méthodologie d'analyse et de gestion des risques liés aux systèmes d'information (MAGERIT)
 - 14.4.1. Méthodologie MAGERIT
 - 14.4.1.1. Objectifs
 - 14.4.1.2. Méthode
 - 14.4.1.3. Éléments
 - 14.4.1.4. Techniques
 - 14.4.1.5. Outils disponibles (PILAR)
- 14.5. Transfert du risque cybernétique
 - 14.5.1. Transfert de risques
 - 14.5.2. Cyber risques. Typologie
 - 14.5.3. Assurance contre les cyberrisques
- 14.6. Méthodologies agiles pour la gestion de risques
 - 14.6.1. Méthodologie agile
 - 14.6.2. Scrum pour la gestion de risque
 - 14.6.3. *Agile Risk Management*
- 14.7. Technologies pour la gestion du risque
 - 14.7.1. L'intelligence artificielle appliquée à la gestion des risques
 - 14.7.2. *Blockchain* et cryptographie. Méthodes de préservation de la valeur
 - 14.7.3. L'informatique quantique Opportunité ou menace
- 14.8. Cartographie des risques informatiques basée sur les méthodologies Agile
 - 14.8.1. Représentation de la vraisemblance et de l'impact dans les environnements agiles
 - 14.8.2. Le risque comme menace pour la valeur
 - 14.8.3. Réévolution dans la gestion de projet et les processus agiles basés sur les KRIs
- 14.9. *Risk Driven* axée sur le risque
 - 14.9.1. *Risk Driven*
 - 14.9.2. *Risk Driven* axée sur le risque
 - 14.9.3. Développement d'un modèle de gestion d'entreprise axé sur le risque
- 14.10. Innovation et transformation numérique dans la gestion des risques informatiques.
 - 14.10.1. La gestion agile des risques comme source d'innovation commerciale
 - 14.10.2. Transformation des données en informations utiles à la prise de décision
 - 14.10.3. Vision holistique de l'entreprise à travers le risque

Module 15. Cryptographie en informatique

- 15.1. Cryptographie
 - 15.1.1. Cryptographie
 - 15.1.2. Bases mathématiques
- 15.2. Cryptologie
 - 15.2.1. Cryptologie
 - 15.2.2. Cryptanalyse
 - 15.2.3. Stéganographie et stéganalyse
- 15.3. Protocoles cryptographiques
 - 15.3.1. Blocs de base
 - 15.3.2. Protocoles de base
 - 15.3.3. Protocoles intermédiaires
 - 15.3.4. Protocoles avancés
 - 15.3.5. Protocoles exotériques
- 15.4. Techniques cryptographiques
 - 15.4.1. Longueur de la clé
 - 15.4.2. Manipulation des clés
 - 15.4.3. Types d'algorithmes
 - 15.4.4. Résumé des fonctions. *Hash*
 - 15.4.5. Générateurs de nombres pseudo-aléatoires
 - 15.4.6. Utilisation d'algorithmes
- 15.5. Cryptographie symétrique
 - 15.5.1. Blocs de chiffrement
 - 15.5.2. DES (*Data Encryption Standard*)
 - 15.5.3. Algorithme RC4
 - 15.5.4. AES (*Advance Encryption Standard*)
 - 15.5.5. Combinaison de chiffrements par blocs
 - 15.5.6. Dérivation de la clé
- 15.6. Cryptographie asymétrique
 - 15.6.1. Diffie-Hellman
 - 15.6.2. DSA (*Digital Signature Algorithm*)
 - 15.6.3. RSA (Rivest, Shamir y Adleman)
 - 15.6.4. Courbe elliptique
 - 15.6.5. Cryptographie asymétrique Typologie

- 15.7. Certificats numériques
 - 15.7.1. Signature numérique
 - 15.7.2. Certificats X509
 - 15.7.3. Infrastructure à clé publique(PKI)
- 15.8. Implémentations
 - 15.8.1. Kerberos
 - 15.8.2. IBM CCA
 - 15.8.3. *Pretty Good Privacy* (PGP)
 - 15.8.4. *ISO Authentication Framework*
 - 15.8.5. SSL et TLS
 - 15.8.6. Cartes à puce dans les moyens de paiement (EMV)
 - 15.8.7. Protocoles de téléphonie mobile
 - 15.8.8. *Blockchain*
- 15.9. Stéganographie
 - 15.9.1. Stéganographie
 - 15.9.2. Steganoanalyse
 - 15.9.3. Applications et utilisations
- 15.10. Cryptographie quantique
 - 15.10.1. Algorithmes quantiques
 - 15.10.2. Protection des algorithmes contre l'informatique quantique
 - 15.10.3. Distribution de clés quantiques

Module 16. Gestion des identités et des accès dans la sécurité informatique

- 16.1. Gestion des identités et des accès (IAM)
 - 16.1.1. Identité numérique
 - 16.1.2. Gestion de l'identité
 - 16.1.3. Fédération d'identité
- 16.2. contrôle d'accès physique
 - 16.2.1. Systèmes de protection
 - 16.2.2. Sécurité de la zone
 - 16.2.3. Installations de récupération
- 16.3. Contrôle d'accès logique
 - 16.3.1. Authentification: typologie
 - 16.3.2. Protocoles d'authentification
 - 16.3.3. Attaques d'authentification

- 16.4. Contrôle d'accès logique Authentification MFA
 - 16.4.1. Contrôle d'accès logique Authentification MFA
 - 16.4.2. Mots de passe. Importance
 - 16.4.3. Attaques d'authentification
- 16.5. Contrôle d'accès logique Authentification biométrique
 - 16.5.1. Contrôle d'accès logique Authentification biométrique
 - 16.5.1.1. Authentification biométrique Exigences
 - 16.5.2. Fonctionnement
 - 16.5.3. Modèles et techniques
- 16.6. Systèmes de gestion de l'authentification
 - 16.6.1. *Single sign on*
 - 16.6.2. Kerberos
 - 16.6.3. Systèmes AAA
- 16.7. Systèmes de gestion de l'authentification: Systèmes AAA
 - 16.7.1. TACACS
 - 16.7.2. RADIUS
 - 16.7.3. DIAMETER
- 16.8. Services de contrôle d'accès
 - 16.8.1. FW - Pare-feu
 - 16.8.2. VPN - Réseaux privés virtuels
 - 16.8.3. Systèmes de contrôle d'accès au réseau
- 16.9. Systèmes de contrôle d'accès au réseau
 - 16.9.1. NAC
 - 16.9.2. Architecture et éléments
 - 16.9.3. Fonctionnement et normalisation
- 16.10. Accès aux réseaux sans fil
 - 16.10.1. Types de réseaux sociaux
 - 16.10.2. Sécurité dans les réseaux sans fil
 - 16.10.3. Attaques contre les réseaux sans fil

Module 17. Sécurité des communications et de l'exploitation du software

- 17.1. Sécurité informatique dans les communications et l'exploitation des logiciels
 - 17.1.1. Sécurité informatique
 - 17.1.2. Cybersécurité
 - 17.1.3. Sécurité du cloud
- 17.2. Sécurité informatique dans les communications et l'exploitation des logiciels. Typologie
 - 17.2.1. Sécurité physique
 - 17.2.2. Sécurité logique
- 17.3. Sécurité des communications
 - 17.3.1. Principaux éléments
 - 17.3.2. Sécurité des réseaux
 - 17.3.3. Meilleures pratiques
- 17.4. Cyber intelligence
 - 17.4.1. Ingénierie sociale
 - 17.4.2. *Deep Web*
 - 17.4.3. *Phishing*
 - 17.4.4. *Malware*
- 17.5. Développement Sécurité des communications et de l'exploitation du software
 - 17.5.1. Développement sécurisé Protocole HTTP
 - 17.5.2. Développement sécurisé Cycle de vie
 - 17.5.3. Développement sécurisé Sécurité PHP
 - 17.5.4. Développement sécurisé Sécurité NET
 - 17.5.5. Développement sécurisé Meilleures pratiques
- 17.6. Systèmes de gestion de la sécurité de l'information des communications et de l'exploitation du software
 - 17.6.1. RGPD
 - 17.6.2. ISO 27021
 - 17.6.3. ISO 27017/ 18
- 17.7. Technologies SIEM
 - 17.7.1. Technologies SIEM
 - 17.7.2. Fonctionnement du SOC
 - 17.7.3. *SIEM vendors*

- 17.8. Le rôle de la sécurité dans les organisations
 - 17.8.1. Rôles dans les organisations
 - 17.8.2. Rôle des spécialistes de l'IdO dans les entreprises
 - 17.8.3. Certifications reconnues sur le marché
- 17.9. Analyse médico-légale
 - 17.9.1. Analyse médico-légale
 - 17.9.2. Analyse médico-légale Méthodologie
 - 17.9.3. Analyse médico-légale Outils et mise en œuvre
- 17.10. La Cybersécurité aujourd'hui
 - 17.10.1. Cyberattaques majeures
 - 17.10.2. Prévisions d'employabilité
 - 17.10.3. Défis

Module 18. Sécurité des Environnements *Cloud*

- 18.1. Sécurité dans les environnements *Cloud computing*
 - 18.1.1. Sécurité dans les environnements *Cloud computing*
 - 18.1.2. Sécurité dans les environnements *Cloud Computing*. Menaces et risques pour la sécurité
 - 18.1.3. Sécurité dans les environnements *Cloud Computing*. Principaux aspects de la sécurité
- 18.2. Types d'infrastructures en *Cloud*
 - 18.2.1. Public
 - 18.2.2. Privé
 - 18.2.3. Hybride
- 18.3. Modèle de gestion partagée
 - 18.3.1. Éléments de sécurité gérés par le fournisseur
 - 18.3.2. Éléments gérés par le client
 - 18.3.3. Définition de la stratégie de sécurité
- 18.4. Mécanismes de prévention
 - 18.4.1. Systèmes de gestion de l'authentification
 - 18.4.2. Système de gestion des autorisations : politiques d'accès
 - 18.4.3. Systèmes de gestion des clés
- 18.5. Sécurisation du système
 - 18.5.1. Sécurisation des systèmes de stockage
 - 18.5.2. Sécurisation des systèmes de bases de données
 - 18.5.3. Sécuriser les données en transit

- 18.6. Protection des infrastructures
 - 18.6.1. Conception et mise en œuvre de réseaux sécurisés
 - 18.6.2. Sécurité des ressources informatiques
 - 18.6.3. Outils et ressources pour la protection des infrastructures
- 18.7. Détection des menaces et des attaques
 - 18.7.1. Systèmes de contrôle, *Logging* d'enregistrement et de surveillance
 - 18.7.2. Systèmes de événements et d'alarmes
 - 18.7.3. Systèmes SIEM
- 18.8. Réponse aux incidents
 - 18.8.1. Plan de réponse aux incidents
 - 18.8.2. Continuité des activités
 - 18.8.3. Analyse médico-légale et remédiation d'incidents de même nature
- 18.9. La sécurité en *Clouds* publics
 - 18.9.1. AWS(Amazon Web Services)
 - 18.9.2. Microsoft Azure
 - 18.9.3. Google &GCP
 - 18.9.4. Oracle *Cloud*
- 18.10. Réglementation et conformité
 - 18.10.1. Conformité en matière de sécurité
 - 18.10.2. Gestion des risques
 - 18.10.3. Personnes et processus dans les organisations

Module 19. Sécurité des communications des dispositifs IoT

- 19.1. De la télémétrie à l'IdO
 - 19.1.1. Télémétrie
 - 19.1.2. Connectivité M2M
 - 19.1.3. Démocratisation de la télémétrie
- 19.2. Modèles de référence de l'IdO
 - 19.2.1. Modèles de référence de l'IdO
 - 19.2.2. Architecture IoT simplifiée
- 19.3. Vulnérabilités de la sécurité de l'IdO
 - 19.3.1. Dispositifs IoT
 - 19.3.2. Dispositifs IoT Études de cas d'utilisation
 - 19.3.3. Dispositifs IoT Vulnérabilités

- 19.4. Connectivité IoT
 - 19.4.1. Réseaux PAN, LAN, WAN
 - 19.4.2. Technologies sans fil non IoT
 - 19.4.3. Technologies sans fil LPWAN
- 19.5. Technologies LPWAN
 - 19.5.1. Le triangle de fer des LPWAN
 - 19.5.2. Bandes de fréquences libres vs. Bandes sous licence
 - 19.5.3. Options technologiques LPWAN
- 19.6. Technologie LoRaWAN
 - 19.6.1. Technologie LoRaWAN
 - 19.6.2. Cas d'utilisation de LoRaWAN. Écosystème
 - 19.6.3. Sécurité dans LoRaWAN
- 19.7. Technologie Sigfox
 - 19.7.1. Technologie Sigfox
 - 19.7.2. Cas d'utilisation de Sigfox. Écosystème
 - 19.7.3. Sécurité dans Sigfox
- 19.8. Technologie cellulaire IoT
 - 19.8.1. Technologie cellulaire IoT (NB-IoT et LTE-M)
 - 19.8.2. Cas d'utilisation de l'IoT cellulaire. Écosystème
 - 19.8.3. Sécurité de l'IdO cellulaire
- 19.9. Technologie Wi-SUN
 - 19.9.1. Technologie Wi-SUN
 - 19.9.2. Cas d'utilisation du Wi-SUN. Écosystème
 - 19.9.3. Sécurité en Wi-SUN
- 19.10. Autres technologies IoT
 - 19.10.1. Autres technologies IoT
 - 19.10.2. Cas d'utilisation et écosystème des autres technologies IoT
 - 19.10.3. Sécurité dans d'autres technologies IoT

Module 20. Plan de continuité des activités associé à la sécurité

- 20.1. Plans de continuité des activités
 - 20.1.1. Planification de la continuité des activités (PCA)
 - 20.1.2. Plan de continuité des activités (PCA). Aspects clés
 - 20.1.3. Plan de continuité des activités (PCA) pour l'évaluation de l'entreprise
- 20.2. Mesures dans un plan de continuité des activités (PCA)
 - 20.2.1. *Recovery Time Objective* (RTO) et *Recovery Point Objective* (RPO)
 - 20.2.2. Durée maximale tolérable (DMT)
 - 20.2.3. Niveaux de récupération minimum (ROL)
 - 20.2.4. Objectif de point de récupération (RPO)
- 20.3. Projets de continuité. Typologie
 - 20.3.1. Plan de continuité des activités (PCA)
 - 20.3.2. Plan d'Continuité des PCTIC)
 - 20.3.3. Plan de reprise après sinistre (PRS)
- 20.4. Gestion des risques associés au PCA
 - 20.4.1. Analyse de l'impact des activités
 - 20.4.2. Avantages de la mise en œuvre d'un PCA
 - 20.4.3. Réflexion sur les risques
- 20.5. Cycle de vie d'un plan de continuité des activités
 - 20.5.1. Phase 1: Analyse de l'organisation
 - 20.5.2. Phase 2: Détermination de la stratégie de continuité
 - 20.5.3. Phase 3: Réponse d'urgence
 - 20.5.4. Phase 4: Tests, maintenance et révision
- 20.6. Phase d'analyse organisationnelle d'un PCA
 - 20.6.1. Identification des processus dans le champ d'application du PCA
 - 20.6.2. Identification des domaines d'activité critiques
 - 20.6.3. Identification des dépendances entre les domaines et les processus
 - 20.6.4. Détermination des MTD appropriées
 - 20.6.5. Produits livrables Création d'un plan
- 20.7. Phase d'analyse Stratégie d' de continuité un PCA
 - 20.7.1. Rôles dans la phase de détermination de la stratégie
 - 20.7.2. Tâches de la phase de détermination de la stratégie
 - 20.7.3. Produits livrables

- 20.8. Phase d'intervention d'urgence d'un PCA
 - 20.8.1. Rôles dans la phase de réponse
 - 20.8.2. Tâches dans cette phase
 - 20.8.3. Produits livrables
- 20.9. Phase de test, de maintenance et de révision d'un PCA
 - 20.9.1. Rôles dans la phase de test, de maintenance et de révision
 - 20.9.2. Tâches de la phase de test, de maintenance et de révision
 - 20.9.3. Produits livrables
- 20.10. Normes ISO associées aux plans de continuité des activités (PCA)
 - 20.10.1. ISO 22301: 2019
 - 20.10.2. ISO 22313: 2020
 - 20.10.3. Autres normes ISO et internationales connexes

Module 21. Analytique des données dans l'organisation de l'entreprise

- 21.1. Analyse d'entreprise
 - 21.1.1. Analyse d'entreprise
 - 21.1.2. Structure des données
 - 21.1.3. Phases et éléments
- 21.2. Analyse des données dans l'entreprise
 - 21.2.1. Tableaux de bord et KPI's des départements
 - 21.2.2. Rapports opérationnels, tactiques et stratégiques
 - 21.2.3. Analyse des données appliquée à chaque département
 - 21.2.3.1. Marketing et communication
 - 21.2.3.2. Commercial
 - 21.2.3.3. Service à la clientèle
 - 21.2.3.4. Achats
 - 21.2.3.5. Administration
 - 21.2.3.6. RH
 - 21.2.3.7. Production
 - 21.2.3.8. IT
- 21.3. Marketing et communication
 - 21.3.1. KPI's à mesurer, applications et avantages
 - 21.3.2. Systèmes de Marketing et *Data Warehouse*
 - 21.3.3. Mise en œuvre d'une structure d'analyse des données dans le domaine du Marketing
 - 21.3.4. Plan de Marketing et de Communication
 - 21.3.5. Stratégies, prévisions et gestion des campagnes
- 21.4. Commercial et ventes
 - 21.4.1. Contributions de l'analyse des données dans le domaine commercial
 - 21.4.2. Besoins du département de ventes
 - 21.4.3. Études de marché
- 21.5. Service à la clientèle
 - 21.5.1. Fidélisation
 - 21.5.2. Qualité personnelle et intelligence émotionnelle
 - 21.5.3. Satisfaction des clients
- 21.6. Achats
 - 21.6.1. Analyse de données pour les études de marché
 - 21.6.2. Analyse de données pour les études de compétences
 - 21.6.3. Autres applications
- 21.7. Administration
 - 21.7.1. Besoins du département des administration
 - 21.7.2. *Data Warehouse* et analyse des risques financiers
 - 21.7.3. *Data Warehouse* et analyse des risques du crédit
- 21.8. Ressources humaines
 - 21.8.1. RH et les avantages de l'analyse des données
 - 21.8.2. Outils d'analyse des données dans le département des RH
 - 21.8.3. Application de l'analyse des données dans les RH
- 21.9. Production
 - 21.9.1. Analyse des données dans un service de production
 - 21.9.2. Applications
 - 21.9.3. Bénéfices



21.10. IT

21.10.1. Département d'IT

21.10.2. Analyse des données et transformation numérique

21.10.3. Innovation et productivité

Module 22. Gestion et manipulation de Données et d'Informations pour la Science de Données

22.1. Statistiques Variables, indices et rapports

22.1.1. Statistiques

22.1.2. Dimensions statistiques

22.1.3. Variables, indices et rapports

22.2. Typologie des données

22.2.1. Qualitatifs

22.2.2. Quantitatifs

22.2.3. Caractérisation et catégories

22.3. Connaissance des données issues des mesures

22.3.1. Mesures de centralisation

22.3.2. Mesures de la dispersion

22.3.3. Corrélation

22.4. Connaissance des données issues de Graphiques

22.4.1. Visualisation selon le type de données

22.4.2. Interprétation des rapports graphiques

22.4.3. Personnalisation des graphiques avec R

22.5. Probabilités

22.5.1. Probabilités

22.5.2. Fonction de probabilité

22.5.3. Distributions

22.6. Collecte des Données

22.6.1. Méthodologie de collecte

22.6.2. Outils de collecte

22.6.3. Canaux de collecte

- 22.7. Nettoyage des données
 - 22.7.1. Phases du nettoyage de Données
 - 22.7.2. Qualité des données
 - 22.7.3. Manipulation de Données (avec R)
- 22.8. Analyse des données, interprétation et et l'évaluation des résultats
 - 22.8.1. Mesures statistiques
 - 22.8.2. Indices de ratios
 - 22.8.3. Extraction de Données
- 22.9. Stockage de données (*Data Warehouse*)
 - 22.9.1. Éléments
 - 22.9.2. Design
- 22.10. Disponibilité des données
 - 22.10.1. Accès
 - 22.10.2. Utilitaire
 - 22.10.3. Sécurité

Module 23. Dispositifs et plateformes IoT comme base de la science des Données

- 23.1. *Internet of things*
 - 23.1.1. Internet du futur, *Internet of Things*
 - 23.1.2. Le Consortium de l'Internet industriel
- 23.2. Architecture de référence
 - 23.2.1. L'architecture de référence
 - 23.2.2. Couches
 - 23.2.3. Composants
- 23.3. Capteurs et dispositifs IoT
 - 23.3.1 Principaux composants
 - 23.3.2. Capteurs et actionneurs
- 23.4. Communication et protocoles
 - 23.4.1. Protocoles Modèle OSI
 - 23.4.2. Technologie et communication
- 23.5. Plateformes Cloud pour l'IoT et l'IIoT
 - 23.5.1. Plats-formes à usage général
 - 23.5.2. Plateformes industrielles
 - 23.5.3. Plats-formes à source ouverte

- 23.6. Gestion des données dans les plateformes IoT
 - 23.6.1. Mécanismes de gestion de Données Données ouvertes
 - 23.6.2. Échange et visualisation de Données
- 23.7. Sécurité IoT
 - 23.7.1. Exigences et domaines de sécurité
 - 23.7.2. Stratégies de sécurité IIoT
- 23.8. Applications IoT
 - 23.8.1. Villes intelligentes
 - 23.8.2. Santé et forme physique
 - 23.8.3. Maison intelligente
 - 23.8.4. Autres applications
- 23.9. Applications IoT
 - 23.9.1. Fabrication
 - 23.9.2. Transport
 - 23.9.3. Énergie
 - 23.9.4. Agriculture et élevage
 - 23.9.5. Autres secteurs
- 23.10. Industrie 4.0
 - 23.10.1. IoRT (*Internet of Robotics Things*)
 - 23.10.2. Fabrication additive 3D
 - 23.10.3. *Big Data Analytics*

Module 24. Représentation graphique pour l'Analyse de Données

- 24.1. Analyses exploratoires
 - 24.1.1. Représentation de l'analyse des données
 - 24.1.2. La valeur de la représentation graphique
 - 24.1.3. Nouveaux paradigmes de la représentation graphique
- 24.2. Optimisation de la science de Données
 - 24.2.1. La gamme de couleurs et le design
 - 24.2.2. La Gestalt dans la représentation graphique
 - 24.2.3. Erreurs à éviter et conseils

- 24.3. Sources des données de base
 - 24.3.1. Pour une représentation de qualité
 - 24.3.2. Pour une représentation de quantité
 - 24.3.3. Pour une représentation de temps
- 24.4. Sources de Données complexes
 - 24.4.1. Fichiers, listes et bases de données
 - 24.4.2. Données ouvertes
 - 24.4.3. Données générées en continu
- 24.5. Types de graphiques
 - 24.5.1. Représentations de base
 - 24.5.2. Représentation par blocs
 - 24.5.3. Représentation de l'analyse de la dispersion
 - 24.5.4. Représentations circulaires
 - 24.5.5. Représentations de bulles
 - 24.5.6. Représentations géographiques
- 24.6. Types de visualisation
 - 24.6.1. Comparatif et relationnel
 - 24.6.2. Distribution
 - 24.6.3. Hiérarchique
- 24.7. Conception de rapports avec représentation graphique
 - 24.7.1. Application des graphiques dans les rapports de Marketing
 - 24.7.2. Application des graphiques dans les tableaux de bord et les KPI's
 - 24.7.3. Application des graphiques dans les plans stratégiques
 - 24.7.4. Autres utilisations: science, santé, affaires
- 24.8. Récit graphique
 - 24.8.1. Récit graphique
 - 24.8.2. Évolution
 - 24.8.3. Utilitaire
- 24.9. Outils orientés vers la visualisation
 - 24.9.1. Outils avancés
 - 24.9.2. Logiciel en ligne
 - 24.9.3. *Open Source*

- 24.10. Nouvelles technologies dans la visualisation de Données
 - 24.10.1. Systèmes de virtualisation de la réalité
 - 24.10.2. Systèmes de et amélioration de la réalité
 - 24.10.3. Systèmes intelligents

Module 25. Outils de science de Données

- 25.1. Science de Données
 - 25.1.1. La science des Données
 - 25.1.2. Outils avancés pour le scientifique de Données
- 25.2. Données, informations et connaissances
 - 25.2.1. Données, informations et connaissances
 - 25.2.2. Types de Données
 - 25.2.3. Sources de Données
- 25.3. Des données aux informations
 - 25.3.1. Analyse des données
 - 25.3.2. Types d'analyses
 - 25.3.3. Extraction d'informations d'un *Dataset*
- 25.4. Extraction d'informations par la visualisation
 - 25.4.1. La Visualisation comme outil d'analyse
 - 25.4.2. Méthodes de visualisation
 - 25.4.3. Visualisation d'un ensemble de Données
- 25.5. Qualité des Données
 - 25.5.1. Données de qualité
 - 25.5.2. Nettoyage des Données
 - 25.5.3. Prétraitement de base de Données
- 25.6. *Dataset*
 - 25.6.1. Enrichissement du *dataset*
 - 25.6.2. La malédiction de la dimensionnalité
 - 25.6.3. Modification de notre jeu de Données
- 25.7. Déséquilibre
 - 25.7.1. Déséquilibre des classes
 - 25.7.2. Techniques d'atténuation des déséquilibres
 - 25.7.3. Équilibrage d'un *dataset*

- 25.8. Modèles non supervisé
 - 25.8.1. Modèle non supervisé
 - 25.8.2. Méthodes
 - 25.8.3. Classification avec des modèles non supervisés
- 25.9. Modèles non supervisés
 - 25.9.1. Modèle non supervisé
 - 25.9.2. Méthodes
 - 25.9.3. Classification avec des modèles supervisés
- 25.10. Outils et bonnes pratiques
 - 25.10.1. Bonnes pratiques pour un scientifique des données
 - 25.10.2. Le meilleur modèle
 - 25.10.3. Outils utiles

Module 26. Extraction de Données; Sélection, pré-traitement et transformation

- 26.1. L'inférence statistique
 - 26.1.1. Statistiques descriptives inférence statistique
 - 26.1.2. Procédures paramétriques
 - 26.1.3. Procédures non paramétriques
- 26.2. Analyses exploratoires
 - 26.2.1. Analyse descriptive
 - 26.2.2. Visualisation
 - 26.2.3. Préparation des Données
- 26.3. Préparation des Données
 - 26.3.1. Intégration et nettoyage de Données
 - 26.3.2. Normalisation des Données
 - 26.3.3. Transformer les attributs
- 26.4. Les valeurs manquantes
 - 26.4.1. Traitement des valeurs manquantes
 - 26.4.2. Méthodes d'imputation par maximum de vraisemblance
 - 26.4.3. Imputation des valeurs manquantes par apprentissage automatique

- 26.5. Bruit dans les Données
 - 26.5.1. Classes et attributs de bruit
 - 26.5.2. Filtrage du bruit
 - 26.5.3. Effet du bruit
- 26.6. La malédiction de la dimensionnalité
 - 26.6.1. *Oversampling*
 - 26.6.2. *Undersampling*
 - 26.6.3. Réduction des Données multidimensionnelles
- 26.7. Des attributs continus aux attributs discrets
 - 26.7.1. Données continues Vs. Discrets
 - 26.7.2. Processus de discrétisation
- 26.8. Les Données
 - 26.8.1. Sélection des Données
 - 26.8.2. Perspectives et critères de sélection
 - 26.8.3. Méthodes de sélection
- 26.9. Sélection d'instances
 - 26.9.1. Méthodes de sélection des instances
 - 26.9.2. Sélection des prototypes
 - 26.9.3. Méthodes avancées pour la sélection des instances
- 26.10. Prétraitement des données dans les environnements *Big Data*
 - 26.10.1. *Big Data*
 - 26.10.2. Prétraitement classique vs. Massif
 - 26.10.3. *Smart Data*

Module 27. Prédicibilité et analyse des phénomènes stochastiques

- 27.1. Séries chronologiques
 - 27.1.1. Séries chronologiques
 - 27.1.2. Utilité et applicabilité
 - 27.1.3. Études de cas connexes
- 27.2. Les séries temporelles
 - 27.2.1. Tendances saisonnières de ST
 - 27.2.2. Variations typiques
 - 27.2.3. Analyse des résidus

- 27.3. Typologies
 - 27.3.1. Stationnaires
 - 27.3.2. Non Stationnaires
 - 27.3.3. Transformations et ajustements
- 27.4. Schémas pour les séries temporelles
 - 27.4.1. Schéma (modèle) additif
 - 27.4.2. Schéma (modèle) multiplicatif
 - 27.4.3. Procédures pour déterminer le type de modèle
- 27.5. Méthodes de base de *Forecast*
 - 27.5.1. Moyenne
 - 27.5.2. *Naïve*
 - 27.5.3. *Naïveté* saisonnière
 - 27.5.4. Comparaison des méthodes
- 27.6. Analyse des résidus
 - 27.6.1. Autocorrélation
 - 27.6.2. ACF des résidus
 - 27.6.3. Test de corrélation
- 27.7. Régression dans le contexte des séries chronologiques
 - 27.7.1. ANOVA
 - 27.7.2. Principes fondamentaux
 - 27.7.3. Application pratique:
- 27.8. Modèles prédictifs de séries chronologiques
 - 27.8.1. ARIMA
 - 27.8.2. Lissage exponentiel
- 27.9. Manipulation et analyse de séries chronologiques avec R
 - 27.9.1. Préparation des Données
 - 27.9.2. Identification des motifs
 - 27.9.3. Analyse du modèle
 - 27.9.4. Pronostic
- 27.10. Analyse graphique combinée avec R
 - 27.10.1. Situations habituelles
 - 27.10.2. Application pratique pour la résolution de problèmes simples
 - 27.10.3. Application pratique pour la résolution de problèmes avancés

Module 28. Conception et développement de systèmes intelligents

- 28.1. Prétraitement des Données
 - 28.1.1. Prétraitement des Données
 - 28.1.2. Transformation des Données
 - 28.1.3. Extraction de Données
- 28.2. Apprentissage automatique
 - 28.2.1. Apprentissage supervisé et non supervisé
 - 28.2.2. Apprentissage par renforcement
 - 28.2.3. Autre paradigmes d'apprentissage
- 28.3. Algorithmes de classification
 - 28.3.1. Apprentissage automatique inductif
 - 28.3.2. SVM y KNN
 - 28.3.3. Métriques et scores pour la classification
- 28.4. Algorithmes de régression
 - 28.4.1. Régression linéaire, régression logistique et modèles non linéaires
 - 28.4.2. Séries temporelles
 - 28.4.3. Métriques et scores de régression
- 28.5. Algorithmes de mise en grappes
 - 28.5.1. Techniques de regroupement hiérarchique
 - 28.5.2. Techniques de regroupement partitionnel
 - 28.5.3. Métriques et scores de *Clustering*
- 28.6. Techniques de règles d'association
 - 28.6.1. Méthodes d'extraction de règles
 - 28.6.2. Métriques et scores pour les algorithmes de règles d'association
- 28.7. Techniques de classification avancées Multiclassificateurs
 - 28.7.1. Algorithmes de *Bagging*
 - 28.7.2. Classificateur "*Random Forests*"
 - 28.7.3. "*Boosting*" pour les arbres de décision
- 28.8. Modèles graphiques probabilistes
 - 28.8.1. Modèles probabilistes
 - 28.8.2. Réseaux bayésiens. Propriétés, représentation et paramétrage
 - 28.8.3. Autres modèles graphiques probabilistes

- 28.9. Réseaux neuronaux
 - 28.9.1. Apprentissage automatique avec les réseaux neuronaux artificielle
 - 28.9.2. Resaux *Feedforward*
- 28.10. Apprentissage profond
 - 28.10.1. Réseaux *Feedforward* profonds
 - 28.10.2. Réseaux neuronaux convolutifs et modèles de séquences
 - 28.10.3. Outils pour la mise en œuvre de réseaux neuronaux profonds

Module 29. Architectures et systèmes à forte intensité de données

- 29.1. Exigences non fonctionnelles. Piliers des applications de Big Data
 - 29.1.1. Fiabilité
 - 29.1.2. Adaptabilité
 - 29.1.3. Maintenabilité
- 29.2. Modèles de Données
 - 29.2.1. Modèle relationnel
 - 29.2.2. Modèle documentaire
 - 29.2.3. Modèle de Données du réseau
- 29.3. Bases de données. Gestion du stockage et de la récupération de Données
 - 29.3.1. Indices *Hash*
 - 29.3.2. Stockage structuré du *Log*
 - 29.3.3. Stockage des tables de segments
- 29.4. Formats d'encodage de Données
 - 29.4.1. Formats spécifique du langage
 - 29.4.2. Formats standardisés
 - 29.4.3. Formats d'encodage binaires
 - 29.4.4. Flux de Données entre processus
- 29.5. Réplication
 - 29.5.1. Objectifs de la réplication
 - 29.5.2. Modèles de réplication
 - 29.5.3. Problèmes de réplication

- 29.6. Transactions distribuées
 - 29.6.1. Transaction
 - 29.6.2. Protocoles pour les transactions distribuées
 - 29.6.3. Transactions sérialisables
- 29.7. Partitionnement
 - 29.7.1. Formes de cloisonnement
 - 29.7.2. Interaction et partitionnement des index secondaires
 - 29.7.3. Rééquilibrage des partitions
- 29.8. Traitement des *Datos Offline*
 - 29.8.1. Traitement par lots
 - 29.8.2. Systèmes de fichiers distribués
 - 29.8.3. MapReduce
- 29.9. Traitement des données en temps réel
 - 29.9.1. Types de *Broker* de messages
 - 29.9.2. Représentation des bases de données en tant que flux de Données
 - 29.9.3. Traitement des flux de Données
- 29.10. Applications commerciales pratiques
 - 29.10.1. Cohérence dans les lectures
 - 29.10.2. Approche holistique des Données
 - 29.10.3. Mise à l'échelle d'un service distribué

Module 30. Application pratique de la science des Données dans les secteurs d'activité

- 30.1. Secteur sanitaire
 - 30.1.1. Implications de l'IA et de l'analyse des données dans le secteur sanitaire
 - 30.1.2. Opportunités et défis
- 30.2. Risques et tendances dans le secteur sanitaire
 - 30.2.1. Utilisation dans le secteur sanitaire
 - 30.2.2. Risques potentiels liés à l'utilisation de l'IA

- 30.3. Services financiers
 - 30.3.1. Implications de l'IA et de l'analyse des données dans le secteur des services financiers
 - 30.3.2. Utilisation dans les services financiers
 - 30.3.3. Risques potentiels liés à l'utilisation de l'IA
- 30.4. *Retail*
 - 30.4.1. Implications de l'IA et de l'analyse des données dans le secteur du *Retail*
 - 30.4.2. Utilisation pendant la *Retail*
 - 30.4.3. Risques potentiels liés à l'utilisation de l'IA
- 30.5. Industrie 4.0
 - 30.5.1. Implications de l'IA et de l'analyse des données dans Industrie 4.0
 - 30.5.2. Utilisation dans l'industrie 4.0
- 30.6. Risques et tendances dans l'Industrie 4.0
 - 30.6.1. Risques potentiels liés à l'utilisation de l'IA
- 30.7. Administration publique
 - 30.7.1. Implications de l'IA et de l'analyse des données dans l'Administration Publique
 - 30.7.2. Utilisation dans l'Administration Publique
 - 30.7.3. Risques potentiels liés à l'utilisation de l'IA
- 30.8. Éducation
 - 30.8.1. Implications de l'IA et de l'analyse des Données pour l'Education
 - 30.8.2. Risques potentiels liés à l'utilisation de l'IA
- 30.9. Sylviculture et agriculture
 - 30.9.1. Implications de l'IA et de l'analyse des Données pour la sylviculture et l'agriculture
 - 30.9.2. Utilisation dans la Sylviculture et l'Agriculture
 - 30.9.3. Risques potentiels liés à l'utilisation de l'IA
- 30.10. Ressources humaines
 - 30.10.1. Implications de l'IA et de l'analyse des données dans la gestion des ressources humaines
 - 30.10.2. Applications pratiques dans le monde des affaires
 - 30.10.3. Risques potentiels liés à l'utilisation de l'IA



TECH vous offre le meilleur programme pour les informaticiens comme vous qui souhaitent un changement de carrière pour donner un coup de pouce à leur carrière professionnelle"

06

Méthodologie

Ce programme de formation offre une manière différente d'apprendre. Notre méthodologie est développée à travers un mode d'apprentissage cyclique: ***le Relearning***.

Ce système d'enseignement est utilisé, par exemple, dans les écoles de médecine les plus prestigieuses du monde et a été considéré comme l'un des plus efficaces par des publications de premier plan telles que le ***New England Journal of Medicine***.



“

Découvrez Relearning, un système qui renonce à l'apprentissage linéaire conventionnel pour vous emmener à travers des systèmes d'enseignement cycliques: une façon d'apprendre qui s'est avérée extrêmement efficace, en particulier dans les matières qui exigent la mémorisation”

Étude de Cas pour mettre en contexte tout le contenu

Notre programme offre une méthode révolutionnaire de développement des compétences et des connaissances. Notre objectif est de renforcer les compétences dans un contexte changeant, compétitif et hautement exigeant.

“

Avec TECH, vous pouvez expérimenter une manière d'apprendre qui ébranle les fondations des universités traditionnelles du monde entier”



Vous bénéficierez d'un système d'apprentissage basé sur la répétition, avec un enseignement naturel et progressif sur l'ensemble du cursus.



L'étudiant apprendra, par des activités collaboratives et des cas réels, à résoudre des situations complexes dans des environnements commerciaux réels.

Une méthode d'apprentissage innovante et différente

Cette formation TECH est un programme d'enseignement intensif, créé de toutes pièces, qui propose les défis et les décisions les plus exigeants dans ce domaine, tant au niveau national qu'international. Grâce à cette méthodologie, l'épanouissement personnel et professionnel est stimulé, faisant ainsi un pas décisif vers la réussite. La méthode des cas, technique qui constitue la base de ce contenu, permet de suivre la réalité économique, sociale et professionnelle la plus actuelle.

“ Notre programme vous prépare à relever de nouveaux défis dans des environnements incertains et à réussir votre carrière ”

La méthode des cas est le système d'apprentissage le plus largement utilisé dans les meilleures écoles d'informatique du monde depuis qu'elles existent. Développée en 1912 pour que les étudiants en Droit n'apprennent pas seulement le droit sur la base d'un contenu théorique, la méthode des cas consiste à leur présenter des situations réelles complexes afin qu'ils prennent des décisions éclairées et des jugements de valeur sur la manière de les résoudre. En 1924, elle a été établie comme méthode d'enseignement standard à Harvard.

Dans une situation donnée, que doit faire un professionnel? C'est la question à laquelle nous sommes confrontés dans la méthode des cas, une méthode d'apprentissage orientée vers l'action. Tout au long du programme, les étudiants seront confrontés à de multiples cas réels. Ils devront intégrer toutes leurs connaissances, faire des recherches, argumenter et défendre leurs idées et leurs décisions.

Relearning Methodology

TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

Nous enrichissons l'Étude de Cas avec la meilleure méthode d'enseignement 100% en ligne: le Relearning.

En 2019, nous avons obtenu les meilleurs résultats d'apprentissage de toutes les universités en ligne du monde.

À TECH, vous apprendrez avec une méthodologie de pointe conçue pour former les managers du futur. Cette méthode, à la pointe de la pédagogie mondiale, est appelée Relearning.

Notre université est la seule université autorisée à utiliser cette méthode qui a fait ses preuves. En 2019, nous avons réussi à améliorer les niveaux de satisfaction globale de nos étudiants (qualité de l'enseignement, qualité des supports, structure des cours, objectifs...) par rapport aux indicateurs de la meilleure université en ligne.





Dans notre programme, l'apprentissage n'est pas un processus linéaire, mais se déroule en spirale (apprendre, désapprendre, oublier et réapprendre). Par conséquent, chacun de ces éléments est combiné de manière concentrique. Cette méthodologie a permis de former plus de 650.000 diplômés universitaires avec un succès sans précédent dans des domaines aussi divers que la biochimie, la génétique, la chirurgie, le droit international, les compétences en gestion, les sciences du sport, la philosophie, le droit, l'ingénierie, le journalisme, l'histoire, les marchés financiers et les instruments. Tout cela dans un environnement très exigeant, avec un corps étudiant universitaire au profil socio-économique élevé et dont l'âge moyen est de 43,5 ans.

Le Relearning vous permettra d'apprendre avec moins d'efforts et plus de performance, en vous impliquant davantage dans votre formation, en développant un esprit critique, en défendant des arguments et en contrastant les opinions: une équation directe vers le succès.

À partir des dernières preuves scientifiques dans le domaine des neurosciences, non seulement nous savons comment organiser les informations, les idées, les images et les souvenirs, mais nous savons aussi que le lieu et le contexte dans lesquels nous avons appris quelque chose sont fondamentaux pour notre capacité à nous en souvenir et à le stocker dans l'hippocampe, pour le conserver dans notre mémoire à long terme.

De cette manière, et dans ce que l'on appelle Neurocognitive context-dependent e-learning, les différents éléments de notre programme sont reliés au contexte dans lequel le participant développe sa pratique professionnelle.

Ce programme offre le support matériel pédagogique, soigneusement préparé pour les professionnels:



Support d'étude

Tous les contenus didactiques sont créés par les spécialistes qui enseigneront le cours, spécifiquement pour le cours, afin que le développement didactique soit vraiment spécifique et concret.

Ces contenus sont ensuite appliqués au format audiovisuel, pour créer la méthode de travail TECH en ligne. Tout cela, avec les dernières techniques qui offrent des pièces de haute qualité dans chacun des matériaux qui sont mis à la disposition de l'étudiant.



Cours magistraux

Il existe des preuves scientifiques de l'utilité de l'observation par un tiers expert.

La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.



Pratiques en compétences et aptitudes

Les étudiants réaliseront des activités visant à développer des compétences et des aptitudes spécifiques dans chaque domaine. Des activités pratiques et dynamiques pour acquérir et développer les compétences et aptitudes qu'un spécialiste doit développer dans le cadre de la mondialisation dans laquelle nous vivons.



Lectures complémentaires

Articles récents, documents de consensus et directives internationales, entre autres. Dans la bibliothèque virtuelle de TECH, l'étudiant aura accès à tout ce dont il a besoin pour compléter sa formation.





Case studies

Ils réaliseront une sélection des meilleures études de cas choisies spécifiquement pour ce diplôme. Des cas présentés, analysés et tutorés par les meilleurs spécialistes de la scène internationale.



Résumés interactifs

L'équipe TECH présente les contenus de manière attrayante et dynamique dans des pilules multimédia comprenant des audios, des vidéos, des images, des diagrammes et des cartes conceptuelles afin de renforcer les connaissances. Ce système éducatif unique pour la présentation de contenu multimédia a été récompensé par Microsoft en tant que "European Success Story".



Testing & Retesting

Les connaissances de l'étudiant sont périodiquement évaluées et réévaluées tout au long du programme, par le biais d'activités et d'exercices d'évaluation et d'auto-évaluation, afin que l'étudiant puisse vérifier comment il atteint ses objectifs.



07 Diplôme

Le Mastère Avancé en Science Informatique, Cybersécurité et Analytique de Données vous garantit, en plus de la formation la plus rigoureuse et la plus actuelle, l'accès à un diplôme universitaire de Mastère Avancé délivré par TECH Université Technologique.



“

Finalisez cette formation avec succès et recevez votre Mastère Avancé sans avoir à vous soucier des déplacements ou des démarches administratives"

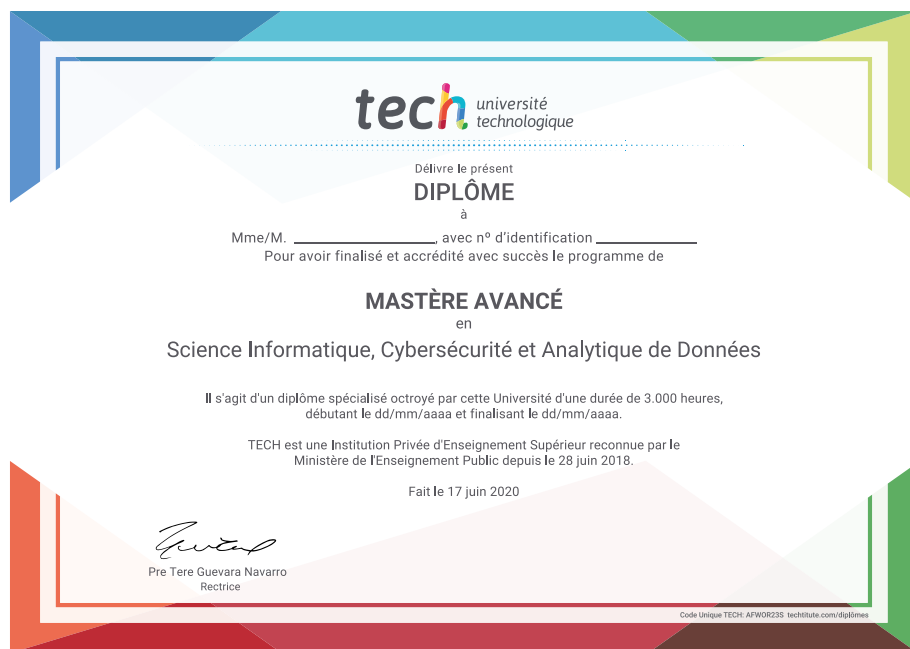
Ce **Mastère Avancé en Science Informatique, Cybersécurité et Analytique de Données** contient le programme le plus complet et le plus actuel du marché.

Après avoir réussi l'évaluation, l'étudiant recevra par courrier postal* avec accusé de réception son correspondant diplôme de **Mastère Avancé** délivré par **TECH Université Technologique**.

Le diplôme délivré par **TECH Université Technologique** indiquera la note obtenue lors du Mastère Avancé, et répond aux exigences communément demandées par les bourses d'emploi, les concours et les commissions d'évaluation des carrières professionnelles.

Diplôme: **Mastère Avancé en Science Informatique, Cybersécurité et Analytique de Données**

N.º d'heures Officielles: **3.000 h.**



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

future

santé confiance personnes

éducation information tuteurs

garantie accréditation enseignement

institutions technologie apprentissage

communauté engagement

tech université
technologique

Mastère Avancé

Science Informatique,
Cybersécurité et

Analytique de Données

- » Modalité: en ligne
- » Durée: 2 ans
- » Qualification: TECH Université Technologique
- » Intensité: 16h/semaine
- » Horaire: à votre rythme
- » Examens: en ligne

Mastère Avancé

Science Informatique, Cybersécurité
et Analytique de Données