Mastère Spécialisé

MBA en Direction de la Cybersécurité (CISO, Responsable de la Sécurité de l'Information)

MBADCCISO

tech université technologique

tech université technologique

Mastère Spécialisé
MBA en Direction de la Cybersécurité (CISO, Responsable de la Sécurité de l'Information)

- 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/ecole-de-commerce/master/master-mba-direction-cybersecurite-ciso-responsable-securite-information**

Sommaire

01

Présentation

La société d'aujourd'hui est hyperconnectée. L'ère de l'information permet aux citoyens de prendre connaissance de n'importe quelle donnée en cliquant sur un bouton. Les entreprises sont donc plus que jamais exposées au risque de recevoir des *logiciels* malveillants susceptibles de nuire à leur production et à leur sécurité, voire d'exposer les données personnelles de leurs clients et de leurs employés, et de mettre en évidence leurs faiblesses informatiques. Bien que la protection dans ce domaine soit l'affaire des spécialistes de l'informatique, de plus en plus des *chief revenue officers*, et d'autres responsables décident de se spécialiser dans ce domaine afin d'essayer d'arrêter les cybercriminels et d'éviter d'être la cible de leurs attaques. C'est pourquoi TECH a créé ce programme, dans lequel les professionnels trouveront les informations les plus pertinentes du moment, grâce à un programme didactique facile à comprendre pour les étudiants. Ainsi, et grâce aux connaissances acquises, le diplômé pourra travailler en toute réussite en tant que Chief Information Security Office, un poste en plein essor et avec de grandes perspectives de croissance.

Mastère Spécialisé en MBA en Direction de la Cybersécurité (CISO, Responsable de la Sécurité de l'Information)
TECH Université Technologique

Améliorez vos compétences en matière de la Direction de la Cybersécurité grâce à 10 Masterclasses animées par un spécialiste de renommée internationale"

02

Pourquoi étudier à TECH?

TECH est la plus grande école de commerce 100% en ligne au monde. Il s'agit d'une École de Commerce d'élite, avec un modèle de normes académiques des plus élevées. Un centre international de formation à la haute performance et aux techniques de gestion intensive.

TECH est une université à la pointe de la technologie, qui met toutes ses ressources à la disposition de l'étudiant pour l'aider à réussir dans son entreprise"

À TECH Université Technologique

Innovation

L'université propose un modèle d'apprentissage en ligne qui associe les dernières technologies éducatives à la plus grande rigueur pédagogique. Une méthode unique, bénéficiant de la plus haute reconnaissance internationale, qui fournira aux étudiants les clés pour évoluer dans un monde en constante évolution, où l'innovation doit être l'engagement essentiel de tout entrepreneur.

« Histoire de Succès Microsoft Europe » pour avoir incorporé un système multi-vidéo interactif innovant dans les programmes.

Exigence maximale

Le critère d'admission de TECH n'est pas économique. Vous n'avez pas besoin de faire un gros investissement pour étudier avec nous. Cependant, pour obtenir un diplôme de TECH, les limites de l'intelligence et des capacités de l'étudiant seront testées. Les normes académiques de cette institution sont très élevées...

95 % | **des étudiants de TECH finalisent leurs études avec succès**

Networking

Chez TECH, des professionnels du monde entier participent, de sorte que les étudiants pourront créer un vaste réseau de contacts qui leur sera utile pour leur avenir.

+100 000 **dirigeants formés chaque année**

+200 **nationalités différentes**

Empowerment

L'étudiant évoluera main dans la main avec les meilleures entreprises et des professionnels de grand prestige et de grande influence. TECH a développé des alliances stratégiques et un précieux réseau de contacts avec les principaux acteurs économiques des 7 continents.

+500 | **accords de collaboration avec les meilleures entreprises**

Talent

Ce programme est une proposition unique visant à faire ressortir le talent de l'étudiant dans le domaine des affaires. C'est l'occasion de mettre en avant leurs intérêts et leur vision de l'entreprise.

TECH aide les étudiants à montrer leur talent au monde entier à la fin de ce programme.

Contexte Multiculturel

En étudiant à TECH, les étudiants bénéficieront d'une expérience unique. Vous étudierez dans un contexte multiculturel. Dans un programme à vision globale, grâce auquel vous apprendrez à connaître la façon de travailler dans différentes parties du monde, en recueillant les dernières informations qui conviennent le mieux à votre idée d'entreprise.

Les étudiants TECH sont issus de plus de 200 nationalités.

Apprenez avec les meilleurs

L'équipe d'enseignants de TECH explique en classe ce qui les a conduits au succès dans leurs entreprises, en travaillant dans un contexte réel, vivant et dynamique. Des enseignants qui s'engagent pleinement à offrir une spécialisation de qualité permettant aux étudiants de progresser dans leur carrière et de se distinguer dans le monde des affaires.

Des professeurs de 20 nationalités différentes.

Chez TECH, vous aurez accès aux études de cas les plus rigoureuses et les plus récentes du monde académique"

TECH recherche l'excellence et, à cette fin, elle possède une série de caractéristiques qui en font une université unique:

Analyse

TECH explore la pensée critique, le questionnement, la résolution de problèmes et les compétences interpersonnelles des étudiants.

Excellence académique

TECH offre aux étudiants la meilleure méthodologie d'apprentissage en ligne. L'université combine la méthode *Relearning* (la méthode d'apprentissage de troisième cycle la plus reconnue au niveau international) avec l'Étude de Cas. Entre tradition et innovation dans un équilibre subtil et dans le cadre d'un parcours académique des plus exigeants.

Économie d'échelle

TECH est la plus grande université en ligne du monde. Elle possède un portefeuille de plus de 10 000 diplômes de troisième cycle. Et dans la nouvelle économie, **volume + technologie = prix de rupture**. De cette manière, elle garantit que les études ne sont pas aussi coûteuses que dans une autre université.

03

Pourquoi notre programme?

Suivre le programme TECH, c'est multiplier ses chances de réussite professionnelle dans le domaine de la gestion supérieure des entreprises.

C'est un défi qui requiert des efforts et du dévouement, mais qui vous offre la possibilité d'un avenir prometteur. Les étudiants apprendront auprès du meilleur personnel enseignant et avec la méthodologie éducative la plus flexible et la plus innovante.

Nous disposons du corps enseignant le plus prestigieux et du programme le plus complet du marché, ce qui nous permet de vous offrir une formation du plus haut niveau académique"

Ce programme apportera une multitude d'avantages aussi bien professionnels que personnels, dont les suivants:

01

Donner un coup de pouce définitif à la carrière des étudiants

En étudiant à TECH, les étudiants seront en mesure de prendre en main leur avenir et de développer tout leur potentiel. À l'issue de ce programme, ils acquerront les compétences nécessaires pour opérer un changement positif dans leur carrière en peu de temps.

70% des participants à cette spécialisation réalisent un changement positif dans leur carrière en moins de 2 ans.

02

Vous acquerrez une vision stratégique et globale de l'entreprise

TECH offre un aperçu approfondi de la gestion générale afin de comprendre comment chaque décision affecte les différents domaines fonctionnels de l'entreprise.

Notre vision globale de l'entreprise améliorera votre vision stratégique.

03

Consolidation des étudiants en gestion supérieure des affaires

Étudier à TECH, c'est ouvrir les portes d'un panorama professionnel de grande importance pour que les étudiants puissent se positionner comme des managers de haut niveau, avec une vision large de l'environnement international.

Vous travaillerez sur plus de 100 cas réels de cadres supérieurs.

04

Vous obtiendrez de nouvelles responsabilités

Au cours du programme, les dernières tendances, évolutions et stratégies sont présentées, afin que les étudiants puissent mener à bien leur travail professionnel dans un environnement en mutation.

À l'issue de cette formation, 45% des étudiants obtiennent une promotion professionnelle au sein de leur entreprise.

05

Accès à un puissant réseau de contacts

TECH met ses étudiants en réseau afin de maximiser les opportunités. Des étudiants ayant les mêmes préoccupations et le même désir d'évoluer. Ainsi, les partenaires, les clients ou les fournisseurs peuvent être partagés.

Vous y trouverez un réseau de contacts essentiel pour votre développement professionnel.

06

Développer des projets d'entreprise de manière rigoureuse

Les étudiants acquerront une vision stratégique approfondie qui les aidera à élaborer leur propre projet, en tenant compte des différents domaines de l'entreprise.

20 % de nos étudiants développent leur propre idée entrepreneuriale.

07

Améliorer les *soft skills* et les compétences de gestion

TECH aide les étudiants à appliquer et à développer les connaissances acquises et à améliorer leurs compétences interpersonnelles pour devenir des leaders qui font la différence.

Améliorez vos compétences en communication ainsi que dans le domaine du leadership pour booster votre carrière professionnelle.

08

Vous ferez partie d'une communauté exclusive

L'étudiant fera partie d'une communauté de managers d'élite, de grandes entreprises, d'institutions renommées et de professeurs qualifiés issus des universités les plus prestigieuses du monde : la communauté de TECH Université Technologique

Nous vous donnons la possibilité de vous spécialiser auprès d'une équipe de professeurs de renommée internationale.

04

Objectifs

Ce Mastère Spécialisé de TECH Global University est conçu pour renforcer les compétences professionnelles des chefs d'entreprise hautement spécialisés dans leur domaine d'activité, et qui trouveront dans ce programme une opportunité unique de se perfectionner dans un secteur de grande importance, puisqu'ils apprendront à prévenir les éventuelles menaces Internet qui peuvent causer de graves dommages aux entreprises. Ainsi, vous deviendrez un expert professionnel dans différentes branches, ce qui vous permettra de contrôler tous les domaines de l'entreprise et de devenir Chief Information Security Officer (Responsable en Chef de la Sécurité de l'Information).

Augmentez votre formation et atteignez vos objectifs professionnels grâce à la formation supérieure offerte par TECH avec ce Mastère Spécialisé"

TECH considère les objectifs de ses étudiants comme les siens
Ils collaborent pour les atteindre

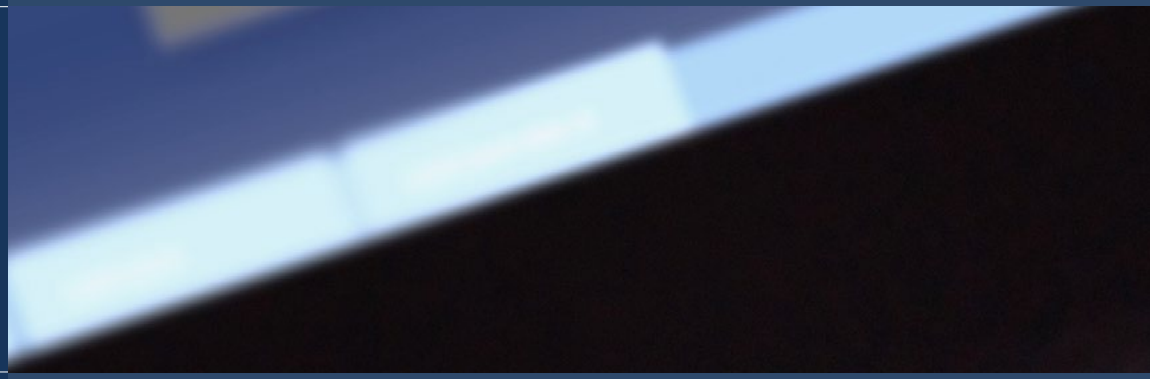
Le **Mastère Spécialisé en MBA en Direction de la Cybersécurité (CISO, Responsable de la Sécurité de l'Information)** permettra à l'étudiant de:

01 Analyser le rôle de l'analyste en cybersécurité

02 Approfondir l'ingénierie sociale et ses méthodes

03 Examiner les méthodologies OSINT, HUMINT, OWASP, PTEC OSSTM, OWISAM

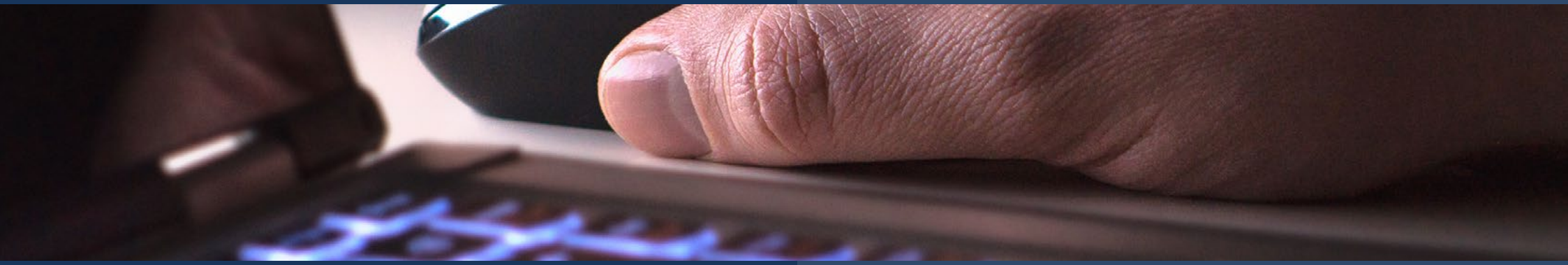
04 Effectuer une analyse des risques et comprendre les mesures de risques



05 Déterminer l'utilisation appropriée de l'anonymisation et l'utilisation de réseaux tels que TOR, I2P et Freenet

06 Générer des connaissances spécialisées pour la réalisation d'un audit de sécurité

08 Examiner les Systèmes de détection et de prévention des menaces les plus importantes



07 Développer des politiques d'utilisation appropriées

09 Évaluation des nouveaux systèmes de détection des menaces et de leur évolution par rapport aux solutions plus traditionnelles

10 Analyser les principales plateformes mobiles actuelles, leurs caractéristiques et leur utilisation

11 Identifier, analyser et évaluer les risques de sécurité des parties du projet IoT

12 Évaluer les informations obtenues et développer des mécanismes de prévention et hacking

13 Appliquer l'ingénierie inverse à l'environnement de la Cyber-sécurité

14 Spécifier les tests à effectuer sur le software développé

15 Rassembler toutes les preuves et données existantes pour réaliser un rapport médico-légal

16 Présenter correctement le rapport médico-légal

17 Analyser l'état actuel et futur de la sécurité informatique

18 Examiner les risques des nouvelles technologies émergentes

19 Compiler les différentes technologies en relation avec la sécurité informatique

05

Compétences

Le Mastère Spécialisé en MBA en Direction de la Cybersécurité (CISO, Responsable de la Sécurité de l'Information) a été conçu pour développer les compétences des professionnels du monde des affaires. Ainsi, à l'issue du programme, le professionnel aura acquis les compétences nécessaires à une pratique de qualité actualisée et basée sur la méthodologie d'enseignement la plus innovante. Un programme qui, sans aucun doute, améliorera la formation et permettra aux managers d'être plus compétitifs dans leur pratique quotidienne, en unifiant tous les aspects pertinents de la sécurité informatique qu'ils doivent connaître et mettre en pratique.

Entrez dans l'étude de la sécurité informatique et améliorez vos compétences pour contrôler les menaces potentielles du réseau"

01 Connaître les méthodologies utilisées en matière de cyber-sécurité

02 Évaluer chaque type de menace afin d'offrir une solution optimale dans chaque cas

03 Générer des solutions intelligentes complètes pour automatiser les comportements d'incidents

04 Évaluer les risques associés aux vulnérabilités, tant à l'intérieur qu'à l'extérieur de l'entreprise

05 Comprendre l'évolution et l'impact de l'IdO au fil du temps

06 Démontrer qu'un système est vulnérable, l'attaquer de manière proactive et résoudre ces problèmes

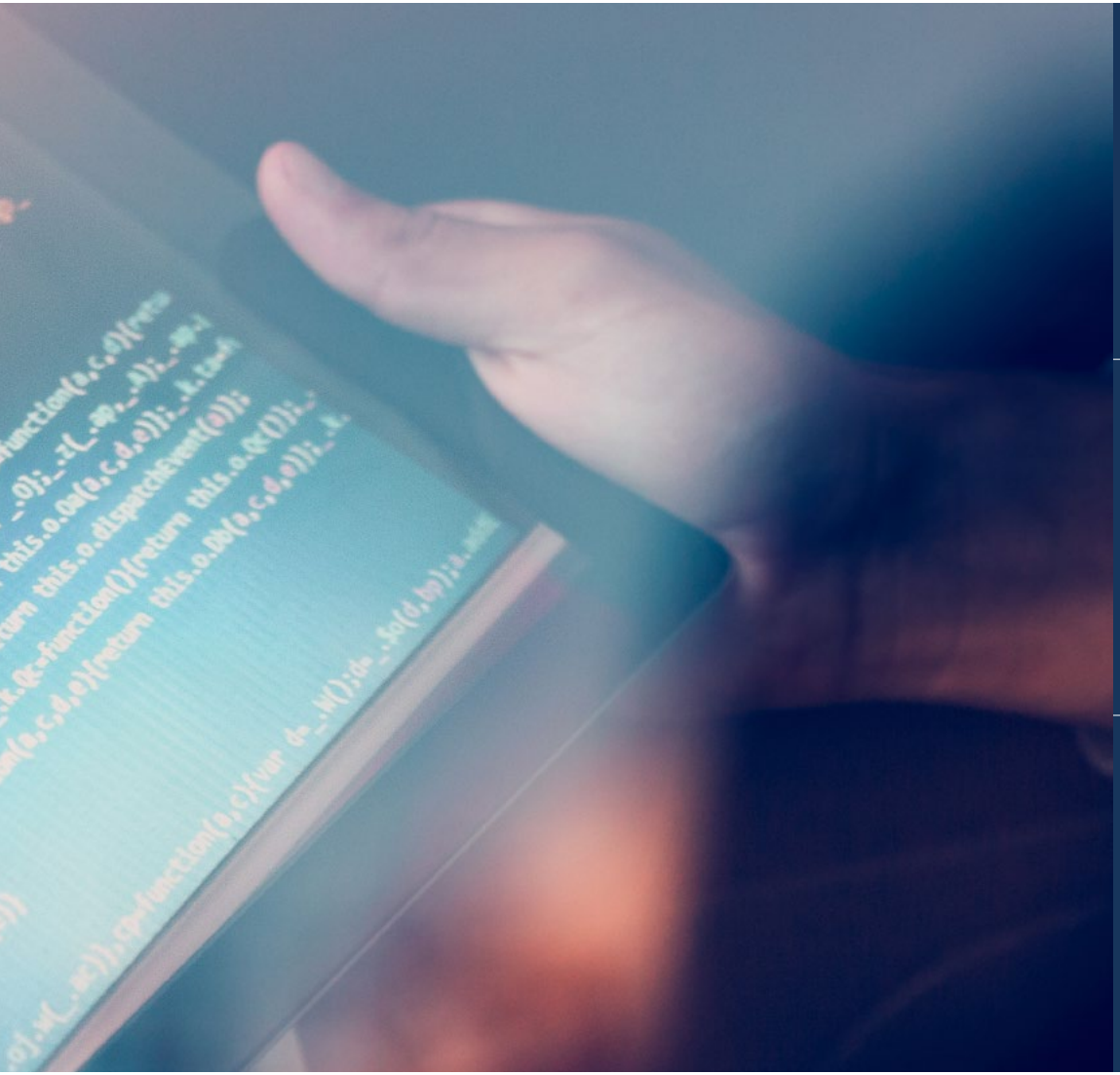
07 Savoir comment appliquer le sandboxing dans différents environnements

08 Connaître les directives qu'un bon développeur doit suivre afin de répondre aux exigences de sécurité nécessaires

09 Réaliser des opérations de sécurité défensive

10 Avoir une perception approfondie et spécialisée de la sécurité informatique

11 Appliquer les processus de sécurité pour les smartphones et les appareils portables



12 Connaître les moyens de réaliser un *Hacking* éthique et protéger une entreprise d'une cyberattaque

13 Être capable d'enquêter sur un incident de cybersécurité

14 Différencier les techniques d'attaque et de défense existantes

06

Structure et contenu

Ce programme TECH a été conçu pour répondre aux besoins de spécialisation des professionnels du monde des affaires qui souhaitent élargir leurs connaissances en matière de sécurité informatique, un domaine fondamental pour pouvoir contrôler les menaces potentielles qui pourraient représenter un grand risque pour l'entreprise. Ainsi, le MBA leur permettra d'acquérir des connaissances spécifiques qu'ils pourront appliquer à leur pratique professionnelle. Et, pour ce faire, ils utiliseront une méthodologie entièrement en ligne qui leur permettra de combiner leurs études avec le reste de leurs obligations quotidiennes.

Ce programme sera essentiel pour détecter d'éventuelles cyber-attaques dans votre entreprise"

Plan d'études

Le MBA en Direction de la Cybersécurité (CISO, Responsable de la Sécurité de l'Information) de TECH Global University est un programme intensif conçu pour promouvoir le développement de compétences managériales qui permettent une prise de décision plus rigoureuse dans des environnements incertains.

Au cours de 2 700 heures d'études, l'étudiant acquerra les compétences nécessaires pour évoluer avec succès dans sa pratique quotidienne. Il s'agit donc d'une véritable immersion dans des situations professionnelles réelles.

Ce programme aborde en profondeur différents domaines de l'entreprise et est conçu pour permettre aux cadres de comprendre la cybersécurité d'un point de vue stratégique, international et innovant.

Un plan conçu spécialement pour les étudiants, axé sur leur perfectionnement professionnel et qui les prépare à atteindre l'excellence dans le domaine de la gestion de la sécurité informatique. Un programme qui comprend vos besoins et ceux de votre entreprise grâce à un contenu innovant basé sur les dernières tendances et soutenu par la meilleure méthodologie éducative et un corps professoral exceptionnel.

À tout cela, il faut ajouter 10 Masterclasses exclusives qui font partie du matériel didactique, à la pointe de la technologie et de l'éducation. Ces leçons ont été conçues par un spécialiste de renommée internationale dans le domaine de l'Intelligence, de la Cybersécurité et des Technologies de Rupture. Des ressources utiles qui aideront le professionnel exécutif à se spécialiser dans la Direction de la Cybersécurité et à gérer efficacement les départements de son entreprise consacrés à ce domaine important.

Ce programme se déroule sur une période de 12 mois et se divise en 15 modules:

Module 1	Cyber intelligence et cybersécurité
Module 2	Sécurité en Host
Module 3	Sécurité des réseaux (périmètre)
Module 4	La sécurité sur les *smartphones*
Module 5	Sécurité IoT
Module 6	*Hacking* éthique
Module 7	Ingénierie inverse
Module 8	Développement sécurisé
Module 9	Analyse médico-légale
Module 10	Défis actuels et futurs en matière de sécurité informatique
Module 11	Leadership, Éthique et Responsabilité Sociale des Entreprises
Module 12	*Gestion des Personnes et des Talents*
Module 13	*Gestion Économique et Financière*
Module 14	*Direction d'Entreprise et Marketing Stratégique*
Module 15	*Management* Exécutif

Où, quand et comment cela se déroule?

TECH offre la possibilité ses étudiants aux de développer ce programme de manière totalement en ligne. Pendant les 12 mois de la formation, pourrez accéder à tous les contenus de ce programme à tout moment, ce qui leur permettra d'auto gérer leur temps d'étude.

Une expérience éducative unique, clé et décisive pour stimuler votre développement professionnel.

Module 1. Cyber intelligence et cybersécurité

1.1. Cyber Intelligence

1.1.1. Cyber Intelligence
- 1.1.1.1. Intelligence
  - 1.1.1.1.1. Cycle de l'intelligence
- 1.1.1.2. Cyber Intelligence
- 1.1.1.3. Cyber intelligence et cybersécurité

1.1.2. L'analyste de l'intelligence
- 1.1.2.1. Le rôle de l'analyste du renseignement
- 1.1.2.2. Biais de l'analyste du renseignement dans l'activité d'évaluation

1.2. Cybersécurité

1.2.1. Couches de sécurité

1.2.2. Identification des cybermenaces
- 1.2.2.1. Menaces extérieures
- 1.2.2.2. Menaces internes

1.2.3. Actions défavorables
- 1.2.3.1. Ingénierie sociale
- 1.2.3.2. Méthodes de communément utilisées

1.3. Techniques et outils des intelligences

1.3.1. OSINT
1.3.2. SOCMINT
1.3.3. HUMIT
1.3.4. Distributions et outils Linux
1.3.5. OWISAM
1.3.6. OWISAP
1.3.7. PTES
1.3.8. OSSTM

1.4. Méthodologie d'évaluation

1.4.1. L'analyse de Intelligence
1.4.2. Techniques d'organisation des informations acquises
1.4.3. Fiabilité et crédibilité des sources d'information
1.4.4. Méthodologie d'analyse
1.4.5. Présentation les résultats de l'Intelligence

1.5. Audits et documentation

1.5.1. Audit de la sécurité informatique
1.5.2. Documentation et autorisations pour l'audit
1.5.3. Types d'audits
1.5.4. Produits livrables
- 1.5.4.1. Rapport technique
- 1.5.4.2. rapport exécutif

1.6. Détection sur le web

1.6.1. Utilisation de l'anonymat
1.6.2. Techniques d'anonymat (Proxy, VPN)
1.6.3. Réseaux TOR, Freenet et IP2

1.7. Menaces et types de sécurité

1.7.1. Types de menaces
1.7.2. Sécurité physique
1.7.3. Sécurité des réseaux
1.7.4. Sécurité logique
1.7.5. Sécurité sur les applications web
1.7.6. Sécurité des appareils mobiles

1.8. Réglementation et *compliance*

1.8.1. Le RGPD
1.8.2. Famille ISO 27000
1.8.3. Cadre de cybersécurité du NIST
1.8.4. PIC
1.8.5. ISO 27032
1.8.6. Réglementation *du Cloud*
1.8.7. SOX
1.8.8. PCI

1.9. Analyse et mesure des risques

1.9.1. Portée des risques
1.9.2. Les actifs
1.9.3. Menaces
1.9.4. Vulnérabilités
1.9.5. Évaluation des risques
1.9.6. Traitement des risques

1.10. Organismes importants en matière de cybersécurité

1.10.1. NIST
1.10.2. ENISA
1.10.4. OEA
1.10.5. UNASUR-PROSUR

Module 2. Sécurité en *Host*

2.1. Copies de sauvegarde
2.1.1. Stratégies de sauvegarde
2.1.2. Outils pour Windows
2.1.3. Outils pour Linux
2.1.4. Outils pour MacOS

2.2. Antivirus utilisateur
2.2.1. Types d'antivirus
2.2.2. Antivirus pour Windows
2.2.3. Antivirus pour Linux
2.2.4. Antivirus pour MacOS
2.2.5. Antivirus pour smartphones

2.3. Détecteurs d'intrusion-HIDS
2.3.1. Méthodes de détection des intrusions
2.3.2. Sagan
2.3.3. Aide
2.3.4. *Rkhunter*

2.4. *Firewall* local
2.4.1. *Firewalls* pour Windows
2.4.2. *Firewalls* pour Linux
2.4.3. *Firewalls* pour MacOS

2.5. Gestionnaires de mots de passe
2.5.1. Mot de passe
2.5.2. LastPass
2.5.3. KeePass
2.5.4. StickyPassword
2.5.5. RoboForm

2.6. Détecteurs pour *phishing*
2.6.1. Détection manuelle du *phishing*
2.6.2. Outils *antiphishing*

2.7. *Spyware*
2.7.1. Mécanismes d'évitement
2.7.2. Outils *antispyware*

2.8. Trackers
2.8.1. Mesures de protection du système
2.8.2. Outils anti-pistage

2.9. *EDR- End point Detection and Response*
2.9.1. Comportement du système EDR
2.9.2. Différences entre EDR et Antivirus
2.9.3. L'avenir des systèmes EDR

2.10. Contrôle de l'installation des software
2.10.1. Dépôts et magasins de logiciels
2.10.2. Listes des logiciels autorisés ou interdits
2.10.3. Critères de mise à jour
2.10.4. Privilèges d'installation des logiciels

Module 3. Sécurité des réseaux (périmètre)

3.1. Systèmes de détection et de prévention des menaces
3.1.1. Cadre général des incidents de sécurité
3.1.2. Les systèmes de défense actuels: *Defense in Depth* et SOC
3.1.3. Architectures de réseau actuelles
3.1.4. Types d'outils de détection et de prévention des incidents
3.1.4.1. Systèmes en réseau
3.1.4.2. Systèmes basés sur Host
3.1.4.3. Systèmes centralisés
3.1.5. Communication et découverte d'instances/ Hosts, conteneurs et Serverless

3.2. *Firewall*
3.2.1. Types de *firewalls*
3.2.2. Attaques et atténuation
3.2.3. *Firewalls* courants du *kernel* Linux
3.2.3.1. UFW
3.2.3.2. *Nftables et iptables*
3.2.3.3. Firewalls
3.2.4. Systèmes de détection basés sur les journaux du système
3.2.4.1. TCP Wrappers
3.2.4.2. BlockHosts et DenyHosts
3.2.4.3. Fai2ban

3.3. Systèmes de détection et de prévention des intrusions (IDS/IPS)
3.3.1. Attaques sur les IDS/IPS
3.3.2. Systèmes d' IDS/IPS
3.3.2.1. Snort
3.3.2.2. Suricata

3.4. *Firewalls* de nouvelle génération (NGFW)
3.4.1. Différences entre les MGFW et les *firewall* traditionnels
3.4.2. Principales capacités
3.4.3. Solutions commerciales
3.4.4. *Firewalls* pour les services en *cloud*
3.4.4.1. Architecture VPC en Cloud
3.4.4.2. ACLs du Cloud
3.4.4.3. Security Group

3.5. *Proxy*
3.5.1. Types de *proxy*
3.5.2. Utilisation du *proxy*. Avantages et inconvénients

3.6. Moteurs antivirus
3.6.1. Contexte général des *malwares* et IOCs
3.6.2. Problèmes de moteur antivirus

3.7. Systèmes de protection du courrier
3.7.1. Antispam
3.7.1.1. Liste blanche et liste noire
3.7.1.2. Filtres bayésiens
3.7.2. Mail Gateway (MGW)

3.8. SIEM
3.8.1. Composants et architecture
3.8.2. Règles de corrélation et cas d'utilisation
3.8.3. Les défis actuels des systèmes SIEM

3.9. SOAR
3.9.1. SOAR et SIEM: ennemis ou alliés
3.9.2. L'avenir des systèmes SOAR

3.10. Autres systèmes en réseau
3.10.1. WAF
3.10.2. NAC
3.10.3. *HoneyPots* y *HoneyNets*
3.10.4. CASB

Module 4. La sécurité sur les *smartphones*

4.1. Le monde de l'appareil mobile
4.1.1. Types de plateformes mobiles
4.1.2. Dispositifs Ios
4.1.3. Dispositifs Android

4.2. Gestion de la sécurité mobile
4.2.1. Projet de sécurité mobile de l'OWASP
4.2.1.1. Les 10 principales vulnérabilités
4.2.2. Communications, réseaux et modes de connexion

4.3. Le dispositif mobile dans l'environnement professionnel
4.3.1. Risques
4.3.2. Surveillance des dispositifs
4.3.4. Gestion des dispositifs mobiles (MDM)

4.4. Vie privée des utilisateurs et sécurité des données
4.4.1. États d'information
4.4.2. Stockage sécurisé des données
4.4.3.1. Stockage sécurisé sur iOS
4.4.3.2. Stockage sécurisé sur Android
4.4.3. Bonnes pratiques en matière de développement d'applications

4.5. Vulnérabilités et vecteurs d'attaque
4.5.1. Vulnérabilités
4.5.2. Vecteurs d'attaque
4.5.2.1. *Malware*
4.5.2.2. Exfiltration de données
4.5.2.3. Manipulation des données

4.6. Principales menaces
4.6.1. Utilisateur non forcé
4.6.2. *Malware*
4.6.2.1. Types de malware
4.6.3. Ingénierie sociale
4.6.4. Fuite de données
4.6.5. Vol d'informations
4.6.6. Réseaux Wi-Fi non sécurisés
4.6.7. Software obsolètes
4.6.8. Applications malveillantes
4.6.9. Mots de passe non sécurisés
4.6.10. Paramètres de sécurité faibles ou inexistants
4.6.11. Accès physique
4.6.12. Perte ou vol de l'appareil
4.6.13. Vol d'identité (intégrité)
4.6.14. Cryptographie faible ou brisée
4.6.15. Déni de service (DoS)

4.7. Attaques majeures
4.7.1. Attaques de *phishing*
4.7.2. Attaques liées aux modes de communication
4.7.3. Attaques de *smishing*
4.7.4. Attaques de *criptojacking*
4.7.5. *Man in The Middle*

4.8. *Hacking*
4.8.1. *Rooting* et *Jailbreaking*
4.8.2. Anatomie d'une attaque mobile
4.8.2.1. Propagation de la menace
4.8.2.2. Installation d'un malware sur l'appareil
4.8.2.3. Persistance
4.8.2.4. Exécution du *payload* et extraction de l'information
4.8.3. *Hacking* des appareils iOS: mécanismes et outils
4.8.4. *Hacking* des appareils Android: mécanismes et outils

4.9. Tests de pénétration
4.9.1. iOS *PenTesting*
4.9.2. Android *PenTesting*
4.9.3. Outils

4.10. Sûreté et sécurité
4.10.1. Paramètres de sécurité
4.10.1.1. Sur les appareils iOS
4.10.1.2. Sur les appareils Android
4.10.2. Mesures de sécurité
4.10.3. Outils de protection

Module 5. Sécurité IoT

5.1. Dispositifs
5.1.1. Types de dispositifs
5.1.2. Architectures standardisées
5.1.2.1. ONEM2M
5.1.2.2. IoTWF
5.1.3. Protocoles d'application
5.1.4. Technologies de la connectivité

5.2. Dispositifs IoT. Domaines d'application
5.2.1. *SmartHome*
5.2.2. *SmartCity*
5.2.3. Transports
5.2.4. *Wearables*
5.2.5. Secteur de la santé
5.2.6. IioT

5.3. Protocoles de communication
5.3.1. MQTT
5.3.2. LWM2M
5.3.3. OMA-DM
5.3.4. TR-069

5.4. *SmartHome*
5.4.1. Domotique
5.4.2. Réseaux
5.4.3. Appareils ménagers
5.4.4. Surveillance et sécurité

5.5. *SmartCity*
5.5.1. Éclairage
5.5.2. Météorologie
5.5.3. Sécurité

5.6. Transports
5.6.1. Localisation
5.6.2. Effectuer des paiements et obtenir des services
5.6.3. Connectivité

5.7. *Wearables*
5.7.1. Vêtements intelligents
5.7.2. Bijoux intelligents
5.7.3. Montres intelligentes

5.8. Secteur de la santé
5.8.1. Surveillance de l'exercice et de la fréquence cardiaque
5.8.2. Surveillance des patients et des personnes âgées
5.8.3. Implantable
5.8.4. Robots chirurgicaux

5.9. Connectivité
5.9.1. Wi-Fi/Gateway
5.9.2. Bluetooth
5.9.3. Connectivité embarquée

5.10. Titrisation
5.10.1. Réseaux dédiés
5.10.2. Gestionnaire de mots de passe
5.10.3. Utilisation de protocoles cryptés
5.10.4. Conseils d'utilisation

Module 6. *Piratage* éthique

6.1. Environnement de travail
6.1.1. Distributions Linux
6.1.1.1. Kali Linux - Offensive Security
6.1.1.2. Parrot OS
6.1.1.3. Ubuntu
6.1.2. Systèmes de virtualisation
6.1.3. *Sandbox*
6.1.4. Déploiement des laboratoires

6.2. Méthodologie
6.2.1. OSSTM
6.2.2. OWASP
6.2.3. NIST
6.2.4. PTES
6.2.5. ISSAF

6.3. *Footprinting*
6.3.1. Renseignement de source ouverte (OSINT)
6.3.2. Recherche de violations de données et de vulnérabilité
6.3.3. Utilisation d'outils passif

6.4. Analyse du réseau
6.4.1. Outils d'analyse
6.4.1.1. Nmap
6.4.1.2. Hping3
6.4.1.3. Autres outils d'analyse
6.4.2. Techniques de balayage
6.4.3. Techniques de contournement des *Firewall* et IDS
6.4.4. *Banner Grabbing*
6.4.5. Diagrammes de réseau

6.5. Énumération
6.5.1. Énumération SMTP
6.5.2. Énumération DNS
6.5.3. Énumération de NetBIOS et de samba
6.5.4. Énumération LDAP
6.5.5. Énumération SNMP
6.5.6. Autres techniques d'énumération

6.6. Analyse des vulnérabilités
6.6.1. Solutions d'analyse des vulnérabilités
6.6.1.1. Qualys
6.6.1.2. Nessus
6.6.1.3. Nessus
6.6.2. Systèmes d'évaluation des vulnérabilités
6.6.2.1. CVSS
6.6.2.2. CVE
6.6.2.3. NVD

6.7. Attaques contre les réseaux sans fil
6.7.1. Méthodologie de *hacking* des réseaux sans fil
6.7.1.1. Wi-Fi *Discovery*
6.7.1.2. Analyse du trafic
6.7.1.3. Attaques d' *Aircrack*
6.7.1.3.1. Attaques WEP
6.7.1.3.2. Attaques WPA/WPA2
6.7.1.4. Les attaques de *Evil Twin*
6.7.1.5. Attaques sur le WPS
6.7.1.6. *Jamming*
6.7.2. Outils pour la sécurité sans fil

6.8. Piratage de serveurs web
6.8.1. *Cross Site Scripting*
6.8.2. CSRF
6.8.3. *Session Hijacking*
6.8.4. *SQLinjection*

6.9. Exploitation des vulnérabilités
6.9.1. Utilisation *exploits* connus
6.9.2. Utilisation des *metasploit*
6.9.3. Utilisation des *Malware*
6.9.3.1. Définition et champ d'application
6.9.3.2. Génération de malware
6.9.3.3. Bypass des solutions anti-virus

6.10. Persistance
6.10.1. Installation de *rootkits*
6.10.2. Utilisation de ncat
6.10.3. Utilisation de tâches planifiées pour les *backdoors*
6.10.4. Création d'utilisateurs
6.10.5. Détection HIDS

Module 7. Ingénierie inverse

7.1. Compilateurs
7.1.1. Types de code
7.1.2. Les phases d'un compilateur
7.1.3. Table des symboles
7.1.4. Gestionnaire d'erreurs
7.1.5. Compilateur GCC

7.2. Types d'analyse de compilateur
7.2.1. Analyse lexicale
7.2.1.1. Terminologie
7.2.1.2. Composante lexicale
7.2.1.3. Analyseur Lexical LEX
7.2.2. Analyse syntaxique
7.2.2.1. Grammaires sans contexte
7.2.2.2. Types d'analyse syntaxique
7.2.2.2.1. Analyse syntaxique descendante
7.2.2.2.2. Analyse ascendante
7.2.2.3. Arbres syntaxiques et dérivations
7.2.2.4. Types d'analyseurs syntaxiques
7.2.2.4.1. Analyseurs LR(*Left To Right*)
7.2.2.4.2. Analyseurs LALR
7.2.3. Analyse sémantique
7.2.3.1. Grammaires d'attributs
7.2.3.2. S-Attributs
7.2.3.3. L-attributs

7.3. Structures de données de l'assemblage
7.3.1. Variables
7.3.2. Tableaux
7.3.3. Pointeurs
7.3.4. Structures
7.3.5. Objets

7.4. Structures du code d'assemblage
7.4.1. Structures de sélection
7.4.1.1. *If, else if, Else*
7.4.1.2. *Switch*
7.4.2. Structures d'itération
7.4.2.1. *For*
7.4.2.2. *While*
7.4.2.3. Utilisation du *Break*
7.4.3. Fonctions

7.5. Architecture Hardware x86
7.5.1. Architecture de processeur x86
7.5.2. Structures de données x86
7.5.3. Structures de code x86

7.6. Architecture hardware ARM
7.6.1. Architecture du processeur ARM
7.6.2. Structures de données ARM
7.6.3. Structures de code ARM

7.7. Analyse du code statique
7.7.1. Démonteurs
7.7.2. IDA
7.7.3. Reconstructeurs de code

7.8. Analyse dynamique du code
7.8.1. Analyse comportementale
7.8.1.1. Communications
7.8.1.2. Suivi
7.8.2. Débogueurs de code Linux
7.8.3. Débogueurs de code sous Windows

7.9. *Sandbox*
7.9.1. Architecture du *sandbox*
7.9.2. Évasion du *sandbox*
7.9.3. Techniques de détection
7.9.4. Techniques d'évasion
7.9.5. Contre-mesures
7.9.6. Sandbox sur Linux
7.9.7. Sandbox sur Windows
7.9.8. Sandbox sur MacOS
7.9.9. Sandbox sur Android

7.10. Analyse des *malware*
7.10.1. Méthodes d'analyse des *malware*
7.10.2. Techniques d'obscurcissement des *malware*
7.10.2.1. Obfuscation des exécutables
7.10.2.2. Restriction des environnements d'exécution
7.10.3. Outils d'analyse des m*alware*

Module 8. Développement sécurisé

8.1. Développement sécurisé
8.1.1. Qualité, fonctionnalité et sécurité
8.1.2. Confidentialité, intégrité et disponibilité
8.1.3. Cycle de vie du développement du *software*

8.2. Phase des exigences
8.2.1. Gestion de l'authentification
8.2.2. Contrôle des rôles et des privilèges
8.2.3. Exigences axées sur le risque
8.2.4. Approbation des privilèges

8.3. Phase d'analyse et de conception
8.3.1. Accès aux composants et administration du système
8.3.2. Pistes d'audit
8.3.3. Gestion des sessions
8.3.4. Données historiques
8.3.5. Traitement approprié des erreurs
8.3.6. Séparation des fonctions

8.4. Phase de mise en œuvre et de codification
8.4.1. Sécuriser l'environnement de développement
8.4.2. Élaboration de la documentation technique
8.4.3. Codage sécurisé
8.4.4. Communications sécurisées

8.5. Bonnes pratiques de codage sécurisé
8.5.1. Validation des données d'entrée
8.5.2. Cryptage des données de sortie
8.5.3. Style de programmation
8.5.4. Traitement du journal des modifications
8.5.5. Pratiques cryptographiques
8.5.6. Gestion des erreurs et des journaux
8.5.7. Gestion des fichiers
8.5.8. Gestion de la Mémoire
8.5.9. Standardisation et réutilisation des fonctions de sécurité

8.6. Préparation du serveur et *hardening*
8.6.1. Gestion des utilisateurs, des groupes et des rôles sur le serveur
8.6.2. Installation du logiciel
8.6.3. *Hardening* du serveur
8.6.4. Configuration robuste de l'environnement de l'application

8.7. Préparation et durcissement de la BBDD et *hardening*
8.7.1. Optimisation de la BBDD
8.7.2. Création d'un utilisateur propre pour l'application
8.7.3. Attribution les privilèges nécessaires à l'utilisateur
8.7.4. *Hardening* de la BBDD

8.8. Phase de test
8.8.1. Contrôle de la qualité des contrôles de sécurité
8.8.2. Inspection progressive du code
8.8.3. Contrôle de la gestion de la configuration
8.8.4. Tests boîte noire

8.9. Préparer la Transition vers la production
8.9.1. Effectuer le contrôle des changements
8.9.2. Effectuer la procédure de changement de production
8.9.3. Exécuter la procédure de *rollback*
8.9.4. Essais de pré-production

8.10. Phase de maintenance
8.10.1. Assurance basée sur le risque
8.10.2. Test de maintenance de la sécurité de la boîte blanche
8.10.3. Tests de maintenance de la sécurité en boîte noire

Module 9. Analyse médico-légale

9.1. Acquisition et réplication des données
9.1.1. Acquisition de données volatiles
9.1.1.1. Informations sur le système
9.1.1.2. Informations sur le réseau
9.1.1.3. Ordre de volatilité
9.1.2. Acquisition de données statiques
9.1.2.1. Création d'une image dupliquée
9.1.2.2. Préparation d'un document de chaîne de contrôle
9.1.3. Méthodes de validation des données acquises
9.1.3.1. Méthodes pour Linux
9.1.3.2. Méthodes pour Windows

9.2. Évaluation et défaite des techniques anti-forensic
9.2.1. Objectifs des technique non-légales
9.2.2. Effacement des données
9.2.2.1. Effacement des données et des fichiers
9.2.2.2. Récupération de fichiers
9.2.2.3. Récupération de partitions supprimées
9.2.3. Protection par mot de passe
9.2.4. Stéganographie
9.2.5. Effacement sécurisé des dispositifs
9.2.6. Cryptage

9.3. Analyse judiciaire des systèmes d'exploitation
9.3.1. Analyse légale de Windows
9.3.2. Analyse légale de Linux
9.3.3. Analyse légale de Mac

9.4. Analyse judiciaire des réseaux
9.4.1. Analyse du logs
9.4.2. Corrélation des données
9.4.3. Enquête sur le réseau
9.4.4. Étapes à suivre pour l'analyse criminelle du réseau

9.5. Analyse légale Web
9.5.1. Enquête sur les attaques sur Internet
9.5.2. Détection des attaques
9.5.3. Localisation de l'adresse IP

9.6. Police scientifique des bases de données
9.6.1. Analyse légale de MSSQL
9.6.2. Analyse légale de MySQL
9.6.3. Analyse légale de PostgreSQL
9.6.4. Analyse légale de MongoDB

9.7. Analyse légale en *Cloud*
9.7.1. Types de délits en *Cloud*
9.7.1.1. Le Cloud comme sujet
9.7.1.2. Le cloud comme objet
9.7.1.3. Le cloud comme outil
9.7.2. Les défis légaux du *Cloud*
9.7.3. Recherche sur les services de stockage en *Cloud*
9.7.4. Outils d'analyse légale pour le *Cloud*

9.8. Enquêtes sur les crimes par courriel
9.8.1. Systèmes de courrier
9.8.1.1. Clients de messagerie
9.8.1.2. Serveur de messagerie
9.8.1.3. Serveur SMTP
9.8.1.4. Serveur POP3
9.8.1.5. Serveur IMAP4
9.8.2. Délits de courrier
9.8.3. Message de courrier
9.8.3.1. En-têtes standard
9.8.3.2. En-têtes étendus
9.8.4. Étapes de l'enquête sur ces crimes
9.8.5. Outils d'analyse des e-mails

9.9. Analyse légale des mobiles
9.9.1. Réseaux cellulaires
9.9.1.1. Types de réseaux
9.9.1.2. Contenu du CDR
9.9.2. *Subscriber Identity Module* (SIM)
9.9.3. Acquisition logique
9.9.4. Acquisition physique
9.9.5. Acquisition du système de fichiers

9.10. Rédaction et soumission de rapports légaux
9.10.1. Aspects importants d'un rapport légal
9.10.2. Classification et types de rapports
9.10.3. Guide pour la rédaction d'un rapport
9.10.4. Présentation du rapport
9.10.4.1. Préparation préalable au témoignage
9.10.4.2. Dépôt
9.10.4.3. Traiter avec les médias

Module 10. Défis actuels et futurs en matière de sécurité informatique

10.1. Technologie de la *blockchain*
10.1.1. Domaines d'application
10.1.2. Garantie de confidentialité
10.1.3. Garantie de non-répudiation

10.2. La monnaie numérique
10.2.1. Bitcoins
10.2.2. Crypto-monnaies
10.2.3. Extraction de crypto-monnaies
10.2.4. Les systèmes pyramidaux
10.2.5. Autres crimes et problèmes potentiels

10.3. *Deepfake*
10.3.1. Impact des médias
10.3.2. Dangers pour la société
10.3.3. Mécanismes de détection

10.4. L'avenir de l'intelligence artificielle
10.4.1. Intelligence artificielle et informatique cognitive
10.4.2. Utilisations pour simplifier le service à la clientèle

10.5. Vie privée numérique
10.5.1. Valeur des données sur le réseau
10.5.2. Utilisation des données sur le réseau
10.5.3. Vie privée et gestion de l'identité numérique

10.6. Cyberconflits, cybercriminels et cyberattaques
10.6.1. Impact de la cybersécurité sur les conflits internationaux
10.6.2. Conséquences des cyberattaques sur la population générale
10.6.3. Types de cybercriminels. Mesures de protection

10.7. Télétravail
10.7.1. La révolution du télétravail pendant et après la Covid19
10.7.2. Goulets d'étranglement dans l'accès
10.7.3. Variation de la surface d'attaque
10.7.4. Besoins des travailleurs

10.8. Technologies *wireless* émergentes
10.8.1. WPA3
10.8.2. 5G
10.8.3. Ondes millimétriques
10.8.4. Tendance *Get Smart* au lieu de *Get more*

10.9. L'adressage futur dans les réseaux
10.9.1. Problèmes actuels de l'adressage IP
10.9.2. IPv6
10.9.3. IPv4+
10.9.4. Avantages d'IPv4+ par rapport à IPv4
10.9.5. Avantages d'IPv6 par rapport à IPv4

10.10. Le défi de la sensibilisation de la population à l'éducation précoce et continue
10.10.1. Stratégies gouvernementales actuelles
10.10.2. Résistance de la population à l'apprentissage
10.10.3. Des plans de formation à adopter par les entreprises

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 internationales 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 de Crise

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 marketing stratégique
14.3.3. Les étapes du processus de planification stratégique du marketing

14.4. Marketing numérique 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 numérique 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 numérique 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 d'image de Branding Personal
15.9.2. Les lois de l'image de marque personnelle
15.9.3. Outils de construction de la marque personnelle

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

Ce programme ouvrira les portes d'un nouveau monde professionnel"

07

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 le Relearning, un système qui laisse de côté l'apprentissage linéaire conventionnel au profit des systèmes d'enseignement cycliques: une façon d'apprendre qui a prouvé son énorme efficacité, notamment dans les matières dont la mémorisation est essentielle"

TECH Business School utilise l'Étude de Cas pour contextualiser 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"

Notre programme vous prépare à relever les défis commerciaux dans des environnements incertains et à faire réussir votre entreprise.

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

Une méthode d'apprentissage innovante et différente

Ce programme TECH est un parcours de formation intensif, créé de toutes pièces pour offrir aux managers des défis et des décisions commerciales au plus haut niveau, 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 commerciale la plus actuelle.

> *Vous apprendrez, par le biais d'activités collaboratives et de cas réels, la résolution de situations complexes dans des environnements professionnels réels"*

La méthode des cas est le système d'apprentissage le plus utilisé dans les meilleures écoles de commerce 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

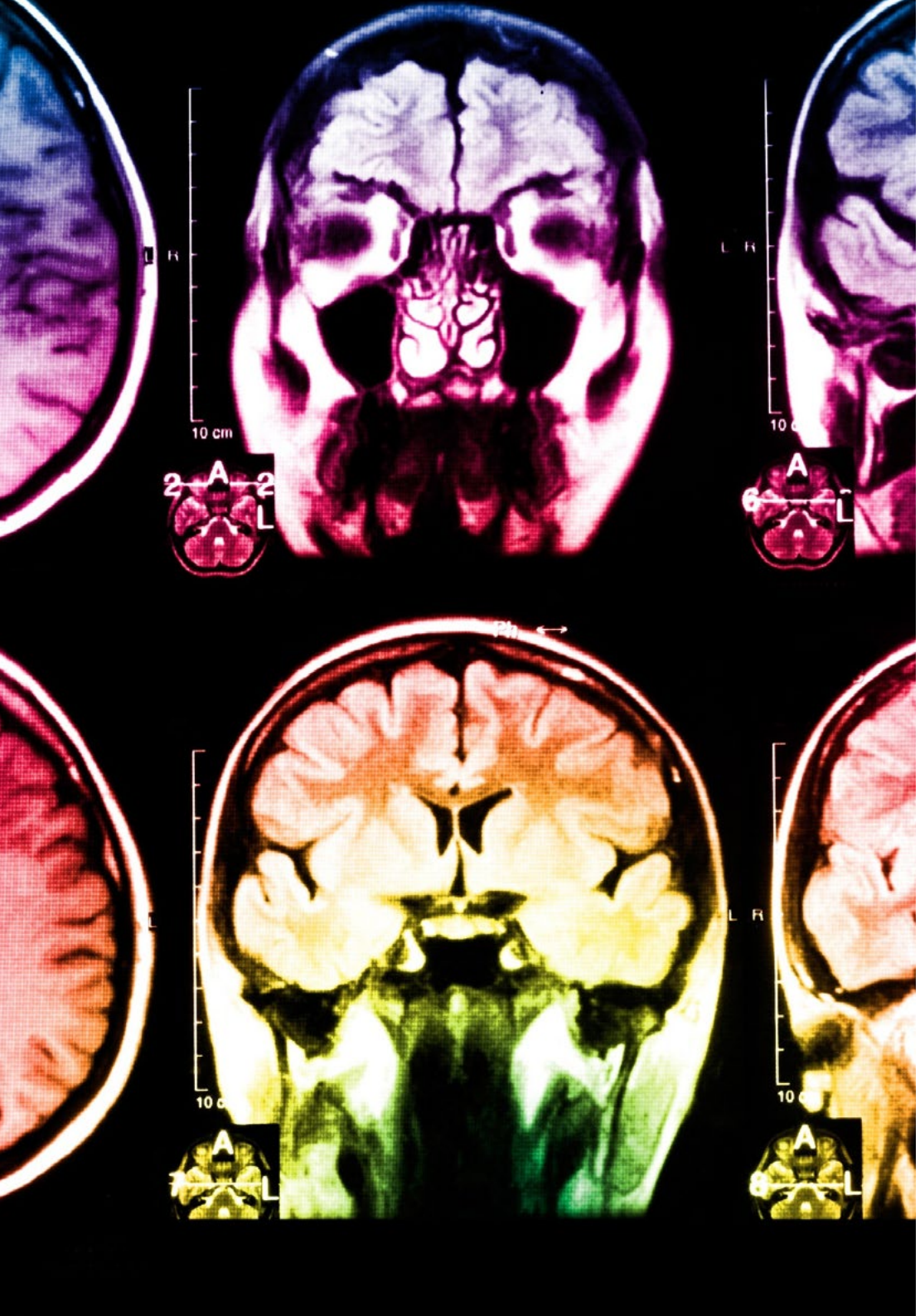
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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

> *Notre système en ligne vous permettra d'organiser votre temps et votre rythme d'apprentissage, en l'adaptant à votre emploi du temps. Vous pourrez accéder aux contenus depuis n'importe quel appareil fixe ou mobile doté d'une connexion Internet.*

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 école de commerce est la seule école autorisée à employer cette méthode fructueuse. 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). C'est pourquoi nous combinons chacun de ces éléments 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 spécialisation, en développant un esprit critique, en défendant des arguments et en contrastant les opinions: une équation directe vers le succès.

D'après les 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 de nombreux faits scientifiques prouvant l'utilité de l'observation par un tiers expert.

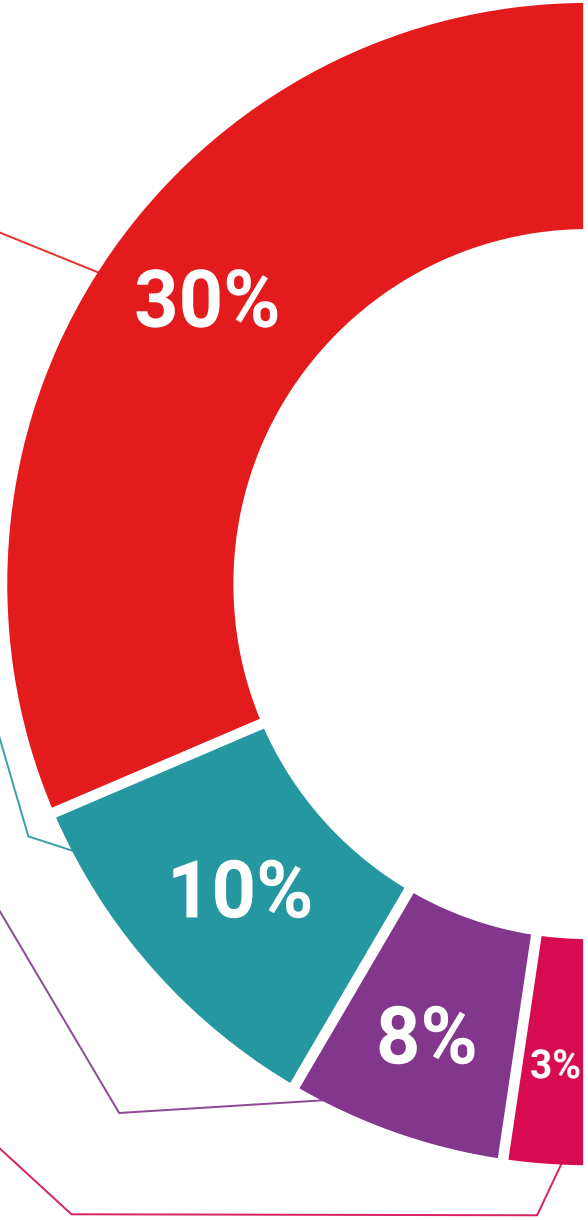
La méthode "Learning from an Expert" permet au professionnel de renforcer ses connaissances ainsi que sa mémoire, puis lui permet d'avoir davantage confiance en lui concernant la prise de décisions difficiles.

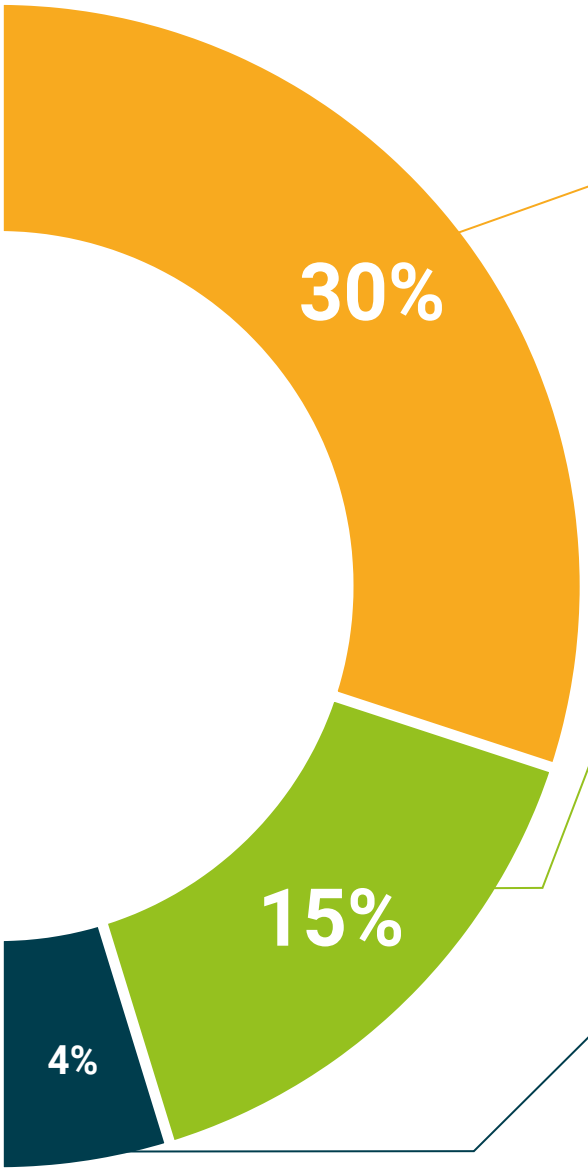
Stages en compétences de gestion

Ceux-ci mèneront des activités visant à développer des compétences de gestion spécifiques dans chaque domaine thématique. Pratiques et dynamiques pour acquérir et développer les compétences et les capacités dont un cadre supérieur a besoin dans le contexte de la mondialisation dans lequel 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 direction d'entreprise sur 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 évaluées et réévaluées périodiquement tout au long du programme, par des activités et des exercices d'évaluation et d'auto-évaluation, afin que l'étudiant puisse vérifier comment il atteint ses objectifs.

08

Profil de nos étudiants

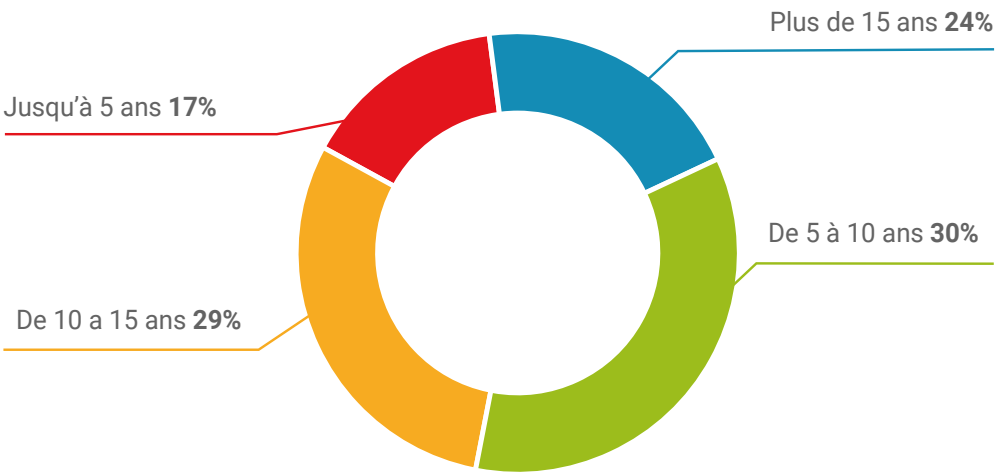
Le Mastère Spécialisé en MBA en Direction de la Cybersécurité (CISO, Responsable de la Sécurité de l'Information) est un programme destiné aux professionnels qui souhaitent améliorer leurs compétences grâce à un enseignement de qualité. Les étudiants qui souhaitent approfondir leurs connaissances dans une autre branche liée à l'entreprise, comme l'informatique, mais plus particulièrement la sécurité informatique. Un programme destiné aux professionnels expérimentés, et qui croient en la spécialisation de haut niveau comme méthode d'amélioration personnelle et professionnelle.

TECH sont des professionnels avec une grande expérience qui cherchent un meilleur emploi"

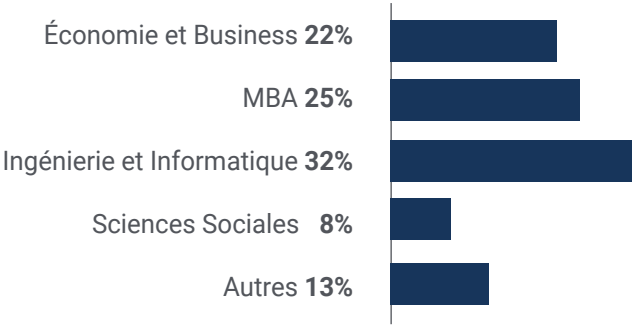
Âge moyen

Entre **35** et **45** ans

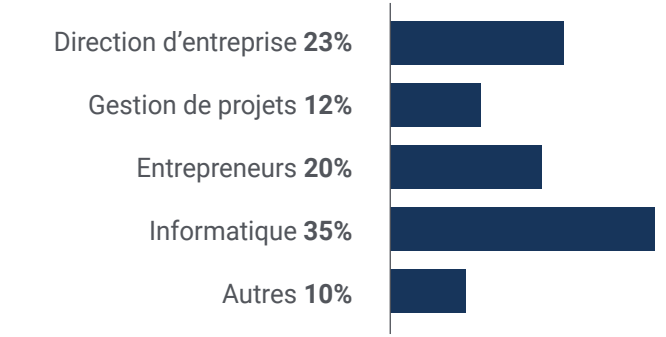
Années d'expérience



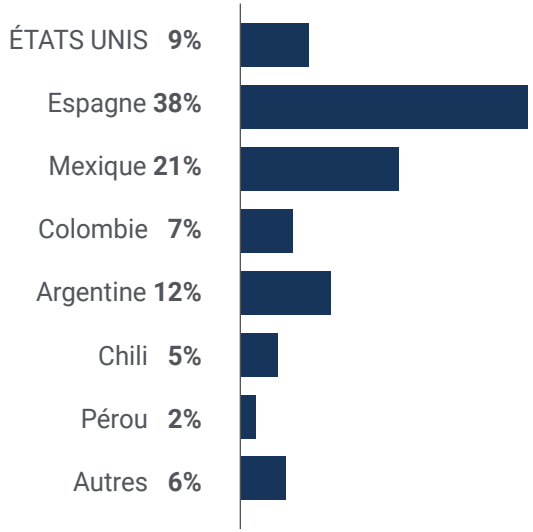
Formation



Profil académique



Distribution géographique



Jaime Díaz

Chief Revenue Officer

"Dans l'environnement professionnel dans lequel je travaille, nous manipulons beaucoup d'informations confidentielles et de données pertinentes qui, entre de mauvaises mains, peuvent créer un gros problème pour l'entreprise. C'est pourquoi j'envisageais depuis un certain temps d'approfondir mes connaissances en matière de cybersécurité, dans le but de contrôler moi-même tous les processus qui pourraient être plus sensibles à une menace informatique. Grâce à ce programme de TECH, j'ai pu améliorer ma formation et agir de manière plus sûre dans mon travail"

09

Direction de la formation

Les enseignants de ce MBA en Direction de la Cybersécurité (CISO, Responsable de la Sécurité de l'Information) sont des professionnels ayant une grande expérience du secteur, tant sur le plan professionnel que pédagogique. Leur spécialisation dans ce domaine leur permet de disposer des qualifications nécessaires pour offrir aux étudiants une étude complète et de qualité sur des sujets, qui leur seront utiles dans leur travail quotidien dans le monde des affaires. Ce sont des professionnels et experts qui misent sur l'enseignement supérieur comme moyen de faire progresser leur profession et d'améliorer la compétitivité de leur entreprise.

Un corps enseignant expérimenté pour soutenir votre spécialisation en cybersécurité"

Directeur Invité International

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

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

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

Dr Lemieux, Frederic

- Directeur du Master en Gestion des Risques de Cybersécurité à Georgetown, Washington, États-Unis
- Directeur du Master en Gestion des Technologies, Université de Georgetown
- Directeur du Master en Intelligence Appliquée à l'Université de Georgetown
- Professeur de Stage à l'Université de Georgetown
- Doctorat en Criminologie de l'École de Criminologie de l'Université de Montréal
- Licence en Sociologie, Mineure en Psychologie, Université de Laval
- Membre du "New Program Roundtable Committee", Université de Georgetown

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

Directeur invité international

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 Media, 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

TECH dispose d'un groupe distingué et spécialisé de Directeurs Internationaux Invités, avec des rôles de leadership importants dans les entreprises les plus avant-gardistes du marché mondial"

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 technologie**. 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 niveau 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 p**ublicités 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"

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

Mme Fernández Sapena, Sonia

- Formatrice en Sécurité Informatique et Piratage Ethique au Centre National de Référence pour l'Informatique et les Télécommunications à Getafe, Madrid
- Formatrice Agréée E-Council
- Formatrice dans les certifications suivantes: EXIN Ethical Hacking Foundation et EXIN Cyber & IT Security Foundation Madrid
- Formatrice Spécialisée accréditée par le CAM pour les Certificats Professionnels suivants: Sécurité Informatique (IFCT0190), Gestion des Réseaux de Voix et de Données (IFCM0310), Administration des Réseaux Départementaux (IFCT0410), Gestion des Alarmes de Réseaux de Télécommunications (IFCM0410), Opérateur de Réseaux de Voix et Données (IFCM0110), et Administration des Services Internet (IFCT0509)
- Collaboratrice Externe CSO/SSA (*Chief Security Officer/Senior Security Architect*) à l'Université des Iles Baléares
- Ingénierie Informatique, Université d'Alcalá de Henares de Madrid
- Master en DevOps: Docker and Kubernetes Cas-Training
- Microsoft Azure Security Techonologies E-Council

Professeurs

M. Catalá Barba, José Francisco

- Technicien en Électronique Expert en Cybersécurité
- Développeur d'Applications Mobiles
- Technicien en Électronique au Service de Commandement Intermédiaire du Ministère de la Défense Espagnol
- Technicien en Électronique à l'usine Ford Sita, à Valence

M. Jiménez Ramos, Álvaro

- Analyste en cybersécurité
- Analyste Principal de la Sécurité à The Workshop
- Analyste en cybersécurité L1 chez Axians
- Analyste en cybersécurité L2 chez Axians
- Analyste en cybersécurité chez SACYR S.A
- Diplôme d'ingénieur en télématique de l'université polytechnique de Madrid.
- Master en cybersécurité et Hacking éthique par le CICE
- Cours avancé en cybersécurité par Deusto Formación

Mme Marcos Sbarbaro, Victoria Alicia

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

M. Peralta Alonso, Jon

- Consultant Senior - Protection des Données et Cybersécurité
- Avocat / Conseiller Juridique chez Arriaga Associés Assessorat Juridique et Economique S.L
- Conseiller Juridique / Stagiaire dans un Cabinet Professionnel: Oscar Padura
- Licence en Droit de l'Université Publique du Pays Basque
- Master en Protection des Données Délégué de l'EIS Innovative School
- Master en Droit de l'Université Publique du Pays Basque
- Master Spécialisé en Pratique du Contentieux Civil de l'Université Internationale Isabel I de Castille
- Professeur du Master en Protection des Données Personnelles, Cybersécurité et Droit des TIC

M. Redondo, Jesús Serrano

- Développeur web et technicien en cybersécurité
- Développeur Web chez Roams, Palencia
- Développeur *FrontEnd* chez Telefónica, Madrid
- Développeur *FrontEnd* chez Best Pro Consulting SL, Madrid
- Installateur d'Équipements et de Services de Télécommunications à Grupo Zener, Castille et Léon
- Installateur d'Équipements et de Services de Télécommunications chez Lican Comunicaciones SL, Castille et Léon
- Certificat en Sécurité informatique, CFTIC Getafe, Madrid
- Technicien Supérieur en Télécommunications et Systèmes Informatiques par l'IES Trinité Arroyo, Palencia
- Technicien Supérieur en Installations Electrotechniques MT et BT, Lycée Trinité Arroyo, Palencia
- Formation en Rétro-Ingénierie, Sténographie et Cryptage par Incibe Hacker Academy

TECH a soigneusement sélectionné l'équipe enseignante de ce programme afin que vous puissiez apprendre des meilleurs spécialistes d'aujourd'hui"

10

Impact sur votre carrière

L'obtention de ce MBA en Direction de la Cybersécurité (CISO, Responsable de la Sécurité de l'Information) ajoutera un plus à la qualification des professionnels de l'entreprise, en offrant toutes ces connaissances qui, bien qu'elles puissent sembler totalement éloignées de leur travail quotidien, peuvent être très utiles pour contrôler ces processus informatiques qui peuvent abriter un élément externe nuisible qui affecte l'ensemble de l'organisation. C'est pourquoi une spécialisation plus poussée dans ce domaine est essentielle, tant pour le niveau personnel et professionnel des étudiants que pour les entreprises dans lesquelles ils travaillent.

TECH met toutes ses ressources académiques à la disposition de ses étudiants afin qu'ils acquièrent les compétences nécessaires qui les mèneront au succès"

L'obtention de ce MBA permettra aux étudiants d'acquérir la compétitivité nécessaire pour réaliser un changement pertinent dans leur carrière.

Êtes-vous prêt à faire le grand saut? Vous allez booster votre carrière professionnelle.

Le MBA en Direction de la Cybersécurité (CISO, Responsable de la Sécurité de l'Information) de TECH Global University est un programme intensif et de grande valeur visant à améliorer les compétences professionnelles des étudiants dans un domaine de compétence très large. C'est sans aucun doute une occasion unique de s'améliorer sur le plan professionnel, mais aussi sur le plan personnel, car cela implique des efforts et du dévouement.

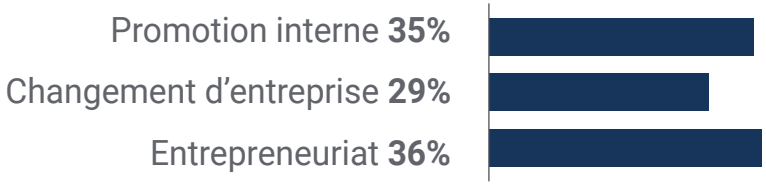
Les étudiants qui souhaitent s'améliorer, réaliser un changement positif au niveau professionnel et interagir avec les meilleurs, trouveront leur place à TECH.

Un programme d'un haut niveau académique pour mener votre carrière vers le succès.

Heure du changement

Pendant le programme	Pendant la première année	Deux ans après
35%	**30%**	**35%**

Type de changement



Amélioration salariale

La réalisation de ce programme se traduit par une augmentation de salaire de plus de **25,22%** pour nos stagiaires

Salaire précédent	Augmentation du salaire de	Salaire suivant
57.900 $	**25,22%**	**72.500 $**

11

Bénéfices pour votre entreprise

Le MBA en Direction de la Cybersécurité (CISO, Responsable de la Sécurité de l'Information) permet d'élever le talent de l'organisation à son plein potentiel en spécialisant les leaders de haut niveau. Ainsi, les professionnels pourront apporter une qualité supplémentaire à leur entreprise en disposant des compétences nécessaires pour contrôler eux-mêmes les processus de cybersécurité. Un programme qui s'adapte aux étudiants pour qu'ils acquièrent les outils nécessaires qu'ils pourront ensuite appliquer dans leur pratique quotidienne, avec de grands avantages pour leur entreprise.

Un programme indispensable pour les professionnels qui veulent surveiller et gérer les problèmes potentiels de cybersécurité"

Développer et retenir les talents dans les entreprises est le meilleur investissement à long terme.

01

Accroître les talents et le capital intellectuel

Le professionnel apportera à l'entreprise de nouveaux concepts, stratégies et perspectives susceptibles d'entraîner des changements importants dans l'organisation.

02

Conserver les cadres à haut potentiel et éviter la fuite des talents

Ce programme renforce le lien entre l'entreprise et le professionnel et ouvre de nouvelles perspectives d'évolution professionnelle au sein de l'entreprise.

03

Former des agents du changement

Vous serez en mesure de prendre des décisions en période d'incertitude et de crise, en aidant l'organisation à surmonter les obstacles.

04

Des possibilités accrues d'expansion internationale

Grâce à ce programme, l'entreprise entrera en contact avec les principaux marchés de l'économie mondiale.

05

Développement de projets propres

Le professionnel peut travailler sur un projet réel, ou développer de nouveaux projets, dans le domaine de la R+D ou le Business Development de son entreprise.

06

Accroître la compétitivité

Ce programme permettra à exiger de leurs professionnels d'acquérir les compétences nécessaires pour relever de nouveaux défis et pour faire progresser l'organisation.

12

Diplôme

Le Mastère Spécialisé en MBA en Direction de la Cybersécurité (CISO, Responsable de la Sécurité de l'Information) 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 (CISO, Responsable de la Sécurité de l'Information)** 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 (CISO, Responsable de la Sécurité de l'Information)**

Modalité: **en ligne**

Durée: **12 mois**


tech université technologique

Délivre le présent

DIPLÔME

à

Mme/M. _____, avec n° d'identification _____

Pour avoir finalisé et accrédité avec succès le programme de

MASTÈRE SPÉCIALISÉ

en

MBA en Direction de la Cybersécurité
(CISO, Responsable de la Sécurité de l'Information)

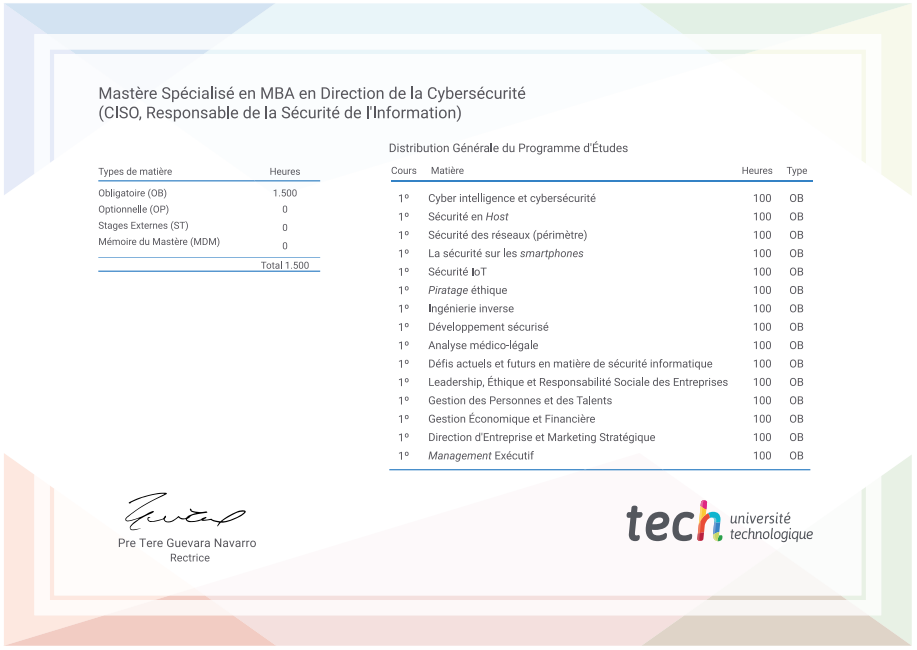
Il s'agit d'un diplôme spécialisé octroyé par cette Université d'une durée de 1.500 heures, débutant le dd/mm/aaaa et finalisant le dd/mm/aaaa.

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
(CISO, Responsable de la Sécurité de l'Information)

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
1°	Cyber intelligence et cybersécurité	100	OB
1°	Sécurité en *Host*	100	OB
1°	Sécurité des réseaux (périmètre)	100	OB
1°	La sécurité sur les *smartphones*	100	OB
1°	Sécurité IoT	100	OB
1°	*Piratage* éthique	100	OB
1°	Ingénierie inverse	100	OB
1°	Développement sécurisé	100	OB
1°	Analyse médico-légale	100	OB
1°	Défis actuels et futurs en matière de sécurité informatique	100	OB
1°	Leadership, Éthique et Responsabilité Sociale des Entreprises	100	OB
1°	Gestion des Personnes et des Talents	100	OB
1°	Gestion Économique et Financière	100	OB
1°	Direction d'Entreprise et Marketing Stratégique	100	OB
1°	*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 (CISO, Responsable de la Sécurité de l'Information)

- 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 (CISO, Responsable de la Sécurité de l'Information)

tech université technologique