Mastère Avancé

Gestion Sécurisée de l'Information

tech université technologique

tech université technologique

Mastère Avancé

Gestion Sécurisée de l'Information

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

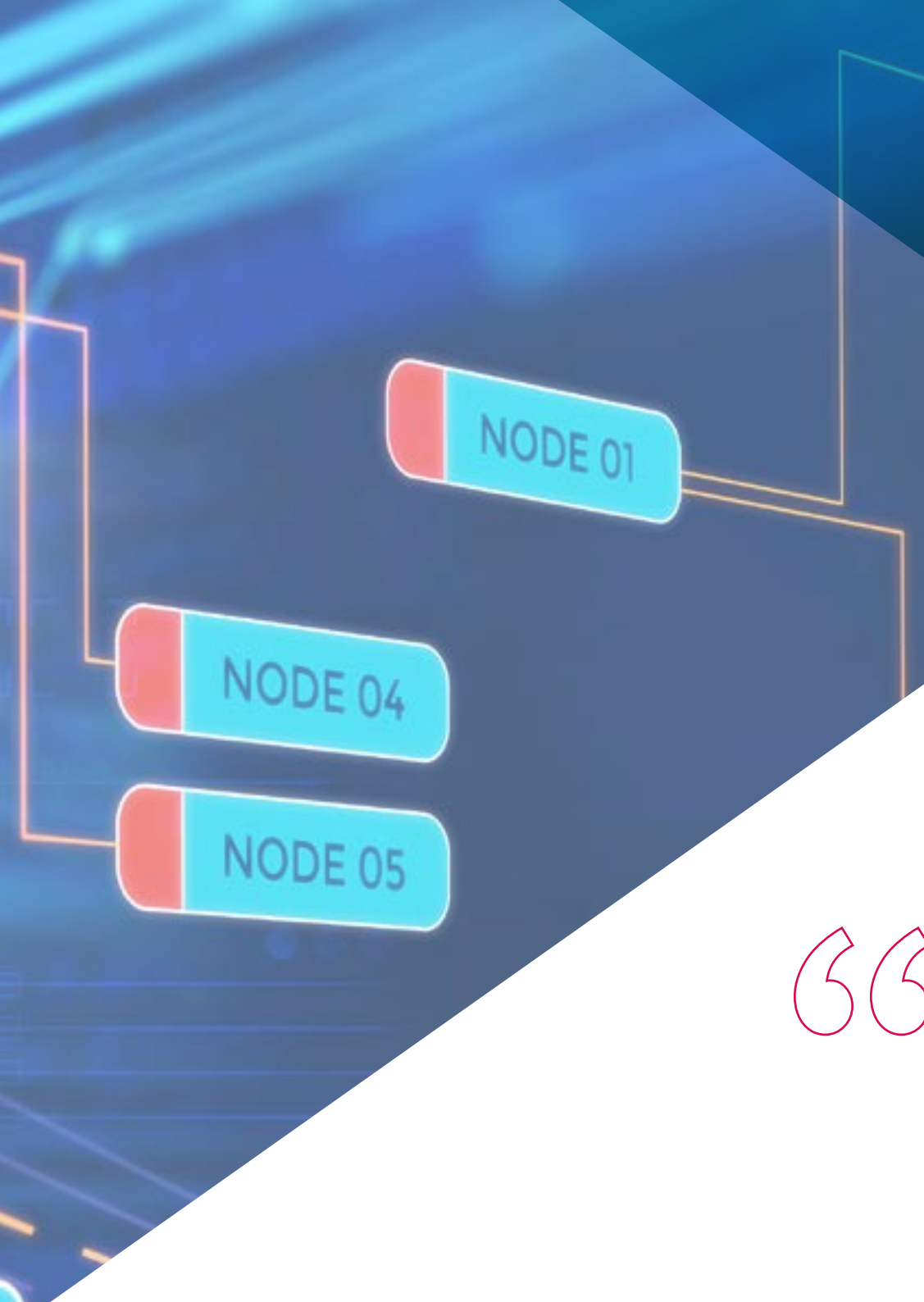
Accès au site web: www.techtitute.com/fr/informatique/mastere-avance/mastere-avance-gestion-securisee-information

Sommaire

01

Présentation

Le monde d'aujourd'hui est dominé par l'environnement numérique. Un grand nombre d'activités dans différents domaines y sont gérées. Les loisirs, le travail ou les contacts avec les amis et la famille ne se comprennent plus sans Internet et tous les outils en ligne existants. C'est pourquoi d'énormes quantités d'informations sont transférées quotidiennement, qu'il s'agisse de données anodines dans des conversations via les réseaux sociaux et les applications de messagerie, ou d'informations personnelles et professionnelles très sensibles hébergées sur des sites web bancaires ou professionnels. Dans ce paysage complexe, il faut des spécialistes capables de gérer tous les types d'informations relatives à ces domaines, tout en accordant une attention adéquate à leur sécurité. De nombreuses entreprises recherchent des personnes ayant ce profil pour protéger leurs informations.



Chaque jour, des personnes malveillantes tentent de compromettre la sécurité d'entreprises et d'institutions qui gèrent données précieuses: vous pourriez être le grand protecteur de cette information"

Chaque jour, des millions de personnes effectuent toutes sortes d'activités sur Internet. Ils consultent les actualités, discutent avec leurs amis et leur famille, partagent leurs opinions sur les réseaux sociaux, effectuent des tâches administratives dans différentes entreprises et institutions, partagent toutes sortes de fichiers ou effectuent des tâches liées au travail. Ainsi, d'innombrables quantités de données sont créées et transférées dans le monde entier à tout moment.

Les gérer avec une sécurité adéquate n'est pas une tâche facile, car elle requiert une série d'expertises spécifiques provenant de différents domaines qui ne seraient normalement pas en contact les uns avec les autres. C'est pourquoi ce Mastère Avancé en Gestion Sécurisée de l'Information est une occasion exceptionnelle pour tous les ingénieurs et professionnels de l'informatique qui souhaitent intégrer la gestion de l'information et la cybersécurité afin de devenir des spécialistes de premier plan dans ces deux domaines.

De nombreuses entreprises et institutions traitent des données très sensibles et précieuses qui doivent être correctement gérées, préservées et contrôlées. Il n'y a pas encore beaucoup d'experts dans les deux disciplines qui peuvent les traiter correctement. Ainsi, les étudiants qui obtiennent ce diplôme seront les mieux placés pour accéder à des postes de premier plan dans les entreprises qui cherchent à sécuriser leurs informations numériques.

À cette fin, TECH a conçu les meilleurs contenus et a réuni les meilleurs enseignants, dotés d'une grande expérience professionnelle dans ces domaines, afin que les étudiants reçoivent l'enseignement le plus complet possible et puissent progresser dans le monde du travail.

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

- Le développement d'études de cas présentées par des experts en informatique
- Le contenu graphique, schématique et éminemment pratique de l'ouvrage fournit des informations scientifiques et pratiques sur les disciplines essentielles à la pratique professionnelle
- Des exercices pratiques où le processus d'auto-évaluation peut être utilisé pour améliorer l'apprentissage
- Elle met l'accent sur les méthodologies innovantes en matière de gestion et de sécurité des données numériques
- Des cours théoriques, des questions à l'expert, des forums de discussion sur des sujets controversés et un travail de réflexion individuel
- Il est possible d'accéder aux contenus depuis tout appareil fixe ou portable doté d'une connexion internet

Tout ce que nous faisons dans la sphère numérique est enregistré Faites d'Internet un endroit plus sûr avec ce Mastère Avancé"

Les meilleures entreprises du pays vous confieront la gestion et la sécurité de leurs données à l'issue de ce programme”

Ce Mastère Avancé combine deux disciplines essentielles pour l'avenir de votre carrière. Inscrivez-vous dès maintenant et atteignez tous vos objectifs.

Apprenez tout sur la gestion et la sécurité des données et voyez comment vous pouvez progresser professionnellement en très peu de temps.

Le corps enseignant du programme englobe des spécialistes réputés dans le domaine de l'informatique qui apportent leur expérience à ce programme, ainsi que des spécialistes reconnus issus de grandes entreprises et d'universités prestigieuses.

Grâce à son contenu multimédia développé avec les dernières technologies éducatives, les spécialistes bénéficieront d'un apprentissage situé et contextuel. Ainsi, ils se formeront dans un environnement simulé qui leur permettra d'apprendre en immersion et de s'entrainer dans des situations réelles.

La conception de ce programme est basée sur l'Apprentissage par Problèmes. Ainsi le médecin devra essayer de résoudre les différentes situations de pratique professionnelle qui se présentent à lui tout au long du programme académique. Pour ce faire, le professionnel sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.

02

Objectifs

L'objectif principal de ce Mastère Avancé en Gestion Sécurisée de l'Information est de fournir aux étudiants les meilleures connaissances dans deux branches distinctes mais interdépendantes de l'informatique et de l'ingénierie: la gestion des données dans l'environnement numérique et la cybersécurité. En associant ces deux domaines, les informaticiens et les professionnels de ce programme seront en mesure d'appliquer les meilleures solutions à toutes les situations qui se présentent dans leur carrière, en offrant les outils les plus appropriés à leurs entreprises pour gérer et protéger toutes sortes d'informations sensibles.

Votre objectif est d'être le meilleur spécialiste de votre entreprise et TECH vous offre les outils pour y parvenir"

Objectifs généraux

- Analyser les avantages de l'application des techniques d'analyse des données dans chaque département de l'entreprise
- Développer la base pour comprendre les besoins et les 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
- Examiner le rôle de l'analyste en cybersécurité
- Approfondir la compréhension de l'ingénierie sociale et de ses méthodes
- Examiner les méthodologies OSINT, HUMINT, OWASP, PTEC, OSSTM et OWISAM
- Effectuer une analyse des risques et comprendre les mesures de risques
- Déterminer l'utilisation appropriée de l'anonymat et l'utilisation de réseaux tels que TOR, I2P et Freenet
- Compiler les réglementations existantes en matière de cybersécurité
- Générer des connaissances spécialisées pour la réalisation d'un audit de sécurité
- élaborer des politiques d'utilisation appropriées
- Étudier les systèmes de détection et de prévention des menaces les plus importantes
- Évaluer les nouveaux systèmes de détection des menaces et leur évolution par rapport aux solutions plus traditionnelles
- Analyser les principales plateformes mobiles actuelles, leurs caractéristiques et leur utilisation
- Identifier, analyser et évaluer les risques de sécurité des parties du projet IoT
- Évaluer les informations obtenues et développer des mécanismes de prévention et de *piratage*
- Appliquer l'ingénierie inverse à l'environnement de la cybersécurité
- Spécifier les tests à effectuer sur le logiciel développé
- Rassembler toutes les preuves et données existantes pour réaliser un rapport judiciaire
- Soumettre dûment le rapport judiciaire
- Analyser l'état actuel et futur de la sécurité informatique
- Examiner les risques des technologies nouvelles et émergentes
- Compiler les différentes technologies en relation avec la sécurité informatique

La cybersécurité et la gestion des données sont des disciplines qui évoluent rapidement. Suivez ce Mastère Avancé et obtenez les connaissances les plus récentes"

Objectifs spécifiques

- 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 d'indicateurs clés de performance (KPI) 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'écoute du client
- Appliquer des connaissances statistiques, quantitatives et techniques dans des situations réelles
- Effectuer l'analyse des 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 de gestion des données en fonction de leur typologie et de leurs utilisations
- Établir des politiques d'accès et de réutilisation des données
- Assurer la sécurité et la disponibilité: disponibilité, intégrité et confidentialité des informations
- Examiner les outils de gestion des données à l'aide de langages de programmation
- Identifier ce qu'est l'IoT (*Internet of Things*) et l'IIoT (*Industrial Internet of Things*)
- Examiner le Consortium de l'Internet industriel
- Analyser ce qu'est l'architecture de référence de l'IoT
- Traiter 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 le domaine de l'IdO: usage général, industriel et open source
- Développer des mécanismes d'échange de données
- Établir des exigences et des stratégies de sécurité
- Présenter les différents domaines d'application de l'IoT et de l'IIoT
- Générer des connaissances spécialisées dans la représentation et 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 l'affichage des données
- Présenter la narration graphique comme un outil
- Analyser les différents outils logiciels pour la réalisation de graphiques et l'analyse exploratoire des 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 pour la modélisation
- Justifier la prise de décision en procédant à une analyse préalable approfondie des données
- Développer des compétences pour résoudre des cas pratiques en utilisant des techniques de science des données
- Établir les outils et méthodes généraux les plus appropriés pour modéliser chaque ensemble de données 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
- Générer des connaissances expertes sur les conditions statistiques préalables à toute analyse et évaluation de 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 à haute dimension
- Développer la mise en œuvre des algorithmes utilisés pour le prétraitement des données
- Démontrer la capacité d'interpréter l'affichage de données pour une analyse descriptive
- Développer des connaissances avancées sur les différentes techniques de préparation des données existantes pour le nettoyage, la normalisation et la transformation des données
- Analyse des séries chronologiques
- Développer la formulation et les propriétés de base des modèles de séries temporelles univariées
- Examiner la méthodologie de modélisation et de prévision des séries en temps réel
- Détermination de modèles univariés incluant des 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
- Analyser le passage de l'information à la connaissance
- Développer les différents types de techniques d'apprentissage automatique
- Examiner les mesures et les 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
- Déterminer les exigences des systèmes d'utilisation des données de masse
- Examiner différents modèles de données et analyser des 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
- Préciser les différents modèles de réplication et les problèmes associés
- Développer des formes de cloisonnement et de transactions distribuées
- Déterminer les systèmes par lots et en (quasi) temps réel
- 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
- Générer une meilleure compréhension de la technologie par 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
- Développer les méthodologies utilisées en matière de cyber-sécurité
- Examiner le cycle du renseignement et établir son application dans le cyber renseignement
- Déterminer le rôle de l'analyste du renseignement et les obstacles à l'activité d'évacuation
- Établir les outils les plus courants pour la production de renseignements
- Effectuer une analyse des risques et comprendre les mesures utilisées
- Concrétiser les possibilités d'anonymat et d'utilisation de réseaux tels que TOR, I2P et FreeNet
- Détailler les réglementations actuelles en matière de cybersécurité
- Concrétiser les politiques de sauvegarde des données personnelles et professionnelles
- Évaluer les différents outils permettant d'apporter des solutions à des problèmes de sécurité spécifiques
- Établir des mécanismes pour disposer d'un système actualisé
- Scannez les équipements pour détecter les intrus
- Déterminer les règles d'accès au système
- Filtrer et classer le courrier pour éviter la fraude
- Générer des listes de logiciels autorisés
- Analyser les architectures de réseau actuelles pour identifier le périmètre à protéger
- Développer des configurations spécifiques de pare-feu et de Linux pour atténuer les attaques les plus courantes
- Compilez les solutions les plus couramment utilisées telles que Snort et Suricata, ainsi que leur configuration
- Examiner les différentes couches supplémentaires fournies par les pare-feu de nouvelle génération et les fonctionnalités réseau dans les environnements en *cloud*
- Identifier les outils de protection des réseaux et démontrer pourquoi ils sont fondamentaux pour une défense à plusieurs niveaux
- Examinez les différents vecteurs d'attaque pour éviter de devenir une cible facile
- Déterminer les principales attaques et les principaux types de *malware* auxquels les utilisateurs d'appareils mobiles sont exposés
- Analyser les derniers dispositifs pour établir une configuration plus sûre
- Préciser les principales étapes pour effectuer un test de pénétration sur les plateformes iOS et Android

- Développer des connaissances spécialisées sur les différents outils de protection et de sécurité
- Établir les meilleures pratiques en matière de programmation orientée vers le mobile
- Analyser les principales architectures IoT
- Examiner les technologies de connectivité
- Développer les principaux protocoles de mise en œuvre
- Pour spécifier les différents types de dispositifs existants
- Évaluer les niveaux de risque et les vulnérabilités connues
- Développer des politiques d'utilisation sûre
- Établir des conditions d'utilisation appropriées pour ces dispositifs
- Examiner les méthodes IOSINT
- Rassembler les informations disponibles dans les médias publics
- Recherche d'informations sur le mode actif dans les réseaux
- Développer des laboratoires d'essai
- Outils d'analyse de la performance du pentesting
- Cataloguer et évaluer les différentes vulnérabilités des systèmes
- Concrétiser les différentes méthodologies de *hacking*
- Analyser les phases d'un compilateur
- Examen de l'architecture des processeurs x86 et de l'architecture des processeurs ARM
- Déterminer les différents types d'analyse
- Appliquer le *sandboxing* dans différents environnements
- Développer les différentes techniques d'analyse de *malware*
- Établir les outils pour l'analyse de *malware*
- Établir les exigences nécessaires au bon fonctionnement d'une application de manière sécurisée
- Examinez les fichiers journaux pour comprendre les messages d'erreur
- Analysez les différents événements et décidez de ce qui doit être montré à l'utilisateur et de ce qui doit être conservé dans les journaux
- Générer un code aseptisé, facilement vérifiable et de qualité
- Évaluer la documentation appropriée pour chaque phase du développement
- Concrétiser le comportement du serveur pour optimiser le système
- Développer un code modulaire, réutilisable et maintenable
- Identifier les différents éléments qui révèlent de l'infraction
- Générer des connaissances spécialisées pour obtenir des données sur différents supports avant qu'elles ne soient perdues
- Récupérer les données intentionnellement supprimées
- Analyser les journaux et les enregistrements du système
- Déterminer comment les données sont dupliquées afin de ne pas altérer les originaux
- Étayer les preuves pour être cohérent
- Générer un rapport solide et sans faille
- Présenter les conclusions de manière cohérente
- Déterminer comment défendre le rapport devant l'autorité compétente
- Concrétiser les stratégies pour un télétravail sûr
- Examen de l'utilisation des crypto-monnaies, de leur impact sur l'économie et de la sécurité
- Analyser la situation des utilisateurs et le degré d'illettrisme numérique
- Déterminer le champ d'utilisation de la blockchain
- Présenter des alternatives à l'IPv4 dans l'adressage des réseaux
- Développer des stratégies pour éduquer la population à l'utilisation correcte des technologies
- Générer des connaissances spécialisées pour relever les nouveaux défis en matière de sécurité et prévenir l'usurpation d'identité
- Concrétiser les stratégies pour un télétravail sûr

03

Compétences

Les étudiants qui obtiennent ce Mastère Avancé en Gestion Sécurisée de l'Information seront capables d'effectuer un grand nombre de tâches hautement spécialisées dans les domaines de la gestion des données et de la cybersécurité Ainsi, ce diplôme combine les deux branches pour offrir des connaissances complémentaires qui peuvent être croisées et utilisées dans différentes situations et environnements professionnels. De cette manière, les étudiants suivront un processus d'apprentissage complet qui les guidera pour devenir de véritables spécialistes dans ce domaine.

Vos nouvelles compétences feront de vous le plus grand spécialiste de votre environnement”

Compétences générales

- Développer une perspective technique et commerciale de l'analyse des données
- Comprendre les derniers algorithmes, plateformes et outils d'exploration, d'affichage, de manipulation, de traitement et d'analyse des données
- Mettre en œuvre une vision d'entreprise nécessaire à la valorisation comme élément clé de la prise de décision
- Pouvoir aborder les problèmes spécifiques à l'analyse des données
- Connaître les méthodologies utilisées en matière de cybersécurité
- Évaluer chaque type de menace afin de fournir une solution optimale dans chaque cas
- Générer des solutions intelligentes complètes pour automatiser le comportement en cas d'incidents
- Savoir évaluer les risques liés aux vulnérabilités à l'intérieur et à l'extérieur de l'entreprise
- Comprendre l'évolution et l'impact de l'IoT au fil du temps
- Démontrer qu'un système est vulnérable, l'attaquer de manière préventive et résoudre ces problèmes
- Appliquer le *sandboxing* dans différents environnements
- Connaître les directives qu'un bon développeur doit suivre afin de se conformer aux exigences de sécurité nécessaires

Compétences spécifiques

- Se spécialiser dans la *data science* d'un point de vue technique et commercial
- Visualiser les données de la manière la plus appropriée pour faciliter le partage et la compréhension par différents profils
- Aborder les domaines fonctionnels clés de l'organisation où la science des données peut apporter le plus de valeur ajoutée
- 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 *machine learning* permettant d'extraire les connaissances cachées des données
- Générer une expertise dans les architectures logicielles et les systèmes requis pour une 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
- Analyser les différentes façons d'appliquer la science des données dans différents secteurs ou verticaux en s'inspirant d'exemples réels
- Mener des opérations de sécurité défensives
- Avoir une perception approfondie et spécialisée de la sécurité informatique
- Posséder des connaissances spécialisées dans le domaine de la cybersécurité et de la cyberespionnage
- Avoir une connaissance approfondie des aspects fondamentaux tels que le cycle du renseignement, les sources de renseignement, l'ingénierie sociale, la méthodologie OSINT, le HUMINT, l'anonymisation et l'analyse des risques, les méthodologies existantes (OWASP, OWISAM, OSSTM, PTES) et la réglementation actuelle en matière de cybersécurité
- Comprendre l'importance de concevoir une défense multicouche, également connue sous le nom *defense in depth*, couvrant tous les aspects d'un réseau d'entreprise où certains des concepts et systèmes que nous verrons peuvent également être utilisés et appliqués dans un environnement domestique
- Savoir appliquer les processus de sécurité pour les smartphones et les appareils portables
- Connaître les moyens de réaliser un *hacking* dit éthique et de protéger une entreprise contre une cyber-attaque
- Enquêter sur un incident de cybersécurité
- Connaître les différentes techniques d'attaque et de défense disponibles
- Analyser le rôle de l'analyste en cybersécurité et apprendre comment fonctionnent l'ingénierie sociale et ses méthodes

04

Direction de la formation

Ce diplôme est enseigné par les meilleurs professeurs dans les domaines de la cybersécurité et de la gestion des données numériques. Son expérience garantit que les étudiants recevront le contenu le plus complet et le plus récent afin qu'ils puissent l'appliquer directement à leur carrière professionnelle. Ainsi, les enseignants de ce Mastère Avancé en Gestion Sécurisée de l'Information transmettront toutes leurs connaissances aux étudiants, en veillant à ce qu'ils deviennent des spécialistes hautement qualifiés et recherchés par les grandes entreprises de leur pays.

Les meilleurs spécialistes vous apprennent à devenir un professionnel de premier plan dans le secteur”

Directeur invité international

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

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

Le Docteur Lemieux a occupé des fonctions éditoriales et d'évaluation dans diverses organisations universitaires, privées et gouvernementales, ce qui témoigne de son influence et de son engagement en faveur de l'excellence dans son domaine d'expertise. Sa prestigieuse carrière universitaire l'a amené à occuper le poste de professeur de pratique et de directeur des programmes MPS **en Intelligence appliquée, Gestion des Risques de Cybersécurité, Gestion de la Technologie et Gestion des Technologies de l'Information à l'Université de Georgetown.**

Dr. Lemieux, Frederic

- Chercheur en Intelligence, Cybersécurité et Technologies de Rupture à l'Université de Georgetown
- Directeur du Master en Information Technology Management à l'Université de Georgetown
- Directeur du Master en Technology Management à l'Université de Georgetown
- Directeur du Master en Cybersecurity Risk Management de l'Université de Georgetown
- Directeur du Master en Applied Intelligence à l'Université de Georgetown
- Professeur de Stage à l'Université de Georgetown
- Licence en Sociologie, Mineure en Psychologie, Université Laval
- Doctorat en Criminologie de l'École de Criminologie de l'Université de Montréal.
  Membre de:
  New Program Roundtable Committee, de l'Université de Georgetown

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

Direction

Dr. Peralta Martín-Palomino, Arturo

- PDG et Directeur Technique de Prometeus Global Solutions
- Directeur Technique à Korporate Technologies
- Directeur Technique à AI Shephers GmbH
- Docteur en Ingénierie Informatique de l'Université de Castilla La Mancha
- Docteur en Économie, Commerce et Finances obtenu l'université Camilo José Cela. Prix du Doctorat Extraordinaire
- Docteur en Psychologie par l'Université de Castilla La Mancha
- Master en Technologies Informatiques 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
- Maître de conférences associé, enseignant en Licence et en Master en Ingénierie Informatique à l'Université de Castilla la Mancha
- Professeur de Master en Big Data et Data Science à l'Université Internationale de Valence
- Professeur de Master en Industrie 4.0 du Master de Design Industriel et Développement de produit
- Membre du Groupe de Recherche SMILe de l'Université de Castilla la Mancha

Mme Fernández Sapena, Sonia

- Formatrice en Sécurité Informatique et en Piratage Éthique. Centre de Référence National de Getafe pour l'Informatique et les Télécommunications. Madrid
- Instructeur certifié E-Council. Madrid
- Formatrice dans les certifications suivantes: EXIN Ethical Hacking Foundation et EXIN Cyber & IT Security Foundation. Madrid
- Formatrice experte accréditée par le CAM pour les certificats de professionnalisme suivants: Sécurité informatique (IFCT0190), Gestion des réseaux voix et données (IFCM0310), Administration des réseaux départementaux (IFCT0410), Gestion des alarmes dans les réseaux de télécommunications (IFCM0410), Opérateur de réseaux voix et données (IFCM0110), et Administration des services Internet (IFCT0509)
- Collaboratrice externe CSO/SSA (*Chief Security Officer/Senior Security Architect*). Université des Îles Baléares
- Ingénieur en Informatique. Université d'Alcalá de Henares. Madrid
- Master en DevOps: Docker and Kubernetes. Cas-Training. Madrid
- Microsoft Azure Security Techonologies. E-Council. Madrid

Professeurs

Mr. Armero Fernández, Rafael

- Business Intelligence Consultant à SDG Group
- Ingénieur Numérique à Mi-GSO
- Ingénieur logistique à Torrecid S.A
- Stagiaire Qualité à INDRA
- Diplômé en Ingénierie Aérospatiale de l'Université Polytechnique de Valence
- Master en Développement Professionnel 4.0 de l'Université d'Alcalá de Henares

Mr. Peris Morillo, Luis Javier

- Technical Lead à Capitole Consulting
- Senior Technical Lead et Delivery Lead Support à HCL
- Agile Coach et Director de Operaciones à Mirai Advisory
- Développeur, Team Lead, Scrum Master, Agile Coach, Product Manager à DocPath
- Ingénierie Supérieure en Informatique par 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.

Mr. Montoro Montarroso, Andrés

- Chercheur dans le groupe SMILe de l'Université de Castilla-La Mancha
- Scientifique des données chez Prometeus Global Solutions
- Diplôme d'Ingénieur en Informatique de l'Université de Castilla-La Mancha, avec une Spécialisation en Sciences de l'Informatique
- Master en Science des Données et Ingénierie Informatique de l'Université de Grenade

Mme Fernández Meléndez, Galina

- Analyste de données chez ADN Mobile Solution
- Processus ETL, data mining, analyse et affichage des données, établissement d'indicateurs clés de performance (KPI), conception et mise en œuvre de Dashboard., contrôle de gestion. Développement en R, gestion SQL, entre autres
- Détermination de motifs, modélisation prédictive, apprentissage machine
- Licence en Administration des Affaires. Université Bicentenaire de Aragua- Caracas- Diplôme en Planification et Finances Publiques École vénézuélienne de Planification-École des Finances
- Master en Analyse de Données et en Intelligence Économique. Université de Oviedo
- MBA en Administration et Gestion des Affaires (Escuela De Negocios Europea De Barcelona)
- Master en Big Data et Business Intelligence (Escuela de Negocios Europea de Barcelona)

Mme Pedrajas Parabás, Elena

- Analyste commercial à Management Solutions à Madrid
- Chercheur au Département d'Informatique et d'Analyse Numérique de l'Université de Cordoue
- Chercheur au Centre Singulier de Recherche en Technologies Intelligentes à Santiago de Compostela
- Diplôme d'Ingénieur en Informatique. Master en Data Science et Ingénierie Informatique Intelligence (European Business School of Barcelona)

Mme Martínez Cerrato, Yésica

- Technicien en produits de sécurité électronique chez Securitas Security Espagne
- Analyste en Business Intelligence à Ricopia Technologies (Alcalá de Henares) Diplôme d'ingénieur en communications électroniques à l'Escuela Politécnica Superior, Université d'Alcalá
- Responsable de la formation des nouvelles recrues aux logiciels de gestion des ventes (CRM, ERP, INTRANET), aux produits et aux procédures chez Ricopia Technologies (Alcalá de Henares)
- Responsable de la formation des nouveaux boursiers incorporés dans les classes d'informatique de l'Université d'Alcalá
- Chef de projet dans le domaine de l'Intégration des Grands Comptes chez Correos y Telégrafos (Madrid)
- Technicien informatique-Responsable des salles informatiques OTEC, Université d'Alcalá (Alcalá de Henares)
- Professeur de cours d'informatique à l'association ASALUMA (Alcalá de Henares)
- Bourse pour la formation de technicien en informatique à l'OTEC, Université d'Alcala (Alcalá de Henares)

Mr. Fondón Alcalde, Rubén

- Analyste commercial en gestion de la valeur client chez Vodafone Espagne
- Responsable de l'intégration des services chez Entelgy pour Telefónica Global Solutions
- Responsable du compte Clone Server Online chez EDM Electronics
- Analyste commercial pour l'Europe du Sud chez Vodafone Global Enterprise
- Ingénieur en télécommunications de l'Université européenne de Madrid
- Master en Big Data et analyse de l'Université internationale de Valence

Mr. Díaz Díaz-Chirón, 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
- Ingénieur Supérieur en Informatique de l'Université de Castilla-La Mancha

Mr. Tato Sánchez, Rafael

- Gestion de projet chez INDRA SISTEMAS S.A. Gestion du contrat de maintenance des installations de systèmes de transport intelligents dépendant du Centre de Contrôle et de Gestion du Trafic de la Direction Générale du trafic à Madrid
- Directeur technique chez INDRA SISTEMAS S.A., responsable du Centre de contrôle et de gestion du trafic de la Direction générale du trafic à Madrid
- Ingénieur système ENA TRÁFICO SAU
- Ingénieur Technique Industriel en Électricité de l'Université Polytechnique de Madrid
- Diplôme d'Ingénieur en Électronique Industrielle et en Automatisation de l'Université Européenne de Madrid
- Certification professionnelle. SSCE0110: Enseignement pour la formation professionnelle à l'emploi
- Master en Industrie 4.0 de l'Université internationale de La Rioja (UNIR)

Mr. Catalá Barba, José Francisco

- L'encadrement intermédiaire au MINISDEF Différentes tâches et responsabilités au sein du GOE III, telles que l'administration et la gestion des incidents du réseau interne, la mise en œuvre de programmes sur mesure pour différents domaines, les cours de formation pour les utilisateurs du réseau et le personnel du groupe en général
- Technicien en électronique dans l'usine Ford située à Almusafes, Valence, programmation de robots, automates, réparation et maintenance
- Technicien en Électronique
- Développeur d'applications pour les appareils mobiles

Mr. Jiménez Ramos, Álvaro

- Analyste de la Sécurité à Capgemini
- Analyste en Cybersécurité L1 à Axians
- Analyste en Cybersécurité L2 à Axians
- Analyste en Cybersécurité à SACYR S.A
- Diplôme d'ingénieur en télématique de l'Université Polytechnique de Madrid
- Master en Cybersécurité et Piratage Éthique par le CICE
- Cours avancé en Cybersécurité par Deusto Formación

Mme Marcos Sbarbaro, Victoria Alicia

- Développeur d'applications mobiles Android natives à B60 UK
- Analyste-Programmeur pour la gestion, la coordination et la documentation d'un environnement d'alarme de sécurité virtualisé dans les locaux du client
- Analyste-Programmeur d'applications Java pour les guichets automatiques du site du client
- Professionnel du Développement de Logiciels pour une application de validation de signature et de gestion de documents sur le site du client
- Technicien système pour la migration des équipements et pour la gestion, la maintenance et la formation des PDA mobiles chez le client
- Ingénierie technique en systèmes informatiques Universitat Oberta de Catalunya
- Master en Sécurité Informatique et Ethical Hacking Official EC- Council et CompTIA par l'École professionnelle des nouvelles technologies CICE

Mr. Peralta Alonso, Jon

- Avocat / DPO Altia Consultores S.A
- Chargé de cours en Master en Protection des Données Personnelles, Cybersécurité et Droit des TIC. Université Publique du Pays basque (UPV-EHU)
- Avocat / Conseiller juridique. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L
- Conseiller juridique / stagiaire. Bureau professionnel: Oscar Padura
- Diplôme en Droit. Université Publique du Pays Basque
- Master en Représentant de la Protection des Données. EIS Innovative School
- Master Universitaire en Droit. Université Publique du Pays Basque
- Master en Pratique du Contentieux Civil. Université Internationale Isabel I de Castille

Mr. Redondo, Jesús Serrano

- Développeur FrontEnd junior et Technicien en Cybersécurité Junior
- Développeur FrontEnd à Telefónica, Madrid
- Développeur à FrontEnd. Best Pro Consulting SL, Madrid
- Installateur d'équipements et de services de Télécommunications. Grupo Zener, Castilla y León
- Installateur d'équipements et de services de Télécommunications. Lican Comunicaciones SL, Castilla y León
- Certificat en Sécurité Informatique CFTIC Getafe, Madrid
- Technicien Supérieur: Télécommunications et Systèmes Informatiques. IES Trinidad Arroyo, Palencia
- Technicien Supérieur: Installations électrotechniques MT et BT. IES Trinidad Arroyo, Palencia
- Formation en reverse engineering, sténographie, cryptage. Incibe Hacker Academy (Talents d'Incibe)

Des professionnels de premier plan dans le domaine se sont réunis pour vous offrir les connaissances les plus complètes dans ce domaine, afin que vous puissiez vous développer avec toutes les garanties de succès"

05

Structure et contenu

Le contenu de ce Mastère Avancé en gestion sécurisée de l'information a été conçu en tenant compte de l'état actuel de la profession, afin que les étudiants reçoivent les meilleures connaissances possibles et puissent les appliquer à leur domaine de travail. Ainsi, tout au long des 20 modules qui composent ce cursus, les étudiants pourront apprendre tout ce qui concerne la gestion et la sécurité des données et des informations numériques, devenant ainsi de véritables spécialistes du domaine.

Il n'y a pas de meilleur programme. Ce Mastère Avancé vous offre tout ce dont vous avez besoin pour devenir le meilleur expert dans ces domaines le principal"

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

1.1. Analyse de l'activité
- 1.1.1. Analyse de l'activité
- 1.1.2. Structuration des données
- 1.1.3. Phases et éléments

1.2. L'analyse des données dans l'entreprise
- 1.2.1. Tableaux de bord et indicateurs de performance clés par départements (KPI)
- 1.2.2. Rapports opérationnels, tactiques et stratégiques
- 1.2.3. L'analyse des données appliquée à chaque département
  - 1.2.3.1. Marketing et communication
  - 1.2.3.2. Commercial
  - 1.2.3.3. Service client
  - 1.2.3.4. Achats
  - 1.2.3.5. Administration
  - 1.2.3.6. RH
  - 1.2.3.7. Production
  - 1.2.3.8. IT

1.3. Marketing et communication
- 1.3.1. Kpi's à mesurer, applications et avantages
- 1.3.2. Systèmes de marketing et *data warehouse*
- 1.3.3. Mise en œuvre d'un cadre d'analyse des données dans le domaine du Marketing
- 1.3.4. Plan de marketing et de communication
- 1.3.5. Stratégie, prévisions et gestion des campagnes

1.4. Commercial et ventes
- 1.4.1. Contributions de l'analyse des données dans le domaine commercial
- 1.4.2. Besoins du département des Ventes
- 1.4.3. Études de marché

1.5. Service client
- 1.5.1. Fidélisation
- 1.5.2. Qualité personnelle et intelligence émotionnelle
- 1.5.3. Satisfaction des clients

1.6. Achats
- 1.6.1. Analyse de données pour les études de marché
- 1.6.2. Analyse de données pour les études de concurrence
- 1.6.3. Autres applications

1.7. Administration
- 1.7.1. Besoins dans le département administratif
- 1.7.2. *Data Warehouse*et analyse des risques financiers
- 1.7.3. *Data Warehouse*et l'analyse du risque de crédit

1.8. Ressources humaines
- 1.8.1. Les RH et les avantages de l'analyse des données
- 1.8.2. Outils d'analyse des données dans le département des RH
- 1.8.3. Application de l'analyse des données dans les RH

1.9. Production
- 1.9.1. Analyse des données dans un service de production
- 1.9.2. Applications
- 1.9.3. Bénéfices

1.10. IT
- 1.10.1. Département informatique
- 1.10.2. Analyse des données et transformation numérique
- 1.10.3. Innovation et productivité

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

2.1. Statistiques Variables, indices et ratios
- 2.1.1. Les Statistiques
- 2.1.2. Dimensions statistiques
- 2.1.3. Variables, indices et ratios

2.2. Typologie des données
- 2.2.1. Qualitatifs
- 2.2.2. Quantitatifs
- 2.2.3. Caractérisation et catégories

2.3. Connaissance des données issues des mesures
- 2.3.1. Mesures de centralisation
- 2.3.2. Mesures de la dispersion
- 2.3.3. Corrélation

2.4. Connaissance des données à partir de graphiques
- 2.4.1. Affichage selon le type de données
- 2.4.2. Interprétation de l'information graphique
- 2.4.3. Personnalisation des graphiques avec R

2.5. Probabilités
- 2.5.1. Probabilités
- 2.5.2. Fonction de probabilité
- 2.5.3. Distribution

2.6. Collecte des données
- 2.6.1. Méthodologie de collecte
- 2.6.2. Outils de collecte
- 2.6.3. Canaux de collecte

2.7. Nettoyage des données
- 2.7.1. Phases du nettoyage des données
- 2.7.2. Qualité des données
- 2.7.3. Manipulation de données (avec R)

2.8. Analyse des données, interprétation et évaluation des résultats
- 2.8.1. Mesures statistiques
- 2.8.2. Indices de relation
- 2.8.3. Extraction de données

2.9. Stockage des données (*Data Warehouse*)
- 2.9.1. Éléments
- 2.9.2. Conception

2.10. Disponibilité des données
- 2.10.1. Accessible
- 2.10.2. Utilité
- 2.10.3. Sécurité

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

3.1. *Internet of Things (IoT)*
- 3.1.1. Internet du futur, *Internet of Things*
- 3.1.2. Le Consortium de l'Internet industriel

3.2. Architecture de référence
- 3.2.1. L'Architecture de référence
- 3.2.2. Couches
- 3.2.3. Composants

3.3. Capteurs et dispositifs IoT
- 3.3.1. Principaux composants
- 3.3.2. Capteurs et actionneurs

3.4. Communications et protocoles
- 3.4.1. Protocoles Modèle OSI
- 3.4.2. Technologies de communication

3.5. Plateformes en *cloud* pour l'IoT et l'IIoT
- 3.5.1. Plateformes à usage général
- 3.5.2. Plateformes industrielles
- 3.5.3. Plateformes à source ouverte

3.6. Gestion des données dans les plateformes IoT
- 3.6.1. Mécanismes de gestion des données. Open Data
- 3.6.2. Échange de données et affichage

3.7. Sécurité de l'IoT
- 3.7.1. Exigences et domaines de sécurité
- 3.7.2. Stratégies de sécurité de l'IIoT

3.8. Applications de l'IoT
- 3.8.1. Villes intelligentes
- 3.8.2. Santé et forme physique
- 3.8.3. Foyer intelligent
- 3.8.4. Autres applications

3.9. Applications de l'IIoT
- 3.9.1. Fabrication
- 3.9.2. Transport
- 3.9.3. Énergie
- 3.9.4. Agriculture et élevage
- 3.9.5. Autres secteurs

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

Module 4. Représentation graphique pour l'analyse des données

4.1. Analyse exploratoire
- 4.1.1. Représentation pour l'analyse de l'information
- 4.1.2. La valeur de la représentation graphique
- 4.1.3. Nouveaux paradigmes de la représentation graphique

4.2. Optimisation pour la science des données
- 4.2.1. Gamme de couleurs et design
- 4.2.2. La Gestalt dans la représentation graphique
- 4.2.3. Erreurs à éviter et conseils

4.3. Sources des données de base
- 4.3.1. Pour une représentation de qualité
- 4.3.2. Pour la représentation des quantités
- 4.3.3. Pour la représentation du temps

4.4. Sources de données complexes
- 4.4.1. Fichiers, listes et bases de données
- 4.4.2. Open Data
- 4.4.3. Données de génération continue

4.5. Types de graphiques
- 4.5.1. Représentations de base
- 4.5.2. Représentation par blocs
- 4.5.3. Représentation pour l'analyse de la dispersion
- 4.5.4. Représentations circulaires
- 4.5.5. Représentations de bulles
- 4.5.6. Représentations géographiques

4.6. Types d'affichage
- 4.6.1. Comparatif et relationnel
- 4.6.2. Distribution
- 4.6.3. Hiérarchique

4.7. Conception de rapports avec représentation graphique
- 4.7.1. Application des graphiques dans les rapports de marketing
- 4.7.2. Application des graphiques dans les tableaux de bord et les Kpi's
- 4.7.3. Application des graphiques dans les plans stratégiques
- 4.7.4. Autres utilisations: science, santé, affaires

4.8. Narration graphique
- 4.8.1. La narration graphique
- 4.8.2. Évolution
- 4.8.3. Utilité

4.9. Outils orientés vers l'affichage
- 4.9.1. Outils avancés
- 4.9.2. Logiciel en ligne
- 4.9.3. *Open Source*

4.10. Nouvelles technologies de l'affichage de données
- 4.10.1. Systèmes de virtualisation de la réalité
- 4.10.2. Systèmes d'amélioration et d'enrichissement de la réalité
- 4.10.3. Systèmes intelligents

Module 5. Outils de science des données Data Science

5.1. Data Science
- 5.1.1. La Data Science
- 5.1.2. Outils avancés pour le scientifique des données

5.2. Données, informations et connaissances
- 5.2.1. Données, informations et connaissances
- 5.2.2. Types de données
- 5.2.3. Sources des données

5.3. Des données aux informations
- 5.3.1. Analyse des données
- 5.3.2. Types d'analyse
- 5.3.3. Extraire des informations d'un *Dataset*

5.4. Extraction d'informations par l'affichage
- 5.4.1. L'affichage comme outil d'analyse
- 5.4.2. Méthodes d'affichage
- 5.4.3. Affichage d'un ensemble de données

5.5. Qualité des données
- 5.5.1. Données de qualité
- 5.5.2. Nettoyage des données
- 5.5.3. Prétraitement de base des données

5.6. *Dataset*
- 5.6.1. Enrichissement du *dataset*
- 5.6.2. La malédiction de la dimensionnalité
- 5.6.3. Modification de notre dataset

5.7. Déséquilibre
- 5.7.1. Déséquilibre des classes
- 5.7.2. Techniques d'atténuation du déséquilibre
- 5.7.3. Équilibre d'un *dataset*

5.8. Modèles non supervisés
- 5.8.1. Modèle non supervisé
- 5.8.2. Méthodes
- 5.8.3. Classification avec des modèles non supervisés

5.9. Modèles non supervisés
- 5.9.1. Modèle supervisé
- 5.9.2. Méthodes
- 5.9.3. Classification avec des modèles supervisés

5.10. Outils et bonnes pratiques
- 5.10.1. Bonnes pratiques pour un scientifique spécialiste des données
- 5.10.2. Le meilleur modèle
- 5.10.3. Outils utiles

Module 6. L'exploration de données. Sélection, prétraitement et transformation

6.1. L'inférence Statistique
- 6.1.1. Statistiques descriptives vs. Inférence Statistique
- 6.1.2. Procédures paramétriques
- 6.1.3. Procédures non paramétriques

6.2. Analyse exploratoire
- 6.2.1. Analyse descriptive
- 6.2.2. Visualisation
- 6.2.3. Préparation des données

6.3. Préparation des données
- 6.3.1. Intégration et nettoyage des données
- 6.3.2. Normalisation des données
- 6.3.3. Transformer les attributs

6.4. Les Valeurs manquantes
- 6.4.1. Traitement des valeurs manquantes
- 6.4.2. Méthodes d'imputation par maximum de vraisemblance
- 6.4.3. Imputation des valeurs manquantes par apprentissage automatique

6.5. Le bruit dans les données
- 6.5.1. Classes et attributs de bruit
- 6.5.2. Filtrage du bruit
- 6.5.3. L'effet du bruit

6.6. La malédiction de la dimensionnalité
- 6.6.1. *Oversampling*
- 6.6.2. *Undersampling*
- 6.6.3. Réduction des données multidimensionnelles

6.7. Des attributs continus aux attributs discrets
- 6.7.1. Données continues versus discrètes
- 6.7.2. Processus de discrétisation

6.8. Les données
- 6.8.1. Sélection des données
- 6.8.2. Perspectives et critères de sélection
- 6.8.3. Méthodes de sélection

6.9. Sélection d'Instances
- 6.9.1. Méthodes de sélection des instances
- 6.9.2. Sélection de prototypes
- 6.9.3. Méthodes avancées pour la sélection des instances

6.10. Prétraitement des données dans les environnements *Big Data*
- 6.10.1. *Big Data*
- 6.10.2. Prétraitement "classique" contre pré-traitement massif
- 6.10.3. *Smart Data*

Module 7. Prévisibilité et analyse des phénomènes stochastiques

7.1. Séries chronologiques
- 7.1.1. Séries chronologiques
- 7.1.2. Utilité et applicabilité
- 7.1.3. Études de cas connexes

7.2. La Série chronologique
- 7.2.1. Tendance Saisonnalité de ST
- 7.2.2. Variations typiques
- 7.2.3. Analyse des résidus

7.3. Typologies
- 7.3.1. Stationnaire
- 7.3.2. Non-stationnaire
- 7.3.3. Transformations et ajustements

7.4. Schémas pour les séries temporelles
- 7.4.1. Schéma additif (modèle)
- 7.4.2. Schéma multiplicatif (modèle)
- 7.4.3. Procédures pour déterminer le type de modèle

7.5. Méthodes de base de *forecast*
- 7.5.1. Médias
- 7.5.2. *Naïve*
- 7.5.3. *Naïve* saisonnière
- 7.5.4. Comparaison des méthodes

7.6. Analyse du reste
- 7.6.1. Autocorrélation
- 7.6.2. ACF de reste
- 7.6.3. Test de corrélation

7.7. Régression dans le contexte des séries chronologiques
- 7.7.1. ANOVA
- 7.7.2. Principes fondamentaux
- 7.7.3. Application pratique

7.8. Modèles prédictifs de séries chronologiques
- 7.8.1. ARIMA
- 7.8.2. Lissage exponentiel

7.9. Manipulation et analyse des séries chronologiques avec R
- 7.9.1. Préparation des données
- 7.9.2. Identification de modèles
- 7.9.3. Analyse du modèle
- 7.9.4. Prédiction

7.10. Analyse graphique combinée avec R
- 7.10.1. Situations typiques
- 7.10.2. Application pratique pour la résolution de problèmes simples
- 7.10.3. Application pratique pour la résolution de problèmes avancés

Module 8. Conception et développement de systèmes intelligents

8.1. Prétraitement de des données
- 8.1.1. Prétraitement de des données
- 8.1.2. Transformation des données
- 8.1.3. L'exploration des données

8.2. Apprentissage Automatique
- 8.2.1. Apprentissage supervisé et non supervisé
- 8.2.2. Apprentissage par renforcement
- 8.2.3. Autres paradigmes d'apprentissage

8.3. Algorithmes de classification
- 8.3.1. Apprentissage Automatique Inductif
- 8.3.2. SVM et KNN
- 8.3.3. Mesures et scores pour le classement

8.4. Algorithmes de régression
- 8.4.1. Régression linéaire, régression logistique et modèles non linéaires
- 8.4.2. Séries chronologiques
- 8.4.3. Mesures et scores de régression

8.5. Algorithmes de regroupement
- 8.5.1. Techniques de regroupement hiérarchique
- 8.5.2. Techniques de regroupement partitionnel
- 8.5.3. Mesures et scores de *Clustering*

8.6. Techniques de règles d'association
- 8.6.1. Méthodes d'extraction de règles
- 8.6.2. Mesures et scores pour les algorithmes de règles d'association

8.7. Techniques de classification avancées. Multiclassificateurs
- 8.7.1. Algorithmes de *bagging*
- 8.7.2. Classificateur *"Random Forests"*
- 8.7.3. "*Boosting*" pour les arbres de décision

8.8. Modèles graphiques probabilistes
- 8.8.1. Modèles probabilistes
- 8.8.2. Les réseaux bayésiens. Propriétés, représentation et paramétrage
- 8.8.3. Autres modèles graphiques probabilistes

8.9. Réseaux neuronaux:
- 8.9.1. Apprentissage automatique avec les réseaux de neurones artificiels
- 8.9.2. Réseaux *feedforward*

8.10. Apprentissage profond
- 8.10.1. Réseaux *feedforward* profonds
- 8.10.2. Réseaux neuronaux convolutifs et modèles de séquence
- 8.10.3. Outils pour la mise en œuvre de réseaux neuronaux profonds

Module 9. Architectures et systèmes à forte intensité de données

9.1. Exigences non fonctionnelles. Piliers des applications big data
- 9.1.1. Fiabilité
- 9.1.2. Adaptabilité
- 9.1.3. Maintenabilité

9.2. Modèles de données
- 9.2.1. Modèle relationnel
- 9.2.2. Modèle documentaire
- 9.2.3. Modèle de données du réseau

9.3. Bases de données. Gestion du stockage et de la récupération des données
- 9.3.1. Index de hachage
- 9.3.2. Stockage structuré des journaux
- 9.3.3. Arbres B

9.4. Formats d'encodage des données
- 9.4.1. Formats spécifiques à la langue
- 9.4.2. Formats standardisés
- 9.4.3. Formats de codage binaire
- 9.4.4. Flux de données entre les processus

9.5. Réplication
- 9.5.1. Objectifs de réplication
- 9.5.2. Modèles de réplication
- 9.5.3. Problèmes de réplication

9.6. Transactions distribuées
- 9.6.1. Transaction
- 9.6.2. Protocoles pour les transactions distribuées
- 9.6.3. Transactions sérialisables

9.7. Partitionnement
- 9.7.1. Les formes de partitionnement
- 9.7.2. Interaction et partitionnement des index secondaires
- 9.7.3. Rééquilibrage des partitions

9.8. Traitement des données *offline*
- 9.8.1. Traitement par lots
- 9.8.2. Systèmes de fichiers distribués
- 9.8.3. *MapReduce*

9.9. Traitement des données en temps réel
- 9.9.1. Types de *courtiers* en messages
- 9.9.2. Représentation des bases de données en tant que flux de données
- 9.9.3. Traitement des flux de données

9.10. Applications pratiques dans les entreprises
- 9.10.1. Cohérence dans les lectures
- 9.10.2. Approche holistique des données
- 9.10.3. Mise à l'échelle d'un service distribué

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

10.1. Secteur de la santé
- 10.1.1. Implications de l'IA et de l'analyse des données dans le secteur de la santé
- 10.1.2. Opportunités et défis

10.2. Risques et tendances dans le secteur de la santé
- 10.2.1. Utilisation dans le secteur de la santé
- 10.2.2. Risques potentiels liés à l'utilisation de l'IA

10.3. Services financiers
- 10.3.1. Implications de l'IA et de l'analyse des données pour le secteur des services financiers
- 10.3.2. Utilisation dans les services financiers
- 10.3.3. Risques potentiels liés à l'utilisation de l'IA

10.4. Vente au détail
- 10.4.1. Implications de l'IA et de l'analyse des données dans le secteur du commerce de détail
- 10.4.2. Utilisation pour le commerce de détail
- 10.4.3. Risques potentiels liés à l'utilisation de l'IA

10.5. Industrie 4.0
- 10.5.1. Implications de l'IA et de l'analyse des données dans l'Industrie 4.0
- 10.5.2. Utilisation dans l'Industrie 4.0

10.6. Risques et tendances de l'Industrie 4.0
- 10.6.1. Risques potentiels liés à l'utilisation de l'IA

10.7. Administration publique
- 10.7.1. Implications de l'IA et l'analyse des données dans l'administration publique
- 10.7.2. Utilisation dans l'administration publique
- 10.7.3. Risques potentiels liés à l'utilisation de l'IA

10.8. Éducation
- 10.8.1. Implications de l'IA et l'analyse des données dans l'éducation
- 10.8.2. Risques potentiels liés à l'utilisation de l'IA

10.9. Sylviculture et agriculture
- 10.9.1. Implications de l'IA et l'analyse des données dans la sylviculture et agriculture
- 10.9.2. Utilisation dans la sylviculture et agriculture
- 10.9.3. Risques potentiels liés à l'utilisation de l'IA

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

Module 11. Cyberespionnage et cybersécurité

11.1. Cyberespionnage
- 11.1.1. Cyberespionnage
  - 11.1.1.2. Renseignements
    - 11.1.1.2.1. Cycle du renseignement
  - 11.1.1.3. Cyberespionnage
  - 11.1.1.4. Cyberespionnage et cybersécurité
- 11.1.2. L'Analyste du renseignement
  - 11.1.2.1. Le rôle de l'analyste du renseignement
  - 11.1.2.2. Les biais de l'analyste du renseignement dans l'activité d'évaluation

11.2. Cybersécurité
- 11.2.1. Les couches de sécurité
- 11.2.2. Identification des cybermenaces
  - 11.2.2.1. Menaces extérieures
  - 11.2.2.2. Menaces intérieures
- 11.2.3. Actions défavorables
  - 11.2.3.1. Ingénierie sociale
  - 11.2.3.2. Méthodes couramment utilisées

11.3. Techniques et outils du renseignement
- 11.3.1. OSINT
- 11.3.2. SOCMINT
- 11.3.3. HUMIT
- 11.3.4. Distributions et outils Linux
- 11.3.5. OWISAM
- 11.3.6. OWISAP
- 11.3.7. PTES
- 11.3.8. OSSTM

11.4. Méthodes d'évaluation
- 11.4.1. Analyse du renseignement
- 11.4.2. Techniques d'organisation des informations acquises
- 11.4.3. Fiabilité et crédibilité des sources d'information
- 11.4.4. Méthodologies d'analyse
- 11.4.5. Présentation des résultats du renseignement

11.5. Audits et documentation
- 11.5.1. L'audit de la sécurité informatique
- 11.5.2. Documentation et autorisations pour l'audit
- 11.5.3. Types d'audit
- 11.5.4. Produits livrables
  - 11.5.4.1. Rapport technique
  - 11.5.4.2. Rapport exécutif

11.6. L'anonymat sur le net
- 11.6.1. Utilisation de l'anonymat
- 11.6.2. Techniques d'anonymat (Proxy, VPN)
- 11.6.3. Réseaux TOR, Freenet et IP2

11.7. Risques et types de sécurité
- 11.7.1. Types de risques
- 11.7.2. Sécurité physique
- 11.7.3. Sécurité des réseaux
- 11.7.4. Sécurité logique
- 11.7.5. Sécurité des applications Web
- 11.7.6. Sécurité des appareils mobiles

11.8. Réglementation et *conformité*
- 11.8.1. RGPD
- 11.8.2. La stratégie nationale de cybersécurité 2011
- 11.8.3. Famille ISO 27000
- 11.8.4. Cadre de cybersécurité du NIST
- 11.8.5. PIC
- 11.8.6. ISO 27032
- 11.8.7. Réglementation du *cloud*
- 11.8.8. SOX
- 11.8.9. PCI

11.9. Analyse et mesure des risques
- 11.9.1. Étendue des risques
- 11.9.2. Les atouts
- 11.9.3. Les menaces
- 11.9.4. Les failles
- 11.9.5. Évaluation du risque
- 11.9.6. Traitement du risque

11.10. Organismes importants en matière de cybersécurité
- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. UNASUR - PROSUR

Module 12. Sécurité de l'hébergeur

12.1. Copies de sauvegarde
- 12.1.1. Stratégies de sauvegarde
- 12.1.2. Outils pour Windows
- 12.1.3. Outils pour Linux
- 12.1.4. Outils pour MacOS

12.2. Anti-virus pour l'utilisateur
- 12.2.1. Types d'antivirus
- 12.2.2. Antivirus pour Windows
- 12.2.3. Antivirus pour Linux
- 12.2.4. Antivirus pour MacOS
- 12.2.5. Antivirus pour les smartpohones

12.3. Détecteurs d'intrusion - HIDS
- 12.3.1. Méthodes de détection des intrusions
- 12.3.2. *Sagan*
- 12.3.3. *Aide*
- 12.3.4. *Rkhunter*

12.4. *Pare-feu* local
- 12.4.1. *Pare-feu* pour Windows
- 12.4.2. *Pare-feu* pour Linux
- 12.4.3. *Pare-feu* pour MacOS

12.5. Gestionnaires de mots de passe
- 12.5.1. *Mot de passe*
- 12.5.2. *LastPass*
- 12.5.3. *KeePass*
- 12.5.4. *Sticky Password*
- 12.5.5. *RoboForm*

12.6. Détecteurs de *phishing*
- 12.6.1. Détection manuelle du *phishing*
- 12.6.2. Outils *antiphishing*

12.7. *Spyware*
- 12.7.1. Mécanismes d'évitement
- 12.7.2. Outils *antispyware*

12.8. Trackers
- 12.8.1. Mesures de protection du système
- 12.8.2. Outils anti-trackers

12.9. EDR- *End Point Detection and Response*
- 12.9.1. Comportement du système EDR
- 12.9.2. Différences entre EDR et antivirus
- 12.9.3. L'avenir des systèmes EDR

12.10. Contrôle de l'installation des logiciels
- 12.10.1. Dépôts et magasins de logiciels
- 12.10.2. Listes des logiciels autorisés ou interdits
- 12.10.3. Critères de mise à niveau
- 12.10.4. Privilèges pour l'installation de logiciels

Module 13. Sécurité des réseaux (périmètre)

13.1. Systèmes de détection et de prévention des menaces
- 13.1.1. Cadre général des incidents de sécurité
- 13.1.2. Les systèmes de défense actuels: *Defense in Depth* et SOC
- 13.1.3. Architectures de réseau actuelles
- 13.1.4. Types d'outils pour la détection et la prévention des incidents
  - 13.1.4.1. Systèmes en réseau
  - 13.1.4.2. Systèmes basés sur l'hébergeur
  - 13.1.4.3. Systèmes centralisés
- 13.1.5. Communication et détection des instances/*hébergements*, conteneurs et *serverless*

13.2. *Pare-feu*
- 13.2.1. Types de *pare-feu*
- 13.2.2. Attaques et atténuation
- 13.2.3. *Pare-feu* courant du kernel Linux
  - 13.2.3.1. UFW
  - 13.2.3.2. Nftables e iptables
  - 13.2.3.3. *Pare-feu*
- 13.2.4. Systèmes de détection basés sur les journaux du système
  - 13.2.4.1. TCP *Wrappers*
  - 13.2.4.2. *BlockHosts* et *DenyHosts*
  - 13.2.4.3. Fai2ban

13.3. Systèmes de détection et de prévention des intrusions (IDS/IPS)
- 13.3.1. Attaques contre les IDS/IPS
- 13.3.2. Systèmes IDS/IPS
  - 13.3.2.1. *Snort*
  - 13.3.2.2. Suricate

13.4. *Pare-feu* de nouvelle génération (NGFW)
- 13.4.1. Différences entre les NGFW et les pare-feu traditionnels
- 13.4.2. Principales capacités
- 13.4.3. Solutions commerciales
- 13.4.4. ***Pare-feu*** pour les services *Cloud*
  - 13.4.4.1. Architecture *Cloud* VPC
  - 13.4.4.2. *Cloud* ACLs
  - 13.4.4.3. *Security Group*

13.5. Proxy
- 13.5.1. Types de Proxy
- 13.5.2. Utilisation du Proxy. Avantages et inconvénients

13.6. Moteurs antivirus
- 13.6.1. Contexte général du *Malware* et IOCs
- 13.6.2. Problèmes de moteur d'antivirus

13.7. Systèmes de protection du courrier
- 13.7.1. Antispam
  - 13.7.1.1. Listes noires et blanches
  - 13.7.1.2. Filtres bayésiens
- 13.7.2. *Mail Gateway* (MGW)

13.8. SIEM
- 13.8.1. Composants et architecture
- 13.8.2. Règles de corrélation et cas d'utilisation
- 13.8.3. Défis actuels des systèmes SIEM

13.9. SOAR
- 13.9.1. SOAR et SIEM: ennemis ou alliés
- 13.9.2. L'avenir des systèmes SOAR

13.10. Autres systèmes en réseau
- 13.10.1. WAF
- 13.10.2. NAC
- 13.10.3. HoneyPots et HoneyNets
- 13.10.4. CASB

Module 14. Sécurité des smartphones

14.1. Le monde de l'appareil mobile
- 14.1.1. Types de plateformes mobiles
- 14.1.2. Dispositifs iOS
- 14.1.3. Dispositifs Android

14.2. Gestion de la Sécurité Mobile
- 14.2.1. Projet de sécurité mobile de l'OWASP
  - 14.2.1.1. Les 10 principales failles
- 14.2.2. Communications, réseaux et modes de connexion

14.3. Le dispositif mobile dans l'environnement professionnel
- 14.3.1. Risques
- 14.3.2. Politiques de sécurité
- 14.3.3. Surveillance des dispositifs
- 14.3.4. Gestion des dispositifs mobiles (MDM)

14.4. Vie privée des utilisateurs et sécurité des données
- 14.4.1. États de l'information
- 14.4.2. Protection et confidentialité des données
  - 14.4.2.1. Permis
  - 14.4.2.2. Cryptage
- 14.4.3. Stockage sécurisé des données
  - 14.4.3.1. Stockage sécurisé sur iOS
  - 14.4.3.2. Stockage sécurisé sur Android
- 14.4.4. Bonnes pratiques dans le développement d'application

14.5. Failles et vecteurs d'attaque
- 14.5.1. Failles
- 14.5.2. Vecteurs d'attaque
  - 14.5.2.1. *Malware*
  - 14.5.2.2. Exfiltration de données
  - 14.5.2.3. Manipulation des données

14.6. Principaux risques
- 14.6.1. Utilisateur non forcé
- 14.6.2. *Malware*
  - 14.6.2.1. Types de *Malware*
- 14.6.3. Ingénierie sociale
- 14.6.4. Fuite de données
- 14.6.5. Vol d'informations
- 14.6.6. Réseaux *Wi-Fi* non sécurisés
- 14.6.7. Logiciels obsolètes
- 14.6.8. Applications malveillantes
- 14.6.9. Mots de passe non sécurisés
- 14.6.10. Paramètres de sécurité faibles ou inexistants
- 14.6.11. Accès physique

14.6.12. Perte ou vol de l'appareil
14.6.13. Usurpation d'identité (intégrité)
14.6.14. Cryptographie faible ou cassée
14.6.15. Déni de service (DoS)
14.7. Principales attaques
14.7.1. Attaques de *phishing*
14.7.2. Attaques liées aux modes de communication
14.7.3. Attaques de *Smishing*
14.7.4. Attaques de *Criptojacking*
14.7.5. *Man in The Middle*
14.8. *Hacking*
14.8.1. *Rooting et Jailbreaking*
14.8.2. Anatomie d'une attaque mobile
14.8.2.1. Propagation de la menace
14.8.2.2. Installation d'un *malware* sur l'appareil
14.8.2.3. Persistance
14.8.2.4. Exécution de la *Payload* et extraction d'informations
14.8.3. *Piratage* sur les appareils iOS: mécanismes et outils
14.8.4. *Piratage* sur les appareils Android: mécanismes et outils
14.9. Tests d'intrusion
14.9.1. *iOS PenTesting*
14.9.2. *Android PenTesting*
14.9.3. Outils
14.10. Sécurité et protection
14.10.1. Paramètres de sécurité
14.10.1.1. Sur les appareils iOS
14.10.1.2. Sur les appareils Android
14.10.2. Mesures de sécurité
14.10.3. Outils de protection

Module 15. Sécurité de l'IoT

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

15.7. *Wearables*
- 15.7.1. Vêtements connectés
- 15.7.2. Bijoux connectés
- 15.7.3. Montres connectées

15.8. Secteur de la santé
- 15.8.1. Surveillance de l'effort et de la fréquence cardiaque
- 15.8.2. Suivi des patients et des personnes âgées
- 15.8.3. Implantable
- 15.8.4. Robots chirurgicaux

15.9. Connectivité
- 15.9.1. *Wi-Fi/Gateway*
- 15.9.2. *Bluetooth*
- 15.9.3. Connectivité intégrée

15.10. Securitisation
- 15.10.1. Réseaux dédiés
- 15.10.2. Gestionnaire de mots de passe
- 15.10.3. Utilisation de protocoles cryptés
- 15.10.4. Conseils d'utilisation

Module 16. *Hacking* éthique

16.1. Environnement de travail
- 16.1.1. Distributions de Linux
  - 16.1.1.1. Kali Linux - Sécurité offensive
  - 16.1.1.2. Parrot OS
  - 16.1.1.3. Ubuntu
- 16.1.2. Systèmes de virtualisation
- 16.1.3. *Sandbox*
- 16.1.4. Déploiement des laboratoires

16.2. Méthodologies
- 16.2.1. OSSTM
- 16.2.2. OWASP
- 16.2.3. NIST
- 16.2.4. PTES
- 16.2.5. ISSAF

16.3. *Footprinting*
- 16.3.1. Renseignement de source ouverte (OSINT)
- 16.3.2. Recherche de violations de données et de vulnérabilités
- 16.3.3. Utilisation d'outils passifs

16.4. Analyse du réseau
- 16.4.1. Outils d'analyse
  - 16.4.1.1. Nmap
  - 16.4.1.2. Hping3
  - 16.4.1.3. Autres outils d'analyse
- 16.4.2. Techniques d'analyse
- 16.4.3. Techniques de contournement *Firewall* et IDS
- 16.4.4. *Banner Grabbing*
- 16.4.5. Diagrammes de réseau

16.5. Énumération
- 16.5.1. Énumération SMTP
- 16.5.2. Énumération DNS
- 16.5.3. Énumération de NetBIOS et Samba
- 16.5.4. Énumération LDAP
- 16.5.5. Énumération SNMP
- 16.5.6. Autres techniques d'énumération

16.6. Analyse de failles
- 16.6.1. Solutions d'analyse des failles
  - 16.6.1.1. Qualys
  - 16.6.1.2. Nessus
  - 16.6.1.3. CFI LanGuard
- 16.6.2. Systèmes d'évaluation des failles
  - 16.6.2.1. CVSS
  - 16.6.2.2. CVE
  - 16.6.2.3. NVD

16.7. Attaques contre les réseaux *sans fil*
- 16.7.1. Méthodologie de piratage dans les réseaux sans fil
  - 16.7.1.1. Wi-Fi Discovery
  - 16.7.1.2. Analyse du trafic
  - 16.7.1.3. Attaques du *aircrack*
    - 16.7.1.3.1. Attaques WEP
    - 16.7.1.3.2. Attaques WPA/WPA2
  - 16.7.1.4. Attaques de *Evil Twin*
  - 16.7.1.5. Attaques a WPS
  - 16.7.1.6. *Jamming*
- 16.7.2. Outils pour la sécurité sans fil

16.8. Piratage de serveurs web
- 16.8.1. *Cross site Scripting*
- 16.8.2. CSRF
- 16.8.3. *Session Hijacking*
- 16.8.4. *SQLinjection*

16.9. Exploitation des failles
- 16.9.1. Utilisation d' *exploits* connus
- 16.9.2. Utilisation de *metaspoit*
- 16.9.3. Utilisation de *malware*
  - 16.9.3.1. Définition et champ d'application
  - 16.9.3.2. Generation de *malware*
  - 16.9.3.3. Contournement des solutions anti-virus

16.10. Persistance
- 16.10.1. Installation de rootkits
- 16.10.2. Utilisation de ncat
- 16.10.3. Utilisation de tâches planifiées pour les backdoors
- 16.10.4. Création d'utilisateurs
- 16.10.5. Détection de HIDS

Module 17. Ingénierie inverse

17.1. Compilateurs
- 17.1.1. Types de codes
- 17.1.2. Phases d'un compilateur
- 17.1.3. Tableau des symboles
- 17.1.4. Gestionnaire d'erreurs
- 17.1.5. Compilateur GCC

17.2. Types d'analyse dans les compilateurs
- 17.2.1. Analyse lexicale
  - 17.2.1.1. Terminologie
  - 17.2.1.2. Composants lexicaux
  - 17.2.1.3. Analyseur lexical LEX
- 17.2.2. Analyse syntaxique
  - 17.2.2.1. Grammaires sans contexte
  - 17.2.2.2. Types d'analyses syntaxiques
    - 17.2.2.2.1. Analyse descendante
    - 17.2.2.2.2. Analyse ascendante
  - 17.2.2.3. Arbres syntaxiques et dérivations
  - 17.2.2.4. Types d'analyseurs syntaxiques
    - 17.2.2.4.1. Analyseurs LR (*Left To Right*)
    - 17.2.2.4.2. Analyseurs LALR
- 17.2.3. Analyse sémantique
  - 17.2.3.1. Grammaires d'attributs
  - 17.2.3.2. S-Attribué
  - 17.2.3.3. L-Attribué

17.3. Structures de données d'assemblage
- 17.3.1. Variables
- 17.3.2. Tableaux
- 17.3.3. Pointeurs
- 17.3.4. Structures
- 17.3.5. Objets

17.4. Structures de code d'assemblage
- 17.4.1. Structures de sélection
  - 17.4.1.1. If, else if, Else
  - 17.4.1.2. Switch
- 17.4.2. Structures d'itération
  - 17.4.2.1. For
  - 17.4.2.2. While
  - 17.4.2.3. Utilisation de la pause
- 17.4.3. Fonctions

17.5. Architecture matérielle x86
- 17.5.1. Architecture de processeur x86
- 17.5.2. Structures de données x86
- 17.5.3. Structures de code x86

17.6. Architecture matérielle ARM
- 17.6.1. Architecture de processeur ARM
- 17.6.2. Structures de données ARM
- 17.6.3. Structures de code ARM

17.7. Analyse du code statique
- 17.7.1. Désassembleurs
- 17.7.2. IDA
- 17.7.3. Reconstructeurs de codes

17.8. Analyse dynamique du code
- 17.8.1. Analyse comportementale
  - 17.8.1.1. Communicateurs
  - 17.8.1.2. Surveillance
- 17.8.2. Débogueurs de code Linux
- 17.8.3. Débogueurs de code Windows

17.9. *Sandbox*
- 17.9.1. Architecture de type *Sandbox*
- 17.9.2. Évasion de *Sandbox*
- 17.9.3. Techniques de détection
- 17.9.4. Techniques d'évasion
- 17.9.5. Contre-mesures
- 17.9.6. *Sandbox* sur Linux
- 17.9.7. *Sandbox* sur Windows
- 17.9.8. *Sandox* sur MacOS
- 17.9.9. *Sandbox* sur Android

17.10. Analyse de malwares
- 17.10.1. Méthodes d'analyse de *malware*
- 17.10.2. Techniques de camouflage de *malware*
  - 17.10.2.1. Camouflage des exécutables
  - 17.10.2.2. Restriction des environnements d'exécution
- 17.10.3. Outils d'analyse de *malware*

Module 18. Développement sécurisé

18.1. Développement sécurisé
- 18.1.1. Qualité, fonctionnalité et sécurité
- 18.1.2. Confidentialité, intégrité et disponibilité
- 18.1.3. Cycle de vie du développement logiciel

18.2. Phase des Exigences
- 18.2.1. Contrôle de l'authentification
- 18.2.2. Contrôle des rôles et des privilèges
- 18.2.3. Exigences axées sur le risque
- 18.2.4. Approbation des privilèges

18.3. Phase d'analyse et de conception
- 18.3.1. Accès aux composants et administration du système
- 18.3.2. Pistes d'audit
- 18.3.3. Gestion des sessions
- 18.3.4. Données historiques
- 18.3.5. Traitement approprié des erreurs
- 18.3.6. Séparation des fonctions

18.4. Phase de mise en œuvre et de codification
- 18.4.1. Sécuriser l'environnement de développement
- 18.4.2. Préparation de la documentation technique
- 18.4.3. Codage sécurisé
- 18.4.4. Sécurité des communications

18.5. Bonnes pratiques de codage sécurisé
- 18.5.1. Validation des données d'entrée
- 18.5.2. Codage des données de sortie
- 18.5.3. Style de programmation
- 18.5.4. Gestion du journal des modifications
- 18.5.5. Pratiques cryptographiques
- 18.5.6. Gestion des erreurs et logs
- 18.5.7. Gestion des fichiers
- 18.5.8. Gestion de la mémoire
- 18.5.9. Standardisation et réutilisation des fonctions de sécurité

18.6. Préparation du serveur et *Hardening*
- 18.6.1. Gestion des utilisateurs, des groupes et des rôles sur le serveur
- 18.6.2. Installation du logiciel
- 18.6.3. *Hardening* du serveur
- 18.6.4. Configuration robuste de l'environnement de l'application

18.7. Préparation la DB et *Hardening*
- 18.7.1. Optimisation du moteur DB
- 18.7.2. Création de son propre utilisateur pour l'application
- 18.7.3. Attribution des privilèges nécessaires à l'utilisateur
- 18.7.4. *Hardening* de la DB

18.8. Phase de test
- 18.8.1. Contrôle de la qualité des contrôles de sécurité
- 18.8.2. Inspection du code par étapes
- 18.8.3. Vérification de la gestion des configurations
- 18.8.4. Tests en boîte noire

18.9. Préparer la transition vers la production
- 18.9.1. Effectuer le contrôle des changements
- 18.9.2. Effectuer la procédure de changement de production
- 18.9.3. Exécuter la procédure de *rollback*
- 18.9.4. Essais de pré-production

18.10. Phase de maintenance
- 18.10.1. Assurance basée sur le risque
- 18.10.2. Test de maintenance de la sécurité en boîte blanche
- 18.10.3. Tests de maintenance de la sécurité en boîte noire

Module 19. Analyse judiciaire

19.1. Acquisition et réplication des données
- 19.1.1. Acquisition de données volatiles
  - 19.1.1.1. Informations sur le système
  - 19.1.1.2. Informations sur le réseau
  - 19.1.1.3. Ordre de volatilité
- 19.1.2. Acquisition de données statiques
  - 19.1.2.1. Création d'une image dupliquée
  - 19.1.2.2. Préparation d'un document de chaîne de contrôle
- 19.1.3. Méthodes de validation des données acquises
  - 19.1.3.1. Méthodes pour Linux
  - 19.1.3.2. Méthodes pour Windows

19.2. Évaluation et défaite des techniques anti-fraudes
- 19.2.1. Objectifs des techniques anti-fraudes
- 19.2.2. Suppression des données
  - 19.2.2.1. Suppression de données et de fichiers
  - 19.2.2.2. Récupération de fichiers
  - 19.2.2.3. Récupération de partitions supprimées
- 19.2.3. Protection par mot de passe
- 19.2.4. Stéganographie
- 19.2.5. Effacement sécurisé des dispositifs
- 19.2.6. Cryptage

19.3. Analyse judiciaire du système d'exploitation
- 19.3.1. Analyse judiciaire de Windows
- 19.3.2. Analyse judiciaire de Linux
- 19.3.3. Analyse judiciaire de Mac

19.4. Analyse judiciaire du réseau
- 19.4.1. Analyse des logs
- 19.4.2. Corrélation des données
- 19.4.3. Recherche sur le réseau
- 19.4.4. Étapes à suivre dans l'analyse criminelle du réseau

19.5. Analyse judiciaire du Web
- 19.5.1. Enquête sur les attaques sur Internet
- 19.5.2. Détection des attaques
- 19.5.3. Localisation des adresses IP

19.6. Analyse judiciaire des bases de données
- 19.6.1. Analyse judiciaire de MSSQL
- 19.6.2. Analyse judiciaire de MySQL
- 19.6.3. Analyse judiciaire de PostgreSQL
- 19.6.4. Analyse judiciaire de MongoDB

19.7. Analyse judiciaire du *cloud*
- 19.7.1. Types de délits dans le *cloud*
  - 19.7.1.1. *Cloud* en tant que sujet
  - 19.7.1.2. *Cloud* en tant qu'objet
  - 19.7.1.3. *Cloud* en tant qu'outil
- 19.7.2. Les défis de l'informatique en *cloud*
- 19.7.3. Recherche sur les services de stockage *cloud*
- 19.7.4. Outils d'analyse criminalistique pour *cloud*

19.8. Enquêtes sur les crimes par courriel
- 19.8.1. Systèmes de messagerie
  - 19.8.1.1. Clients de messagerie
  - 19.8.1.2. Serveur de messagerie
  - 19.8.1.3. Serveur SMTP
  - 19.8.1.4. Serveur POP3
  - 19.8.1.5. Serveur IMAP4
- 19.8.2. Délits de messagerie
- 19.8.3. Message de courrier
  - 19.8.3.1. En-têtes standard
  - 19.8.3.2. En-têtes étendus
- 19.8.4. Étapes de l'enquête sur ces crimes
- 19.8.5. Outils d'analyse des e-mails

19.9. Analyse judiciaire de mobiles
- 19.9.1. Réseaux cellulaires
  - 19.9.1.1. Types de réseaux
  - 19.9.1.2. Contenu du CdR
- 19.9.2. *Subscriber Identity Module* (SIM)
- 19.9.3. Acquisition logique
- 19.9.4. Acquisition physique
- 19.9.5. Acquisition du système de fichiers

19.10. Rédaction et présentation de rapports judiciaires
- 19.10.1. Aspects importants d'un rapport judiciaire
- 19.10.2. Classification et types de rapports
- 19.10.3. Guide pour la rédaction d'un rapport
- 19.10.4. Présentation du rapport
  - 19.10.4.1. Préparation préalable au témoignage
  - 19.10.4.2. Déposition
  - 19.10.4.3. Traiter avec les médias

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

20.1. Technologie *blockchain*
- 20.1.2. Domaines d'application
- 20.1.3. Garantie de confidentialité
- 20.1.4. Garantie de non-répudiation

20.2. La monnaie numérique
- 20.2.1. Bitcoins
- 20.2.2. Crypto-monnaies
- 20.2.3. Extraction de crypto-monnaies
- 20.2.4. Les systèmes pyramidaux
- 20.2.5. Autres crimes et problèmes potentiels

20.3. *Deepfake*
- 20.3.2. Impact des médias
- 20.3.3. Dangers pour la société
- 20.3.4. Mécanismes de détection

20.4. L'avenir de l'intelligence artificielle
- 20.4.1. Intelligence artificielle et informatique cognitive
- 20.4.2. Utilisations pour simplifier le service client

20.5. Vie privée numérique
- 20.5.1. Valeur des données dans le réseau
- 20.5.2. Utilisation des données sur le réseau
- 20.5.3. Vie privée et gestion de l'identité numérique

20.6. Cyberconflits, cybercriminels et cyberattaques
- 20.6.1. Impact de la cybersécurité sur les conflits internationaux
- 20.6.2. Conséquences des cyber-attaques sur la population générale
- 20.6.3. Types de cybercriminels. Mesures de protection

20.7. Télétravail
- 20.7.1. La révolution du télétravail pendant et après Covid19
- 20.7.2. Goulots d'étranglement en matière d'accès
- 20.7.3. Variation de la surface d'attaque
- 20.7.4. Besoins des travailleurs

20.8. Technologies *sans fil* émergentes
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. Ondes millimétriques
- 20.8.4. Tendance de *"Get Smart"* au lieu *"Get more"*

20.9. L'adressage futur dans les réseaux
- 20.9.1. Problèmes actuels de l'adressage IP
- 20.9.2. IPv6
- 20.9.2. IPv4+
- 20.9.3. Avantages d'IPv4+ par rapport à IPv4
- 20.9.4. Avantages d'IPv6 par rapport à IPv4

20.10. Le défi de la sensibilisation de la population à l'éducation précoce et continue
- 20.10.1. Stratégies gouvernementales actuelles
- 20.10.2. Résistance de la population à l'apprentissage
- 20.10.3. Des plans de formation à adopter par les entreprises

06

Méthodologie

Ce programme de formation offre une manière différente d'apprendre. Notre méthodologie est développée à travers un mode d'apprentissage cyclique: ***el 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 le Relearning, un système qui laisse de côté l'apprentissage linéaire conventionnel au profit des systèmes d'enseignement cycliques: une façon d'apprendre qui a prouvé son énorme efficacité, notamment dans les matières dont la mémorisation est essentielle"

À TECH, nous utilisons la méthode des cas

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 exigeant.

Avec TECH, vous pourrez découvrir une façon d'apprendre qui fait avancer les fondations des universités traditionnelles du monde entier"

Notre école est la première au monde à combiner les études de cas de l'université d'Harvard avec un système d'apprentissage 100% en ligne basé sur la pratique.

L'apprenant 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

Ce programme intensif en informatique de la TECH Université Technologique vous prépare à relever tous les défis dans ce domaine, tant au niveau national qu'international. Nous nous engageons à promouvoir la croissance personnelle et professionnelle, la meilleure façon de marcher vers le succès, c'est pourquoi à TECH Université Technologique vous utiliserez des *études de cas* , de Harvard, avec qui nous avons un accord stratégique, ce qui nous permet de fournir à nos étudiants des matériaux de la meilleure université du monde.

> *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. Elle a été établie comme méthode d'enseignement standard à Harvard en 1924.

Face à une situation donnée, que doit faire un professionnel? C'est la question à laquelle nous vous confrontons 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

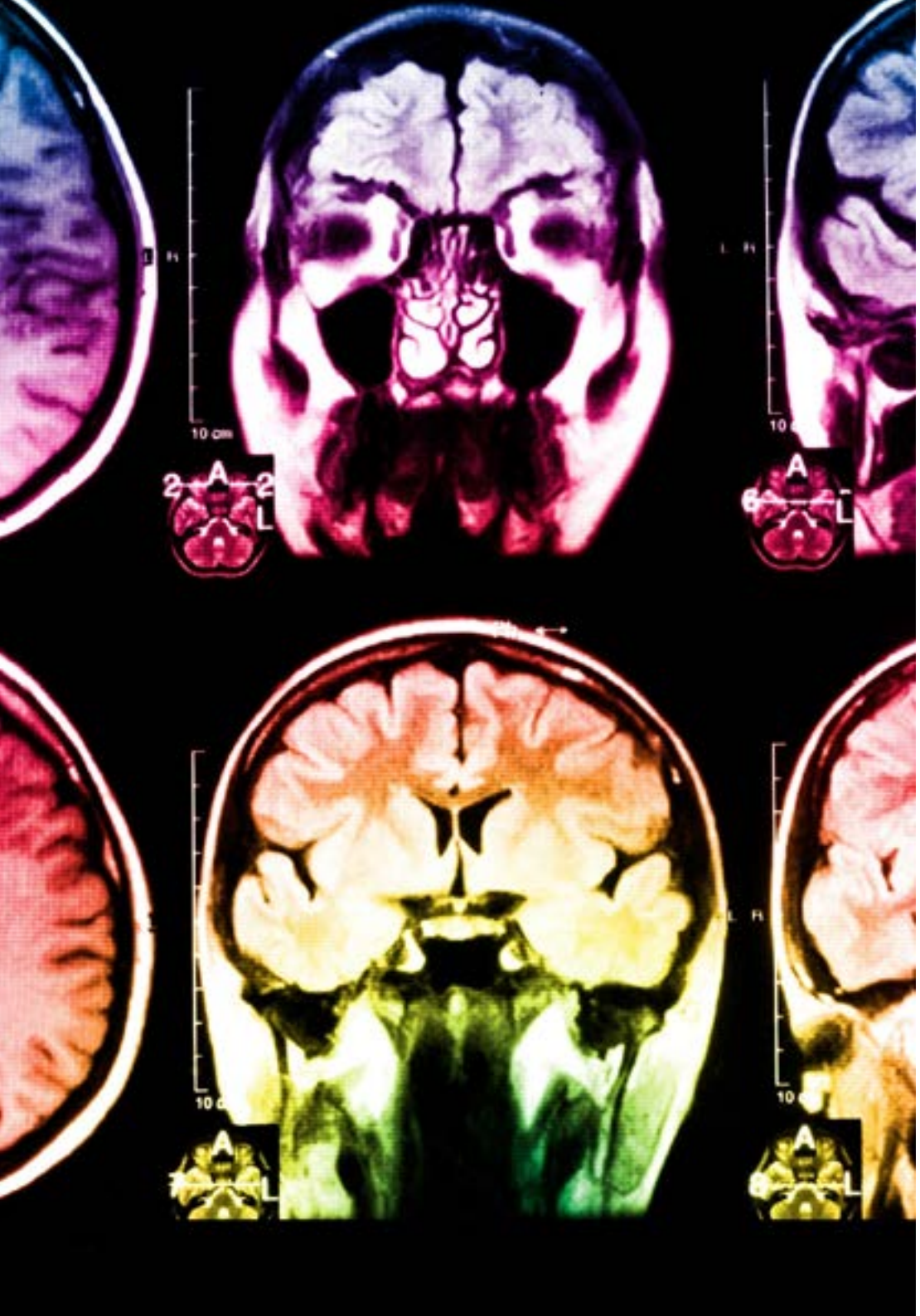
Notre université est la première au monde à combiner les *études de cas* de l'Université de Harvard avec un système d'apprentissage 100% en ligne basé sur la répétition, qui combine éléments didactiques différents dans chaque leçon.

Nous enrichissons les *études de cas* de Harvard 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 efficace. 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 il se déroule en spirale (nous apprenons, désapprenons, oublions et réapprenons). Par conséquent, ils combinent chacun de ces éléments de manière concentrique. Grâce à cette méthodologie, nous avons formé plus de 650.000 diplômés universitaires avec un succès sans précédent et ce dans toutes les spécialités aussi divers que la biochimie, la génétique, la chirurgie, le droit international, les compétences en matière de gestion, les sciences du sport, la philosophie, le droit, l'ingénierie, le journalisme, l'histoire ou les marchés et instruments financiers. 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 plus facilement et de manière plus productive tout en développant un esprit critique, en défendant des arguments et en contrastant des opinions: une équation directe vers le succès.

D'après les dernières données 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 façon, et dans ce que l'on appelle Neurocognitive context-dependent e-learning les différents éléments de notre programme sont liés au contexte dans lequel le participant développe sa pratique professionnelle.

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

Support d'étude

Tous les contenus didactiques sont créés par les spécialistes qui enseignent les cours. Ils ont été conçus en exclusivité pour la formation 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, élaboré avec les dernières techniques afin d'offrir des éléments de haute qualité dans chacun des supports qui sont mis à la disposition de l'apprenant.

Cours magistraux

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

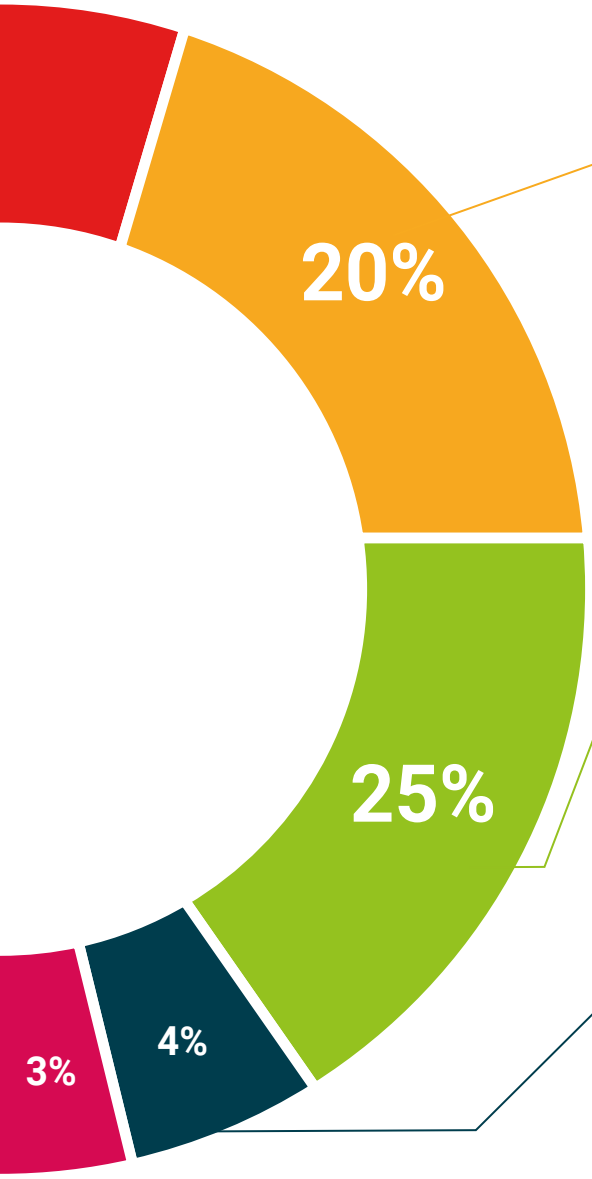
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

Pratique des aptitudes et des compétences

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

Bibliographie complémentaire

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

Vous réaliserez une sélection des meilleures études de cas dans le domaine utilisé à Harvard. Des cas présentés, analysés et encadrés par les meilleurs spécialistes de la scène internationale.

Résumés interactifs

Nous présentons les contenus de manière attrayante et dynamique dans des dossiers multimédias comprenant des fichiers audios, des vidéos, des images, des diagrammes et des cartes conceptuelles afin de consolider 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 Spécialisé en Gestion Sécurisée de l'Information garantit, en plus d'une formation des plus rigoureuses et actualisées, l'accès à un diplôme de Mastère délivré par TECH Université technologique.

Finalisez cette formation avec succès et recevez votre diplôme universitaire sans avoir à vous soucier des déplacements ou des démarches administratives”

Ce **Mastère Avancé en Gestion Sécurisée de l'Information** contient le programme le plus complet et le plus à jour du marché.

Après avoir réussi les évaluations, l'étudiant recevra par courrier postal* avec accusé de réception le diplôme de **Mastère Avancé** 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 Gestion Sécurisée de l'Information**

ECTS: **120**

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


tech université technologique

Délivre le présent

DIPLÔME

à

Mme/M. _____, avec nº d'identification _____

Pour avoir finalisé et accrédité avec succès le programme de

MASTÈRE AVANCÉ

en

Gestion Sécurisée de l'Information

Il s'agit d'un diplôme spécialisé octroyé par cette Université d'une durée de 3.000 heures, débutant le dd/mm/aaaa et finalisant le dd/mm/aaaa.

TECH est une Institution Privée d'Enseignement Supérieur reconnue par le Ministère de l'Enseignement Public depuis le 28 juin 2018.

Fait le 17 juin 2020

Pre Tere Guevara Navarro
Rectrice

Code Unique TECH: AFWOR23S techtitute.com/diplômes


Mastère Avancé en Gestion Sécurisée de l'Information

Distribution Générale du Programme d'Études

Cours	Matière	ECTS	Type
1º	L'analyse des données dans l'organisation de l'entreprise	6	OB
1º	Gestion des données, manipulation des données et informations pour la science des données	6	OB
1º	Les dispositifs et plateformes IoT comme base de la science des données	6	OB
1º	Représentation graphique pour l'analyse des données	6	OB
1º	Outils de science des données Data Science	6	OB
1º	L'exploration de données. Sélection, prétraitement et transformation	6	OB
1º	Prévisibilité et analyse des phénomènes stochastiques	6	OB
1º	Conception et développement de systèmes intelligents	6	OB
1º	Architectures et systèmes à forte intensité de données	6	OB
1º	Application pratique de la science des données dans les secteurs d'activité	6	OB

Cours	Matière	ECTS	Type
2º	Cyberespionnage et cybersécurité	6	OB
2º	Sécurité de l'hébergeur	6	OB
2º	Sécurité des réseaux (périmètre)	6	OB
2º	Sécurité des smartphones	6	OB
2º	Sécurité de l'IoT	6	OB
2º	Hacking éthique	6	OB
2º	Ingénierie inverse	6	OB
2º	Développement sécurisé	6	OB
2º	Analyse judiciaire	6	OB
2º	VV	6	OB

Pre Tere Guevara Navarro
Rectrice

tech université technologique

*Apostille de La Haye 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.

tech université technologique

Mastère Avancé
Gestion Sécurisée de l'Information

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

Mastère Avancé

Gestion Sécurisée de l'Information

tech universidad tecnológica