Certificat Avancé

Administration de la Sécurité des Technologies de l'Information

tech université technologique

tech université technologique

Certificat Avancé
Administration de la Sécurité des Technologies de l'Information

- Modalité: **en ligne**
- Durée: **6 mois**
- Qualification: **TECH Université Technologique**
- Intensité: **16h/semaine**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Accès au site web: www.techtitute.com/fr/informatique/diplome-universite/diplome-universite-administration-securite-technologies-information

Sommaire

01

Présentation

L'intégration des technologies de l'information dans de nombreuses entreprises a eu un effet collatéral: leurs risques en matière de sécurité informatique ont augmenté. Les entreprises doivent désormais être à l'affût des différentes attaques et vulnérabilités qui peuvent affecter leur bon fonctionnement et leurs services. C'est pourquoi il est essentiel de disposer dans l'entreprise d'un spécialiste chargé de gérer la sécurité de ces technologies. Ce programme offre aux professionnels la possibilité de se familiariser avec les méthodes de protection informatique les plus avancées dans ce domaine, puisqu'ils approfondiront des aspects tels que l'évaluation des risques en fonction de paramètres commerciaux, la gestion des identités et des accès ou les tests d'intrusion.

De plus en plus d'entreprises ont besoin de spécialistes de la gestion de la sécurité appliquée aux technologies de l'information. Ce programme vous permettra de progresser professionnellement en approfondissant des questions telles que le plan de continuité des activités associé à la sécurité"

C'est un fait: il n'y a pratiquement plus d'entreprises qui n'utilisent pas d'outils numériques et informatiques dans leurs processus internes. Les activités et les opérations telles que l'identification des employés, les systèmes logistiques ou les contacts avec les fournisseurs et les clients sont désormais principalement réalisées à l'aide des technologies de l'information. Mais ces technologies doivent faire l'objet d'une conception et d'une surveillance appropriées, car elles peuvent être exploitées pour obtenir des données ou accéder à des aspects sensibles de l'entreprise.

C'est pourquoi le spécialiste de l'administration de la sécurité est un poste de plus en plus demandé, qui ne peut être occupé par n'importe quel spécialiste en informatique. Il faut des connaissances très actualisées qui tiennent compte des derniers développements en matière de cybersécurité. Ainsi, ce Certificat Avancé a été conçu pour offrir aux professionnels les dernières avancées dans ce domaine, en approfondissant des questions telles que les audits de sécurité, la sécurité des équipements des terminaux, ou la réponse la plus efficace à différents incidents.

Ce programme est également développé dans un format 100% en ligne qui s'adapte aux circonstances du professionnel, lui permettant d'étudier quand, où et comme il le souhaite. Il disposera également d'un corps enseignant de grand prestige dans le domaine de la cybersécurité qui sera soutenu par de nombreuses ressources multimédias afin de rendre le processus d'apprentissage confortable, rapide et efficace.

Ce **Certificat Avancé en Administration de la Sécurité des Technologies de l'Information** contient le programme éducatif plus complet et le plus récent du marché. Ses principales caractéristiques sont:

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

Ce programme vous permettra d'approfondir des aspects tels que le cycle de vie d'un plan de Continuité des Activités ou la gestion des vulnérabilités"

TECH met à votre disposition les meilleures ressources multimédia: études de cas, activités théoriques-pratiques, vidéos, résumés interactifs, etc. Tout pour que le processus d'apprentissage soit agile et que vous puissiez tirer le meilleur parti de chaque minute investie"

Vous serez en mesure de répondre de manière appropriée à tous les types de menaces en matière de cybersécurité. Inscrivez-vous et devenez un grand spécialiste.

Étudiez à votre propre rythme, sans interruptions ni horaires rigides: la méthode d'enseignement de TECH est aussi pratique que cela.

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

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

La conception de ce programme est axée sur l'apprentissage par les problèmes, grâce auquel le professionnel doit essayer de résoudre les différentes situations de pratique professionnelle qui se présentent tout au long du cours académique. Pour ce faire, l'étudiant sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.

02

Objectifs

Compte tenu de la complexité croissante du domaine de la cybersécurité, l'objectif principal de ce Certificat Avancé en Administration de la Sécurité des Technologies de l'Information est de rapprocher les professionnels des développements les plus importants dans ce domaine. Vous pourrez ainsi devenir un grand spécialiste du domaine, capable de travailler à la gestion et à la direction de la cybersécurité d'entreprises de tous types de secteurs.

TECH vous aide à atteindre vos objectifs grâce à ce programme, avec lequel vous pourrez postuler à des postes professionnels importants dans les plus grandes entreprises nationales et internationales"

Objectifs généraux

- Développez un Systèmes de Gestion de Sécurité de l'Information (SGSI)
- Identifier les éléments clés qui composent un SMSI
- Évaluer les différents modèles d'architecture de sécurité afin d'établir le modèle le plus approprié pour l'organisation
- Identifier les cadres réglementaires d'application et leurs bases réglementaires
- Analyser la structure organisationnelle et fonctionnelle d'un secteur de sécurité de l'information (le bureau du CISO)
- Établir un programme d'audits pour couvrir les besoins d'auto-évaluation de l'organisation en matière de cybersécurité
- Développer un programme d'analyse et de surveillance des vulnérabilités et un plan de réponse aux incidents de cybersécurité
- Déterminer les éléments de base d'un plan de continuité des activités (PCA) en se basant sur la norme ISO-22301
- Examiner les risques découlant de l'absence d'un plan de continuité d'activité (PCA)
- Analyser les critères de réussite d'un PCA et son intégration dans la gestion globale des risques de l'entreprise
- Préciser les phases de mise en œuvre d'un plan de continuité des activités

Objectifs spécifiques

Module 1. Architectures et modèles de sécurité de l'information

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

Module 2. Gestion de la sécurité IT

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

Module 3. Plan de continuité des activités associé à la sécurité

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

Vous serez le principal spécialiste de la sécurité informatique dans votre environnement. N'attendez pas plus longtemps: inscrivez-vous maintenant"

03

Direction de la formation

Avoir à sa disposition les plus grands spécialistes internationaux de la gestion de la sécurité dans le domaine des technologies de l'information est une grande chance pour le professionnel. Et c'est exactement ce que propose cette université experte, qui dispose d'un corps enseignant composé d'ingénieurs et d'informaticiens prestigieux qui fourniront à l'étudiant les techniques et les procédures les plus avancées pour garantir la sécurité interne adéquate d'une entreprise.

Vous entrerez en contact avec les meilleurs spécialistes de la cybersécurité, qui vous donneront toutes les clés pour travailler au plus haut niveau dans ce domaine"

Direction

M. Olalla Bonal, Martín

- Spécialiste technique client Blockchain chez IBM
- Architecte *Blockchain*
- Architecte d'infrastructure dans le secteur bancaire
- Gestion de projet et mise en œuvre de solutions en production
- Technicien en Électronique Numérique
- Professeur: Formation *Hyperledger Fabric* pour les entreprises
- Professeur: Formation *Blockchain* en entreprise

Professeurs

M. Fernandez, Juan Luis

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

M. Embid Ruiz, Mario

- Avocat spécialisé dans le droit des TIC et de la protection des données
- Responsable juridique de Branddocs, SL, une entreprise technologique entreprise de solutions technologiques de confiance
- Diplôme de Droit et d'Administration des Activités de l'Université Rey Juan Carlos, Madrid
- Master en droit des nouvelles technologies, de l'Internet et de l'audiovisuel du Centre d'études Universitaires Villanueva et Cremades & Calvo Sotelo

M. Rodrigo, Juan Manuel

- Fondateur d'ISMET TECH S.L.
- Diplôme en Ingénierie de l'Université de Valladolid
- Master en Systèmes de Gestion Intégrée par CFE-CEU
- ISO 27001 Lead Auditor (IMQ)
- ISO 27001 Lead Implementor (IMQ)
- NATO Standards HPS (OTAN)

04

Structure et contenu

Le programme de ce Certificat Avancé en Administration de la Sécurité des Technologies de l'Information a été structuré en 3 module qui est développé sur 450 heures d'apprentissage. Pendant cette période, le professionnel approfondira les aspects pertinents de ce secteur tels que l'analyse forensique, les modèles de sécurité de l'information, le cadre réglementaire applicable dans ce domaine ou la configuration des règles de sécurité des réseaux, parmi de nombreuses autres questions.

Vous aurez à votre disposition le syllabus le plus complet, présenté à travers des ressources didactiques auxquelles vous pourrez accéder 24 heures sur 24"

Module 1. Architectures et modèles de sécurité de l'information

1.1. Architecture de sécurité de l'information
- 1.1.1. SGSI / PDS
- 1.1.2. Alignement stratégique
- 1.1.3. Gestion des risques
- 1.1.4. Mesure de la performance

1.2. Modèles de sécurité de l'information
- 1.2.1. Modèles de sécurités basé sur des politiques
- 1.2.2. Basés sur des politiques, les modèles de sécurité
- 1.2.3. Basés sur des outils de protection

1.3. Modèle de sécurité. Principaux éléments
- 1.3.1. Identification des risques
- 1.3.2. Définition des contrôles
- 1.3.3. Évaluation continue des niveaux de risque
- 1.3.4. Plan de sensibilisation des employés, fournisseurs, partenaires, etc.

1.4. Processus de gestion des risques
- 1.4.1. Identification des actifs
- 1.4.2. Identification des menaces
- 1.4.3. Évaluation des risques
- 1.4.4. Priorité des contrôles
- 1.4.5. Réévaluation et risque résiduel

1.5. Processus d'entreprise et sécurité de l'information
- 1.5.1. Processus d'activité
- 1.5.2. Évaluation des risques sur la base de paramètres commerciaux
- 1.5.3. Analyse de l'impact des activités
- 1.5.4. Les opérations d'entreprise et sécurité de l'information

1.6. Processus d'amélioration continue
- 1.6.1. Le cycle de Deming
  - 1.6.1.1. Planification
  - 1.6.1.2. Faire
  - 1.6.1.3. Vérifier
  - 1.6.1.4. Agir

1.7. Architectures de sécurité
- 1.7.1. Sélection et homogénéisation des technologies
- 1.7.2. Gestion de l'identité. Authentification
- 1.7.3. Gestion de l'accès. Autorisation
- 1.7.4. Sécurité de l'infrastructure des réseaux
- 1.7.5. Technologies et solutions de cryptage
- 1.7.6. Sécurité des dispositifs terminaux (EDR)

1.8. Le cadre réglementaire
- 1.8.1. Réglementations sectorielles
- 1.8.2. Certifications
- 1.8.3. Législation

1.9. La norme ISO 27001
- 1.9.1. Mise en œuvre
- 1.9.2. Certification
- 1.9.3. Contrôles et tests de pénétration
- 1.9.4. Gestion continue des risques
- 1.9.5. classification des informations

1.10. Législation sur la protection de la vie privée. RGPD (GDPR)
- 1.10.1. Portée du Règlement Général sur la Protection des Données (RGPD)
- 1.10.2. Données personnelles
- 1.10.3. Rôles dans le traitement des données personnelles
- 1.10.4 Droits d'ARCO
- 1.10.5. Le DPD. Fonctions

Module 2. Gestion de la sécurité IT

2.1. Gestion de la sécurité
- 2.1.1. Opérations de sécurité
- 2.1.2. Aspect juridique et réglementaire
- 2.1.3. Soutien aux entreprises
- 2.1.4. Gestion des risques
- 2.1.5. Gestion des identités et des accès

2.2. Structure de la zone de sécurité. Le bureau du CISO
- 2.2.1. Structure organisationnelle Position du CISO dans la structure
- 2.2.2. Les lignes de défense
- 2.2.3. Organigramme du bureau du CISO
- 2.2.4. Gestion du budget

2.3. Gouvernance de la sécurité
- 2.3.1. Comité de sécurité
- 2.3.2. Comité de suivi des risques
- 2.3.3. Comité de contrôle
- 2.3.4. Comité de crise

2.4. Gouvernance de la sécurité. Fonctions
- 2.4.1. Politiques et normes
- 2.4.2. Plan directeur de sécurité
- 2.4.3. Tableaux de bord
- 2.4.4. Sensibilisation et formation
- 2.4.5. Sécurité de la chaîne d'approvisionnement

2.5. Opérations de sécurité
- 2.5.1. Gestion des identités et des accès
- 2.5.2. Configuration des règles de sécurité du réseau. Firewalls
- 2.5.3. Gestion de la plateforme IDS/IPS
- 2.5.4. Analyse de vulnérabilité

2.6. Cadre de cybersécurité. NIST CSF
- 2.6.1. Méthodologie NIST
  - 2.6.1.1. Identifier
  - 2.6.1.2. Protéger
  - 2.6.1.3. Détecter
  - 2.6.1.4. Répondre
  - 2.6.1.5. Récupérer

2.7. Centre des opérations de sécurité (SOC). Fonctions
- 2.7.1. Protection. *Red Team, pentesting, threat intelligence*
- 2.7.2. Détection. SIEM, *user behavior analytics, fraud prevention*
- 2.7.3. Réponse

2.8. Contrôles de sécurité
- 2.8.1. Tests d'intrusion
- 2.8.2. Exercices de *red team*
- 2.8.3. Contrôles du code source. Développement sécurisé
- 2.8.4. Sécurité des composants (*software supply chain*)
- 2.8.5. Analyse médico-légale

2.9. Réponse aux incidents
- 2.9.1. Préparation
- 2.9.2. Détection, analyse et rapports
- 2.9.3. Confinement, éradication et récupération
- 2.9.4. Activité après l'incident
  - 2.9.4.1. Conservation des preuves
  - 2.9.4.2. Analyse médico-légale
  - 2.9.4.3. Gestion des lacunes
- 2.9.5. Lignes directrices officielles pour la gestion des cyberincidents

2.10. Gestion des vulnérabilités
- 2.10.1. Analyse de vulnérabilité
- 2.10.2. Évaluation de vulnérabilité
- 2.10.3. Base des systèmes
- 2.10.4. Les vulnérabilités de type "zero-day" *Zero-day*

Module 3. Plan de continuité des activités associé à la sécurité

3.1. Plan de continuité des activités
- 3.1.1. Planification de la continuité des activités (PCA)
- 3.1.2. Plan de continuité des activités (PCA). Aspects clés
- 3.1.3. Plan de continuité des activités (PCA) pour l'évaluation de l'entreprise

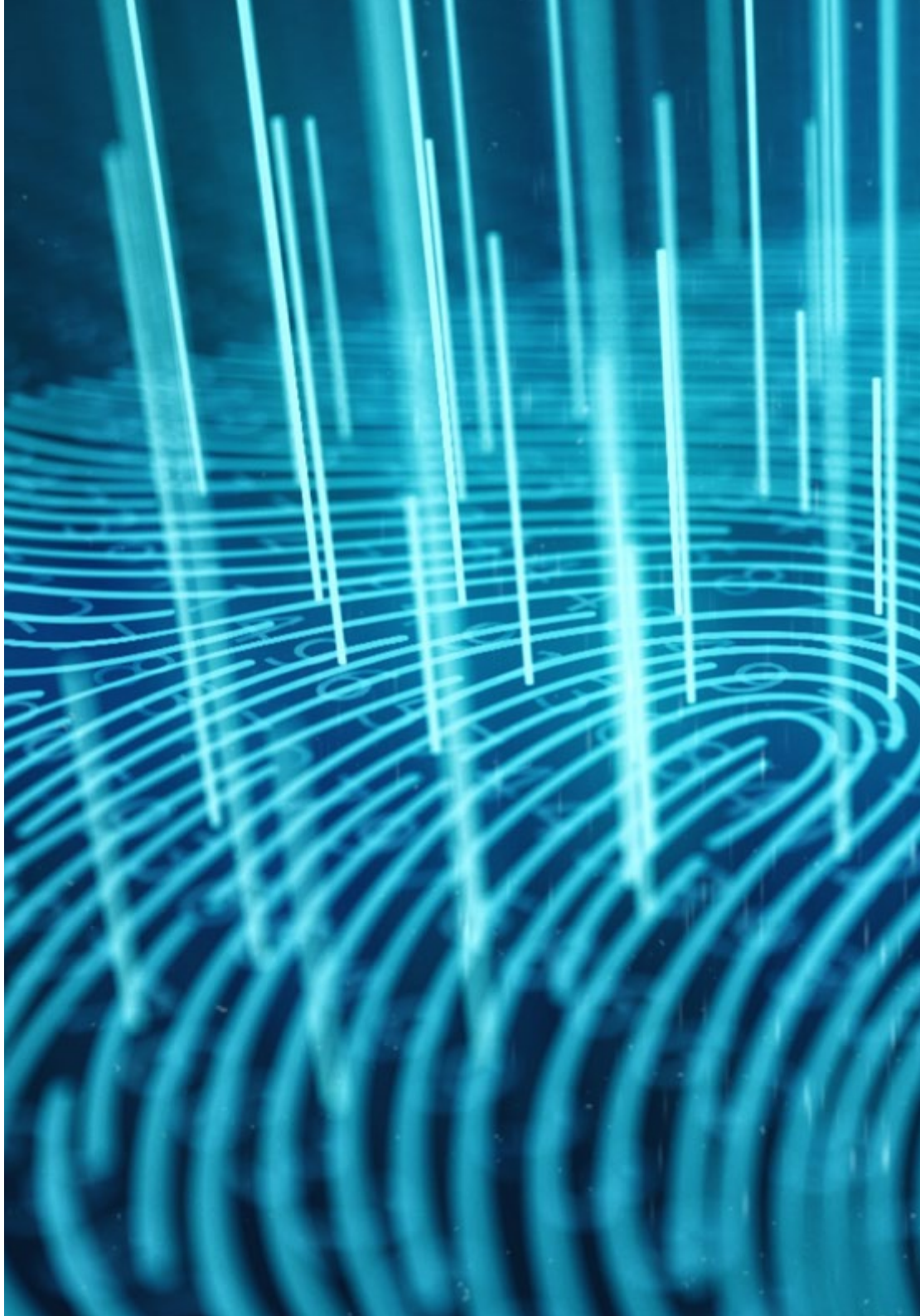
3.2. Mesures dans un plan de continuité des activités (PCA)
- 3.2.1. *Recovery Time Objective* (RTO) et *Recovery Point Objective* (RPO)
- 3.2.2. Durée maximale tolérable (DMT)
- 3.2.3. Niveaux de récupération minimum (ROL)
- 3.2.4. Objectif de point de récupération (RPO)

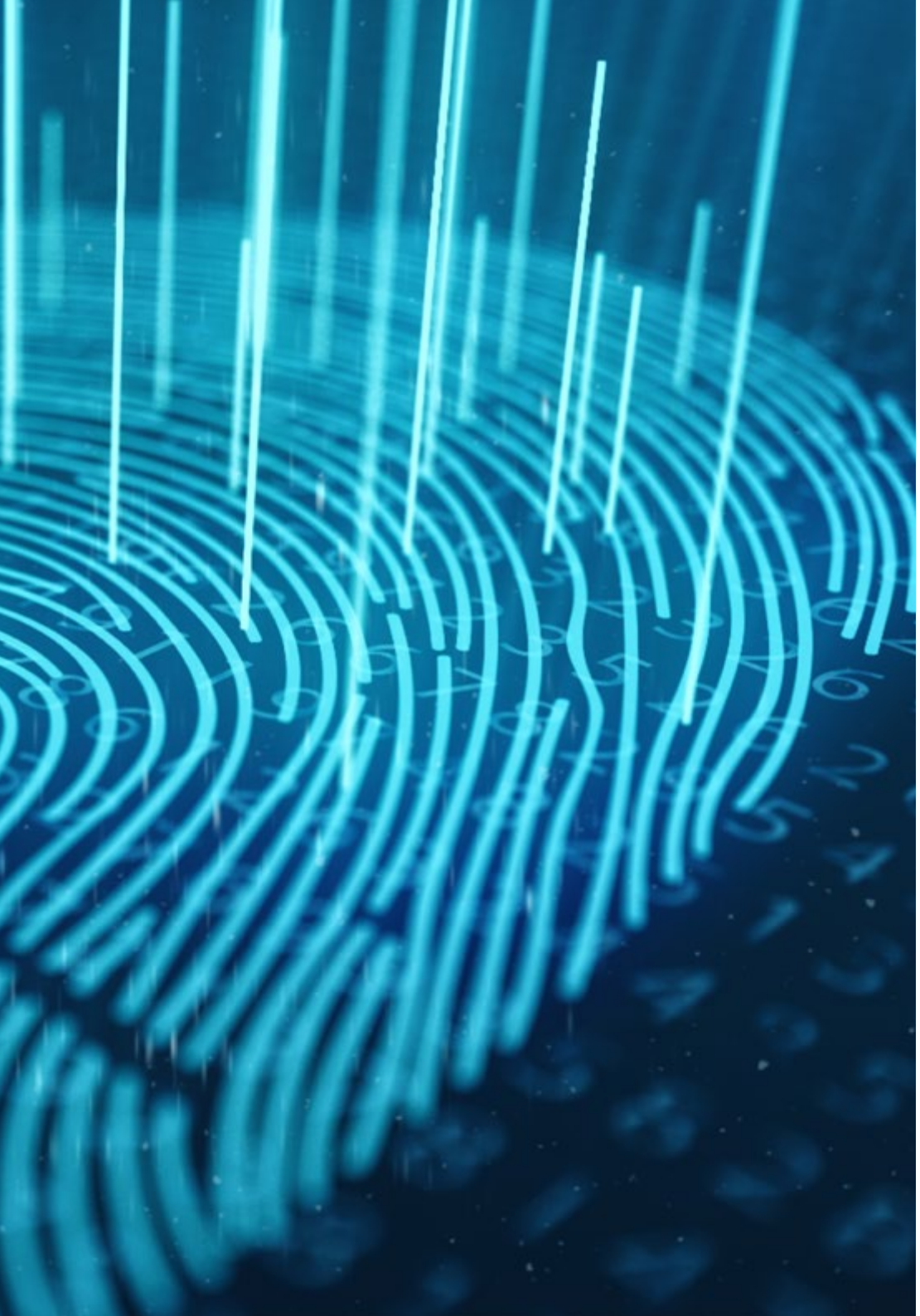
3.3. Projets de continuité. Typologie
- 3.3.1. Plan de continuité des activités (PCA)
- 3.3.2. Plan d' Continuité des PCTIC)
- 3.3.3. Plan de reprise après sinistre (PRS)

3.4. Gestion des risques associés au PCA
- 3.4.1. Analyse de l'impact des activités
- 3.4.2. Avantages de la mise en œuvre d'un PCA
- 3.4.3. Réflexion sur les risques

3.5. Cycle de vie d'un plan de continuité des activités
- 3.5.1. Phase 1: Analyse de l'organisation
- 3.5.2. Phase 2: Détermination de la stratégie de continuité
- 3.5.3. Phase 3: Réponse d'urgence
- 3.5.4. Phase 4: Tests, maintenance et révision

3.6. Phase d'analyse organisationnelle d'un PCA
- 3.6.1. Identification des processus dans le champ d'application du PCA
- 3.6.2. Identification des domaines d'activité critiques
- 3.6.3. Identification des dépendances entre les domaines et les processus
- 3.6.4. Détermination des MTD appropriées
- 3.6.5. Produits livrables Création d'un plan





3.7. Phase d'analyse Stratégie d' de continuité un PCA
- 3.7.1. Rôles dans la phase de détermination de la stratégie
- 3.7.2. Tâches de la phase de détermination de la stratégie
- 3.7.3. Produits livrables

3.8. Phase d'intervention d'urgence d'un PCA
- 3.8.1. Rôles dans la phase de réponse
- 3.8.2. Tâches dans cette phase
- 3.8.3. Produits livrables

3.9. Phase de test, de maintenance et de révision d'un PCA
- 3.9.1. Rôles dans la phase de test, de maintenance et de révision
- 3.9.2. Tâches de la phase de test, de maintenance et de révision
- 3.9.3. Produits livrables

3.10. Normes ISO associées aux plans de continuité des activités (PCA)
- 3.10.1. ISO 22301: 2019
- 3.10.2. ISO 22313: 2020
- 3.10.3. Autres normes ISO et internationales connexes

Ce programme vous permettra d'approfondir des questions telles que l'identification des dépendances entre les domaines et les processus, un aspect fondamental pour établir une cybersécurité correcte"

05

Méthodologie

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

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

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

Étude de Cas pour mettre en contexte tout le contenu

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

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

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

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

Une méthode d'apprentissage innovante et différente

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

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

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

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

Relearning Methodology

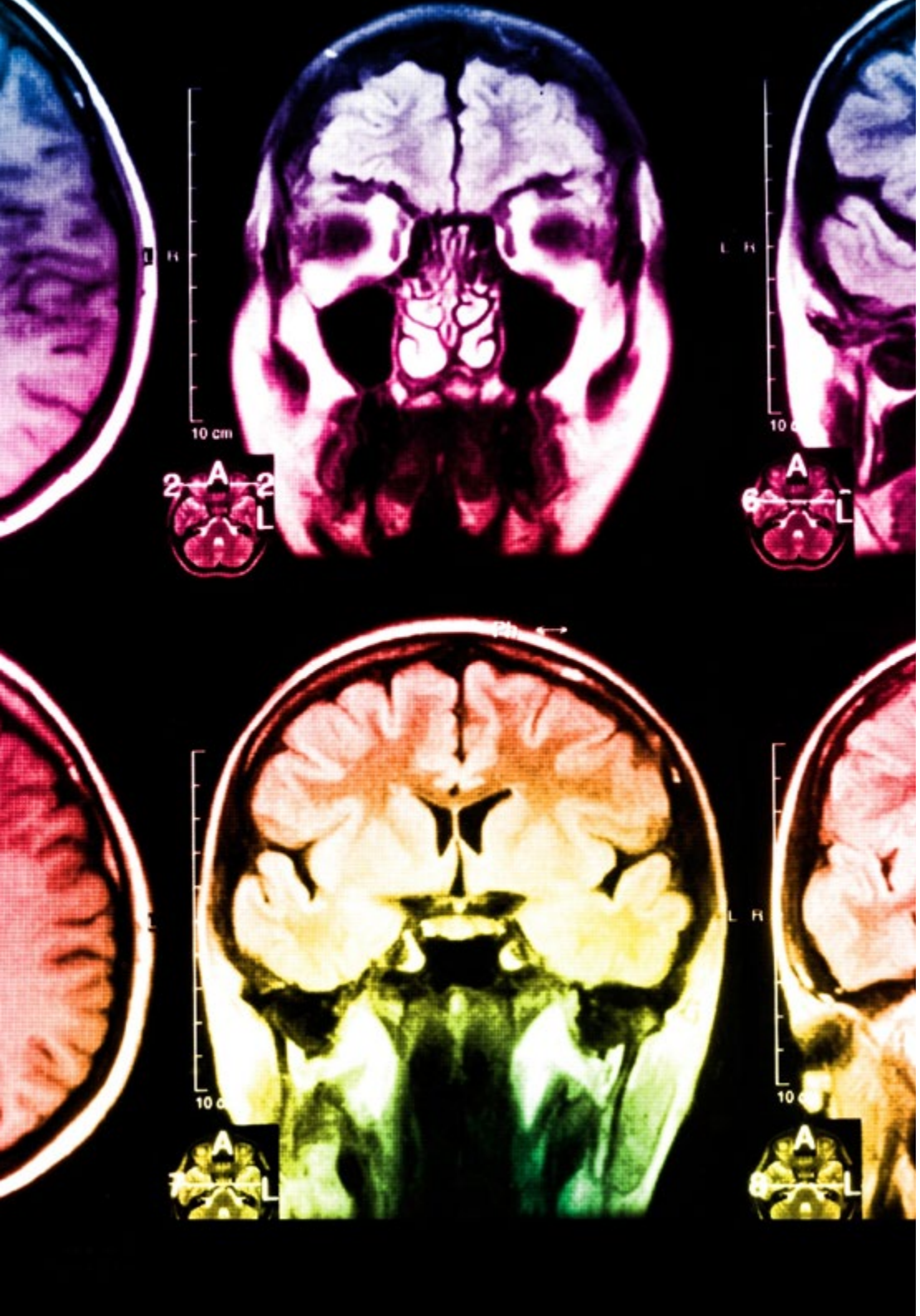
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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

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

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

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



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

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

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

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

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

Support d'étude

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

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

Cours magistraux

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

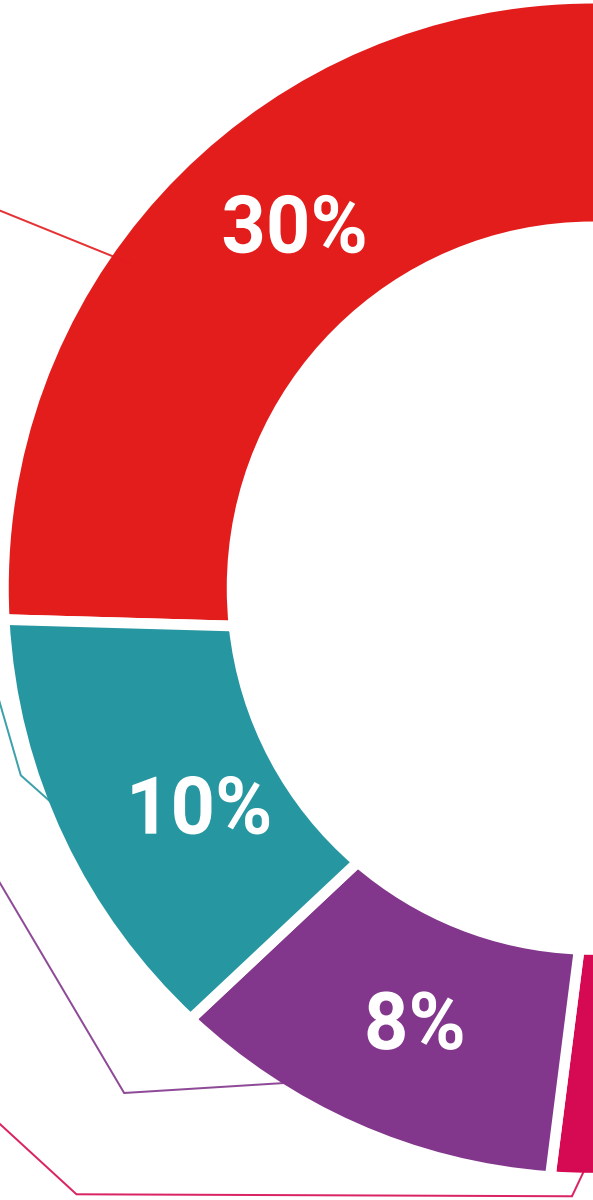
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

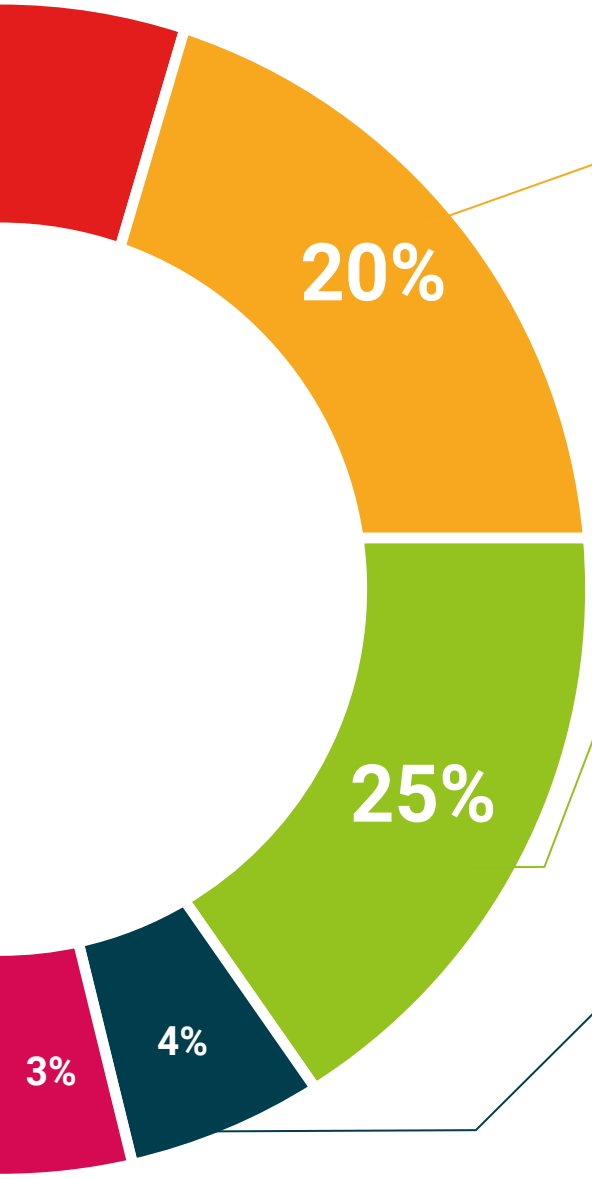
Pratiques en compétences et aptitudes

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

Lectures complémentaires

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





Case studies

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

Résumés interactifs

L'équipe TECH présente les contenus de manière attrayante et dynamique dans des pilules multimédia comprenant des audios, des vidéos, des images, des diagrammes et des cartes conceptuelles afin de renforcer les connaissances.

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

Testing & Retesting

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

06

Diplôme

Le Certificat Avancé en Administration de la Sécurité des Technologies de l'Information vous garantit, en plus de la formation la plus rigoureuse et la plus actuelle, l'accès à un diplôme universitaire de Certificat Avancé délivré par TECH Université Technologique.

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

Ce **Certificat Avancé en Direction de la Communication et de l'Identité Corporative** contient le programme le plus complet et le plus actuel du marché.

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

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

Diplôme: **Certificat Avancé en Administration de la Sécurité des Technologies de l'Information**

N.º d'heures Officielles: **450 h.**


tech université technologique

Délivre le présent

DIPLÔME

à

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

Pour avoir finalisé et accrédité avec succès le programme de

CERTIFICAT AVANCÉ

en

Administration de la Sécurité des Technologies de l'Information

Il s'agit d'un diplôme spécialisé octroyé par cette Université d'une durée de 450 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

Ce diplôme doit être impérativement accompagné d'un diplôme universitaire reconnu par les autorités compétentes pour exercer la profession dans chaque pays. Code Unique TECH: AFWOR23S techtitute.com/diplômes

*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

Certificat Avancé
Administration de la Sécurité des Technologies de l'Information

- Modalité: **en ligne**
- Durée: **6 mois**
- Qualification: **TECH Université Technologique**
- Intensité: **16h/semaine**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Certificat Avancé

Administration de la Sécurité des Technologies de l'Information

tech université technologique