# Mastère Spécialisé

## Gestion des Politiques de Cybersécurité dans l'Entreprise

MGPCE

tech université technologique

tech université technologique

# Mastère Spécialisé

## Gestion des Politiques de Cybersécurité dans l'Entreprise

- Modalité: **en ligne**
- Durée: **12 mois**
- Qualification: **TECH Université Technologique**
- Intensité: **16h/semaine**
- Horaire: **à votre rythme**
- Examens: **en ligne**
- Dirigé aux: **Les diplômés de l'université, les titulaires de diplômes qui ont précédemment obtenu un diplôme dans le domaine des sciences sociales et juridiques, de l'administration et des affaires.**

Accès web: **www.techtitute.com/fr/ecole-de-commerce/master/gestion-politiques-cybersecurite-entreprise**

# Sommaire

01

# Accueil

Aujourd'hui, on estime que les pertes dues aux cyber-attaques se chiffrent en millions et bien en millions. L'exposition aux cyber-attaques est telle que même les États peuvent être visés par des cyber-incidents. Cela a mis en évidence l'importance de disposer de responsables spécialisés dans la gestion des politiques de cybersécurité, disposant des connaissances appropriées en matière d'organisation, de mise en œuvre et d'outils de suivi pour coordonner tous les efforts en matière de cybersécurité. Ce programme prépare les gestionnaires à faire face à des scénarios incertains avec la sécurité et des connaissances avancées, en fournissant des solutions de qualité dans le domaine de la sécurité de l'information. Grâce à un contenu théorique exhaustif, basé sur des cas pratiques réels, vous obtiendrez une perspective moderne et complète de toutes les fonctions qu'un responsable de la cybersécurité doit remplir. Tout cela, en outre, dans un format 100 % en ligne, sans cours en face à face ni horaires préétablis, avec une flexibilité totale.

Mastère Spécialisé en Gestion des Politiques de Cybersécurité dans l'Entreprise
TECH Université Technologique

*Il apporte une valeur incalculable à vos politiques de cybersécurité, en connaissant toutes ses nuances, des systèmes de sécurité eux-mêmes aux pratiques d'analyse des menaces qui vous donneront les clés pour vous positionner avec un avantage dans votre organisation"*

02

# Pourquoi étudier chez TECH?

TECH est la plus grande École de Commerce 100% en ligne au monde. Nous sommes une École de Commerce d'élite, fondée sur un modèle de normes académiques très exigeantes. Un centre de formation hautement performant, de renommée internationale concernant la préparation aux techniques de management.

*Nous sommes une université à la pointe de la technologie et nous mettons toutes nos ressources à votre disposition pour vous aider à réussir"*

## À TECH Université Technologique

### Innovation

Nous mettons à votre disposition un rigoureux modèle d'apprentissage en ligne qui associe les dernières technologies éducatives à la plus grande rigueur pédagogique. Une méthode unique, mondialement reconnue, qui vous procurera les clés afin d'être en mesure d'évoluer dans un monde en constante mutation, où l'innovation doit être le principale défi de tout entrepreneur.

*""Microsoft Europe Success Story"* pour avoir intégré un système multi-vidéo interactif innovant dans les programmes.

### Exigence maximale

Notre critère d'admission n'est pas économique. Pour étudier chez nous, il n'est pas nécessaire de faire un investissement démesuré. Cela dit, pour être diplômé(e) TECH, nous pousserons votre intelligence et vos capacités de résolution de problèmes à leur limite. Nos critères académiques sont très élevés...

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

### Networking

Des professionnels de tous les pays collaborent avec TECH, ce qui vous permettra de créer un vaste réseau de contacts qui vous sera particulièrement utile pour votre 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 l'environnement des affaires. Une opportunité de mettre en valeur vos aspirations et votre 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 pourrez vous familiariser avec 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 de TECH sont issus de plus de 200 nationalités.

## Apprenez avec les meilleurs

Pendant les cours, notre équipe d'enseignants explique 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 universitaire"*



**À TECH nous visons l'excellence et pour cela, nous possédons des caractéristiques qui nous rendent uniques:**

## Analyse

Nous explorons votre sens critique, votre capacité à remettre les choses en question, votre aptitude à résoudre les problèmes ainsi que vos compétences interpersonnelles.

## Excellence académique

Nous mettons à votre disposition la meilleure méthodologie d'apprentissage en ligne. L'université combine la méthode *Relearning* 100% (la méthode d'apprentissage de troisième cycle la plus reconnue au niveau international) avec les" case studies " de Harvard Business School. 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. TECH dispose de plus de 10000 certificats universitaires en français. Et dans la nouvelle économie, **volume + technologie = prix de rupture.**. De cette façon, nous veillons à ce que les études ne soient pas aussi coûteuses que dans une autre université.

03

# Pourquoi notre programme?

Choisir de vous former chez TECH signifie multiplier vos chances de réussir professionnellement dans le domaine du management des entreprises.

C'est un défi qui requiert des efforts et du dévouement, mais qui vous offre la possibilité d'un avenir prometteur. Vous apprendrez auprès de la meilleure équipe pédagogique et avec la méthodologie éducative la plus flexible et la plus innovante qu'il soit.

*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 vous apportera une multitude de bénéfices aussi bien professionnels que personnels, dont les suivants:**

01

## Cela marquera un véritable tournant dans votre carrière

Nous vous offrons l'opportunité d'être maitre de votre avenir et de développer tout votre potentiel. En étudiant ce programme vous allez acquérir les compétences nécessaires pour apporter un changement positif à votre carrière en peu de temps.

*70% des participants de cette formation connaissent une évolution positive de leur carrière en moins de deux ans.*

02

## Vous acquerrez une vision stratégique et globale de l'entreprise

Vous allez acquérir une vision approfondie du management ce qui vous permettra de comprendre la façon dont chaque décision affecte les différents départements fonctionnels de l'entreprise.

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

03

## Vous vous ferez une place parmi les cadres supérieurs de l'entreprise.

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

Nous vous formerons concernant les dernières tendances, avancées et stratégies afin que vous soyez en mesure de mener à bien votre travail professionnel dans un environnement en perpétuel évolution.

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

05

### Vous aurez accès à un important réseau de contacts

Nous vous mettons en relation avec des professionnels comme vous. Ayant des aspirations similaires et ayant la même envie de progresser. Vous serez en relation avec différents partenaires, clients et fournisseurs.

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

06

### Développer des projets d'entreprise de manière rigoureuse.

Vous allez acquérir une vision stratégique approfondie qui vous aidera à développer votre propre projet tout en tenant compte des différents domaines de l'entreprise.

*20 % de nos étudiants développent leur propre idée entrepreneuriale.*

07

### Vous améliorerez vos *soft skills* ainsi que vos compétences en matière de management.

Nous vous accompagnons dans l'application et dans le développement de vos connaissances ainsi que dans l'amélioration de vos compétences interpersonnelles afin de devenir un leader qui fait 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

Nous vous offrons la possibilité d'intégrer une communauté de managers d'élite, de grandes entreprises, d'institutions renommées et de professeurs hautement 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

La cybersécurité étant un aspect crucial du développement de toute entreprise moderne, l'objectif de ce programme ne pouvait être autre que d'offrir la meilleure formation possible dans le domaine de la gestion des politiques de cybersécurité. À cette fin, le groupe d'experts en informatique a compilé un matériel didactique exhaustif, entièrement axé sur l'amélioration des aptitudes, des compétences et des capacités du gestionnaire.

*Dirigez la cybersécurité de votre organisation en apprenant les tenants et aboutissants des politiques de cybersécurité les plus efficaces"*

## TECH fait sien les objectifs de ses étudiants. Ils travaillent ensemble pour les atteindre

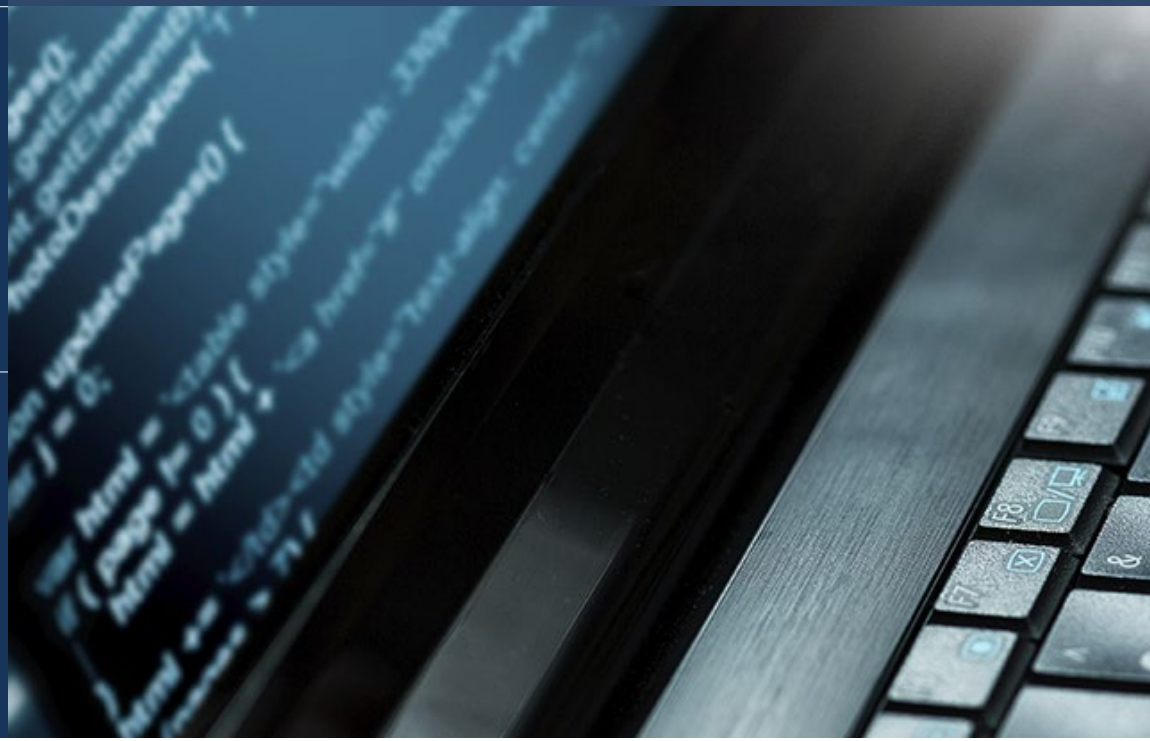
Le **Mastère Spécialisé en Gestion des Politiques de Cybersécurité dans l'Entreprise** vous permettra de:

01 Approfondir leur connaissance des concepts clés de la sécurité de l'information.

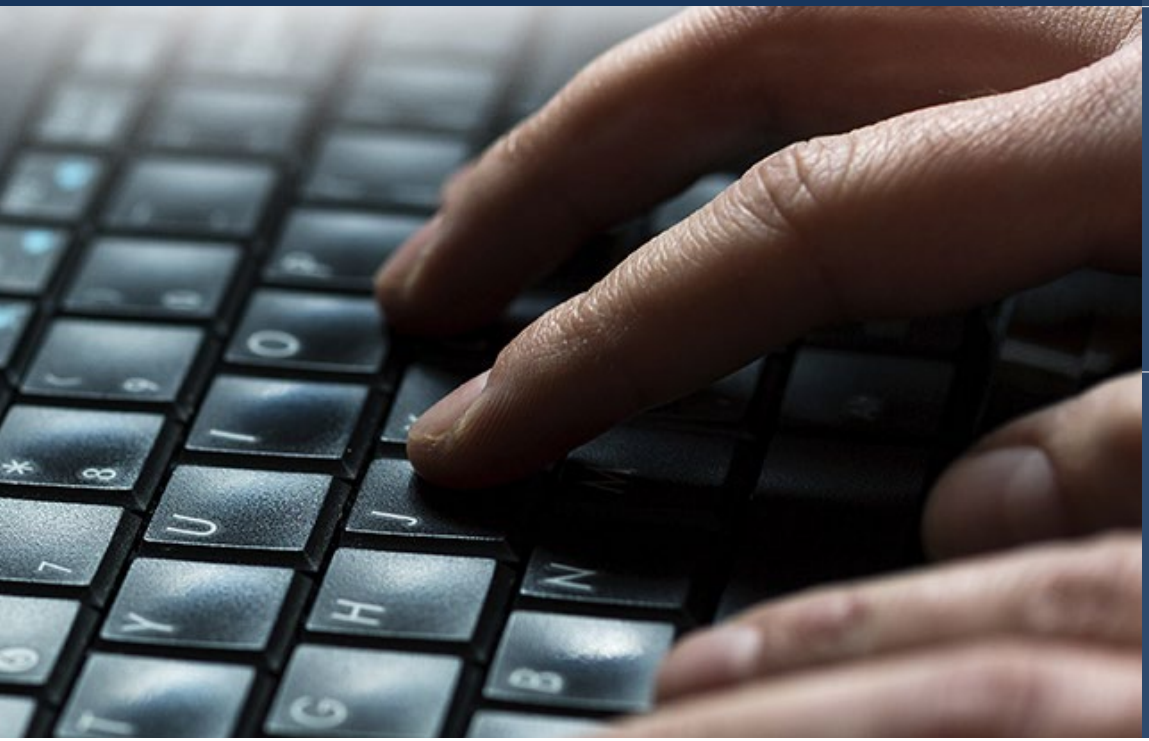
02 Analyser les réglementations et les normes actuellement applicables aux SMSI.

03 Mettre en œuvre un SMSI dans l'entreprise

04 Déterminer les départements que la mise en œuvre du système de gestion de la sécurité doit couvrir.



05 Développer les mesures nécessaires pour assurer de bonnes pratiques en matière de sécurité de l'information.



06 Déterminer ce que sont l'authentification et l'identification

07 Analyser les différentes méthodes d'authentification existantes et leur mise en œuvre pratique.

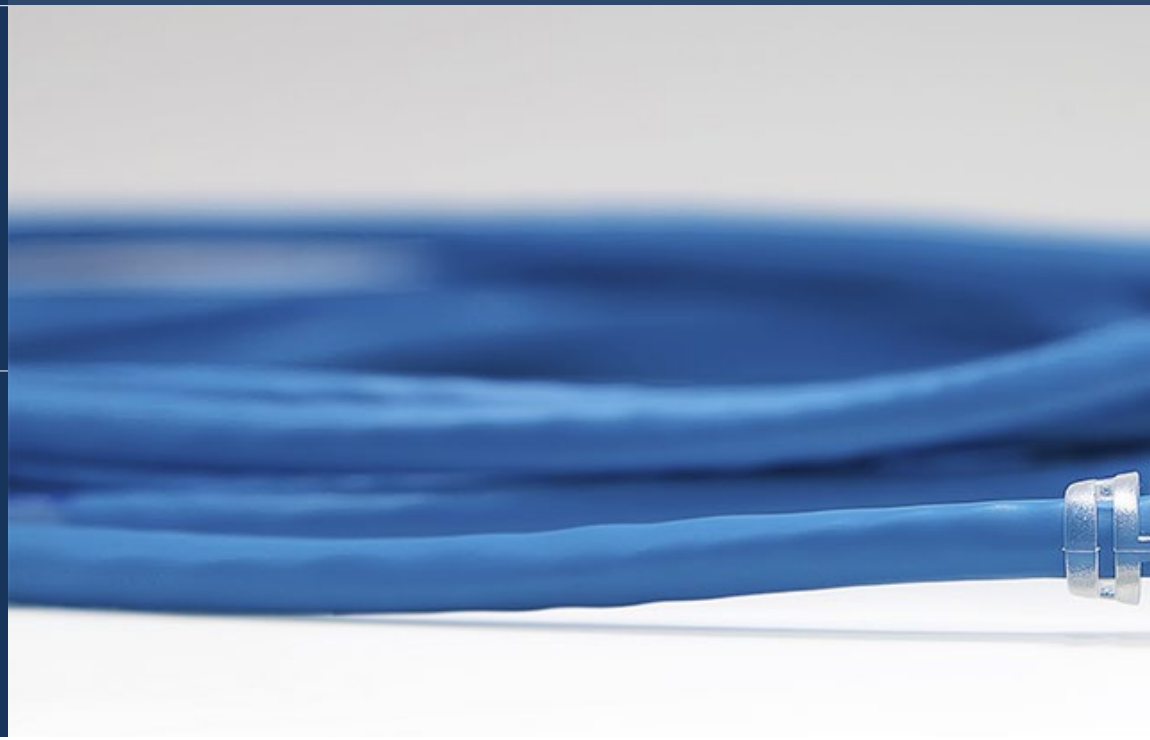
08 Mettre en œuvre la bonne politique de contrôle d'accès pour les logiciels et les systèmes.

09 | Objectifs
Développer des connaissances spécialisées sur la manière de traiter les incidents causés par des événements de sécurité informatique.

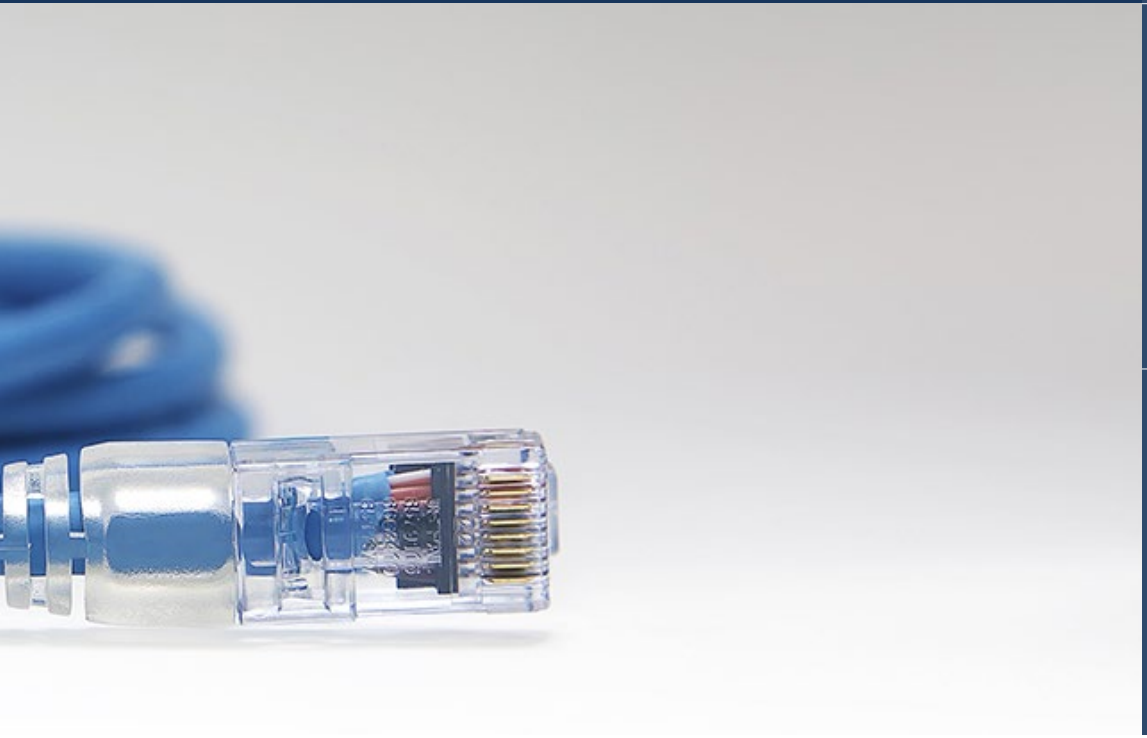
10 Analyser les termes zone sécurisée et périmètre sécurisé

11 Analyser les différents algorithmes de cryptage utilisés dans les réseaux de communication.

12 Déterminer les différentes attaques réelles sur notre système d'information



13 Évaluer les différentes politiques de sécurité pour atténuer les attaques.



14 Développer le concept de suivi et de mise en œuvre des mesures

15 Générer des connaissances spécialisées sur le concept de continuité de la sécurité de l'information

16 Déterminer ce qu'est la cryptographie et les types de cryptographie

05

# Compétences

Pour gérer correctement les politiques de cybersécurité, il est essentiel d'avoir une grande capacité d'organisation, en plus de posséder des connaissances et des compétences supérieures en matière informatique et technologique. C'est pourquoi, tout au long de ce programme, le manager trouvera non seulement un guide de référence utile pour la gestion de la sécurité informatique, mais verra également ses compétences de leadership et de gestion administrative renforcées.

*Vous affinerez les compétences nécessaires pour vous distinguer en tant que manager expert en politique de cybersécurité, ce qui vous donnera l'avantage pour occuper les postes de direction les plus importants"*

01 Déterminer l'implication d'un SMSI dans l'organisation interne de l'entité, ainsi que son statut.

02 Établir les politiques de sécurité dans l'entreprise

03 Déterminer les mesures que nous devons mettre en œuvre avec les fournisseurs et la maintenance des systèmes d'information.

04 Générer des connaissances spécialisées sur le contrôle des menaces

05 Déterminer les phases de la gestion préventive des menaces

06 Développer des méthodologies pour l'analyse des menaces informatiques

07 Classer les menaces en fonction de leur impact et de leur gravité

08 Concevoir une méthodologie propre pour l'analyse et le contrôle préventif des menaces

09 Mettre en œuvre une politique de contrôle d'accès correcte pour les réseaux et les services.

10 Analyser l'importance d'un traitement correct des incidents de sécurité

11 Compiler les différents systèmes biométriques disponibles

12 Examiner la biométrie et les systèmes biométriques


13 Mettre en œuvre les bonnes politiques de sécurité physique et les systèmes de contrôle d'accès physique dans les centres de traitement des données.

14 Mise en œuvre d'un réseau sécurisé

15 Examiner les vulnérabilités des plateformes mobiles et IoT et comment les prévenir.

16 Établir les types d'ingénierie sociale et apprendre à les atténuer.

17 Analyser le concept de suivi et les paramètres de mise en œuvre

18 Déterminer le besoin de continuité de la sécurité de l'information

06

# Structure et contenu

TECH a structuré ce programme sur la base de la méthodologie *Relearning*, ce qui signifie que le manager ne devra pas passer de longues heures d'étude pour acquérir toutes les connaissances proposées. Les termes et concepts clés du domaine des politiques de cybersécurité sont présentés de manière naturelle et répétitive tout au long du diplôme, ce qui se traduit par un processus d'apprentissage beaucoup plus progressif.

*Vous serez libre d'entrer dans la classe virtuelle 24 heures sur 24, en pouvant choisir et adapter le rythme de vos études à vos propres intérêts".*

## Programme d'études

Le Mastère Spécialisé en Gestion des Politiques de Cybersécurité dans l'Entreprise est un programme intensif qui prépare les étudiants aux domaines les plus exigeants de la cybersécurité en entreprise.

Le contenu du Mastère Spécialisé en Gestion des Politiques de Cybersécurité dans l'Entreprise est conçu pour favoriser le développement de compétences managériales permettant de prendre des décisions avec plus de rigueur dans des environnements incertains.

Ce Mastère Spécialisé traite en profondeur du monde numérique, de la sécurité dans cet environnement et de la mise en œuvre du commerce électronique dans les entreprises. Il est conçu pour former des professionnels qui comprennent la gestion des politiques de cybersécurité dans les entreprises d'un point de vue stratégique, international et innovant.

Ce Mastère Spécialisé se déroule sur 12 mois et est divisé en 10 modules :

| | |
|---|---|
| **Module 1** | Système de gestion de la sécurité de l'information (SGSI) |
| **Module 2** | Aspects organisationnels de la politique de sécurité de l'information |
| **Module 3** | Politiques de sécurité pour l'analyse des menaces dans les systèmes d'information |
| **Module 4** | Mise en œuvre pratique des politiques de sécurité logicielle et matérielle |
| **Module 5** | Politiques de gestion des incidents de sécurité |
| **Module 6** | Mise en œuvre de politiques de sécurité physique et environnementale dans l'entreprise |
| **Module 7** | Politiques de communications sécurisées dans l'entreprise |
| **Module 8** | Mise en œuvre pratique des politiques de sécurité face aux attaques |
| **Module 9** | Outils de surveillance des politiques de sécurité des systèmes d'information |
| **Module 10** | Politique pratique de sécurité en cas de catastrophe |

## Où, quand et comment se déroule la formation?

TECH offre la possibilité de développer ce Mastère Spécialisé en Gestion des Politiques de Cybersécurité dans l'Entreprise entièrement en ligne. Pendant les 12 mois de spécialisation, l'étudiant pourra accéder à tout moment à l'ensemble des contenus de ce programme, ce qui vous permettra de gérer vous-même votre temps d'étude.

*Une expérience éducative unique, clé et décisive pour stimuler votre développement professionnel et faire le saut définitif.*

**Module 1.** Système de gestion de la sécurité de l'information (SGSI)

### 1.1. Sécurité de l'information. Aspects clés
1.1.1. Sécurité de l'information
1.1.1.1. Confidentialité
1.1.1.2. Intégration
1.1.1.3. Disponibilité
1.1.1.4. Mesures de sécurité de l'information

### 1.2. Système de gestion de la sécurité de l'information
1.2.1. Modèles de gestion de la sécurité de l'information
1.2.2. Documents pour la mise en œuvre d'un SGSI
1.2.3. Niveaux et contrôles d'un SGSI

### 1.3. Normes et standards internationaux
1.3.1. Normes internationales en matière de sécurité de l'information
1.3.2. Origine et évolution de la norme
1.3.3. Normes internationales de gestion de la sécurité de l'information
1.3.4. Autres normes de référence

### 1.4. Normes ISO/IEC 27000
1.4.1. Objectif et champ d'application
1.4.2. Structure de la norme
1.4.3. Certification
1.4.4. Phases de l'accréditation
1.4.5. Avantages des normes ISO/IEC 27.000

### 1.5. Conception et mise en œuvre d'un système général de sécurité de l'information
1.5.1. Phases de mise en œuvre d'un système général de sécurité de l'information
1.5.2. Plan de continuité des activités

### 1.6. Phase I : diagnostic
1.6.1. Diagnostic préliminaire
1.6.2. Identification du niveau de stratification
1.6.3. Niveau de conformité aux standards/normes

### 1.7. Phase II : Préparation
1.7.1. Contexte organisationnel
1.7.2. Analyse des règlements de sécurité applicables
1.7.3. Portée du système global de sécurité de l'information
1.7.4. Politique générale du système de sécurité des informations
1.7.5. Objectifs du système général de sécurité de l'information

### 1.8. Phase III : Planification
1.8.1. Classification des actifs
1.8.2. Évaluation des risques
1.8.3. Identification des menaces et des risques

### 1.9. Phase IV : Mise en œuvre et suivi
1.9.1. Analyse des résultats
1.9.2. Attribution des responsabilités
1.9.3. Calendrier du plan d'action
1.9.4. Suivi et audits

### 1.10. Politiques de sécurité en matière de gestion des incidents
1.10.1. Phases
1.10.2. Catégorisation des incidents
1.10.3. Procédures et gestion des incidents

**Module 2.** Aspects organisationnels de la politique de sécurité de l'information

### 2.1. Organisation interne
2.1.1. Attribution des responsabilités
2.1.2. Séparation des tâches
2.1.3. Contacts avec les autorités
2.1.4. Sécurité de l'information dans la gestion de projet

### 2.2. Gestion des actifs
2.2.1. Responsabilité des biens
2.2.2. Classification des informations
2.2.3. Manipulation des supports de stockage

### 2.3. Politiques de sécurité dans les processus d'entreprise
2.3.1. Analyse des processus commerciaux vulnérables
2.3.2. Analyse de l'impact sur les affaires
2.3.3. Classement des processus en fonction de leur impact sur l'entreprise

### 2.4. Politiques de sécurité liées aux ressources humaines
2.4.1. Pré-embauche
2.4.2. Pendant le recrutement
2.4.3. Cessation ou changement de poste

### 2.5. Politiques de sécurité au niveau de la direction
2.5.1. Lignes directrices en matière de gestion de la sécurité de l'information
2.5.2. BIA - Analyse de l'impact
2.5.3. Le plan de reprise comme politique de sécurité

### 2.6. Acquisition et maintenance des systèmes d'information
2.6.1. Exigences de sécurité des systèmes d'information
2.6.2. Développement et soutien de la sécurité des données
2.6.3. Données d'essai

### 2.7. Sécurité avec les fournisseurs
2.7.1. Sécurité informatique avec les fournisseurs
2.7.2. Gestion de la fourniture du service avec garantie
2.7.3. Sécurité de la chaîne d'approvisionnement

### 2.8. Sécurité opérationnelle
2.8.1. Responsabilités opérationnelles
2.8.2. Protection contre les codes malveillants
2.8.3. Copies de sauvegarde
2.8.4. Journaux d'activité et suivi

### 2.9. Gestion et réglementation de la sécurité
2.9.1. Respect des exigences légales
2.9.2. Examens de la sécurité de l'information

### 2.10. La sécurité dans la gestion de la continuité des activités
2.10.1. Continuité de la sécurité de l'information
2.10.2. Licenciements

## **Module 3.** Politiques de sécurité pour l'analyse des menaces dans les systèmes d'information

### 3.1. Gestion des menaces dans les politiques de sécurité
3.1.1. Gestion des risques
3.1.2. Risque de sécurité
3.1.3. Méthodologies de gestion des menaces
3.1.4. Mise en œuvre des méthodologies

### 3.2. Phases de la gestion des menaces
3.2.1. Identification
3.2.2. Analyse
3.2.3. Localisation
3.2.4. Mesures de sauvegarde

### 3.3. Audit des systèmes pour la localisation des menaces
3.3.1. Classification et flux d'informations
3.3.2. Analyse des processus vulnérables

### 3.4. Classification des risques
3.4.1. Types de risques
3.4.2. Calcul de la probabilité de la menace
3.4.3. Risque résiduel

### 3.5. Traitement des risques
3.5.1. Mise en œuvre des mesures de sauvegarde
3.5.2. Transfert ou reprise

### 3.6. Contrôle des risques
3.6.1. Processus continu de gestion des risques
3.6.2. Mise en œuvre des mesures de sécurité
3.6.3. Modèle stratégique des mesures de sécurité de l'information

### 3.7. Méthodologies pratiques pour l'analyse et le contrôle des menaces
3.7.1. Catalogue des menaces
3.7.2. Catalogue des mesures de contrôle
3.7.3. Catalogue des mesures de sauvegarde

### 3.8. Norme ISO 27005
3.8.1. Identification des risques
3.8.2. Analyse des risques
3.8.3. Évaluation des risques

### 3.9. Matrice des risques, des impacts et des menaces
3.9.1. Données, systèmes et personnel
3.9.2. Probabilité de la menace
3.9.3. Ampleur des dommages

### 3.10. Phases et processus de conception de l'analyse des risques
3.10.1. Identification des éléments critiques de l'organisation
3.10.2. Détermination des menaces et des impacts
3.10.3. Analyse d'impact et de risque
3.10.4 Méthodologies

## **Module 4.** Mise en œuvre pratique des politiques de sécurité logicielle et matérielle

### 4.1. Mise en œuvre pratique des politiques de sécurité des logiciels et des matériels
4.1.1. Mise en œuvre de l'identification et de l'autorisation
4.1.2. Mise en œuvre des techniques d'identification
4.1.3. Mesures techniques d'autorisation

### 4.2. Technologies d'identification et d'autorisation
4.2.1. Identifiant et OTP
4.2.2. Clé USB ou carte à puce PKI
4.2.3. La touche "Confidentiel Défense".
4.2.4. RFID active

### 4.3. Politiques de sécurité d'accès aux logiciels et aux systèmes
4.3.1. Mise en œuvre des politiques de contrôle d'accès
4.3.2. Mise en œuvre des politiques d'accès aux communications
4.3.3. Types d'outils de sécurité pour le contrôle d'accès

### 4.4. Gestion de l'accès des utilisateurs
4.4.1. Gestion des droits d'accès
4.4.2. Séparation des rôles et des fonctions d'accès
4.4.3. Mise en œuvre des droits d'accès dans les systèmes

### 4.5. Contrôle de l'accès aux systèmes et aux applications
4.5.1. Règle d'accès minimal
4.5.2. Technologies de connexion sécurisée
4.5.3. Politiques de sécurité des mots de passe

### 4.6. Technologies des systèmes d'identification
4.6.1. Active Directory
4.6.2. OTP
4.6.3. PAP, CHAP
4.6.4. KERBEROS, DIAMETER, NTLM

### 4.7. Contrôles CIS pour le bastioning du système
4.7.1. Contrôles de base du CIS
4.7.2. Contrôles fondamentaux du CIS
4.7.3. Contrôles organisationnels CIS

### 4.8. Sécurité opérationnelle
4.8.1. Protection contre les codes malveillants
4.8.2. Copies de sauvegarde
4.8.3. Enregistrement et suivi des activités

### 4.9. Gestion des vulnérabilités techniques
4.9.1. Vulnérabilités techniques
4.9.2. Gestion des vulnérabilités techniques
4.9.3. Restrictions relatives à l'installation du logiciel

### 4.10. Mise en œuvre des pratiques de la politique de sécurité
4.10.1. Vulnérabilités logiques
4.10.2. Mise en œuvre des politiques de défense

**Module 5.** Politiques de gestion des incidents de sécurité

5.1. Politiques de gestion de Incidence sécurité de l'information des améliorations
5.1.1. Gestion des incidents
5.1.2. Responsabilités et procédures
5.1.3. Notification d'événement
5.2. Systèmes de détection et de prévention des Intrusion: (IDS/IPS)
5.2.1. Données de fonctionnement du système
5.2.2. Types de systèmes de détection d'intrusion
5.2.3. Critères de placement des IDS/IPS
5.3. Réponse aux incidents de sécurité
5.3.1. Procédure de collecte d'informations
5.3.2. Processus de vérification des intrusions
5.3.3. Organismes CERT
5.4. Processus de notification et de gestion des tentatives d'intrusion
5.4.1. Responsabilités dans le processus de notification
5.4.2. Classification des incidents
5.4.3. Processus de résolution et de récupération
5.5. L'analyse médico-légale comme politique de sécurité
5.5.1. Preuves volatiles et non volatiles
5.5.2. Analyse et collecte de preuves électroniques
5.5.2.1. Analyse des preuves électroniques
5.5.2.2. Collecte de preuves électroniques
5.6. Outils de systèmes de détection et de prévention des intrusions (IDS/IPS)
5.6.1. Snort
5.6.2. Suricata
5.6.3. Solar-Winds
5.7. Outils de centralisation des événements
5.7.1. SIM
5.7.2. SEM
5.7.3. SIEM
5.8. Guide de sécurité CCN-STIC 817
5.8.1. Guide de sécurité CCN-STIC 817
5.8.2. Gestion des cyberincidents
5.8.3. Métriques et indicateurs
5.9. NIST SP800-61
5.9.1. Capacité de réponse aux incidents de sécurité informatique
5.9.2. Traitement des incidents
5.9.3. Coordination et partage d'informations
5.10. Norme ISO 27035
5.10.1. ISO 27035. Principes de la gestion des incidents
5.10.2. Lignes directrices pour l'élaboration d'un plan de gestion des incidents
5.10.3. Lignes directrices pour les opérations de réponse aux incidents

## **Module 6.** Mise en œuvre de politiques de sécurité physique et environnementale dans l'entreprise

### 6.1. Zones sécurisées
6.1.1. Périmètre de sécurité physique
6.1.2. Travailler dans des zones sécurisées
6.1.3. Sécurité des bureaux, des locaux et des ressources

### 6.2. Contrôles physiques d'entrée
6.2.1. Politiques de contrôle d'accès physique
6.2.2. Systèmes de contrôle des entrées physiques

### 6.3. Vulnérabilités de l'accès physique
6.3.1. Principales vulnérabilités physiques
6.3.2. Mise en œuvre des mesures de sauvegarde

### 6.4. Systèmes biométriques physiologiques
6.4.1. Empreinte digitale
6.4.2. Reconnaissance faciale
6.4.3. Reconnaissance de l'iris et de la rétine
6.4.4. Autres systèmes biométriques

physiologiques

### 6.5. Systèmes biométriques comportementaux
6.5.1. Reconnaissance de la signature
6.5.2. Reconnaissance des écrivains
6.5.3. Reconnaissance vocale
6.5.4. Autres systèmes biométriques comportementaux

### 6.6. Gestion du risque en biométrie
6.6.1. Mise en œuvre des systèmes biométriques
6.6.2. Vulnérabilités des systèmes biométriques

### 6.7. Mise en œuvre des politiques d' *Hosts*
6.7.1. Installation du câblage
Provisionnement et sécurité
6.7.2. Emplacement de l'équipement
6.7.3. Sortie de l'équipement à l'extérieur des locaux
6.7.4. Politique relative aux équipements informatiques non surveillés et aux postes clairs

### 6.8. Protection de l'environnement
6.8.1. Systèmes de protection contre l'incendie
6.8.2. Systèmes de protection contre les tremblements de terre
6.8.3. Systèmes de protection contre les tremblements de terre

### 6.9. Sécurité du centre de traitement des données
6.9.1. Portes de sécurité
6.9.2. Systèmes de vidéosurveillance (CCTV)
6.9.3. Contrôle de sécurité

### 6.10. Règlement international sur la sécurité physique
6.10.1. IEC 62443-2-1 (européen)
6.10.2. NERC CIP-005-5 (U.S.A.)
6.10.3. NERC CIP-014-2 (U.S.A.)

## **Module 7.** Politiques de communications sécurisées dans l'entreprise

### 7.1. Gestion de la sécurité des réseaux
7.1.1. Surveillance et contrôle du réseau
7.1.2. Ségrégation des réseaux
7.1.3. Systèmes de sécurité des réseaux

### 7.2. Protocoles de communication sécurisés
7.2.1. Modèle TCP/IP
7.2.2. Protocole IPSEC
7.2.3. Protocole TLS

### 7.3. Protocole TLS 1;3
7.3.1. Phases d'un processus TLS1.3
7.3.2. Protocole *Handshake*
7.3.3. Protocole d'enregistrement
7.3.4. Différences avec TLS 1.2

### 7.4. Algorithmes cryptographiques
7.4.1. Algorithmes cryptographiques utilisés dans les communications
7.4.2. *Suites à ciphers*
7.4.3. Algorithmes cryptographiques autorisés pour TLS 1.3

### 7.5. Fonctions de digestion
7.5.1. Fonctions de digestion
7.5.2. MD6
7.5.3. SHA

### 7.6. PKI. Infrastructure à clé publique
7.6.1. PKI et ses entités
7.6.2. Certificat numérique
7.6.3. Types de certificats numériques

### 7.7. Communications dans les tunnels et les transports
1.7.1. Tunnel de communication
1.7.2. Communications de transport
1.7.3. Mise en œuvre du tunnel crypté

### 7.8. SSH *Secure Shell*
1.7.1. SSH Secure Shell
1.7.2. Opération SSH
1.7.3. Outils de SSH

### 7.9. Vérification des systèmes cryptographiques
1.7.1. Test d'intégrité
1.7.2. Test de systèmes cryptographiques

### 7.10. Systèmes cryptographiques
7.10.1. Vulnérabilités des systèmes cryptographiques
7.10.2. Garanties cryptographiques

**Module 8.** Mise en œuvre pratique des politiques de sécurité face aux attaques

8.1. *System Hacking*
8.1.1. Risques et vulnérabilités
8.1.2. Contre-mesures

8.2. DoS dans les services
8.2.1. Risques et vulnérabilités
8.2.2. Contre-mesures

8.3. *Session Hijacking*
1.7.1. Le processus de *Hijacking*
1.7.2. Contre-mesures au *Hijacking*

8.4. Évasion des IDS, *Firewalls* et des pots de miel
8.4.1. Techniques d'évasion
8.4.2. Mise en œuvre de contre-mesures

8.5. *Piratage des serveurs Web*
8.5.1. Attaques contre les serveurs web
8.5.2. Mise en œuvre des mesures de défense

8.6. *Piratage des applications Web*
8.6.1. Attaques contre les applications Web
8.6.2. Mise en œuvre des mesures de défense

8.7. *Hacking Wireless Networks*
8.7.1. Vulnérabilités du réseau Wifi
8.7.2. Mise en œuvre des mesures de défense

8.8. *Hacking Mobile Platforms*
8.8.1. Vulnérabilités des plates-formes mobiles
8.8.2. Mise en œuvre de contre-mesures

8.9. *Ramsonware*
1.7.1. Vulnérabilités causant le *Ramsonware*
1.7.2. Mise en œuvre de contre-mesures

8.10. Ingénierie sociale
8.10.1. Types d'ingénierie sociale
8.10.2. Contre-mesures à l'ingénierie sociale

**Module 9.** Outils de surveillance des politiques de sécurité des systèmes d'information

9.1. Politiques de surveillance des systèmes d'information
9.1.1. Surveillance du système
9.1.2. Métriques
9.1.3. Types de mesures

9.2. Vérification et enregistrement dans les systèmes
9.2.1. Audit et journalisation dans les systèmes
9.2.2. Audit et journalisation de Windows
9.2.3. Journalisation et audit de Linux

9.3. Protocole SNMP. *Simple Network Management Protocol*
9.3.1. Protocole SNMP
9.3.2. Opération SNMP
9.3.3. Outils de SNMP

9.4. Surveillance du réseau
1.7.1. Surveillance du réseau dans les systèmes de contrôle
1.7.2. Outils de surveillance des systèmes de contrôle

9.5. Nagios. Système de surveillance du réseau
1.7.1. Nagios
1.7.2. Fonctionnement de Nagios
1.7.3. Installation de Nagios

9.6. Zabbix. Système de surveillance du réseau
1.7.1. Zabbix
1.7.2. Fonctionnement de Zabbix
1.7.3. Installation de Zabbix

9.7. Cacti. Système de surveillance du réseau
1.7.1. Cacti.
1.7.2. Fonctionnement de Cacti
1.7.3. Installation de Cacti

9.8. Pandora Système de surveillance du réseau
9.8.1. Pandora
9.8.2. Fonctionnement de Pandora
9.8.3. Installation de Pandora

9.9. SolarWinds. Système de surveillance du réseau
1.7.1. SolarWinds.
1.7.2. Fonctionnement de SolarWinds
1.7.3. Installation de SolarWinds

9.10. Suivi des règlements
9.10.1. Contrôles CIS sur l'audit et l'enregistrement
9.10.2. NIST 800-123 (ÉTATS-UNIS)

## **Module 10.** Politique pratique de sécurité en cas de catastrophe

### 10.1. DRP Plan de reprise après sinistre
1.7.1. Objectif d'un DRP
1.7.2. Avantages d'un DRP
1.7.3. Conséquences de ne pas avoir de PRA et de ne pas le tenir à jour

### 10.2. Guide pour la définition d'un DRP (plan de reprise après sinistre)
1.7.1. Portée et objectifs
1.7.2. Conception de la stratégie de récupération
1.7.3. Répartition des rôles et des responsabilités
1.7.4. Inventaire du matériel, des logiciels et des services
1.7.5. Tolérance aux temps d'arrêt et aux pertes de données
1.7.6. Déterminer les types spécifiques de PRD requis
1.7.7. Mise en œuvre d'un plan de formation, de sensibilisation et de communication

### 10.3. Portée et objectifs d'un DRP (Disaster Recovery Plan)
1.7.1. Assurer la réponse
1.7.2. Composants technologiques
1.7.3. Champ d'application de la politique de continuité

### 10.4. Conception d'une stratégie de reprise après sinistre (DRP)
1.7.1. Stratégie de reprise après sinistre
1.7.2. Budget
1.7.3. Ressources humaines et physiques
1.7.4. Postes de direction à risque
1.7.5. Technologie
1.7.6. Données

### 10.5. Continuité des processus d'information
10.5.1. Planification de la continuité
10.5.2. Mise en œuvre de la continuité
10.5.3. Vérification et évaluation de la continuité

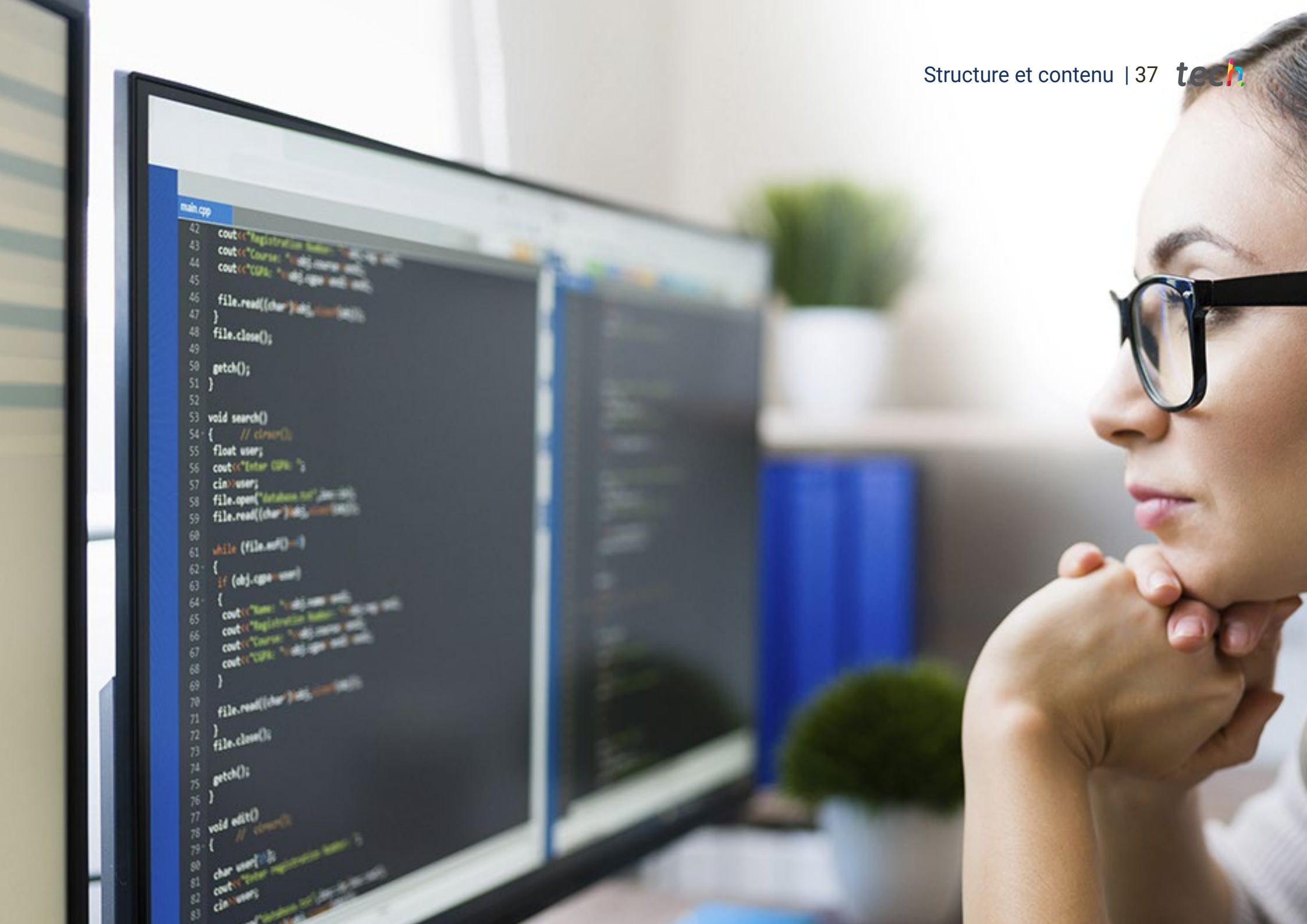
### 10.6. Portée d'un PCA (Plan de continuité des activités)
1.7.1. Détermination des processus les plus critiques
1.7.2. Approche fondée sur les actifs
1.7.3. Approche par processus

### 10.7. Mise en œuvre de processus d'affaires assurés
10.7.1. Activités prioritaires (AP)
10.7.2. Temps de récupération idéal (TRI)
10.7.3. Stratégies de survie

### 10.8. Analyse organisationnelle
1.7.1. Collecte d'informations
1.7.2. Analyse de l'impact sur les entreprises (BIA)
1.7.3. Analyse des risques organisationnels

### 10.9. Réponse aux situations d'urgence
1.7.1. Plan de crise
1.7.2. Plans de rétablissement de l'environnement opérationnel
1.7.3. Procédures techniques de travail ou d'incident

### 10.10. Norme internationale ISO 27031 BCP
10.10.1. Objectifs
10.10.2. 2015 : références, normes et champ d'application
10.10.3. Opération


main.cpp

07

# Méthodologie

Cette formation vous propose une manière différente d'apprendre. Notre méthodologie est développée à travers un mode d'apprentissage cyclique : ***Le Relearning***.
Ce système d'enseignement s'utilise, notamment, dans les Écoles de Médecine les plus prestigieuses du monde. De plus il a été considéré comme l'une des Méthodes les plus efficaces par des magazines scientifiques de renom comme par exemple le ***New England Journal of Medicine.***

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

## TECH Université Technologique utilise l'étude de cas pour contextualiser tout le contenu.

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

*Avec TECH, vous ferez l'expérience d'une méthode d'apprentissage qui ébranle les fondements des universités traditionnelles du monde entier"*


*Ce programme vous prépare à relever les défis commerciaux dans des environnements incertains et à assurer la réussite de votre entreprise.*

*Notre programme vous prépare à réussir votre carrière professionnelle en relevant de nouveaux défis dans des environnements incertains.*

## Une méthode d'apprentissage innovante et différente

Ce Programme de TECH est un programme d'enseignement intensif, créé de toutes pièces pour offrir aux managers des défis et des décisions d'affaires au plus haut niveau, que ce soit au niveau national ou international. Grâce à cette méthodologie, l'épanouissement personnel et professionnel est stimulé, faisant ainsi un pas décisif vers la réussite. La méthode des cas, une technique qui jette les bases de ce contenu, garantit que la réalité économique, sociale et commerciale la plus actuelle est suivie.

> *Vous apprendrez à travers des études de cas réels ainsi qu'en vous exerçant à résoudre des situations complexes dans des environnements professionnels réels"*

La méthode des cas est le système d'apprentissage le plus largement utilisé dans les meilleures Écoles de Commerce du monde et ce depuis leur fondement. Développée en 1912 à Harvard pour que les étudiants en Droit n'apprennent pas uniquement sur la base d'un contenu théorique, la méthode des cas consistait à leur présenter des situations réelles complexes pour que les apprenants s'entraînent à les résoudre et à prendre des décisions. Elle a été établie comme méthode d'enseignement standard à Harvard en 1924.

Face à une situation donnée, que doit faire un professionnel? C'est la question à laquelle nous vous confrontons dans la méthode des cas, une méthode d'apprentissage orientée vers l'action. Tout au long du programme, vous serez confronté à de multiples cas réels. Vous allez devoir mobiliser toutes vos connaissances, faire des recherches, argumenter et défendre vos idées ainsi vos décisions.

## Relearning Methodology

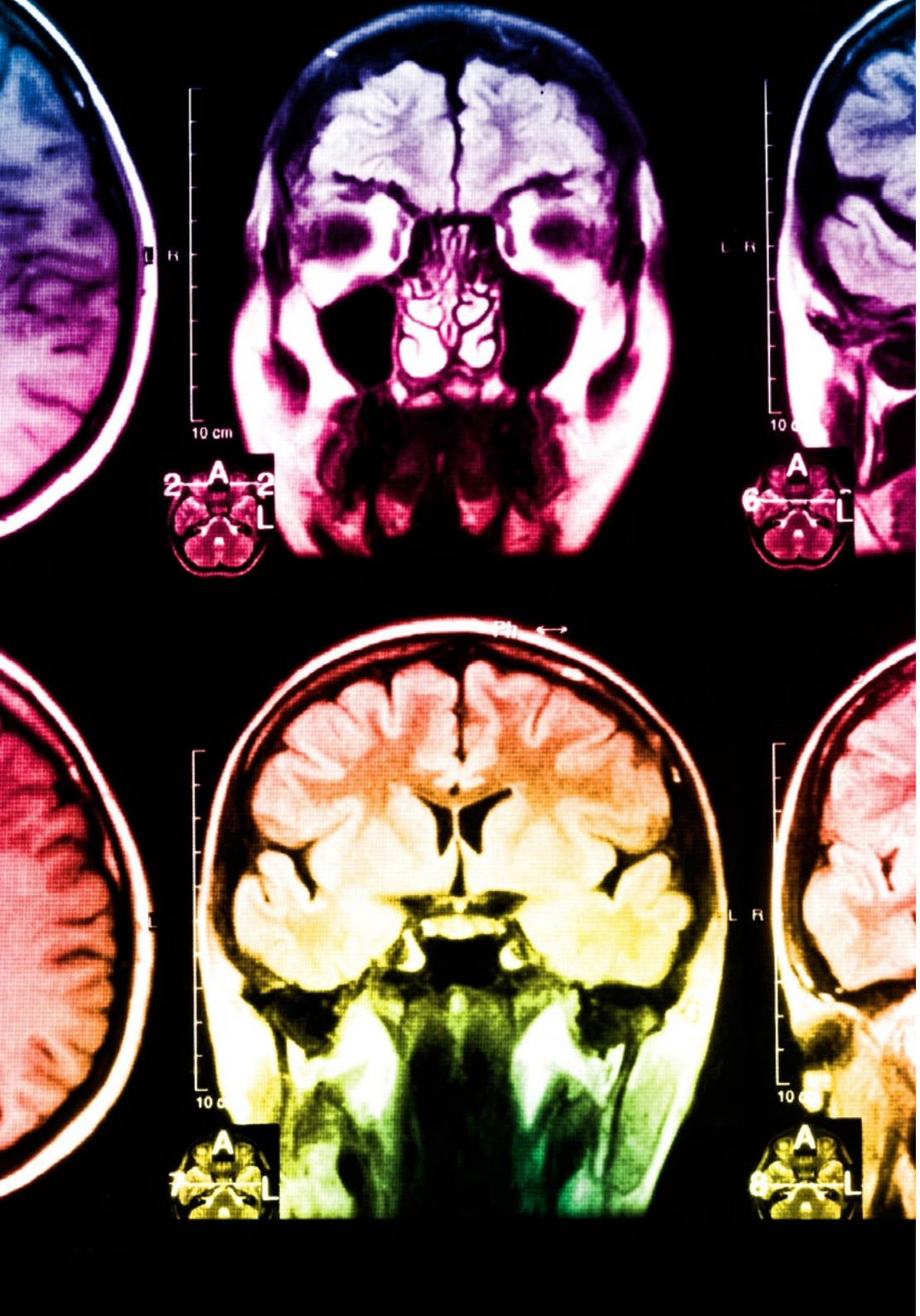
TECH est la première Université au monde à combiner les case studies avec un système d'apprentissage 100% en ligne basé sur la répétition, qui combine éléments didactiques différents dans chaque leçon.

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

> *Notre système de formation 100% à distance vous permettra d'organiser votre temps et votre rythme de travail en fonction de votre emploi du temps. Vous pourrez accéder aux contenus à partir de n'importe quel appareil fixe ou mobile doté d'une connexion internet.*

À TECH, vous serez formé 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 utiliser cette méthode si efficace. Selon les indicateurs de qualité de la meilleure université en ligne du monde, en 2019 nous avons réussi à améliorer le niveau de satisfaction globale des professionnels finalisant leurs études chez nous (qualité du corps professoral, qualité des supports didactiques, structure des cours, objectif etc.).



Dans notre programme, l'apprentissage n'est pas un processus linéaire mais il se déroule en spirale (nous apprenons, désapprenons, oublions et réapprenons). C'est pourquoi nous combinons chacun de ces éléments de manière concentrique. Grâce à cette méthodologie, nous avons formé plus de 650.000 diplômés universitaires avec un succès sans précédent et ce dans toutes les spécialités aussi divers que la biochimie, la génétique, la chirurgie, le droit international, les compétences en matière de gestion, les sciences du sport, la philosophie, le droit, l'ingénierie, le journalisme, l'histoire ou les marchés et instruments financiers. Tout cela dans un environnement très exigeant, avec un corps étudiant universitaire au profil socio-économique élevé et dont l'âge moyen est de 43,5 ans.

*Le Relearning vous permettra d'apprendre plus facilement et de manière plus productive tout en 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 données scientifiques dans le domaine des neurosciences, non seulement nous savons la manière dont le cerveau organise les informations, les idées, les images et les souvenirs, mais nous savons aussi que le lieu et le contexte dans lesquels nous apprenons quelque chose est fondamental pour s'en souvenir et le stocker dans l'hippocampe afin de le conserver ensuite dans notre mémoire à long terme.

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

Ce programme offre les meilleurs supports pédagogiques, préparés à l'intention des professionnels :

### Support d'étude

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

Ces contenus sont ensuite appliqués au format audiovisuel, pour créer la méthode de travail TECH online. Ils sont élaborés à l'aide des dernières techniques ce qui nous permet de vous offrir une grande qualité dans chacun des supports que nous partageons avec vous.

### Cours magistraux

Il existe de nombreux faits scientifiques prouvant l'utilité de l'observation par un tiers expert.

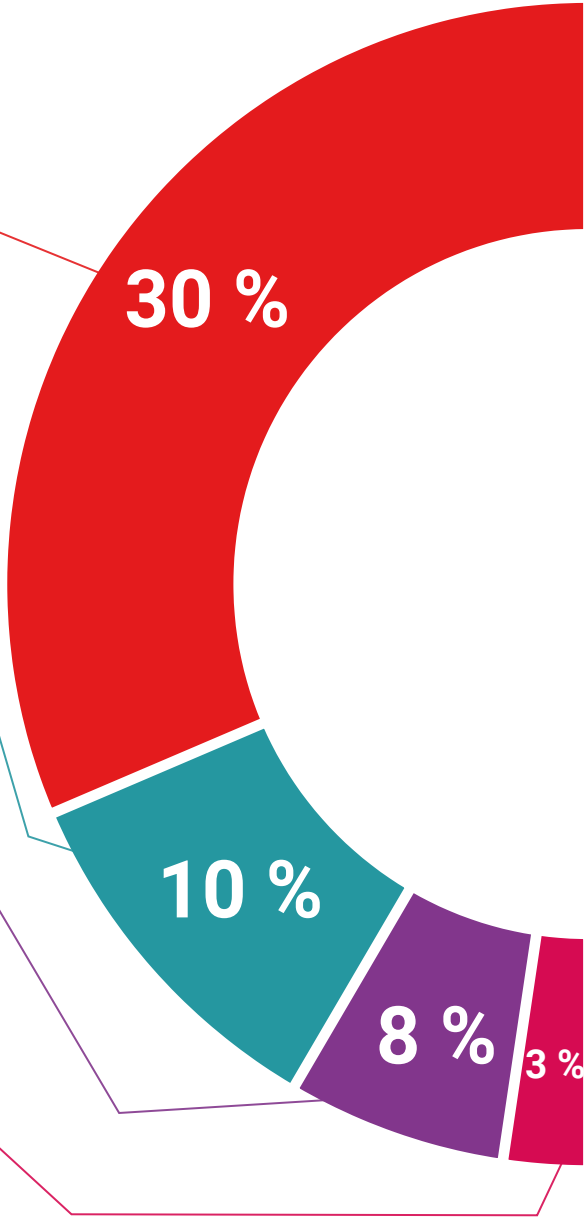
La méthode Learning from an Expert renforce les connaissances et la mémoire, et génère de la confiance dans les futures décisions difficiles.

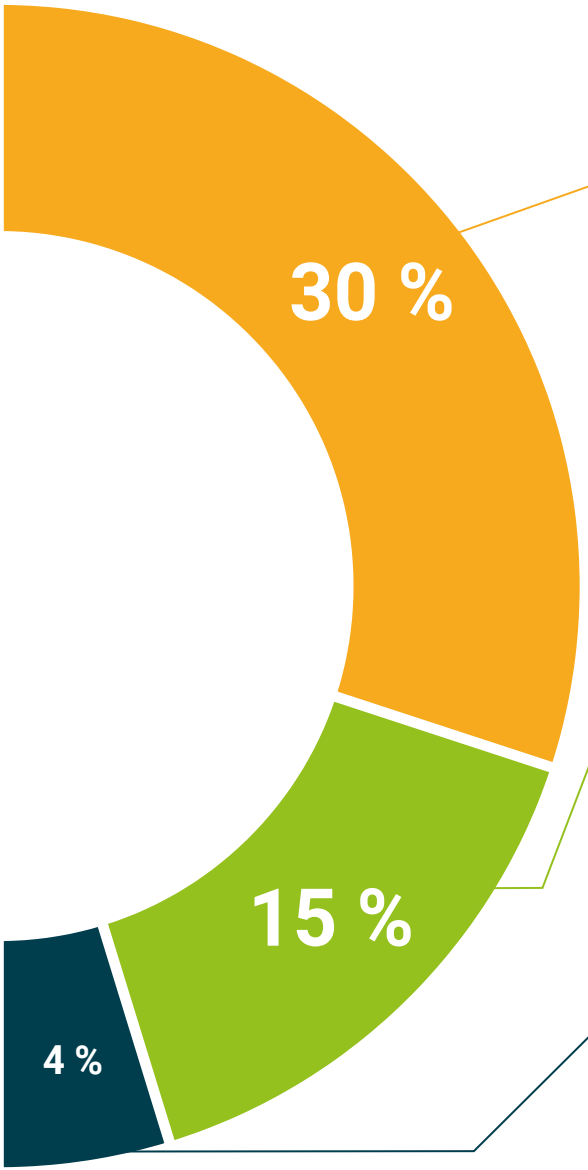
### Exercices de compétences en management

Vous réaliserez des activités visant à développer des compétences de direction spécifiques dans chaque domaine. Cette formation se veut pratique et dynamique pour que les apprenants puissent acquérir et développer les compétences et les capacités nécessaires à un cadre supérieur dans le contexte actuel de mondialisation.

### Lectures complémentaires

Articles récents, documents de consensus et directives internationales, entre autres. Dans notre bibliothèque virtuelle TECH, vous aurez accès à tout ce dont vous avez besoin pour compléter votre formation :






### Case Studies

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

### Résumés interactifs

Nous présentons les contenus de manière attrayante et dynamique dans des dossiers multimédias comprenant des fichiers audios, des vidéos, des images, des diagrammes et des cartes conceptuelles afin de consolider les connaissances.

Ce système unique de formation à la présentation de contenu multimédia a été récompensé par Microsoft en tant que "European Success Story".

### Testing & Retesting

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

08

# Profil de nos étudiants

Le Mastère Spécialisé s'adresse aux diplômés de l'université, aux diplômés et aux personnes ayant déjà obtenu l'un des diplômes suivants dans le domaine des sciences sociales et juridiques, de l'administration et de l'économie.

La diversité des participants aux différents profils académiques et aux multiples nationalités, constitue l'approche multidisciplinaire de ce programme.

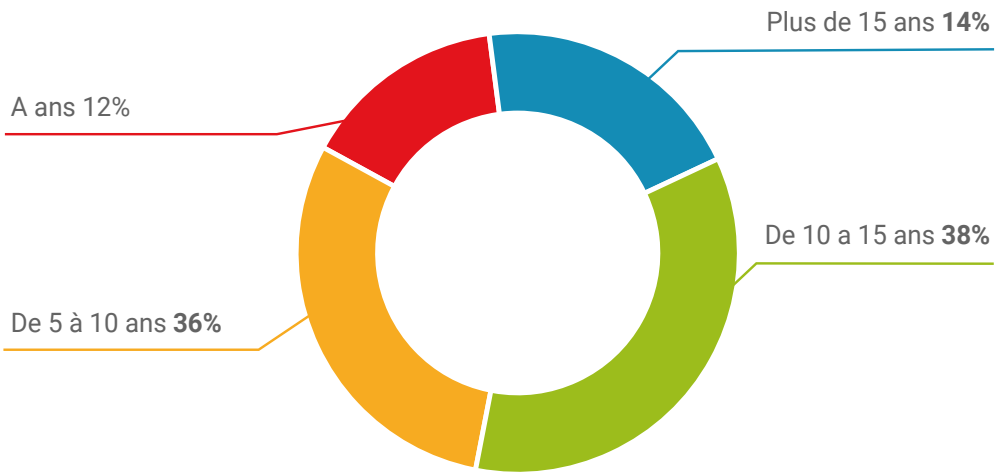
Le Mastère Spécialisé peut pourront également suivi par des professionnels qui, en tant que diplômés universitaires dans n'importe quel domaine, ont une expérience professionnelle de deux ans dans le domaine de la Gestion des Politiques de Cybersécurité.

*Si vous cherchez à dynamiser votre carrière professionnelle avec des connaissances de qualité, basées sur la réalité la plus actuelle de la cybersécurité, inscrivez-vous dès maintenant à ce programme"*

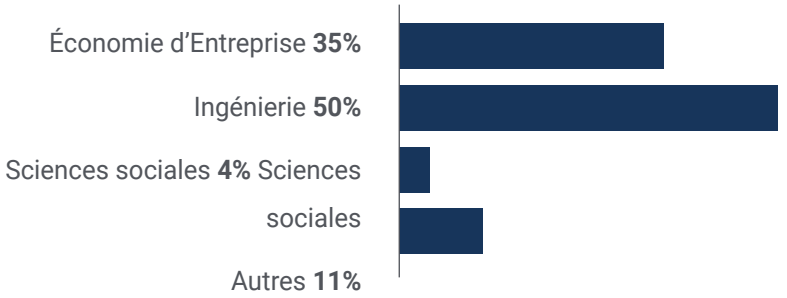
## Âge moyen

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

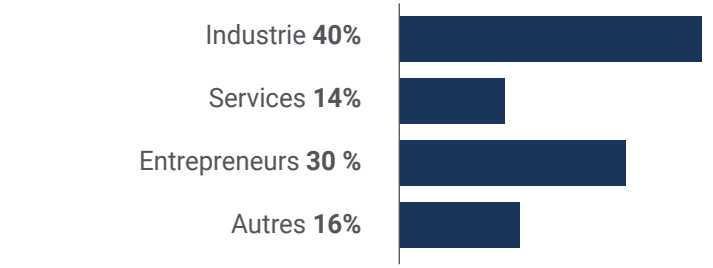
## Années d'expérience



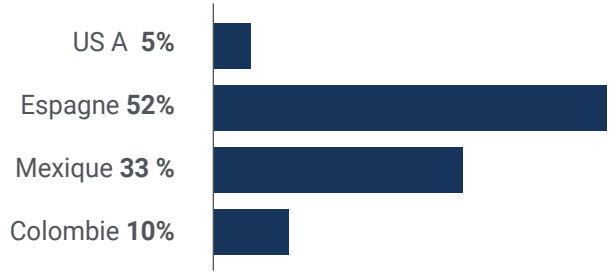

## Formation




## Profil Académique



## Distribution géographique




# Gabriel Gutiérrez Gómez

**Chef de la cybersécurité**

*"Après avoir subi une grave cyberattaque dans notre organisation, nous avons mis davantage l'accent sur la protection de nos bases de données et y avons consacré un petit département. Grâce à ce programme, j'ai pu diriger cet effort, en concevant et en mettant en œuvre les politiques de cybersécurité que nous utilisons encore aujourd'hui"*

09

# Direction de la formation

Afin d'obtenir la meilleure qualité possible de tous les contenus didactiques, TECH a sélectionné un groupe d'enseignants experts dans les différents domaines couverts par la cybersécurité. Ainsi, le gestionnaire aura accès à un syllabus rédigé par des professionnels ayant une grande expérience de la gestion des politiques de cybersécurité, qui ont apporté à toute la théorie leur vision pratique distinctive pour chacun des sujets traités.

*Vous bénéficierez de l'appui d'un corps enseignant expérimenté dans la gestion de la sécurité informatique complexe, avec des sujets consacrés à la maintenance des systèmes d'information, à l'analyse forensique et au détournement"*

## Direction

### Mme Fernández Sapena, Sonia

- Formateur en sécurité informatique et Ethical Hacking au Centre National de Référence pour l'informatique et les télécommunications. de Madrid
- Instructeur certifié E-Council
- Formateur dans les certifications suivantes : EXIN Ethical Hacking Foundation y EXIN Cyber & IT Security Foundation. Madrid
- Formateur expert accrédité par le CAM pour les certificats de professionnalisme suivants : Sécurité informatique (IFCT0190), Gestion des réseaux voix et données (IFCM0310), Administration des réseaux départementaux (IFCT0410), Gestion des alarmes dans les réseaux de télécommunications (IFCM0410), Opérateur de réseaux voix et données (IFCM0110), et Administration des services Internet (IFCT0509).
- Collaborateur externe CSO/SSA (Chief Security Officer/Senior Security Architect) à l'Université des Baléares.
- Diplôme d'ingénieur en informatique de l'université d'Alcalá de Henares à Madrid.
- Master en DevOps : Docker et Kubernetes. Cas-Training
- Technologies de sécurité Microsoft Azure. E-Council

## Professeurs

### M. Solana Villarias, Fabián

- Consultant en technologie de l'information
- Développeur et administrateur de services d'enquête chez Investigación, Planificación y Desarrollo, S.A.
- Spécialiste des marchés financiers et de la maintenance des systèmes informatiques chez Iberia Financial Software.
- Développeur web et spécialiste de l'accessibilité chez Indra
- Diplôme en ingénierie des systèmes supérieurs à l'Université du Pays de Galles/ CESINE
- Diplôme d'ingénieur technique en ingénierie des systèmes informatiques de l'Université du Pays de Galles/ CESINE

### Mme López García, Rosa María

- Spécialiste de l'information de gestion
- Conférencier au Linux Professional Institute
- Collaborateur de l'Incibe Hacker Academy
- Capitaine des talents en cybersécurité chez Teamciberhack
- Responsable administratif, comptable et financier chez Integra2Transportes
- Assistante administrative en charge des achats de ressources au centre éducatif Cardenal Marcelo Espínola.
- Technicien supérieur en cybersécurité et piratage éthique
- Membre de Ciberpatrulla

### M. Oropesiano Carrizosa, Francisco

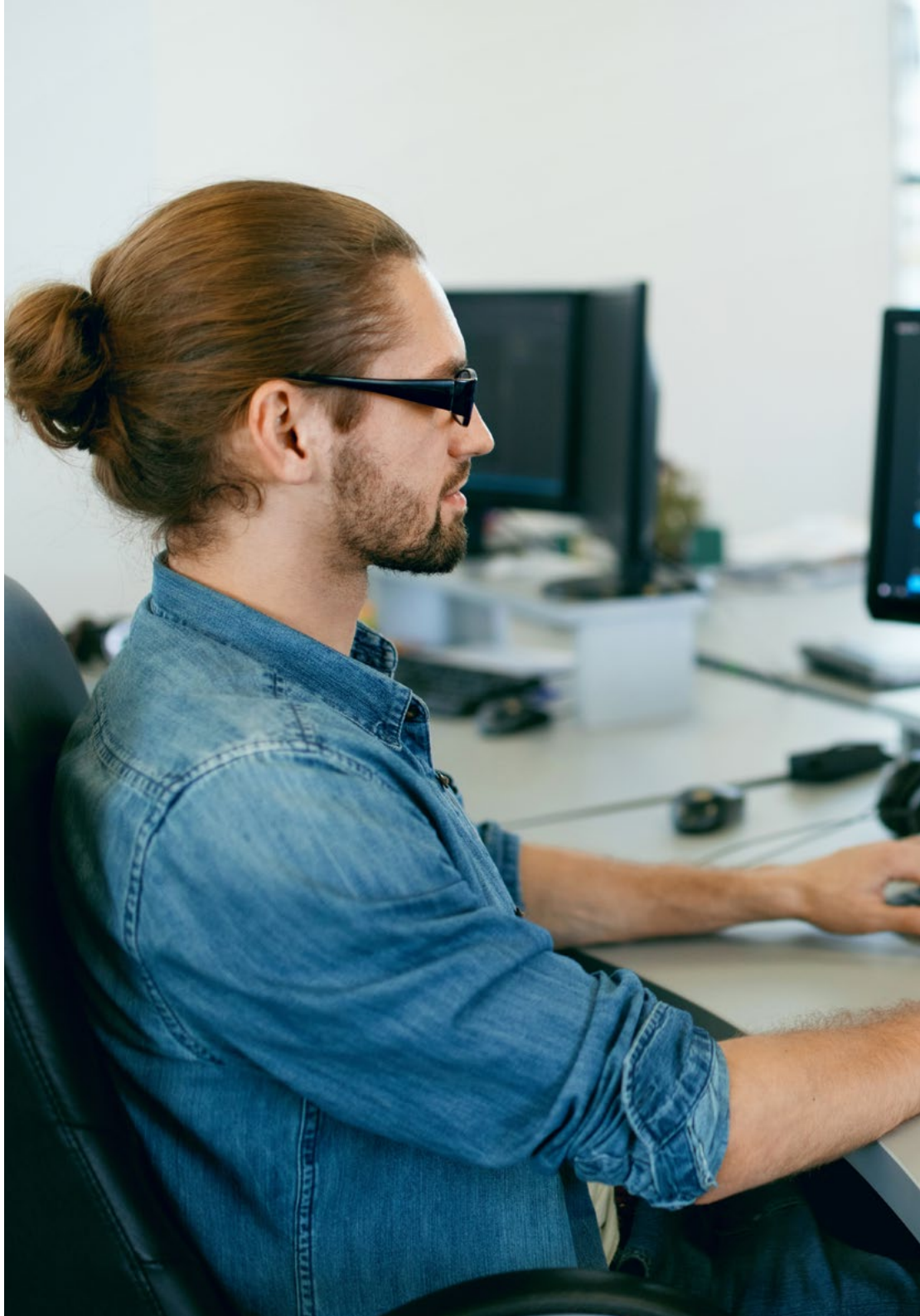
- Ingénieur en informatique
- Technicien en micro-informatique, réseaux et sécurité chez Cas-Training
- Développeur de services Web, CMS, e-Commerce, UI et UX chez Fersa Reparaciones
- Gestionnaire de services Web, de contenu, de courrier et de DNS dans Oropesia Web & Network
- Concepteur d'applications graphiques et web chez Xarxa Sakai Projectes
- Diplômé en systèmes informatiques à l'Université d'Alcalá de Henares
- Master en DevOps : Docker et Kubernetes par le Cyber Business Center
- Technicien en réseaux et sécurité informatique de l'Université des Baléares
- Expert en design graphique de l'Université polytechnique de Madrid

### M. Ortega López, Florencio

- Consultant en sécurité (gestion des identités) chez SIA Group
- Consultant en TIC et sécurité en tant que professionnel indépendant
- Formateur d'enseignants dans le secteur de l'informatique
- Diplômé en ingénierie technique industrielle de l'université d'Alcalá de Henares
- Maîtrise pour les enseignants de l'UNIR (UNIR)
- MBA en gestion et administration des affaires de l'IDE-CESEM
- Maîtrise en gestion des technologies de l'information par IDE-CESEM
- Gestion certifiée de la sécurité de l'information (CISM) par l'ISACA

**M. Peralta Alonso, Jon**

- Consultant senior - Protection des données et cybersécurité. Altia
- Avocat / Conseiller juridique. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Conseiller juridique / Stagiaire. Bureau professionnel : Oscar Padura
- Diplôme en droit. Université publique du Pays basque
- Master en protection des données Délégué. EIS Innovative School
- Maîtrise en droit. Université publique du Pays basque
- Maîtrise spécialisée en pratique du contentieux civil. Université internationale Isabel I de Castille
- Chargé de cours pour le Master en protection des données personnelles, cybersécurité et droit des TIC



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

10

# Impact sur votre carrière

TECH est conscient de l'effort que doit fournir le gestionnaire pour assumer un certain degré de ces caractéristiques, c'est pourquoi il fait un effort particulier pour s'assurer que tous les contenus et le matériel pédagogique fournis répondent aux normes de qualité les plus élevées. Ainsi, la médiathèque à laquelle vous accédez constitue une référence exceptionnelle en matière de cybersécurité, et peut même être téléchargée dans son intégralité pour continuer à l'utiliser une fois le diplôme obtenu.

*Vous atteindrez la projection économique et professionnelle que vous recherchez grâce au soutien constant d'une équipe pédagogique et technique qui s'engage à vous amener au zénith du leadership en matière de politique de cybersécurité"*

*Inscrivez-vous dès maintenant à ce Mastère Spécialisé et n'attendez plus pour apporter un changement positif à votre environnement.*

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

Le Mastère Spécialisé en Gestion des Politiques de Cybersécurité dans l'Entreprise de TECH est un programme intensif qui prépare l'étudiant défis et aux décisions commerciales dans le domaine de la cybersécurité. Son principal objectif est de soutenir votre développement personnel et professionnel et de vous aider à réussir.

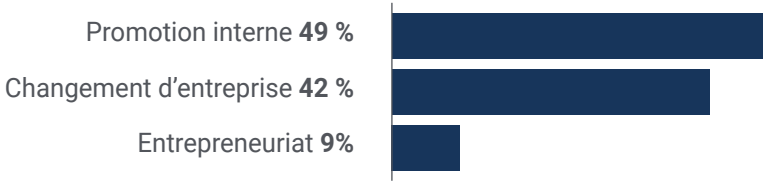
Si vous étude souhaitez améliorer vos compétences, réaliser un changement positif au niveau professionnel et interagir avec les meilleurs, vous êtes au bon programme.

*Vous obtiendrez l'amélioration de l'emploi que vous recherchez en moins de temps que vous ne le pensez grâce à la méthodologie pédagogique de TECH.*

### Le moment du changement

| Pendant le programme, le | Pendant la première année | Deux ans après |
|---|---|---|
| **11 %** | **63 %** | **26 %** |

### Type de changement



## Amélioration du salaire

L'achèvement de ce programme représente une augmentation de salaire de plus de **25,22%** pour nos étudiants.

| Salaire précédent | Augmentation du salaire de | Salaire suivant |
|---|---|---|
| **57.900 €** | **25,22%** | **72.500 €** |

11

# Bénéfices pour votre entreprise

Le Gestion des Politiques de Cybersécurité dans l'Entreprise contribue à élever le talent de l'organisation à son potentiel maximal par la formation de dirigeants de haut niveau.

De plus, rejoindre la communauté éducative TECH est une occasion unique d'accéder à un puissant réseau de contacts dans lequel vous pourrez trouver de futurs partenaires professionnels, clients ou fournisseurs.

*Les cybermenaces constituent l'une des plus grandes vulnérabilités auxquelles sont exposées les entreprises de tous types et de toutes tailles. Se spécialiser dans le domaine où l'avenir est le plus prometteur"*

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

01

### Accroître les talents et le capital intellectuel

### 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 capable de prendre des décisions en période d'incertitude et de crise, aidant ainsi 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 du Business Development de son entreprise.

06

### Augmentation de la compétitivité

Ce Mastère Spécialisé dotera vos professionnelles des compétences nécessaires pour relever de nouveaux défis et faire progresser l'organisation.

12

# Diplôme

Le Mastère Spécialisé Gestion des Politiques de Cybersécurité dans l'Entreprise garantit, outre la formation la plus rigoureuse et la plus actuelle, l'accès à un Mastère Spécialisé délivré par TECH Université Technologique.

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

Ce **Mastère Spécialisé en Gestion des Politiques de Cybersécurité dans l'Entreprise** 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 le diplôme de **Mastère Spécialisé** correspondant délivré par **TECH Université Technologique**

Le diplôme délivré par **TECH Université Technologique** attestera de la qualification obtenue dans le cadre du Mastère Spécialisé TECH 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 Gestion des Politiques de Cybersécurité dans l'Entreprise**

N.º d'Heures Officielles : **1.500 h.**


tech universidad tecnológica

Otorga la presente

CONSTANCIA

a

C. _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

MÁSTER TÍTULO PROPIO

en

Gestión de Políticas de Ciberseguridad en la Empresa

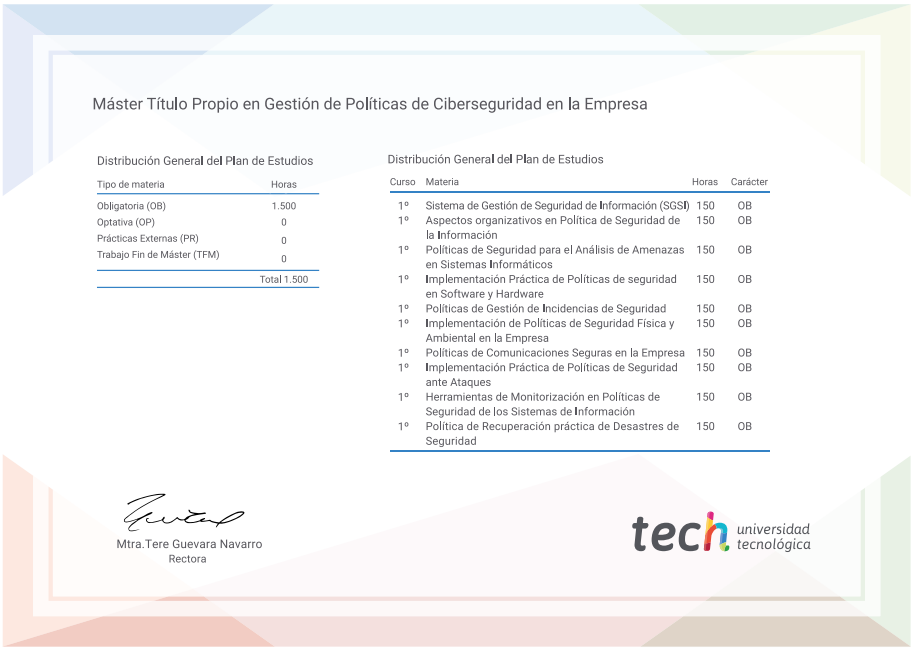
Se trata de un título propio de esta Universidad con una duración de 1.500 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH es una Institución Particular de Educación Superior reconocida por la Secretaría de Educación Pública a partir del 28 de junio de 2018.

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

código único TECH: AFWOR23S techtitute.com/titulos


Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa

Distribución General del Plan de Estudios

| Tipo de materia | Horas |
|---|---|
| Obligatoria (OB) | 1.500 |
| Optativa (OP) | 0 |
| Prácticas Externas (PR) | 0 |
| Trabajo Fin de Máster (TFM) | 0 |
| | Total 1.500 |

Distribución General del Plan de Estudios

| Curso | Materia | Horas | Carácter |
|---|---|---|---|
| 1º | Sistema de Gestión de Seguridad de Información (SGSI) | 150 | OB |
| 1º | Aspectos organizativos en Política de Seguridad de la Información | 150 | OB |
| 1º | Políticas de Seguridad para el Análisis de Amenazas en Sistemas Informáticos | 150 | OB |
| 1º | Implementación Práctica de Políticas de seguridad en Software y Hardware | 150 | OB |
| 1º | Políticas de Gestión de Incidencias de Seguridad | 150 | OB |
| 1º | Implementación de Políticas de Seguridad Física y Ambiental en la Empresa | 150 | OB |
| 1º | Políticas de Comunicaciones Seguras en la Empresa | 150 | OB |
| 1º | Implementación Práctica de Políticas de Seguridad ante Ataques | 150 | OB |
| 1º | Herramientas de Monitorización en Políticas de Seguridad de los Sistemas de Información | 150 | OB |
| 1º | Política de Recuperación práctica de Desastres de Seguridad | 150 | OB |

Mtra.Tere Guevara Navarro
Rectora

tech universidad tecnológica

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

tech université technologique

# Mastère Spécialisé
## Gestion des Politiques de Cybersécurité dans l'Entreprise

- Modalité: **en ligne**
- Durée: **12 mois**
- Qualification: **TECH Université Technologique**
- Intensité: **16h/semaine**
- Horaire: **à votre rythme**
- Examens: **en ligne**

# Mastère Spécialisé

## Gestion des Politiques de Cybersécurité dans l'Entreprise

tech université technologique