Mastère Spécialisé

MBA en Direction de la Cybersécurité Avancée (CISO)

tech université technologique

tech université technologique

Mastère Spécialisé
MBA en Direction de la Cybersécurité Avancée (CISO)

- Modalité: **en ligne**
- Durée: **12 mois**
- Qualification: **TECH Université Technologique**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Accès au site web: www.techtitute.com/fr/informatique/master/master-mba-direction-cybersecurite-avancee-ciso

Sommaire

01

Présentation

Le monde d'aujourd'hui évolue vers une numérisation complète. De plus en plus de processus de base, d'opérations et de tâches de toutes sortes sont effectués à l'aide d'un appareil électronique. Mais ce progrès s'accompagne aussi de certains risques, car les ordinateurs, les *smartphones*, les *tablettes* et toutes sortes d'applications numériques sont susceptibles de faire l'objet de cyberattaques. C'est pourquoi de nombreuses entreprises recherchent des experts capables de diriger et de gérer efficacement la cybersécurité de leurs services. Ce nouveau profil professionnel est très demandé, c'est pourquoi ce programme a été conçu pour fournir les dernières connaissances et techniques à l'informaticien, qui sera préparé à devenir le directeur de la cybersécurité dans toute entreprise qui le demande.

Ce programme vous préparera intensivement à vous spécialiser dans la gestion de la cybersécurité, le profil professionnel le plus demandé dans le domaine des technologies de l'information aujourd'hui"

Ces dernières années, le processus de numérisation s'est accéléré grâce aux progrès constants des technologies de l'information. Ainsi, ce n'est pas seulement la technologie qui a bénéficié de grandes améliorations, mais aussi les outils numériques avec lesquels de nombreuses tâches sont effectuées aujourd'hui. Par exemple, ces développements ont permis à de nombreuses transactions bancaires d'être effectuées à partir d'une application mobile. Des développements ont également eu lieu dans le secteur de la santé, dans les systèmes de rendez-vous ou dans l'accès aux dossiers médicaux. De plus, grâce à ces technologies, il est possible de consulter des factures ou de demander des services à des entreprises dans des domaines tels que la téléphonie.

Mais ces avancées ont également entraîné une augmentation des vulnérabilités informatiques. Ainsi, si les possibilités de réaliser diverses activités et tâches se sont élargies, les attaques contre la sécurité des appareils, des applications et des sites web ont augmenté proportionnellement. 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.

Ainsi, le profil de Directeur de la Cybersécurité est l'un des plus recherchés par les entreprises qui opèrent sur Internet ou qui ont des services dans l'environnement numérique. Et pour répondre à cette demande, TECH a conçu ce MBA en Direction de la Cybersécurité Avancée (CISO), qui fournira à l'informaticien tous les outils nécessaires pour exercer cette fonction de manière efficace et en tenant compte des derniers développements en matière de protection et de vulnérabilités dans ce domaine technologique.

Ce programme vous permettra d'approfondir des aspects tels que la sécurité dans le développement et la conception de systèmes, les meilleures techniques de cryptographie et la sécurité dans les environnements de cloud computing. Et vous le ferez en utilisant une méthodologie 100% en ligne avec laquelle vous pourrez combiner votre travail professionnel avec vos études, sans horaires rigides ou déplacements inconfortables vers un centre académique. Vous bénéficierez également de nombreuses ressources pédagogiques multimédias, dispensées par les enseignants les plus prestigieux et les plus spécialisés dans le domaine de la cybersécurité.

Ce **Mastère Spécialisé en MBA en Direction de la Cybersécurité Avancée (CISO)** contient le programme le plus complet et le plus actualisé du marché. Ses caractéristiques sont les suivantes:

- Le développement d'études de cas présentées par des experts en Informatiques et Cybersécurité
- Les contenus graphiques, schématiques et éminemment pratiques avec lesquels ils sont conçus fournissent des informations scientifiques et sanitaires essentielles à la pratique professionnelle
- Exercices pratiques permettant de réaliser le processus d'auto-évaluation afin d'améliorer l'apprentissage
- Il met l'accent sur les méthodologies innovantes
- Leçons théoriques, questions à l'expert, forums de discussion sur des sujets controversés et travail de réflexion individuel
- La possibilité d'accéder au contenu à partir de n'importe quel appareil fixe ou portable doté d'une connexion internet

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

Vous bénéficierez de nombreux contenus multimédias pour accélérer votre processus d'apprentissage, tout en recevant le soutien d'une faculté de grand prestige dans le domaine de la cybersécurité"

La méthodologie en ligne de TECH vous permettra de choisir le moment et le lieu où vous étudierez, sans entraver votre travail professionnel.

Vous pourrez devenir le Directeur de la Cybersécurité des meilleures entreprises de votre région.

Le corps enseignant du programme comprend , des professionnels du secteur qui apportent l'expérience de leur travail, à cette formation, 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 axée sur l'Apprentissage Par les Problèmes, grâce auquel le professionnel doit essayer de résoudre les différentes situations de la pratique professionnelle qui se présentent tout au long du programme académique. Pour ce faire, l'étudiant sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.

02

Objectifs

Le développement rapide des technologies de l'information a permis de grandes avancées, offrant de nombreux services à l'ensemble de la population. Cependant, le nombre de vulnérabilités et de cyber-attaques a également augmenté, c'est pourquoi l'objectif principal de ce programme est de faire de l'informaticien un véritable spécialiste de la gestion de la cyber-sécurité, en lui garantissant une progression professionnelle énorme et immédiate. Vos nouvelles compétences vous p ermettront d'accéder à de grandes entreprises actives dans le domaine numérique dans divers secteurs.

L'objectif de ce programme est de faire de vous un professionnel prêt à diriger le département de cybersécurité d'une grande entreprise"

Objectifs généraux

- Générer des connaissances spécialisées sur un système d'information, les types et les aspects de sécurité à prendre en compte
- Identifier les vulnérabilités d'un système d'information
- Développer la réglementation juridique et la criminalisation 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 applicables 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 et d'incertitude dans l'environnement dans lequel nous vivons
- Examiner le Modèle de Gestion des Risques basé sur la norme ISP 31.000
- Examiner la science de la cryptologie et la relation avec ses branches: cryptographie, cryptanalyse, stéganographie et stégo-analyse
- Analyser les types de cryptographie en fonction du type d'algorithme et de leur 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 la sécurité du *Cloud*
- Analyser les services et outils de chacun des domaines de sécurité
- Développer les spécifications de sécurité de chaque technologie LPWAN
- Analyse comparative de la sécurité des technologies LPWAN

Vos objectifs professionnels sont désormais à votre portée grâce à ce Mastère Spécialisé qui offre les connaissances les plus avancées en matière de cybersécurité"

Objectifs spécifiques

Module 1. La 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 à la sécurité et leurs tendances
- Établir des lignes directrices en matière de sécurité en définissant des politiques et des 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 faille de sécurité
- Protéger les informations sensibles stockées dans le système d'information
- Disposer du cadre juridique et de la typologie du délit, en complétant la vision par la typologie du délinquant et de sa victime

Module 2. Architectures et modèles de sécurité de l'information

- Aligner le plan directeur de sécurité sur les objectifs stratégiques de l'organisation
- Établir un cadre de gestion continue 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 fondée sur une politique
- Analyser les objectifs et les procédures associés au plan de sensibilisation des employés, des fournisseurs et des partenaires
- Identifier, dans le cadre réglementaire, les réglementations, certifications et lois applicables à chaque organisation
- Développer les éléments fondamentaux requis par la norme ISO 27001:2013
- Mettre en œuvre un modèle de gestion de la confidentialité conforme au règlement européen GDPR/RGPD

Module 3. Gestion de la sécurité IT

- Identifier les différentes structures qu'une zone de sécurité peut avoir des informations
- Développer un modèle de sécurité basé sur trois lignes de défense
- Présenter les différents comités périodiques et extraordinaires dans lesquels intervient le domaine de la cybersécurité
- Identifier les outils technologiques qui soutiennent les principales fonctions de l'équipe des opérations de sécurité (SOC)
- Évaluer les mesures de contrôle des vulnérabilités appropriées à chaque scénario
- Développer le cadre des opérations de sécurité basé sur le NIST CSF
- Préciser la portée des différents types d'audits (*Red Team*, *Pentesting*, *Bug Bounty*, etc.)
- Proposer les activités à mener suite à 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 4. Analyse des risques et environnement de sécurité IT

- Examiner, dans une perspective holistique, l'environnement dans lequel nous nous déplaçons
- Identifier les principaux risques et opportunités susceptibles d'affecter la réalisation 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 gérer les risques et les opportunités de manière à maximiser la valeur ajoutée
- Examiner en profondeur les différentes techniques de transfert de risque et de valeur
- Générer de la valeur à partir de la conception de modèles propriétaires pour la gestion agile des risques
- Examiner les résultats pour proposer des améliorations continues dans la gestion des projets et des processus sur la base de modèles de gestion axés sur les risques ou *Risk-Driven*
- Innover et transformer les données générales en informations pertinentes pour une prise de décision basée sur le risque

Module 5. Cryptographie dans les IT

- Compiler les opérations fondamentales (XOR, grands nombres, substitution et transposition) et les différents composants (fonctions à sens unique, 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 des clés
- Analyser le cycle de vie des clés
- Évaluer les modes de chiffrement par bloc et de chiffrement par flot
- Déterminer les générateurs de nombres pseudo-aléatoires
- Développer des cas réels d'applications cryptographiques, telles que Kerberos, PGP ou les cartes à puce
- Examiner les associations et organismes concernés, tels que l'ISO, le NIST ou le NCSC
- Déterminer les défis de la cryptographie de l'informatique quantique

Module 6. Gestion des identités et des accès dans le cadre de la sécurité Informatique

- Développer le concept d'identité numérique
- Évaluer le contrôle d'accès physique à l'information
- Principes fondamentaux de l'authentification biométrique et de l'authentification MFA
- Évaluer les attaques contre la confidentialité des informations
- Analyser la fédération d'identité
- Mettre en place un contrôle d'accès au réseau

Module 7. Sécurité des communications et du fonctionnement des logiciels

- Développer une expertise en matière de sécurité physique et logique
- Démontrer ses connaissances en matière de communications et de réseaux
- Identifier les principales attaques malveillantes
- Établir un cadre de développement sécurisé
- Démontrer une compréhension des principaux règlements relatifs aux systèmes de gestion de la sécurité de l'information
- Fonder le fonctionnement d'un centre d'opérations de cybersécurité
- Démontrer l'importance des pratiques de cybersécurité pour les catastrophes organisationnelles

Module 8. La sécurité dans les environnements Cloud

- Identifier les risques liés au déploiement d'une infrastructure de *Cloud* public
- Définir les exigences de sécurité
- Élaborer un plan de sécurité pour le déploiement d'une infrastructure *Cloud*
- Identifier les services *Cloud* à déployer pour la mise en œuvre d'un plan de sécurité
- Déterminer les opérations requises pour les mécanismes de prévention
- Établir les lignes directrices d'un système de *Logging* et de surveillance
- Proposer des actions de réponse aux incidents

Module 9. Sécurité des communications des dispositifs IoT

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

Module 10. 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)
- Justifier la nécessité d'un Plan de Continuité des Activités
- Déterminer les cartes de succès et de risques pour 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)
- Élaborer un Plan pour la Mise en Œuvre réussie d'un Plan de Continuité des Activités (PCA)

Module 11. Leadership, Éthique et Responsabilité Sociale des Entreprises

- Analyser l'impact de la mondialisation sur la gouvernance et le gouvernement d'entreprise
- Évaluer l'importance d'un leadership efficace dans la gestion et la réussite des entreprises
- Définir des stratégies de gestion interculturelle et leur pertinence dans des environnements commerciaux diversifiés
- Développer des compétences en matière de leadership et comprendre les défis actuels auxquels sont confrontés les dirigeants
- Déterminer les principes et les pratiques de l'éthique des affaires et leur application dans la prise de décision au sein de l'entreprise
- Structurer des stratégies pour la mise en œuvre et l'amélioration de la durabilité et de la responsabilité sociale dans les entreprises

Module 12. Gestion des Personnes et des Talents

- Déterminer la relation entre l'orientation stratégique et la gestion des ressources humaines
- Approfondir les compétences requises pour une gestion efficace des ressources humaines basée sur les compétences
- Approfondir les méthodologies d'évaluation et de gestion des performances
- Intégrer les innovations en matière de gestion des talents et leur impact sur la rétention et la fidélisation du personnel
- Développer des stratégies de motivation et de développement d'équipes performantes
- Proposer des solutions efficaces pour la gestion du changement et la résolution des conflits dans les organisations

Module 13. Gestion Économique et Financière

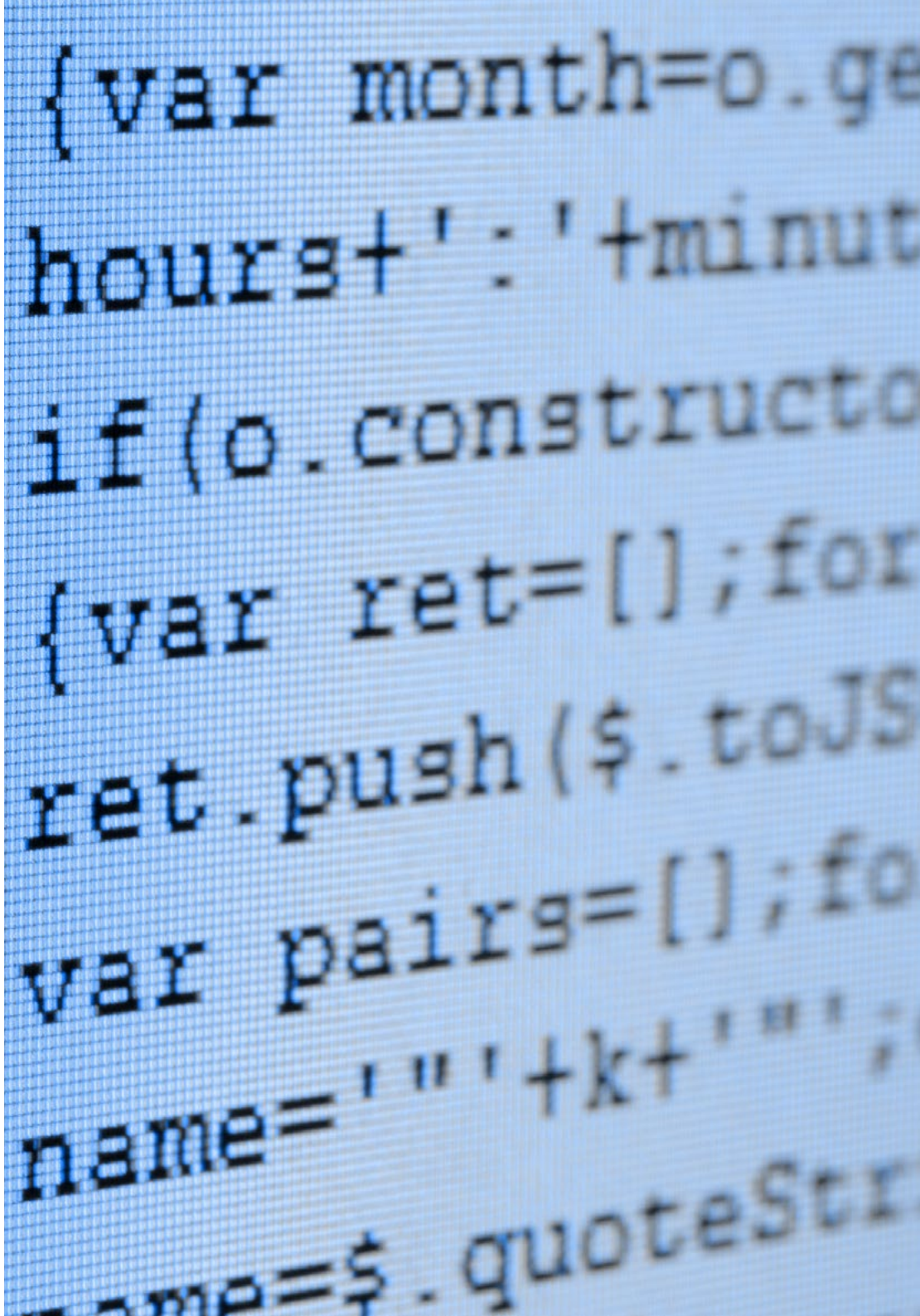
- Analyser l'environnement macroéconomique et son influence sur le système financier international
- Définir les systèmes d'information et la Business Intelligence pour la prise de décision financière
- Distinguer les décisions financières clés et la gestion des risques dans la gestion financière
- Évaluer les stratégies de planification financière et d'obtention d'un financement d'entreprise

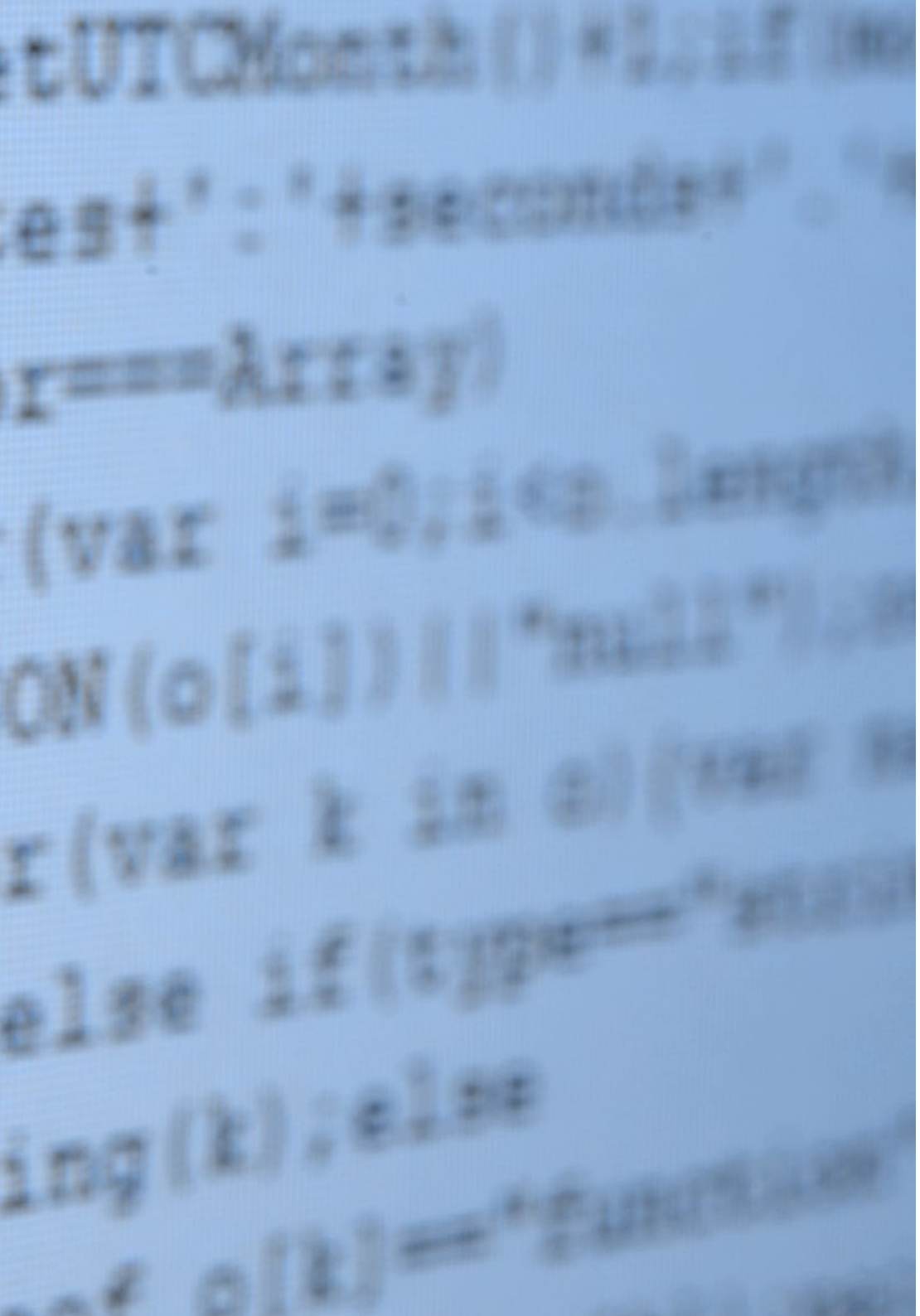
Module 14. Direction d'Entreprise et Marketing Stratégique

- Structurer le cadre conceptuel et l'importance de la gestion du marketing dans les entreprises
- Approfondir les éléments et activités fondamentaux du marketing et leur impact sur l'organisation
- Déterminer les étapes du processus de planification stratégique du marketing
- Évaluer les stratégies visant à améliorer la communication et la réputation numérique de l'entreprise

Module 15. *Management* Exécutif

- Définir le concept de Gestion Générale et sa pertinence dans la gestion d'entreprise
- Évaluer les rôles et les responsabilités de la direction dans la culture organisationnelle
- Analyser l'importance de la gestion des opérations et de la gestion de la qualité dans la chaîne de valeur
- Développer des compétences en matière de communication interpersonnelle et de prise de parole en public pour la formation des porte-parole





Vos objectifs professionnels sont désormais à votre portée grâce à ce Mastère Spécialisé qui offre les connaissances les plus avancées en matière de cybersécurité"

03

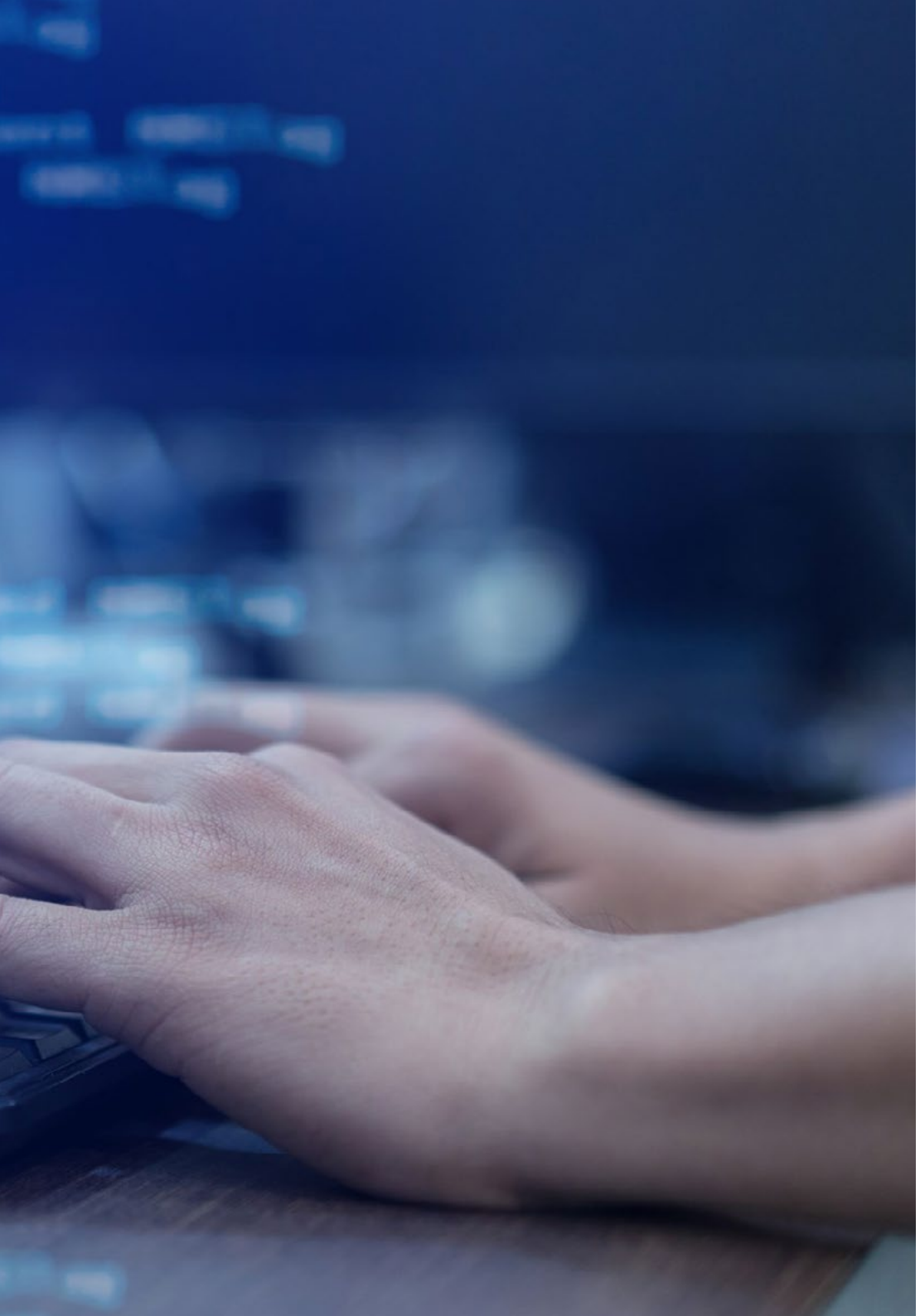
Compétences

Grâce à ce Mastère Spécialisé, le professionnel acquerra de nombreuses compétences nouvelles dans le domaine de la cybersécurité. L'émergence, ces dernières années, de technologies telles que la *Blockchain*, le *Cloud Computing* et l'intelligence artificielle a conduit au développement de nouveaux domaines de cybersécurité. C'est pourquoi ce programme a été spécialement conçu pour fournir aux professionnels toutes les compétences nécessaires pour s'adapter à ces technologies en plein essor.

Les compétences que ce programme vous apportera vous permettront de vous mettre à jour et de vous adapter au nouvel environnement informatique, où des technologies telles que la Blockchain et l'intelligence artificielle ont fait irruption"

Compétences générales

- Appliquer les mesures de sécurité les plus appropriées en fonction des menaces
- Déterminer la politique et le plan de sécurité des systèmes d'information d'une entreprise, en achevant la conception et la mise en œuvre du Plan d'Urgence
- Établir un programme d'audit qui répond aux besoins d'auto-évaluation de la cybersécurité de l'organisation
- Développer un programme d'analyse et de surveillance des vulnérabilités et un plan de réponse aux incidents de cybersécurité
- Maximiser les possibilités offertes et éliminer l'exposition à tous les risques potentiels liés à la conception elle-même
- 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 encourus par les entreprises qui ne disposent pas d'un environnement de sécurité informatique



Compétences spécifiques

- Développer un Système de Management de la Sécurité de l'Information (SMSI)
- Identifier les éléments clés qui composent un SMSI
- Appliquer la méthodologie MAGERIT pour faire évoluer le modèle et aller plus loin
- 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 basée sur un modèle *Risk-Driven* ou sur les risques qui permet non seulement de survivre dans son propre environnement, mais aussi d'apporter sa propre contribution à la valeur ajoutée
- Examiner le processus de conception d'une stratégie de sécurité lors du déploiement de services d'entreprise en *Cloud*
- Évaluer les différences dans les implémentations concrètes des différents fournisseurs de *Cloud* publique
- 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

04

Direction de la formation

La complexité même de la cybersécurité d'aujourd'hui exige un processus d'apprentissage approfondi et détaillé. C'est pourquoi TECH a pris l'initiative de réunir les meilleurs enseignants spécialisés dans ce domaine. Ainsi, le professionnel bénéficiera de l'accompagnement et de la supervision d'un corps enseignant au fait des dernières avancées dans ce domaine, ce qui lui permettra d'intégrer les meilleures techniques de cybersécurité dans son travail quotidien, tout en acquérant les compétences nécessaires en matière de gestion dans ce domaine.

Vous aurez à votre disposition de véritables spécialistes de la cybersécurité. C'est l'opportunité que vous attendiez"

Directrice Invitée Internationale

Avec plus de 20 ans d'expérience dans la conception et la direction d'équipes mondiales d'acquisition de talents, Jennifer Dove est une experte en recrutement et en stratégie technologique. Tout au long de sa carrière, elle a occupé des postes de direction dans plusieurs organisations technologiques au sein d'entreprises figurant au classement Fortune 50, notamment NBCUniversal et Comcast. Son parcours lui a permis d'exceller dans des environnements compétitifs et à forte croissance.

En tant que Vice-présidente de l'Acquisition des Talents chez Mastercard, elle est chargée de superviser la stratégie et l'exécution de l'intégration des talents, en collaborant avec les chefs d'entreprise et les responsables des Ressources Humaines afin d'atteindre les objectifs opérationnels et stratégiques en matière de recrutement. Elle vise notamment à créer des équipes diversifiées, inclusives et performantes qui stimulent l'innovation et la croissance des produits et services de l'entreprise. Elle est également experte dans l'utilisation d'outils permettant d'attirer et de retenir les meilleurs professionnels du monde entier. Elle est également chargée d'amplifier la marque employeur et la proposition de valeur de Mastercard par le biais de publications, d'événements et de médias sociaux.

Jennifer Dove a démontré son engagement en faveur du développement professionnel continu, en participant activement à des réseaux de professionnels des Ressources Humaines et en contribuant au recrutement de nombreux employés dans différentes entreprises. Après avoir obtenu un diplôme en Communication Organisationnelle à l'Université de Miami, elle a occupé des postes de recruteuse senior dans des entreprises de divers domaines.

En outre, elle a été reconnue pour sa capacité à mener des transformations organisationnelles, à intégrer les technologies dans les processus de recrutement et à développer des programmes de leadership qui préparent les institutions à relever les défis futurs. Elle a également mis en œuvre avec succès des programmes de bien-être qui ont considérablement augmenté la satisfaction et la fidélisation des employés.

Mme Dove, Jennifer

- Vice- présidente de l'Acquisition des Talents, Mastercard, New York, États-Unis
- Directrice de l'Acquisition de Talents chez NBCUniversal, New York, États-Unis
- Responsable du Recrutement chez Comcast
- Directrice du Recrutement chez Rite Hire Advisory
- Vice-présidente Exécutive, Division des Ventes chez Ardor NY Real Estate
- Directrice du Recrutement chez Valerie August & Associates
- Chargée de Clientèle chez BNC
- Chargée de Clientèle chez Vault
- Diplôme en Communication Organisationnelle de l'Université de Miami

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

Directeur Invité International

Leader technologique possédant des décennies d'expérience au sein de **grandes multinationales technologiques**, Rick Gauthier s'est distingué dans le domaine des **service**s en **nuage** et de l'amélioration des processus de bout en bout. Il a été reconnu comme un chef d'équipe et un manager très efficace, faisant preuve d'un talent naturel pour assurer un haut niveau d'engagement parmi ses employés.

Il est doué pour la stratégie et l'innovation exécutive, développant de nouvelles idées et étayant ses succès par des données de qualité. Son expérience à **Amazon** lui a permis de gérer et d'intégrer les services informatiques de l'entreprise aux États-Unis. Chez **Microsoft**, il a dirigé une équipe de 104 personnes, chargée de fournir une infrastructure informatique à l'échelle de l'entreprise et de soutenir les départements d'ingénierie des produits dans l'ensemble de l'entreprise.

Cette expérience lui a permis de se distinguer en tant que manager à fort impact, doté de remarquables capacités à accroître l'efficacité, la productivité et la satisfaction globale des clients.

M. Gauthier, Rick

- Directeur régional des Technologies de l'Information chez Amazon, Seattle, États-Unis
- Directeur de programme senior chez Amazon
- Vice-président, Wimmer Solutions
- Directeur principal des services d'ingénierie de production chez Microsoft
- Diplôme en Cybersécurité de l'Université Western Governors
- Certificat Technique en *Plongée Commerciale* de l'Institut de Technologie de la Diversité
- Diplôme en Études Environnementales de l'Evergreen State College

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

Directeur Invité International

Romi Arman est un expert international de renom qui compte plus de vingt ans d'expérience dans les domaines de la **Transformation Numérique**, du **Marketing,** de la Stratégie et du **Conseil**. Tout au long de sa longue carrière, il a pris de nombreux risques et est un **défenseur** constant de **l'innovation** et du **changement** dans l'environnement professionnel. Fort de cette expertise, il a travaillé avec des PDG et des organisations d'entreprises du monde entier, les poussant à s'éloigner des modèles d'entreprise traditionnels. Ce faisant, il a aidé des entreprises comme Shell Energy à devenir de **véritables leaders du marché,** axés sur leurs **clients** et le **monde numérique.**

Les stratégies conçues par Arman ont un impact latent, car elles ont permis à plusieurs entreprises **d'améliorer l'expérience des consommateurs, du personnel** et **des actionnaires** . Le succès de cet expert est quantifiable par des mesures tangibles telles que le **CSAT**, **l'engagement des employés** dans les institutions où il a travaillé et la croissance de **l'indicateur financier EBITDA** dans chacune d'entre elles.

De plus, au cours de sa carrière professionnelle, il a nourri et **dirigé des équipes très performantes** qui ont même été récompensées pour leur **potentiel de transformation**. Chez Shell, en particulier, le dirigeant s'est toujours efforcé de relever trois défis: répondre aux **demandes** complexes des clients en matière de **décarbonisation**, **soutenir** une "**décarbonisation rentable**" et **réorganiser** un paysage fragmenté sur le plan des **données**, **numérique et de la technologi**e. Ainsi, ses efforts ont montré que pour obtenir un succès durable, il est essentiel de partir des besoins des consommateurs et de jeter les bases de la transformation des processus, des données, de la technologie et de la culture.

D'autre part, le dirigeant se distingue par sa maîtrise des **applications commerciales** de **l'Intelligence Artificielle,** sujet dans lequel il est titulaire d'un diplôme post-universitaire de l'École de Commerce de Londres. Parallèlement, il a accumulé de l'expérience dans les domaines de **l'IoT** et de **Salesforce.**

M. Arman, Romi

- Directeur de la Transformation Numérique (CDO) chez Shell Energy Corporation, Londres, Royaume-Uni
- Directeur Mondial du Commerce Électronique et du Service à la Clientèle chez Shell Energy Corporation
- Gestionnaire National des Comptes Clés (équipementiers et détaillants automobiles) pour Shell à Kuala Lumpur, Malaisie
- Consultant en Gestion Senior (Secteur des Services Financiers) pour Accenture basé à Singapour
- Licence de l'Université de Leeds
- Diplôme Supérieur en Applications Commerciales de l'IA pour les Cadres Supérieurs de l'École de Commerce de Londres
- Certification Professionnelle en Expérience Client CCXP
- Cours de Transformation Numérique pour les Cadres de l'IMD

Vous souhaitez mettre à jour vos connaissances en bénéficiant d'une qualité éducative optimale? TECH vous offre le contenu le plus récent du marché universitaire, conçu par des experts de renommée internationale"

Directeur Invité International

Manuel Arens est un **professionnel expérimenté** de la gestion des données et le chef d'une équipe hautement qualifiée. En fait, M. Arens occupe le poste de **responsable mondial des achats** au sein de la division Infrastructure Technique et Centre de Données de Google, où il a passé la plus grande partie de sa carrière. Basée à Mountain View, en Californie, elle a fourni des solutions aux défis opérationnels du géant technologique, tels que **l'intégrité des données de base,** les **mises à jour des données des fournisseurs** et la **hiérarchisation des données** des fournisseurs. Il a dirigé la planification de la chaîne d'approvisionnement des centres de données et l'évaluation des risques liés aux fournisseurs, en apportant des améliorations aux processus et à la gestion des flux de travail, ce qui a permis de réaliser d'importantes économies.

Avec plus de dix ans d'expérience dans la fourniture de solutions numériques et de leadership pour des entreprises de divers secteurs, il possède une vaste expérience dans tous les aspects de la fourniture de solutions stratégiques, y compris le **Marketing, l''analyse des médias, la mesure** et **l'attribution.** Il a d'ailleurs reçu plusieurs prix pour son travail, notamment le **Prix du Leadership BIM**, le **Prix du Leadership en matière de Recherche**, le **Prix du Programme de Génération de Leads à l'Exportation** et le **Prix du Meilleur Modèle de Vente pour la région EMEA.**

M. Arens a également occupé le poste de **Directeur des Ventes** à Dublin, en Irlande. À ce titre, il a constitué une équipe de 4 à 14 membres en trois ans et a amené l'équipe de vente à obtenir des résultats et à bien collaborer avec les autres membres de l'équipe et avec les équipes interfonctionnelles. Il a également occupé le poste **d'Analyste Principal** en Industrieà Hambourg, en Allemagne, où il a créé des scénarios pour plus de 150 clients à l'aide d'outils internes et tiers pour soutenir l'analyse. Il a élaboré et rédigé des rapports approfondis pour démontrer sa maîtrise du sujet, y compris la compréhension des **facteurs macroéconomiques et politiques/réglementaires** affectant l'adoption et la diffusion des technologies.

Il a également dirigé des équipes dans des entreprises telles que **Eaton, Airbus et Siemens**, où il a acquis une expérience précieuse en matière de gestion des comptes et de la chaîne d'approvisionnement. Il est particulièrement réputé pour dépasser continuellement les attentes en **établissant des relations précieuses avec les clients** et en **travaillant de manière transparente avec des personnes à tous les niveaux d'une organisation**, y compris les parties prenantes, la direction, les membres de l'équipe et les clients. Son approche fondée sur les données et sa capacité à développer des solutions innovantes et évolutives pour relever les défis de l'industrie ont fait de lui un leader éminent dans son domaine.

M. Arens, Manuel

- Directeur des Achats Globaux chez Google, Mountain View, États-Unis
- Responsable principal de l'Analyse et de la Technologie B2B chez Google, États-Unis
- Directeur des ventes chez Google, Irlande
- Analyste Industriel Senior chez Google, Allemagne
- Gestionnaire des comptes chez Google, Irlande
- Account Payable chez Eaton, Royaume-Uni
- Responsable de la Chaîne d'Approvisionnement chez Airbus, Allemagne

Misez sur la TECH! Vous aurez accès au meilleur matériel didactique, à la pointe de la technologie et de l'éducation, mis en œuvre par des spécialistes de renommée internationale dans ce domaine"

Directeur Invité International

Andrea La Sala est un cadre **expérimenté** en **Marketing** dont les projets ont eu un impact **significatif** sur **l'environnement de la Mode**. Tout au long de sa carrière, il a développé différentes tâches liées aux **Produits**, au **Merchandising** et à la **Communication**. Tout cela, lié à des marques prestigieuses telles que **Giorgio Armani**, **Dolce&Gabbana**, **Calvin Klein**, entre autres.

Les résultats de ce manage de **haut niveaur international** sont liés à sa capacité avérée à **synthétiser les informations** dans des cadres clairs et à exécuter des **actions concrètes** alignées sur des objectifs **commerciaux spécifiques**. En outre, il est reconnu pour sa **proactivité** et sa capacité à **s'adapter à des rythmes** de travail rapides. À tout cela, cet expert ajoute une **forte conscience commerciale**, une **vision du marché** et une **véritable passion** pour les **produits**.

En tant que **Directeur Mondial de la Marque et du Merchandising** chez **Giorgio Armani**, il a supervisé une variété de **stratégies de Marketing** pour **l'habillement** et les **accessoires**. Ses tactiques se sont également **concentrées** sur les **besoins** et le comportement des **détaillants et des consommateurs**. Dans ce cadre, La Sala a également été responsable de la commercialisation des produits sur les différents marchés, en tant que **chef d'équipe** dans les **services de Design**, de **Communication** et de **Ventes**.

D'autre part, dans des entreprises telles que **Calvin Klein** ou **Gruppo Coin**, il a entrepris des projets visant à stimuler la **structure**, le **développement** et la **commercialisation** de **différentes collections**. Parallèlement, il a été chargé de créer des **calendriers efficaces** pour les **campagnes** d'achat et de vente. Il a également été chargé des **conditions**, des **coûts**, des **processus** et des **délais de livraison** pour les différentes opérations.

Ces expériences ont fait d'Andrea La Sala l'un des **dirigeants d'entreprise** les plus qualifiés dans le secteur de la **Mode** et du **Luxe**. Une grande capacité managériale qui lui a permis de mettre en œuvre efficacement le **positionnement positif** de **différentes marques** et de redéfinir leurs indicateurs clés de performance (KPI).

M. La Sala, Andrea

- Directeur Mondial de la Marque et du Merchandising Armani Exchange chez Giorgio Armani, Milan, Italie
- Directeur du Merchandising chez Calvin Klein
- Chef de Marque chez Gruppo Coin
- Brand Manager chez Dolce&Gabbana
- Brand Manager chez Sergio Tacchini S.p.A.
- Analyste de Marché chez Fastweb
- Diplôme en Business and Economics à l'Université degli Studi du Piémont Oriental

Les professionnels internationaux les plus qualifiés et les plus expérimentés vous attendent à TECH pour vous offrir un enseignement de premier ordre, actualisé et fondé sur les dernières données scientifiques. Qu'attendez-vous pour vous inscrire?"

Directeur Invité International

Mick Gram est synonyme d'innovation et d'excellence dans le domaine de **l'Intelligence des Affaires** au niveau international. Sa carrière réussie est liée à des postes de direction dans des multinationales telles que **Walmart** et **Red Bull.** Il est également connu pour sa capacité à **identifier les technologies émergentes** qui, à long terme, auront un impact durable sur l'environnement des entreprises.

D'autre part, le dirigeant est considéré comme un **pionnier** dans **l'utilisation de techniques de visualisation de données** qui simplifient des ensembles complexes, les rendent accessibles et facilitent la prise de décision. Cette compétence est devenue le pilier de son profil professionnel, le transformant en un atout recherché par de nombreuses organisations qui misent sur la **collecte d'informations** et la **création d'actions** concrètes à partir de celles-ci.

L'un de ses projets les plus remarquables de ces dernières années a été la **plateforme Walmart Data Cafe**, la plus grande de ce type au monde, ancrée dans le nuage pour **l'analyse** des ***Big Data***. En outre, il a occupé le poste de **Directeur** de la **Business Intelligence** chez **Red Bull,** couvrant des domaines tels que les **Ventes, la Distribution, le Marketing et les Opérations de la Chaîne d'Approvisionnement**. Son équipe a récemment été récompensée pour son innovation constante dans l'utilisation de la nouvelle API de Walmart Luminate pour les insights sur les Acheteurs et les Canaux de distribution.

En ce qui concerne sa formation, le cadre possède plusieurs Masters et études supérieures dans des centres prestigieux tels que **l'Université de Berkeley**, aux États-Unis et **l'Université de Copenhague**, au Danemark. Grâce à cette mise à jour continue, l'expert a acquis des compétences de pointe. Il est ainsi considéré comme un **leader né** de la **nouvelle économie mondiale**, centrée sur la recherche de données et ses possibilités infinies.

M. Gram, Mick

- Directeur de la *Business Intelligence* et des Analyses chez Red Bull, Los Ángeles, États-Unis
- Architecte de solutions de *Business Intelligence* pour Walmart Data Cafe
- Consultant indépendant de *Business Intelligence* et de *Data Science*
- Directeur de *Business Intelligence* chez Capgemini
- Analyste en Chef chez Nordea
- Consultant en Chef de *Bussiness Intelligence* pour SAS
- Executive Education en IA et Machine Learning au UC Berkeley College of Engineering
- MBA Executive en e-commerce à l'Université de Copenhague
- Licence et Master en Mathématiques et Statistiques à l'Université de Copenhague

Étudiez dans la meilleure université en ligne du monde selon Forbes! Dans le cadre de ce MBA, vous aurez accès à une vaste bibliothèque de ressources multimédias, élaborées par des professeurs de renommée internationale"

Directeur Invité International

Scott Stevenson est un éminent expert en **Marketing Numérique** qui, pendant plus de 19 ans, a travaillé pour l'une des sociétés les plus puissantes de l'industrie du divertissement, **Warner Bros. Discovery.** À ce titre, il a joué un rôle essentiel dans la **supervision de la logistique** et des **flux de travail créatifs** sur de multiples plateformes numériques, y compris les médias sociaux, la recherche, le display et les médias linéaires.

Son leadership a été déterminant dans la mise en place de **stratégies de production** de **médias payants**, ce qui a entraîné une nette **amélioration** des **taux de conversion** de son entreprise. Parallèlement, il a assumé d'autres fonctions telles que celles de Directeur des Services Marketing et de Responsable du Trafic au sein de la même multinationale pendant la période où il occupait un poste de direction.

Stevenson a également participé à la distribution mondiale de jeux vidéo et de **campagnes de propriété numérique**. Il a également été responsable de l'introduction de stratégies opérationnelles liées à l'élaboration, à la finalisation et à la diffusion de contenus sonores et visuels pour les **publicités télévisées** et ***lesbandes-annonces***.

En outre, il est titulaire d'une Licence en Télécommunications de l'Université de Floride et d'un Master en Création Littéraire de l'Université de Californie, ce qui témoigne de ses compétences en matière de **communication** et de **narration**. En outre, il a participé à l'École de Développement Professionnel de l'Université de Harvard à des programmes de pointe sur l'utilisation de **l'Intelligence Artificielle** dans le monde des **affaires**. Son profil professionnel est donc l'un des plus pertinents dans le domaine actuel du **Marketing** et des **Médias Numériques**.

M. Stevenson, Scott

- Directeur du Marketing Numérique chez Warner Bros. Discovery, Burbank, États-Unis
- Responsable du Trafic chez Warner Bros. Entertainment
- Master en Création Littéraire de l'Université de Californie
- Licence en Télécommunications de l'Université de Floride

Atteignez vos objectifs académiques et professionnels avec les experts les plus qualifiés au monde! Les enseignants de ce MBA vous guideront tout au long du processus d'apprentissage. processus d'apprentissage"

Directeur Invité International

Le Docteur Eric Nyquist est un grand professionnel du **sport international**, qui s'est construit une carrière impressionnante, reconnue pour son **leadership stratégique** et sa capacité à conduire le changement et **l'innovation** dans des **organisations sportives** de classe mondiale.

En fait, il a occupé des postes de haut niveau, notamment celui de **Directeur de la Communication et de l'Impact** à la **NASCAR**, basée en **Floride, aux États-Unis.** Fort de ses nombreuses années d'expérience, le Docteur Nyquist a également occupé un certain nombre de postes de direction, dont ceux de premier **Vice-président** du **Développement Stratégique** et de **Directeur Général des Affaires Commerciales,** gérant plus d'une douzaine de disciplines allant du **développement stratégique** au **Marketing du divertissement.**

Nyquist a également laissé une marque importante sur les principales **franchises sportives** de Chicago. En tant que **Vice-président Exécutif** des **Bulls de Chicago** et des **White Sox de Chicago**, il a démontré sa capacité à mener à bien des **affaires** et des **stratégies** dans le monde du **sport professionnel**.

Enfin, il a commencé sa carrière **dans le sport** en travaillant à **New York** en tant **qu'analyste stratégique principal** pour **Roger Goodell** au sein de la **National Football League (NFL)** et, avant cela, en tant que **Stagiaire Juridique** auprès de la **Fédération de Football des États-Unis.**

Dr Nyquist, Eric

- Directeur de la Communication et de l'Impact, NASCAR, Floride, États-Unis
- Vice-président Senior du Développement Statégique, NASCAR, Floride, États-Unis
- Vice-président de la Planification stratégique, NASCAR
- Directeur Senior des Affaires Commerciales à NASCAR
- Vice-président Exécutif, Franchises Chicago White Sox
- Vice-président Exécutif, Franchises des Bulls de Chicago
- Responsable de la Planification des Affaires à la National Football League (NFL)
- Stagiaire en Affaires Commerciales et Juridiques à la Fédération Américaine de Football
- Docteur en Droit de l'Université de Chicago
- Master en Administration des Affaires (MBA) de L'Université de Chicago (Booth School of Business)
- Licence en Économie Internationale du Carleton College

Grâce à ce diplôme universitaire 100% en ligne, vous pourrez combiner vos études avec vos obligations quotidiennes, avec l'aide des meilleurs experts internationaux dans le domaine qui vous intéresse. Inscrivez-vous dès maintenant!"

Direction

M. Olalla Bonal, Martín

- Responsable de la Pratique Blockchain chez EY
- Spécialiste Technique Client Blockchain pour IBM
- Directeur de l'Architecture de Blocknitive
- Coordinateur de l'Équipe Bases de Données Distribuées non Relationnelles pour wedoIT, Filiale d'IBM
- Architecte d'Infrastructure chez Bankia
- Chef du Département Mise en Page chez T-Systems
- Coordinateur de Département pour Bing Data España SL

Professeurs

Dr Nogales Ávila, Javier

- Enterprise Cloud et consultant senior en sourcing Quint
- Cloud and Technology Consultant. Indra
- Associate Technology Consultant. Accenture
- Diplôme de l'Université de Jaén et de l'Université de Technologie et d'Economie de Budapest (BME)
- Diplôme en Ingénierie de l'Organisation Industrielle

M. Rodrigo Estébanez, Juan Manuel

- Co-fondateur d'Ismet Tech
- Directeur de la Sécurité de l'Information chez Ecix Group
- *Operational Security Officer* chez Atos IT Solutions and Services A/S
- Chargé de cours en Gestion de la Cybersécurité dans le cadre d'Études Universitaires
- Diplôme d'Ingénieur de l'Université de Valladolid
- Master en Systèmes de Gestion Intégrée de l'Université CEU San Pablo

M. Gonzalo Alonso, Félix

- Directeur Général et Fondateur de 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'Expertise Technologique Spécialisé)
- Licence en Ingénierie de l'Organisation Industrielle de l'Université Pontificale de Comillas ICAI
- Diplôme en Ingénierie technique industrielle avec spécialisation en Électronique Industrielle de l'Université Pontificale de Comillas ICAI
- Master en Gestion des Assurances de l'ICEA (Institut de Collaboration entre les Compagnies d'Assurances)

Dr Entrenas, Alejandro

- Chef de projet en Cybersécurité Entelgy Innotec Security
- Consultant en Cybersécurité Entelgy
- Analyste en Sécurité de l'Information Innovery Espagne
- Analyste en Sécurité de l'Information Atos
- Licence en Ingénierie Technique des Systèmes Informatiques de l'Université de Cordoue
- Master en Gestion de la Sécurité de l'Information de l'Université Polytechnique de Madrid
- ITIL v4 Foundation Certificate in IT Service Management. ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced. Avnet
- IBM Security QRadar SIEM 7.1 Foundations. Avnet

Dr Gómez Rodríguez, Antonio

- Ingénieur Principal de Solutions Cloud chez Oracle
- Co-organisateur de Malaga Developer Meetup
- Consultant Spécialisé pour Sopra Group et Everis
- Chef d'équipe chez System Dynamics
- Développeur de Logiciels chez SGO Software
- Master en E-Business de l'École de Commerce de La Salle
- Diplôme en Technologies et Systèmes d'Information, Institut Catalan de Technologie
- Licence en Génie Supérieur des Télécommunications de l'Université Polytechnique de Catalogne

Dr Del Valle Arias, Jorge

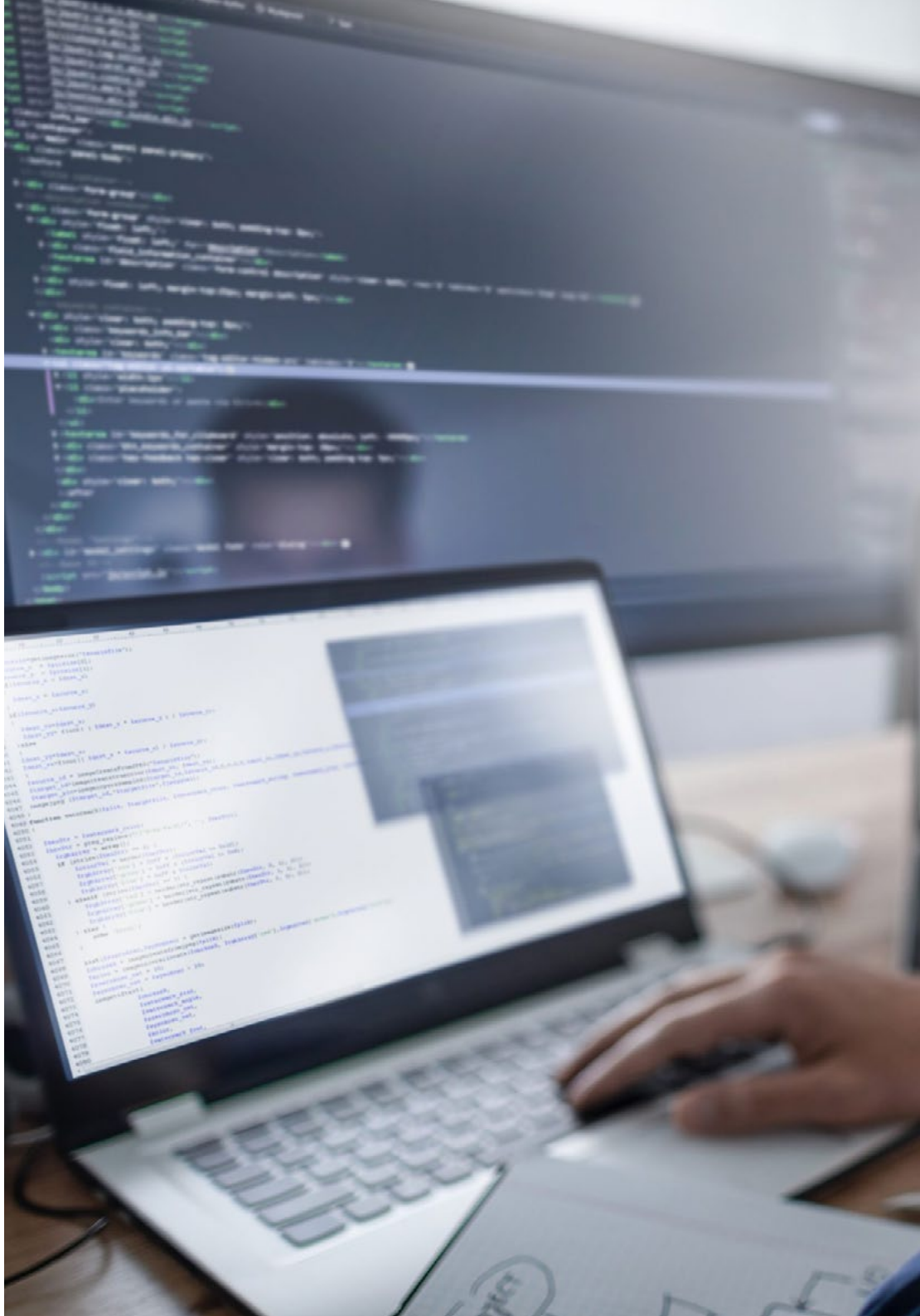
- Smart City Solutions & Software Business Development Manager Espagne Itron, Inc Consultor IoT
- Directeur Commercial IoT par Intérim TCOMET
- Responsable de l'Unité Commerciale IoT, Industrie 4.0 Diode Espagne
- Directeur de la Zone de Ventes de l'IoT et des Télécommunications Aicox Solutions
- Directeur Technique (CTO) et Directeur du Développement des Affaires Consultation TELYC
- Fondateur et PDG de Sensor Intelligence
- Chef des Opérations et des Projets Codio
- Directeur des Opérations chez Codium Networks
- Ingénieur en Chef de la Conception du hardware et du firmware AITEMIN
- Responsable Régional de la Planification et de l'Optimisation RF - Réseau LMDS 3.5 GHz Clearwire
- Ingénieur en Télécommunications de l'Université Polytechnique de Madrid
- Executive MBA de l'International Graduate School de La Salle de Madrid
- Master en Énergies Renouvelables CEPYME

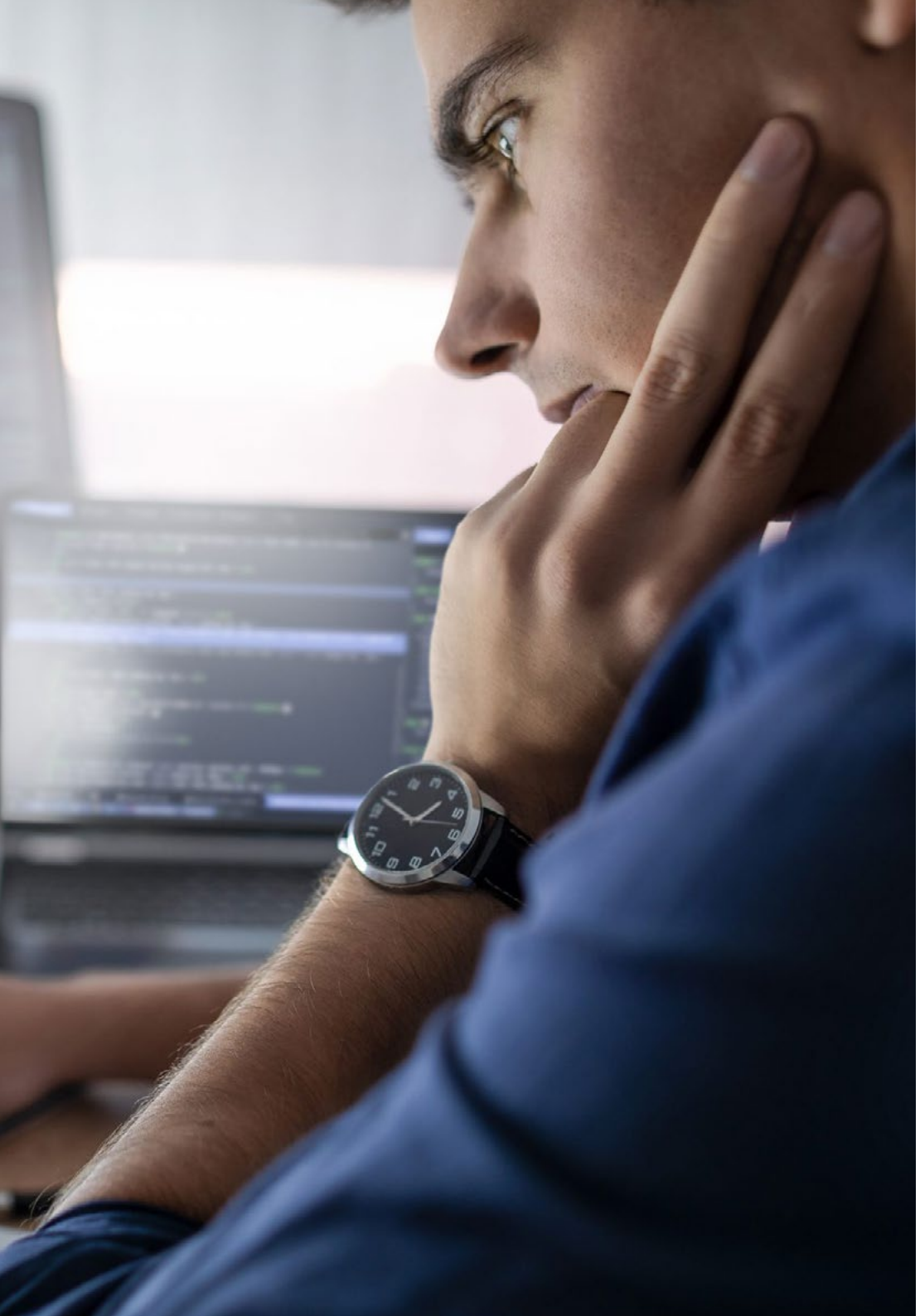
Dr Gozalo Fernández, Juan Luis

- Gestionnaire de Produits basés sur la blockchain pour Open Canarias
- Directeur Blockchain DevOps chez Alastria
- Responsable de la Technologie des Niveaux de Service chez Santander Espagne
- Directeur du Développement des Applications Mobiles Tinkerlink chez Cronos Telecom
- Directeur de la Technologie de Gestion des Services Informatiques à la Barclays Bank Espagne
- Licence en Ingénierie Informatique à l'UNED
- Spécialisation en *Deep Learning* chez DeepLearning.ai

Dr Jurado Jabonero, Lorena

- Responsable de la Sécurité de l'Information (CISO) chez Groupe Pascual
- Cybersecurity Manager en KPMG. Espagne
- Consultante en Processus Informatique et Contrôle d'Infrastructure et en Gestion de Projet chez Bankia
- Ingénieuse en Outils d'Exploitation chez Dalkia
- Développeuse au Sein du Groupe Banco Popular
- Développeuse des Applications à l'Université Polytechnique de Madrid
- Diplôme en Ingénierie Informatique de l'Université Alfonso X el Sabio
- Ingénieure Technique en Gestion Informatique de l'Université Polytechnique de Madrid Certifié Ingénieur en Solutions de Confidentialité des Données (CDPSE) par l'ISACA





M. Ortega, Octavio

- Spécialiste du Marketing et du Développement Web
- Programmeur d'Applications Informatiques et Développeur Web *Indépendant*
- *Chief Operating* Officer chez Smallsquid SL
- Administrateur du E-commerce pour Ortega et Serrano
- Conférencier pour les cours de Certificat de Professionnalisme en Informatique et Communications
- Conférencier pour les cours de Sécurité Informatique
- Licence en Psychologie de l'Université Ouverte de Catalogne
- Technicien Supérieur d'Analyse, de Conception et de Solutions *Logicielles*
- Technicien Supérieur en Programmation Avancée

M. Embid Ruiz, Mario

- Avocat Expert en TIC et protection des données chez Martínez-Echevarría Avocats
- Directeur Juridique de Branddocs SL
- Analyste des Risques dans le Segment PME de BBVA
- Chargé de cours dans le cadre d'études universitaires de troisième cycle en rapport avec le Droit
- Licence en Droit de l'Université Roi Juan Carlos
- Licence en Administration et Gestion d'Entreprises à l'Université Roi Juan Carlos
- Master en Droit des Nouvelles Technologies, de l'Internet et de l'Audiovisuel du Centre d'Etudes Universitaires Villanueva

05

Structure et contenu

Ce MBA en Direction de la Cybersécurité Avancée (CISO) est structuré en 10 modules spécialisés qui permettront au professionnel d'étudier en profondeur 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 les communications et l'exploitation des logiciels ou l'élaboration du plan de continuité des activités associé à la sécurité. Cela permettra à l'informaticien d'avoir une compréhension globale de toutes les questions pertinentes en matière de cybersécurité aujourd'hui.

Vous ne trouverez pas de contenu plus complet et plus innovant que celui-ci pour vous spécialiser dans la gestion avancée de la cybersécurité"

Module 1. La sécurité dans la conception et le développement des systèmes

1.1. Systèmes d'information
- 1.1.1. Domaines d'un système d'information
- 1.1.2. Composants des systèmes d'information
- 1.1.3. Activités d'un système d'information
- 1.1.4. Cycle de vie d'un système d'information
- 1.1.5. Ressources d'un système d'information

1.2. Systèmes d'information. Typologie
- 1.2.1. Types de systèmes d'information
  - 1.2.1.1. Commerciale
  - 1.2.1.2. Stratégique
  - 1.2.1.3. Selon le domaine d'application
  - 1.2.1.4. Spécifique
- 1.2.2. Systèmes d'information Exemples concrets
- 1.2.3. Évolution des systèmes d'information: étapes
- 1.2.4. Méthodologies des systèmes d'information

1.3. Sécurité des systèmes d'information. Implications juridiques
- 1.3.1. Accès aux données
- 1.3.2. Menaces sur la sécurité: vulnérabilités
- 1.3.3. Implications juridiques: infractions pénales
- 1.3.4. Procédures de maintenance des systèmes d'information

1.4. Sécurité d'un système d'information. Protocole de sécurité
- 1.4.1. Sécurité d'un système d'information
  - 1.4.1.1. Intégrité
  - 1.4.1.2. Confidentialité
  - 1.4.1.3. Disponibilité
  - 1.4.1.4. Authentification
- 1.4.2. Services de sécurité
- 1.4.3. Protocoles de sécurité de l'information. Typologie
- 1.4.4. Sensibilité d'un système d'information

1.5. Sécurité d'un système d'information Mesures et systèmes de contrôle d'accès
- 1.5.1. Mesures de sécurité
- 1.5.2. Type de mesures de sécurité
  - 1.5.2.1. Prévention
  - 1.5.2.2. Détection
  - 1.5.2.3. Correction
- 1.5.3. Systèmes de contrôle d'accès Typologie
- 1.5.4. Cryptographie

1.6. Sécurité dans les réseaux sur l'internet
- 1.6.1. Firewalls
- 1.6.2. Identification numérique
- 1.6.3. Virus et vers
- 1.6.4. *Hacking*
- 1.6.5. Exemples et cas réels

1.7. Criminalité informatique
- 1.7.1. Criminalité informatique
- 1.7.2. Criminalité informatique Typologie
- 1.7.3. Criminalité informatique L'attaque Typologie
- 1.7.4. Le cas de la réalité virtuelle
- 1.7.5. Profils des délinquants et des victimes. Typification de la criminalité
- 1.7.6. Criminalité informatique Exemples et cas réels

1.8. Plan de sécurité du système d'information
- 1.8.1. Plan de sécurité. Objectifs
- 1.8.2. Plan de sécurité. Planification
- 1.8.3. Plan de risque Analyse
- 1.8.4. Politique de sécurité. Mise en œuvre dans l'organisation
- 1.8.5. Plan de sécurité. Mise en œuvre dans l'organisation
- 1.8.6. Procédures de sécurité. Types
- 1.8.7. Plans de sécurité Exemples

1.9. Plan de contingence
- 1.9.1. Plan de contingence Fonctions
- 1.9.2. Plan d'urgence: Éléments et objectifs
- 1.9.3. Plan d'urgence dans l'organisation Mise en œuvre
- 1.9.4. Plans de contingence Exemples

1.10. Gouvernance de la sécurité des systèmes d'information
- 1.10.1. Réglementation juridique
- 1.10.2. Normes
- 1.10.3. Certifications
- 1.10.4. Technologies

Module 2. Architectures et modèles de sécurité de l'information

2.1. Architecture de la sécurité de l'information
- 2.1.1. ISMS/PDS
- 2.1.2. Alignement stratégique
- 2.1.3. Gestion des risques
- 2.1.4. Mesure de la performance

2.2. Modèles de sécurité de l'information
- 2.2.1. Modèles de sécurité fondés sur des politiques
- 2.2.2. Basés sur des outils de protection
- 2.2.3. Basé sur l'équipe de travail

2.3. Modèle de sécurité. Éléments clés
- 2.3.1. Identification des risques
- 2.3.2. Définition des contrôles
- 2.3.3. Évaluation continue des niveaux de risque
- 2.3.4. Plan de sensibilisation pour les employés, les fournisseurs, les partenaires, etc

2.4. Processus de gestion des risques
- 2.4.1. Identification des actifs
- 2.4.2. Identification des menaces
- 2.4.3. Évaluation des risques
- 2.4.4. Hiérarchisation des contrôles
- 2.4.5. Réévaluation et risque résiduel

2.5. Processus d'entreprise et sécurité de l'information
- 2.5.1. Processus d'entreprise
- 2.5.2. Évaluation des risques sur la base des paramètres de l'entreprise
- 2.5.3. Analyse de l'impact sur l'entreprise
- 2.5.4. Les opérations d'entreprise et sécurité de l'information

2.6. Processus d'amélioration continue
- 2.6.1. Le cycle de Deming
  - 2.6.1.1. Planification
  - 2.6.1.2. Faire
  - 2.6.1.3. Vérifier
  - 2.6.1.4. Agir

2.7. Architectures de sécurité
- 2.7.1. Sélection et normalisation des technologies
- 2.7.2. Gestion de l'identité Authentification
- 2.7.3. Gestion des accès Autorisation
- 2.7.4. Sécurité de l'infrastructure du réseau
- 2.7.5. Technologies et solutions de chiffrement
- 2.7.6. Sécurité des Équipements Terminaux (EDR)

2.8. Le cadre réglementaire
- 2.8.1. Réglementations sectorielles
- 2.8.2. Certifications
- 2.8.3. Législation

2.9. Norme ISO 27001
- 2.9.1. Mise en œuvre
- 2.9.2. Certification
- 2.9.3. Audits et tests de pénétration
- 2.9.4. Gestion continue des risques
- 2.9.5. Classification des informations

2.10. Législation en matière de protection de la vie privée RGPD (GDPR)
- 2.10.1. Champ d'application du Règlement Général sur la Protection des Données (RGPD)
- 2.10.2. Données personnelles
- 2.10.3. Rôles dans le traitement des données à caractère personnel
- 2.10.4. Droits de l'ARCO
- 2.10.5. Le DPO Fonctions

Module 3. Gestion de la sécurité IT

3.1. Gestion de la sécurité
- 3.1.1. Opérations de sécurité
- 3.1.2. Aspects juridique et réglementaire
- 3.1.3. Qualification des entreprises
- 3.1.4. Gestion des risques
- 3.1.5. Gestion des identités et des accès

3.2. Structure du domaine de la sécurité. Le bureau du CISO
- 3.2.1. Structure de l'organisation Position du CISO dans la structure
- 3.2.2. Les lignes de défense
- 3.2.3. Organigramme du bureau du CISO
- 3.2.4. Gestion du budget

3.3. Gouvernance de la sécurité
- 3.3.1. Comité de sécurité
- 3.3.2. Comité de suivi des risques
- 3.3.3. Comité d'audit
- 3.3.4. Comité de crise

3.4. Gouvernance de la sécurité. Fonctions
- 3.4.1. Politiques et normes
- 3.4.2. Plan directeur de la sécurité
- 3.4.3. Tableaux de bord
- 3.4.4. Sensibilisation et formation
- 3.4.5. Sécurité de la chaîne d'approvisionnement

3.5. Opérations de sécurité
- 3.5.1. Gestion des identités et des accès
- 3.5.2. Configuration des règles de sécurité du réseau *Firewalls*
- 3.5.3. Gestion des plateformes IDS/IPS
- 3.5.4. Analyse des vulnérabilités

3.6. Cadre de cybersécurité. NIST CSF
- 3.6.1. Méthodologie NIST
  - 3.6.1.1. Identifier
  - 3.6.1.2. Protéger
  - 3.6.1.3. Détecter
  - 3.6.1.4. Répondre
  - 3.6.1.5. Récupérer

3.7. Centre des Opérations de Sécurité (SOC). Fonctions
- 3.7.1. Protection *Red Team, pentesting, threat intelligence*
- 3.7.2. Détection. SIEM, *user behavior analytics, fraud prevention*
- 3.7.3. Réponse

3.8. Audit de sécurité
- 3.8.1. Tests de pénétration
- 3.8.2. Exercices de *red team*
- 3.8.3. Audits du code source. Développement sécurisé
- 3.8.4. Sécurité des composants (*software supply chain*)
- 3.8.5. Analyse médico-légale

3.9. Réponse aux incidents
- 3.9.1. Préparation
- 3.9.2. Détection, analyse et rapport
- 3.9.3. Confinement, éradication et récupération
- 3.9.4. Activité post-incident
  - 3.9.4.1. Conservation des preuves
  - 3.9.4.2. Analyse médico-légale
  - 3.9.4.3. Gestion des écarts
- 3.9.5. Guides officiels de gestion des cyberincidents

3.10. Gestion des vulnérabilités
- 3.10.1. Analyse des vulnérabilités
- 3.10.2. Évaluation de vulnérabilité
- 3.10.3. Base de données système
- 3.10.4. Vulnérabilités au jour 0 *Zero-day*

Module 4. Analyse des risques et environnement de sécurité IT

4.1. Analyse de l'environnement
- 4.1.1. Analyse de la situation économique
  - 4.1.1.1. Environnement VUCA
    - 4.1.1.1.1. Volatilité
    - 4.1.1.1.2. Incertain
    - 4.1.1.1.3. Complexe
    - 4.1.1.1.4. Ambiguë:
  - 4.1.1.2. Environnement BANI
    - 4.1.1.2.1. Fragile
    - 4.1.1.2.2. Anxieux
    - 4.1.1.2.3. Non linéaire
    - 4.1.1.2.4. Incompréhensible
- 4.1.2. Analyse de l'environnement général PESTEL
  - 4.1.2.1. Politique
  - 4.1.2.2. Économique
  - 4.1.2.3. Social
  - 4.1.2.4. Technologique
  - 4.1.2.5. Écologique/Environnemental
  - 4.1.2.6. Juridique
- 4.1.3. Analyse de la situation interne. SWOT
  - 4.1.3.1. Objectifs
  - 4.1.3.2. Menaces
  - 4.1.3.3. Opportunités
  - 4.1.3.4. Points forts

4.2. Risques et incertitudes
- 4.2.1. Risques
- 4.2.2. Gestion des risques
- 4.2.3. Normes de gestion des risques

4.3. Lignes directrices ISO 31.000:2018 relatives au management du risque
- 4.3.1. Objet
- 4.3.2. Principes
- 4.3.3. Cadre de référence
- 4.3.4. Processus

4.4. Méthodologie d'Analyse et de Gestion des Risques des Systèmes d'Information (MAGERIT)
- 4.4.1. Méthodologie MAGERIT
  - 4.4.1.1. Objectifs
  - 4.4.1.2. Méthode
  - 4.4.1.3. Éléments
  - 4.4.1.4. Techniques
  - 4.4.1.5. Outils disponibles (PILAR)

4.5. Transfert du risque cybernétique
- 4.5.1. Transfert de risque
- 4.5.2. Les cyber-risques Typologie
- 4.5.3. Assurance des cyber-risques

4.6. Méthodologies agiles pour la gestion des risques
- 4.6.1. Méthodologies agiles
- 4.6.2. Scrum pour la gestion des risques
- 4.6.3. *Agile risk management*

4.7. Technologies pour la gestion des risques
- 4.7.1. Intelligence artificielle appliquée à la gestion des risques
- 4.7.2. *Blockchain* et cryptographie Méthodes de préservation de la valeur
- 4.7.3. L'informatique quantique Opportunité ou menace

4.8. Cartographie des risques IT basée sur les méthodologies agiles
- 4.8.1. Représentation de la probabilité et de l'impact dans les environnements agiles
- 4.8.2. Le risque en tant que menace pour la valeur
- 4.8.3. Réévolution dans la gestion de projet agile et les processus agiles basés sur les KRIs

4.9. *Risk driven* en matière de gestion des risques
- 4.9.1. *Risk driven*
- 4.9.2. *Risk driven* en matière de gestion des risques
- 4.9.3. Développer un modèle de gestion d'entreprise axé sur le risque

4.10. Innovation et transformation numérique dans la gestion des risques Informatiques
- 4.10.1. La gestion agile des risques comme source d'innovation commerciale
- 4.10.2. Transformation des données dans informations utiles à la prise de décision
- 4.10.3. Vue holistique de l'entreprise à travers le risque

Module 5. Cryptographie dans les IT

5.1. Cryptographie
- 5.1.1. Cryptographie
- 5.1.2. Fondements mathématiques

5.2. Cryptologie
- 5.2.1. Cryptologie
- 5.2.2. Cryptanalyse
- 5.2.3. Stéganographie et stégananalyse

5.3. Protocoles cryptographiques
- 5.3.1. Blocs de base
- 5.3.2. Protocoles de base
- 5.3.3. Protocoles intermédiaires
- 5.3.4. Protocoles avancés
- 5.3.5. Protocoles exotériques

5.4. Techniques cryptographiques
- 5.4.1. Longueur de clé
- 5.4.2. Traitement des clés
- 5.4.3. Types d'Algorithmes
- 5.4.4. Fonctions récapitulatives *Hash*
- 5.4.5. Générateurs de nombres pseudo-aléatoires
- 5.4.6. Utilisation d'algorithmes

5.5. Cryptographie symétrique
- 5.5.1. Chiffrement par blocs
- 5.5.2. DES (*Data Encryption Standard*)
- 5.5.3. Algorithme RC4
- 5.5.4. AES (*Advanced Encryption Standard*)
- 5.5.5. Combinaison de chiffrement par blocs
- 5.5.6. Dérivation des clés

5.6. Cryptographie symétrique
- 5.6.1. Diffie-Hellman
- 5.6.2. DSA (*Digital Signature Algorithm*)
- 5.6.3. RSA (Rivest, Shamir et Adleman)
- 5.6.4. Courbe elliptique
- 5.6.5. Cryptographie asymétrique Typologie

5.7. Certificats numériques
- 5.7.1. Signature numérique
- 5.7.2. Certificats X509
- 5.7.3. Infrastructure à clé publique(PKI)

5.8. Mise en œuvre
- 5.8.1. Kerberos
- 5.8.2. IBM CCA
- 5.8.3. *Pretty Good Privacy* (PGP)
- 5.8.4. ISO *Authentication Framework*
- 5.8.5. SSL y TLS
- 5.8.6. Cartes à puce dans les moyens de paiement (EMV)
- 5.8.7. Protocoles de téléphonie mobile
- 5.8.8. *Blockchain*

5.9. Stéganographie
- 5.9.1. Stéganographie
- 5.9.2. Stéganalyse
- 5.9.3. Applications et utilisations

5.10. Cryptographie quantique
- 5.10.1. Algorithmes quantiques
- 5.10.2. Protection des algorithmes contre l'informatique quantique
- 5.10.3. Distribution quantique des clés

Module 6. Gestion des identités et des accès dans le cadre de la sécurité Informatique

6.1. Gestion des identités et des accès (IAM)
- 6.1.1. Identité numérique
- 6.1.2. Gestion des identités
- 6.1.3. Fédération d'identité

6.2. Contrôle d'accès physique
- 6.2.1. Systèmes de protection
- 6.2.2. Sécurité des zones
- 6.2.3. Installations de récupération

6.3. Contrôle d'accès logique
- 6.3.1. Authentification: typologie
- 6.3.2. Protocoles d'authentification
- 6.3.3. Attaques d'authentification

6.4. Contrôle d'accès logique Authentification MFA
- 6.4.1. Contrôle d'accès logique Authentification MFA
- 6.4.2. Mots de passe. Importance
- 6.4.3. Attaques d'authentification

6.5. Contrôle d'accès logique Authentification biométrique
- 6.5.1. Contrôle d'Aaccès Logique Authentification biométrique
  - 6.5.1.1. Authentification biométrique Exigences
- 6.5.2. Fonctionnement
- 6.5.3. Modèles et techniques

6.6. Systèmes de gestion de l'authentification
- 6.6.1. *Single sign on*
- 6.6.2. Kerberos
- 6.6.3. Systèmes AAA

6.7. Systèmes de gestion de l'authentification: Systèmes AAA
- 6.7.1. TACACS
- 6.7.2. RADIUS
- 6.7.3. DIAMETER

6.8. Services de contrôle d'accès
- 6.8.1. FW - Pare-feu
- 6.8.2. VPN - Réseaux Privés Virtuels
- 6.8.3. IDS - Système de Détection d'Intrusion

6.9. Systèmes de contrôle d'accès au réseau
- 6.9.1. NAC
- 6.9.2. Architecture et éléments
- 6.9.3. Fonctionnement et normalisation

6.10. Accès aux réseaux sans fil
- 6.10.1. Types de réseaux sans fil
- 6.10.2. Sécurité dans les réseaux sans fil
- 6.10.3. Attaques contre les réseaux sans fil

Module 7. Sécurité des communications et du fonctionnement des logiciels

7.1. Sécurité informatique dans les communications et l'exploitation des logiciels
- 7.1.1. Sécurité informatique
- 7.1.2. Cybersécurité
- 7.1.3. Sécurité dans le cloud

7.2. Sécurité informatique dans les communications et l'exploitation des logiciels Typologie
- 7.2.1. Sécurité physique
- 7.2.2. Sécurité logique

7.3. Sécurité des communications
- 7.3.1. Principaux éléments
- 7.3.2. Sécurité des réseaux
- 7.3.3. Meilleures pratiques

7.4. Cyber Intelligence
- 7.4.1. Ingénierie sociale
- 7.4.2. *Deep web*
- 7.4.3. *Phishing*
- 7.4.4. *Malware*

7.5. Développement sécurisé des communications et de l'exploitation des logiciels
- 7.5.1. Développement sécurisé Protocole HTTP
- 7.5.2. Développement sécurisé Cycle de vie
- 7.5.3. Développement sécurisé Sécurité de PHP
- 7.5.4. Développement sécurisé Sécurité de NET
- 7.5.5. Développement sécurisé Meilleures pratiques

7.6. Systèmes de gestion de la sécurité de l'information dans les communications
- 7.6.1. GDPR
- 7.6.2. ISO 27021
- 7.6.3. ISO 27017/18

7.7. Technologies SIEM
- 7.7.1. Technologies SIEM
- 7.7.2. Opérations SOC
- 7.7.3. SIEM *Vendors*

7.8. Le rôle de la sécurité dans les organisations
- 7.8.1. Rôles dans les organisations
- 7.8.2. Rôle des spécialistes de l'IdO dans les entreprises
- 7.8.3. Certifications reconnues sur le marché

7.9. Analyse médico-légale
- 7.9.1. Analyse médico-légale
- 7.9.2. Analyse médico-légale Méthodologie
- 7.9.3. Analyse médico-légale Outils et mise en œuvre

7.10. La cbersécurité aujourd'hui
- 7.10.1. Principales cyberattaques
- 7.10.2. Prévisions en matière d'employabilité
- 7.10.3 Défis

Module 8. La sécurité dans les environnements Cloud

8.1. La sécurité dans les environnements *Cloud Computing*
- 8.1.1. La sécurité dans les environnements *Cloud Computing*
- 8.1.2. Sécurité dans les environnements *Cloud Computing*. Menaces et risques pour la sécurité
- 8.1.3. Sécurité dans les environnements *Cloud Computing*. Aspects clés de la sécurité

8.2. Types d'infrastructures *Cloud*
- 8.2.1. Public
- 8.2.2. Privé
- 8.2.3. Hybride

8.3. Modèle de gestion partagé
- 8.3.1. Éléments de sécurité gérés par fournisseur
- 8.3.2. Éléments gérés par le client
- 8.3.3. Définition de la stratégie de sécurité

8.4. Mécanismes de prévention
- 8.4.1. Systèmes de gestion de l'authentification
- 8.4.2. Système de gestion des autorisations: politiques d'accès
- 8.4.3. Systèmes de gestion des clés

8.5. Sécurisation des systèmes
- 8.5.1. Sécurisation des systèmes de stockage
- 8.5.2. Protection de systèmes de bases de données
- 8.5.3. Sécurisation des données en transit

8.6. Protection de l'infrastructure
- 8.6.1. Conception et mise en œuvre d'un réseau sécurisé
- 8.6.2. Sécurité des ressources informatiques
- 8.6.3. Outils et ressources pour la protection des infrastructures

8.7. Détection des menaces et des attaques
- 8.7.1. Systèmes d'audit, *Logging* et de surveillance
- 8.7.2. Systèmes d'événements et d'alarmes
- 8.7.3. Systèmes SIEM

8.8. Réponse aux incidents
- 8.8.1. Plan de réponse aux incidents
- 8.8.2. Continuité des Activités
- 8.8.3. Analyse médico-légale et remédiation d'incidents de même nature

8.9. Sécurité dans les *Clouds* publics
- 8.9.1. AWS (Amazon Web Services)
- 8.9.2. Microsoft Azure
- 8.9.3. Google GCP
- 8.9.4. Oracle Cloud

8.10. Réglementation et conformité
- 8.10.1. Respect des règles de sécurité
- 8.10.2. Gestion des risques
- 8.10.3. Les personnes et les processus dans les organisations

Module 9. Sécurité des communications des dispositifs IoT

9.1. De la télémétrie à IoT
- 9.1.1. La télémétrie
- 9.1.2. Connectivité M2M
- 9.1.3. Démocratisation de la télémétrie

9.2. Modèles de référence IoT
- 9.2.1. Modèle de référence IoT
- 9.2.2. Architecture simplifiée IoT

9.3. Vulnérabilités de la sécurité IoT
- 9.3.1. Dispositifs IoT
- 9.3.2. Dispositifs IoT. Études de cas d'utilisation
- 9.3.3. Dispositifs IoT. Vulnérabilités

9.4. Connectivité IoT
- 9.4.1. Réseaux PAN, LAN, WAN
- 9.4.2. Technologies sans fil non liées à IoT
- 9.4.3. Technologies sans fil LPWAN

9.5. Technologies LPWAN
- 9.5.1. Le triangle de fer des LPWAN
- 9.5.2. Bandes de fréquences libres vs. Bandes sous licence
- 9.5.3. Options technologiques LPWAN

9.6. Technologie LoRaWAN
- 9.6.1. Technologie LoRaWAN
- 9.6.2. Cas d'utilisation LoRaWAN Éco-système
- 9.6.3. Sécurité dans LoRaWAN

9.7. Technologie Sigfox
- 9.7.1. Technologie Sigfox
- 9.7.2. Cas d'utilisation de Sigfox. Éco-système
- 9.7.3. La sécurité dans Sigfox

9.8. Technologie Cellulaire IoT
- 9.8.1. Technologie Cellulaire IoT (NB-IoT et LTE-M)
- 9.8.2. Cas d'utilisation Cellulaire IoT Éco-système
- 9.8.3. Sécurité en Cellulaire IoT

9.9. Technologie WiSUN
- 9.9.1. Technologie WiSUN
- 9.9.2. Cas d'utilisation de WiSUN Éco-système
- 9.9.3. Sécurité du WiSUN

9.10. Autres technologies IoT
- 9.10.1. Autres technologies IoT
- 9.10.2. Cas d'utilisation et écosystème des autres technologies IoT
- 9.10.3. Sécurité dans les autres technologies IoT

Module 10. Plan de continuité des activités associé à la sécurité

10.1. Plan de Continuité des Activités
- 10.1.1. Plans de Continuité des Activités (PCA)
- 10.1.2. Plan de Continuité des Activités (PCA) Aspects clés
- 10.1.3. Plan de Continuité des Activités (PCA) pour l'évaluation de l'entreprise

10.2. Mesures dans un plan de Continuité des Activités (PCA)
- 10.2.1. *Recovery Time Objective* (RTO) et *Recovery Point Objective* (RPO)
- 10.2.2. Délai Maximum Tolérable (MTD)
- 10.2.3. Niveaux Minimaux de Récupération (ROL)
- 10.2.4. Objectif de Point de Récupération (RPO)

10.3. Projets de continuité Typologie
- 10.3.1. Plan de Continuité des Activités (PCA)
- 10.3.2. Plan de continuité des TIC (PCTIC)
- 10.3.3. Plan de reprise après sinistre (PRS)

10.4. Gestion des risques associés au PCA
- 10.4.1. Analyse de l'impact sur les activités
- 10.4.2. Avantages de la mise en œuvre d'un PCA
- 10.4.3. Réflexion basée sur les risques

10.5. Cycle de vie d'un plan de Continuité des Activités
- 10.5.1. Phase 1: Analyse organisationnelle
- 10.5.2. Phase 2: Déterminer la stratégie de continuité
- 10.5.3. Phase 3: Réponse aux situations d'urgence
- 10.5.4. Phase 4: Essais, maintenance et révision

10.6. Phase d'analyse organisationnelle d'un PCA
- 10.6.1. Identification des processus entrant dans le champ d'application du PCA
- 10.6.2. Identification des domaines d'activité critiques
- 10.6.3. Identification des dépendances entre les domaines et les processus
- 10.6.4. Détermination des MTD appropriées
- 10.6.5. Produits livrables Création d'un plan

10.7. Phase de détermination de la stratégie de continuité dans un PCA
- 10.7.1. Rôles dans la phase de détermination de la stratégie
- 10.7.2. Tâches dans la phase de définition de la stratégie
- 10.7.3. Produits livrables

10.8. Phase d'intervention d'urgence d'un PCA
- 10.8.1. Rôles dans la phase de réponse
- 10.8.2. Tâches au cours de cette phase
- 10.8.3. Produits livrables

10.9. Phase de test, de maintenance et de révision d'un PCA
- 10.9.1. Rôles dans la phase de test, de maintenance et de révision
- 10.9.2. Tâches de la phase de test, de maintenance et de révision
- 10.9.3. Produits livrables

10.10. Normes ISO associées aux plans de Continuité des Activités (PCA)
- 10.10.1. ISO 22301:2019
- 10.10.2. ISO 22313:2020
- 10.10.3. Autres normes ISO et internationales connexes

Module 11. Leadership, Éthique et Responsabilité Sociale des Entreprises

11.1. Mondialisation et Gouvernance
- 11.1.1. Gouvernance et Gouvernement d'Entreprise
- 11.1.2. Principes fondamentaux de la Gouvernance d'Entreprise dans les entreprises
- 11.1.3. Le Rôle du Conseil d'Administration dans le cadre de la Gouvernance d'Entreprise

11.2. Leadership
- 11.2.1. Leadership Une approche conceptuelle
- 11.2.2. Leadership dans l'entreprise
- 11.2.3. L'importance du dirigeant dans la gestion d'entreprise

11.3. *Cross Cultural Management*
- 11.3.1. Concept de *Cross Cultural Management*
- 11.3.2. Contributions à la Connaissance des Cultures Nationales
- 11.3.3. Gestion de la Diversité

11.4. Développement de la gestion et le leadership
- 11.4.1. Concept de développement de la gestion
- 11.4.2. Le concept de Leadership
- 11.4.3. Théories du Leadership
- 11.4.4. Styles de Leadership
- 11.4.5. L'intelligence dans le Leadership
- 11.4.6. Les défis du leadership aujourd'hui

11.5. Éthique des affaires
- 11.5.1. Éthique et Morale
- 11.5.2. Éthique des Affaires
- 11.5.3. Leadership et éthique dans les affaires

11.6. Durabilité
- 11.6.1. Durabilité et développement durable
- 11.6.2. Agenda 2030
- 11.6.3. Entreprises durables

11.7. Responsabilité Sociale des Entreprises
- 11.7.1. Dimension internationale de la Responsabilité Sociale des Entreprises
- 11.7.2. Mise en œuvre de la Responsabilité Sociale des Entreprises
- 11.7.3. Impact et mesure de la Responsabilité Sociale des Entreprises

11.8. Systèmes et outils de Gestion responsables
- 11.8.1. RSC: Responsabilité sociale des entreprises
- 11.8.2. Questions clés pour la mise en œuvre d'une stratégie de gestion responsable
- 11.8.3. Étapes de la mise en œuvre d'un système de gestion de la responsabilité sociale des entreprises
- 11.8.4. Outils et normes en matière de RSE

11.9. Multinationales et droits de l'homme
- 11.9.1. Mondialisation, entreprises multinationales et droits de l'homme
- 11.9.2. Entreprises multinationales et droit international
- 11.9.3. Instruments juridiques pour les multinationales dans le domaine des droits de l'homme

11.10. Environnement juridique et *Corporate Governance*
- 11.10.1. Importation et exportation
- 11.10.2. Propriété intellectuelle et industrielle
- 11.10.3. Droit international du travail

Module 12. Gestion des Personnes et des Talents

12.1. La Direction Stratégique des personnes
- 12.1.1. Direction Stratégique et Ressources Humaines
- 12.1.2. La direction stratégique des personnes

12.2. Gestion des ressources humaines basée sur les compétences
- 12.2.1. Analyse du potentiel
- 12.2.2. Politique de rémunération
- 12.2.3. Plans de carrière/succession

12.3. Évaluation et gestion des performances
- 12.3.1. Gestion des performances
- 12.3.2. Gestion des performances: objectifs et processus

12.4. Innovation dans la gestion des talents et des personnes
- 12.4.1. Modèles de gestion stratégique des talents
- 12.4.2. Identification, formation et développement des talents
- 12.4.3. Fidélisation et rétention
- 12.4.4. Proactivité et innovation

12.5. Motivation
- 12.5.1. La nature de la motivation
- 12.5.2. La théorie de l'espérance
- 12.5.3. Théories des besoins
- 12.5.4. Motivation et compensation économique

12.6. Développer des équipes performantes
- 12.6.1. Équipes performantes: équipes autogérées
- 12.6.2. Méthodologies de gestion des équipes autogérées très performantes

12.7. Gestion du changement
- 12.7.1. Gestion du changement
- 12.7.2. Types de processus de gestion des changements
- 12.7.3. Étapes ou phases de la gestion du changement

12.8. Négociation et gestion des conflits
- 12.8.1 Négociation
- 12.8.2 Gestion des Conflits
- 12.8.3 Gestion des Crises

12.9. La communication managériale
- 12.9.1. Communication interne et externe dans l'environnement professionnel
- 12.9.2. Département de communication
- 12.9.3. Le responsable de la communication de l'entreprise. Le profil du Dircom

12.10. Productivité, attraction, rétention et activation des talents
- 12.10.1. Productivité
- 12.10.2. Leviers d'attraction et de rétention des talents

Module 13. Gestion Économique et Financière

13.1. Environnement Économique
- 13.1.1. Environnement macroéconomique et système financier
- 13.1.2. Institutions financières
- 13.1.3. Marchés financiers
- 13.1.4. Actifs financiers
- 13.1.5. Autres entités du secteur financier

13.2. Comptabilité de Gestion
- 13.2.1. Concepts de base
- 13.2.2. Les Actifs de l'entreprise
- 13.2.3. Le Passif de l'entreprise
- 13.2.4. La Valeur Nette de l'entreprise
- 13.2.5. Le Compte de Résultat

13.3. Systèmes d'information et*business intelligence*
- 13.3.1. Principes fondamentaux et classification
- 13.3.2. Phases et méthodes de répartition des coûts
- 13.3.3. Choix du centre de coûts et de l'effet

13.4. Budget et Contrôle de Gestion
- 13.4.1. Le modèle budgétaire
- 13.4.2. Budget d'Investissement
- 13.4.3. Le Budget de Fonctionnement
- 13.4.5. Le Budget de Trésorerie
- 13.4.6. Le Suivi Budgétaire

13.5. Direction Financière
- 13.5.1. Les décisions financières de l'entreprise
- 13.5.2. Département financier
- 13.5.3. Les excédents de trésorerie
- 13.5.4. Les risques liés à la gestion financière
- 13.5.5. Gestion des risques liés à la gestion financière

13.6. Planification Financière
- 13.6.1. Définition de la planification financière
- 13.6.2. Mesures à prendre dans le cadre de la planification financière
- 13.6.3. Création et mise en place de la stratégie d'entreprise
- 13.6.4. Le schéma *Cash Flow*
- 13.6.5. Le tableau des fonds de roulement

13.7. Stratégie Financière de l'Entreprise
- 13.7.1. Stratégie de l'entreprise et sources de financement
- 13.7.2. Produits de financement des entreprises

13.8. Financement Stratégique
- 13.8.1. Autofinancement
- 13.8.2. Augmentation des fonds propres
- 13.8.3. Ressources Hybrides
- 13.8.4. Financement par des intermédiaires

13.9. Analyse et planification financières
- 13.9.1. Analyse du Bilan
- 13.9.2. Analyse du Compte de Résultat
- 13.9.3. Analyse de la Rentabilité

13.10. Analyses et résolution de problèmes
- 13.10.1. Informations financières de Industria de Diseño y Textil, S.A. (INDITEX)

Module 14. Direction d'Entreprise et Marketing Stratégique

14.1. Gestion commerciale
- 14.1.1. Cadre conceptuel de la gestion commerciale
- 14.1.2. Stratégie et planification commerciales
- 14.1.3. Le rôle des responsables commerciaux

14.2. Marketing
- 14.2.1. Concept de Marketing
- 14.2.2. Éléments de base du marketing
- 14.2.3. Activités de Marketing de l'entreprise

14.3. Gestion Stratégique du Marketing
- 14.3.1. Concept de Marketing stratégique
- 14.3.2. Concept de planification stratégique du marketing
- 14.3.3. Les étapes du processus de planification stratégique du marketing

14.4. Marketing digital et e-commerce
- 14.4.1. Objectifs du Marketing numérique et du commerce électronique
- 14.4.2. Marketing Numérique et médias utilisés
- 14.4.3. Commerce électronique Contexte général
- 14.4.4. Catégories de commerce électronique
- 14.4.5. Avantages et inconvénients *d'E-commerce* par rapport au commerce traditionnel

14.5. Marketing digital pour renforcer la marque
- 14.5.1. Stratégies en ligne pour améliorer la réputation de votre marque
- 14.5.2. *Branded Content* & *Storytelling*

14.6. Marketing digital pour attirer et fidéliser les clients
- 14.6.1. Stratégies de fidélisation et de liaison par Internet
- 14.6.2. *Visitor Relationship Management*
- 14.6.3. Hyper-segmentation

14.7. Gestion des campagnes numériques
- 14.7.1. Qu'est-ce qu'une campagne de publicité numérique?
- 14.7.2. Étapes du lancement d'une campagne de marketing en ligne
- 14.7.3. Erreurs dans les campagnes de publicité numérique

14.8. Stratégie de vente
- 14.8.1. Stratégie de vente
- 14.8.2. Méthodes de vente

14.9. Communication d'Entreprise
- 14.9.1. Concept
- 14.9.2. Importance de la communication dans l'organisation
- 14.9.3. Type de communication dans l'organisation
- 14.9.4. Fonctions de la communication dans l'organisation
- 14.9.5. Éléments de communication
- 14.9.6. Problèmes de communication
- 14.9.7. Scénarios de communication

14.10. Communication et réputation numérique
- 14.10.1. Réputation en ligne
- 14.10.2. Comment mesurer la réputation numérique?
- 14.10.3. Outils de réputation en ligne
- 14.10.4. Rapport sur la réputation en ligne
- 14.10.5. *Branding* online

Module 15. *Management* Exécutif

15.1. General Management
- 15.1.1. Concept General Management
- 15.1.2. L'action du Directeur Général
- 15.1.3. Le Directeur Général et ses fonctions
- 15.1.4. Transformation du travail de la Direction

15.2. Le manager et ses fonctions. La culture organisationnelle et ses approches
- 15.2.1. Le manager et ses fonctions. La culture organisationnelle et ses approches

15.3. Direction des opérations
- 15.3.1. Importance de la gestion
- 15.3.2. La chaîne de valeur
- 15.3.3. Gestion de qualité

15.4. Discours et formation de porte-parole
- 15.4.1. Communication interpersonnelle
- 15.4.2. Compétences communicatives et l'influence
- 15.4.3. Obstacles à la communication

15.5. Outils de communication personnels et organisationnels
- 15.5.1. Communication interpersonnelle
- 15.5.2. Outils de communication interpersonnelle
- 15.5.3. La communication dans l'organisation
- 15.5.4. Outils dans l'organisation

15.6. La communication en situation de crise
- 15.6.1. Crise
- 15.6.2. Phases de la crise
- 15.6.3. Messages: contenu et calendrier

15.7. Préparer un plan de crise
- 15.7.1. Analyse des problèmes potentiels
- 15.7.2. Planification
- 15.7.3. Adéquation du personnel

15.8. Intelligence émotionnelle
- 15.8.1. Intelligence émotionnelle et communication
- 15.8.2. Affirmation, empathie et écoute active
- 15.8.3. Estime de soi et communication émotionnelle

15.9. *Branding* Personnel
- 15.9.1. Stratégies pour développer le personal branding
- 15.9.2. Les lois de l'image de marque personnelle
- 15.9.3. Outils de construction du personal branding

15.10. Leadership et gestion d'équipes
- 15.10.1. Leadership et styles de leadership
- 15.10.2. Capacités et défis des Leaders
- 15.10.3. Gestion des Processus de Changement
- 15.10.4. Gestion d'Équipes Multiculturelles

Le meilleur corps enseignant et un système d'enseignement innovant, combinés au programme le plus complet et le plus récent: voilà une excellente occasion de progresser en tant qu'informaticien"

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

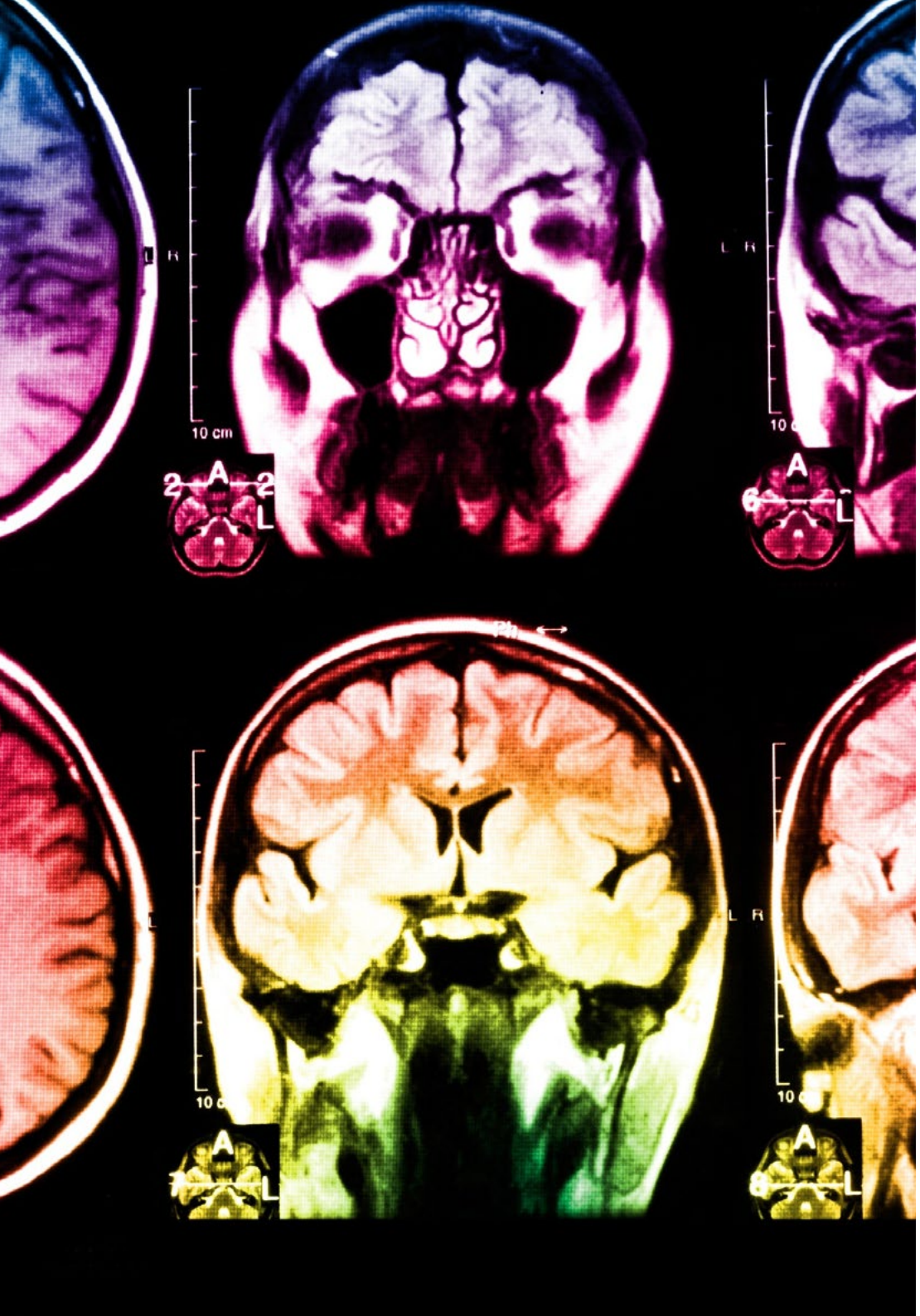
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

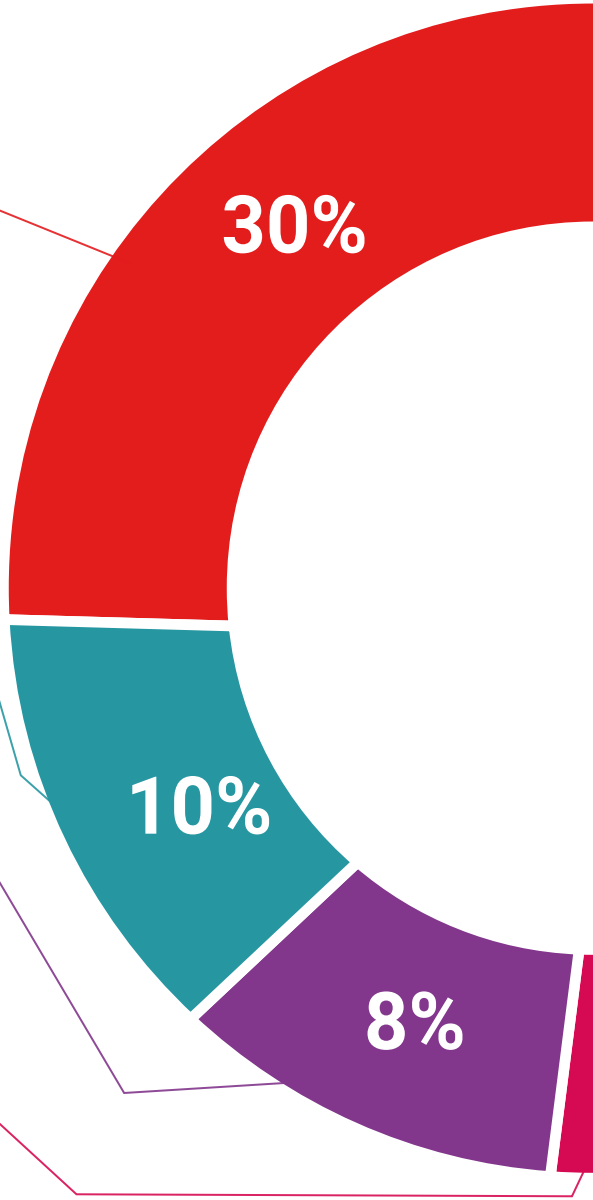
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

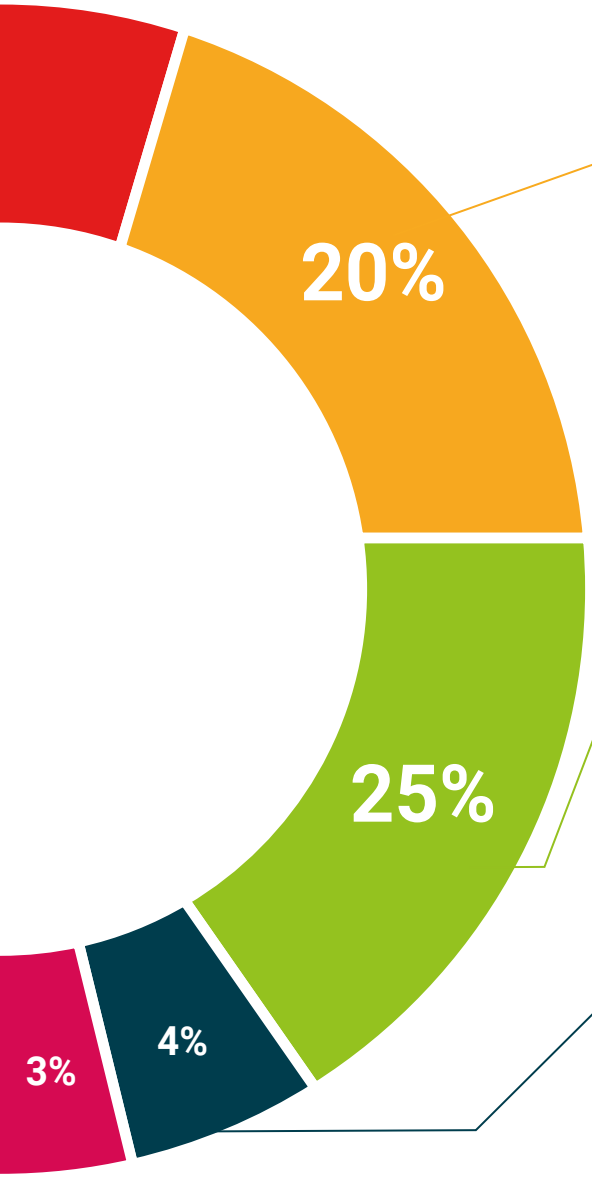
Pratiques en compétences et aptitudes

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 Spécialisé en MBA en Direction de la Cybersécurité Avancée (CISO) garantit, outre la formation la plus rigoureuse et la plus actualisée, l'accès à un diplôme de Mastère Spécialisé délivré par TECH Université Technologique.

Terminez ce programme avec succès et recevez votre diplôme sans avoir à vous soucier des déplacements ou des formalités administratives”

Ce **Mastère Spécialisé en MBA en Direction de la Cybersécurité Avancée (CISO)** contient le programme le plus complet et le plus actualisé du marché.

Après avoir passé l'évaluation, l'étudiant recevra par courrier* avec accusé de réception son diplôme de **Mastère Spécialisé** délivrée par **TECH Université Technologique.**

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

Diplôme: **Mastère Spécialisé en MBA en Direction de la Cybersécurité Avancée (CISO)**

Modalité: **en ligne**

Durée: **12 mois**

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 SPÉCIALISÉ

en

MBA en Direction de la Cybersécurité Avancée (CISO)

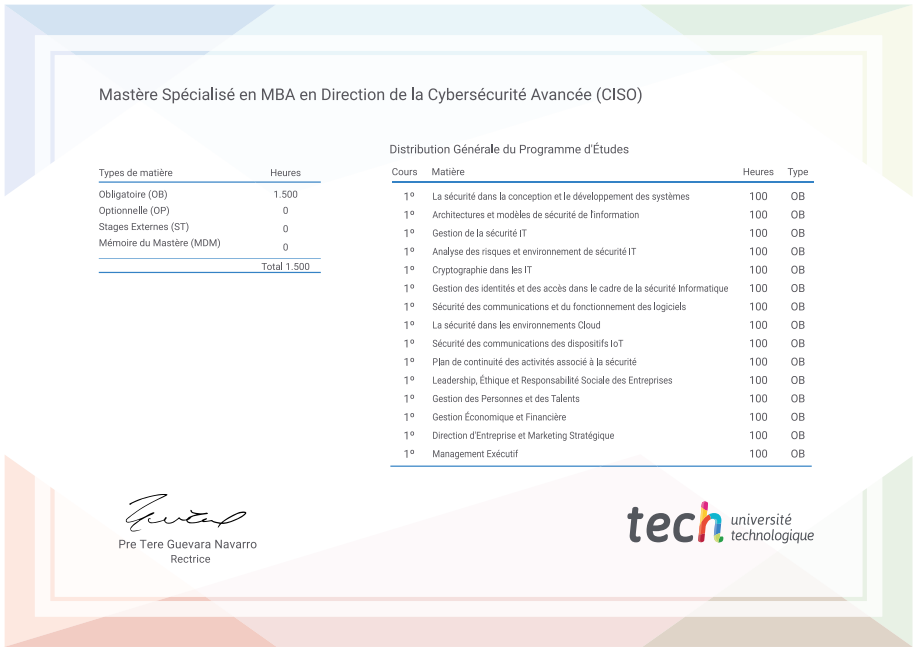
Il s'agit d'un diplôme spécialisé octroyé par cette Université d'une durée de 1.500 heures, débutant le dd/mm/aaaa et finalisant le dd/mm/aaaa.

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 Spécialisé en MBA en Direction de la Cybersécurité Avancée (CISO)

Types de matière	Heures
Obligatoire (OB)	1.500
Optionnelle (OP)	0
Stages Externes (ST)	0
Mémoire du Mastère (MDM)	0
	Total 1.500

Distribution Générale du Programme d'Études

Cours	Matière	Heures	Type
1º	La sécurité dans la conception et le développement des systèmes	100	OB
1º	Architectures et modèles de sécurité de l'information	100	OB
1º	Gestion de la sécurité IT	100	OB
1º	Analyse des risques et environnement de sécurité IT	100	OB
1º	Cryptographie dans les IT	100	OB
1º	Gestion des identités et des accès dans le cadre de la sécurité Informatique	100	OB
1º	Sécurité des communications et du fonctionnement des logiciels	100	OB
1º	La sécurité dans les environnements Cloud	100	OB
1º	Sécurité des communications des dispositifs IoT	100	OB
1º	Plan de continuité des activités associé à la sécurité	100	OB
1º	Leadership, Éthique et Responsabilité Sociale des Entreprises	100	OB
1º	Gestion des Personnes et des Talents	100	OB
1º	Gestion Économique et Financière	100	OB
1º	Direction d'Entreprise et Marketing Stratégique	100	OB
1º	Management Exécutif	100	OB

Pre Tere Guevara Navarro
Rectrice

tech université technologique

*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 Spécialisé
MBA en Direction de la Cybersécurité Avancée (CISO)

- Modalité: **en ligne**
- Durée: **12 mois**
- Qualification: **TECH Université Technologique**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Mastère Spécialisé

MBA en Direction de la Cybersécurité Avancée (CISO)

tech université technologique