

# Certificat Avancé

## Sécurité IT



## Certificat Avancé Sécurité IT

- » 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-securite-it](http://www.techtitute.com/fr/informatique/diplome-universite/diplome-universite-securite-it)

# Sommaire

01

Présentation

---

*page 4*

02

Objectifs

---

*page 8*

03

Direction de la formation

---

*page 12*

04

Structure et contenu

---

*page 16*

05

Méthodologie

---

*page 22*

06

Diplôme

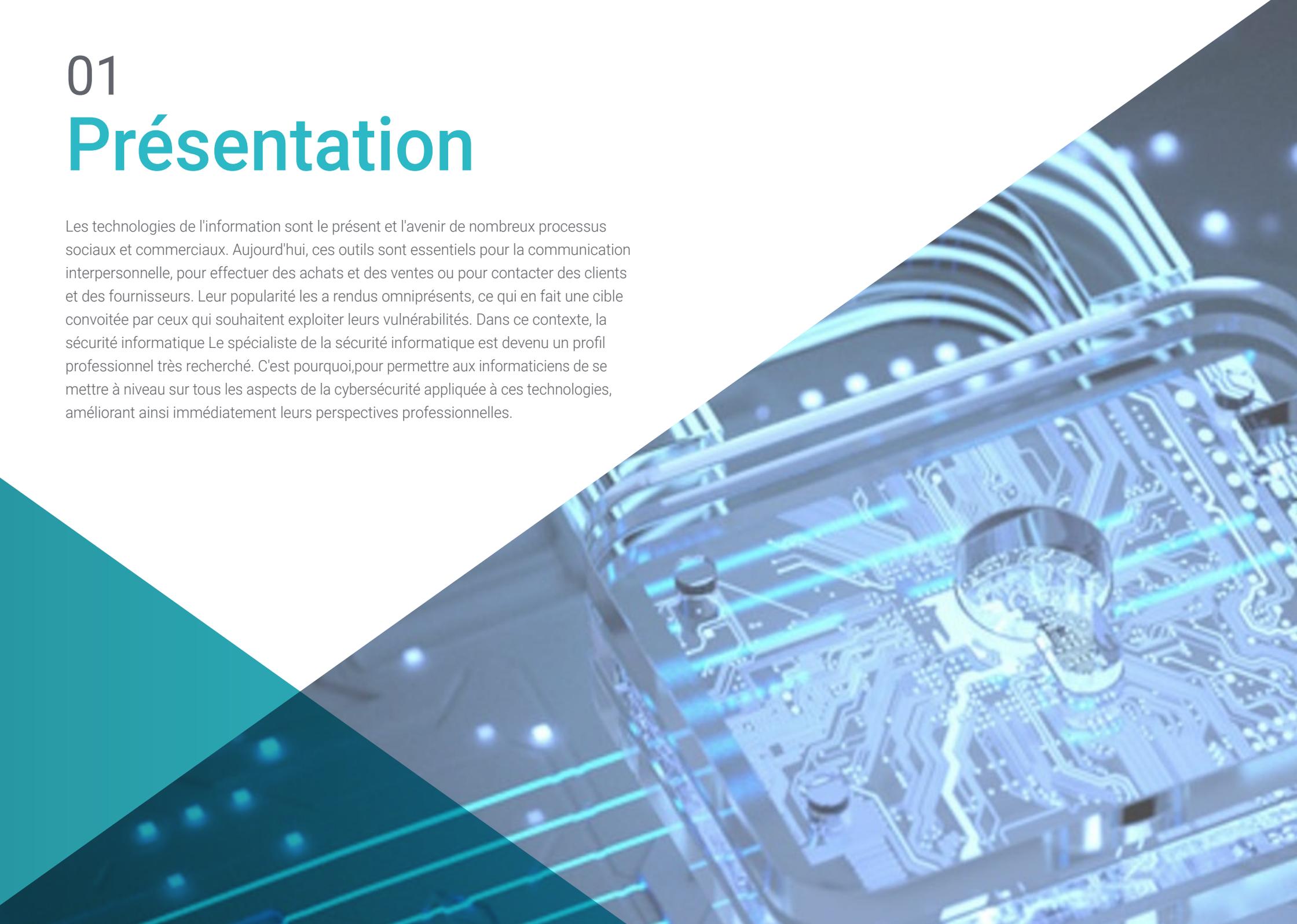
---

*page 30*

# 01

# Présentation

Les technologies de l'information sont le présent et l'avenir de nombreux processus sociaux et commerciaux. Aujourd'hui, ces outils sont essentiels pour la communication interpersonnelle, pour effectuer des achats et des ventes ou pour contacter des clients et des fournisseurs. Leur popularité les a rendus omniprésents, ce qui en fait une cible convoitée par ceux qui souhaitent exploiter leurs vulnérabilités. Dans ce contexte, la sécurité informatique Le spécialiste de la sécurité informatique est devenu un profil professionnel très recherché. C'est pourquoi, pour permettre aux informaticiens de se mettre à niveau sur tous les aspects de la cybersécurité appliquée à ces technologies, améliorant ainsi immédiatement leurs perspectives professionnelles.



“

*Ce programme vous permettra de vous spécialiser dans la Sécurité IT, ce qui vous donnera accès à de grandes opportunités de carrière dans un domaine de l'IT qui est de plus en plus demandé”*

Le nouveau contexte technologique exige que le professionnel aille plus loin afin de s'adapter aux transformations existantes en matière de Sécurité IT. Ainsi, ces technologies de l'information sont omniprésentes et sont utilisées dans tous les types de processus commerciaux et sociaux. Par conséquent, de nombreux aspects risquent d'être exposés à des vulnérabilités exploitables.

Cette situation préoccupe beaucoup les entreprises, qui voient à quel point une sécurité insuffisante peut mettre en péril leur activité. La solution est donc d'engager La solution consiste donc à engager des professionnels spécialisés dans ce domaine. C'est pourquoi l'informaticien spécialisé dans la Sécurité IT est actuellement l'un des profils les plus recherchés et les plus appréciés par les entreprises de différents domaines et secteurs.

C'est pour répondre à cette demande qu'est présenté ce Certificat Avancé, qui se développe à travers un format 100% en ligne, et qui dispose d'un corps enseignant d'un énorme prestige international dans ce domaine de la cybersécurité. En outre, ce programme présente ses contenus sous différents formats multimédias: résumés interactifs, vidéos, études de cas, master classes, vidéos, études de cas, master classes, activités pratiques, etc. Le tout dans le but de fournir aux professionnels les derniers développements en matière de sécurité appliquée aux technologies de l'information.

Ce **Certificat Avancé en Sécurité IT** contient le programme le plus complet et le plus à jour 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
- ♦ Des cours théoriques, des questions à l'expert, des forums de discussion sur des sujets controversés et un travail de réflexion individuel
- ♦ Il est possible d'accéder aux contenus depuis tout appareil fixe ou portable doté d'une connexion à internet.



*Ce programme vous permettra d'approfondir les aspects pertinents de la Sécurité IT tels que le développement sécurisé dans les communications et l'exploitation des softwares"*

“

*Le système d'enseignement 100% en ligne de TECH vous permettra de combiner votre travail avec vos études, car il s'adapte à toutes vos circonstances personnelles et professionnelles"*

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'entraîner 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.

*Le corps enseignant de ce programme est composé de professionnels actifs qui connaissent tous les derniers développements dans ce domaine de la cybersécurité.*

*Votre profil professionnel s'améliorera une fois que vous aurez terminé ce Certificat Avancé, qui est enseigné à l'aide de nombreuses ressources multimédia.*



# 02 Objectifs

L'objectif principal de ce Certificat Avancé en Sécurité IT est de fournir aux professionnels les meilleurs outils pour pouvoir s'adapter au nouveau contexte informatique, transformé par le processus de numérisation qui s'est étendu à tous les domaines de la société. Ainsi, vous serez dans la meilleure position pour travailler en tant que spécialiste de la cybersécurité dans toute entreprise qui souhaite protéger ses activités contre les nouvelles menaces informatiques.



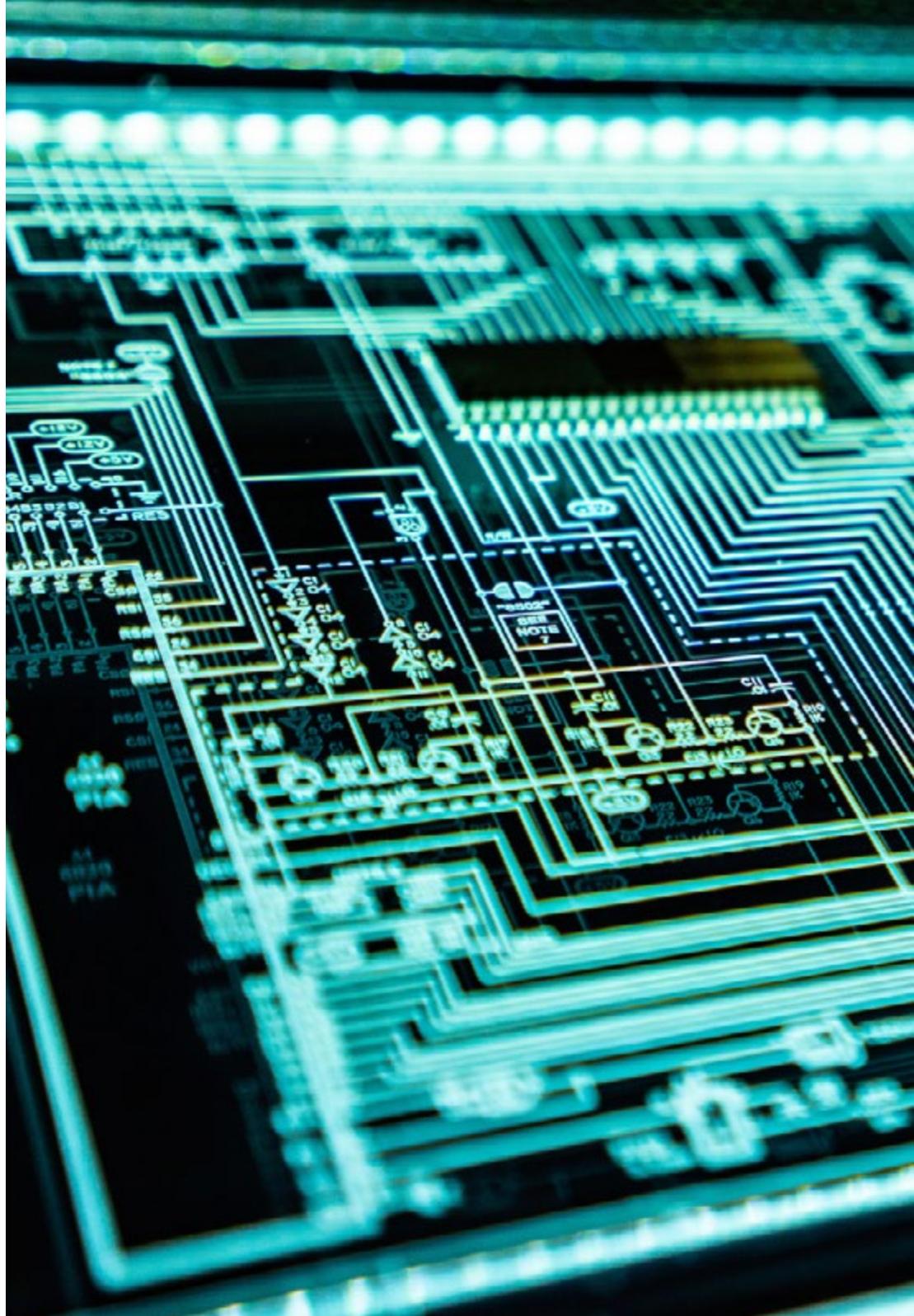
“

*L'objectif de TECH est de vous fournir les connaissances les plus récentes afin que vous puissiez réaliser votre travail avec le maximum de garanties, faisant de vous un professionnel de référence dans le secteur"*



## Objectifs généraux

- ◆ Générer des connaissances spécialisées sur un système d'information, les types et les aspects de sécurité à prendre en compte. les aspects de sécurité à prendre en compte
- ◆ Identifier les vulnérabilités d'un système d'information
- ◆ Appliquer les mesures de sécurité les plus appropriées en fonction des menaces
- ◆ Développer les réglementations légales et la typification de la criminalité en s'attaquant à un système d'information
- ◆ Déterminer la politique et le plan de sécurité dans le système d'information d'une entreprise, achever la conception et la mise en œuvre du plan d'urgence
- ◆ Générer des connaissances spécialisées sur l'écosystème de la sécurité informatique
- ◆ Évaluer les connaissances en matière de cybersécurité
- ◆ Développer les meilleures pratiques en matière de développement sécurisé
- ◆ Présenter les risques pour les entreprises de ne pas avoir mis en place un environnement de sécurité informatique
- ◆ Examiner le processus de conception d'une stratégie de sécurité lors du déploiement de services de *Cloud* d'entreprise
- ◆ Identifier les domaines de sécurité dans le *Cloud*
- ◆ Analyser les services et les outils dans chacun des domaines de sécurité
- ◆ Évaluer les différences dans les implémentations spécifiques des différents fournisseurs de *Cloud* publics





## Objectifs spécifiques

---

### Module 1. Sécurité dans la conception et le développement des systèmes

- ♦ Évaluer la sécurité d'un système d'information dans toutes ses composantes et couches
- ♦ Identifier les types actuels de menaces pour la sécurité et leurs tendances
- ♦ Établir des directives de sécurité en définissant politiques et plans de sécurité et d'urgence
- ♦ Analyser les stratégies et les outils permettant de garantir l'intégrité et la sécurité des systèmes d'information
- ♦ Appliquer des techniques et des outils spécifiques pour chaque type d'attaque ou de vulnérabilité de sécurité
- ♦ Protéger les informations sensibles stockées dans le système d'information
- ♦ Disposer du cadre juridique et de la typologie du crime, en complétant la vision par la typologie du délinquant et de sa victime

### Module 2. Sécurité des communications et de l'exploitation du software

- ♦ Développer des connaissances spécialisées en matière de sécurité physique et logique
- ♦ Démontrer une connaissance des communications et des réseaux
- ♦ Identifier les principales attaques malveillantes
- ♦ Établir un cadre de développement sécurisé
- ♦ Démontrer une compréhension des principales réglementations relatives aux systèmes de gestion de la sécurité de l'information
- ♦ Démontrer le bien-fondé de l'exploitation d'un centre opérationnel de cybersécurité
- ♦ Démontrer l'importance des pratiques de cyber-sécurité pour les catastrophes organisationnelles

### Module 3. Sécurité dans les environnements *Cloud*

- ♦ Identifier les risques liés au déploiement d'une infrastructure de *Cloud* publique
- ♦ Définir les exigences de sécurité
- ♦ Élaborer un plan de sécurité pour un déploiement dans le *Cloud*
- ♦ Identifier les services *Cloud* à déployer pour l'exécution d'un plan de sécurité
- ♦ Déterminer les exigences opérationnelles des mécanismes de prévention
- ♦ Établir des lignes directrices pour un système *Logging* et de suivi
- ♦ Proposer des actions de réponse aux incidents



*Vous pourrez progresser rapidement sur le plan professionnel, car vos nouvelles connaissances feront de vous un spécialiste très recherché*

# 03

## Direction de la formation

La sécurité des technologies de l'information est un domaine en constante évolution, qui nécessite des connaissances de pointe que seul un professionnel en exercice peut fournir. C'est pourquoi TECH s'est efforcé de confier l'enseignement du programme à des spécialistes prestigieux dans ce domaine, offrant à l'étudiant les meilleures compétences pour se développer efficacement dans la conception de la protection de toute entreprise.





“

*Ce programme est ce dont vous avez besoin: vous aurez à portée de main les meilleurs spécialistes de la Sécurité IT au niveau international"*

## 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. Nogales Avila, Javier

- ◆ Enterprise Cloud and sourcing senior consultant. Quint
- ◆ Cloud and Technology Consultant. Indra
- ◆ Associate Technology Consultant. Accenture
- ◆ Diplômé de l'Université de Jaén et de l'Université de Technologie et d'Économie de Budapest (BME)
- ◆ Diplôme d'ingénieur en Gestion Industrielle

### M. Gómez Rodríguez, Antonio

- ◆ Ingénieur en solutions Cloud chez Oracle
- ◆ Directeur de projet chez Sopra Group
- ◆ Directeur de projet chez Everis
- ◆ Chef de projet chez Empresa pública de Gestion de Programas Culturales Ministère andalou de la culture
- ◆ Analyste des systèmes d'information Sopra Group
- ◆ Diplôme d'ingénieur en télécommunications de l'Université polytechnique de Catalogne
- ◆ Diplômé en technologies et systèmes d'information, Institut catalan de technologie.
- ◆ Master E-Business, La Salle Business School

### Mme Jurado Jabonero, Lorena

- ◆ Responsable de la sécurité de l'information (CISO) au Groupe Pascual
- ◆ Diplômé en Ingénierie informatique de l'Université Alfonso X El Sabio
- ◆ Ingénieur Technique en Informatique de gestion de l'Université Polytechnique de Madrid
- ◆ Connaissances: ISO 27001, ISO 27701, ISO 22301, ISO 20000, RGPD/LOPDGDD, NIST CSF, CSA, ITIL, PCI, etc.

# 04

## Structure et contenu

Afin d'atteindre les objectifs proposés, ce Certificat Avancé en Sécurité IT a été divisé en 3 modules spécialisés, qui peuvent être complétés sur 450 heures d'apprentissage. Ainsi, tout au long de ce programme, l'informaticien pourra se familiariser avec les dernières avancées en matière de sécurité informatique dans les communications et l'exploitation des logiciels, la sécurité dans les environnements de *Cloud Computing*, la sécurité des systèmes de stockage ou des systèmes d'autorisation, parmi de nombreux autres aspects pertinents dans ce domaine.



“

*Ce programme vous permettra d'appliquer  
les meilleures techniques d'analyse  
forensique appliquées à la Sécurité IT"*

## Module 1. Sécurité dans la conception et le développement des systèmes

- 1.1. Systèmes d'information
  - 1.1.1. Domaines de systèmes d'information
  - 1.1.2. Composants de systèmes d'information
  - 1.1.3. Activités de systèmes d'information
  - 1.1.4. Cycle de vie de systèmes d'information
  - 1.1.5. Ressources de systèmes d'information
- 1.2. Systèmes d'information. Typologie
  - 1.2.1. Types des systèmes d'information
    - 1.2.1.1 Entreprise
    - 1.2.1.2 Stratégiques
    - 1.2.1.3 Selon le champ d'application
    - 1.2.1.4 Spécifiques
  - 1.2.2. Systèmes d'information. Exemples concrets
  - 1.2.3. Évolution des systèmes d'information: étapes
  - 1.2.4. Méthodologies des systèmes d'information
- 1.3. Sécurité des systèmes d'information. Implications juridiques
  - 1.3.1. Accès aux données
  - 1.3.2. Menaces pour la sécurité: vulnérabilités
  - 1.3.3. Implications juridiques: infractions pénales
  - 1.3.4. Procédures de maintenance des systèmes d'information
- 1.4. Sécurité des systèmes d'information. Protocole de sécurité
  - 1.4.1. Sécurité de systèmes d'information
    - 1.4.1.1 Intégration
    - 1.4.1.2 Confidentialité
    - 1.4.1.3 Disponibilité
    - 1.4.1.4 Authentification
  - 1.4.2. Services de sécurité
  - 1.4.3. Protocoles de sécurité de l'information. Typologie
  - 1.4.4. Sensibilité de systèmes d'information
- 1.5. Sécurité des systèmes d'information Mesures et systèmes de contrôle d'accès
  - 1.5.1. Mesures de sécurité
  - 1.5.2. Type de mesures de sécurité
    - 1.5.2.1 Prévention
    - 1.5.2.2 Détection
    - 1.5.2.3 Correction
  - 1.5.3. Systèmes de contrôle de Accès Typologie
  - 1.5.4. Cryptographie
- 1.6. Sécurité des réseaux et de l'internet
  - 1.6.1. *Firewalls*
  - 1.6.2. Identification numérique
  - 1.6.3. Virus et vers
  - 1.6.4. *Hacking*
  - 1.6.5. Exemples et cas réels
- 1.7. Délits informatiques
  - 1.7.1. Délit informatique
  - 1.7.2. Délits informatiques Typologie
  - 1.7.3. Délit informatique Ataque. Typologies
  - 1.7.4. Le cas de la réalité virtuelle
  - 1.7.5. Profils des délinquants et des victimes. Qualification pénale de l'infraction
  - 1.7.6. Délits informatiques Exemples et cas réels
- 1.8. Plan de sécurité d'un système d'information
  - 1.8.1. Plan de sécurité. Objectifs
  - 1.8.2. Plan de sécurité. Planification
  - 1.8.3. Plan de risques. Analyse
  - 1.8.4. Politique de sécurité. Mise en œuvre dans l'organisation
  - 1.8.5. Plan de sécurité. Mise en œuvre dans l'organisation
  - 1.8.6. Procédures de sécurité. Types
  - 1.8.7. Plan de sécurité. Exemples

- 1.9. Plan d'urgence
  - 1.9.1. Plan d'urgence. Fonctions
  - 1.9.2. Plan d'urgence: éléments et objectifs
  - 1.9.3. Plans des imprévu dans l'organisation. Mise en œuvre
  - 1.9.4. Plans d'intervention. Exemples
- 1.10. Gouvernance de la sécurité de systèmes d' information
  - 1.10.1. Réglementation juridique
  - 1.10.2. Normes
  - 1.10.3. Certifications
  - 1.10.4. Technologies

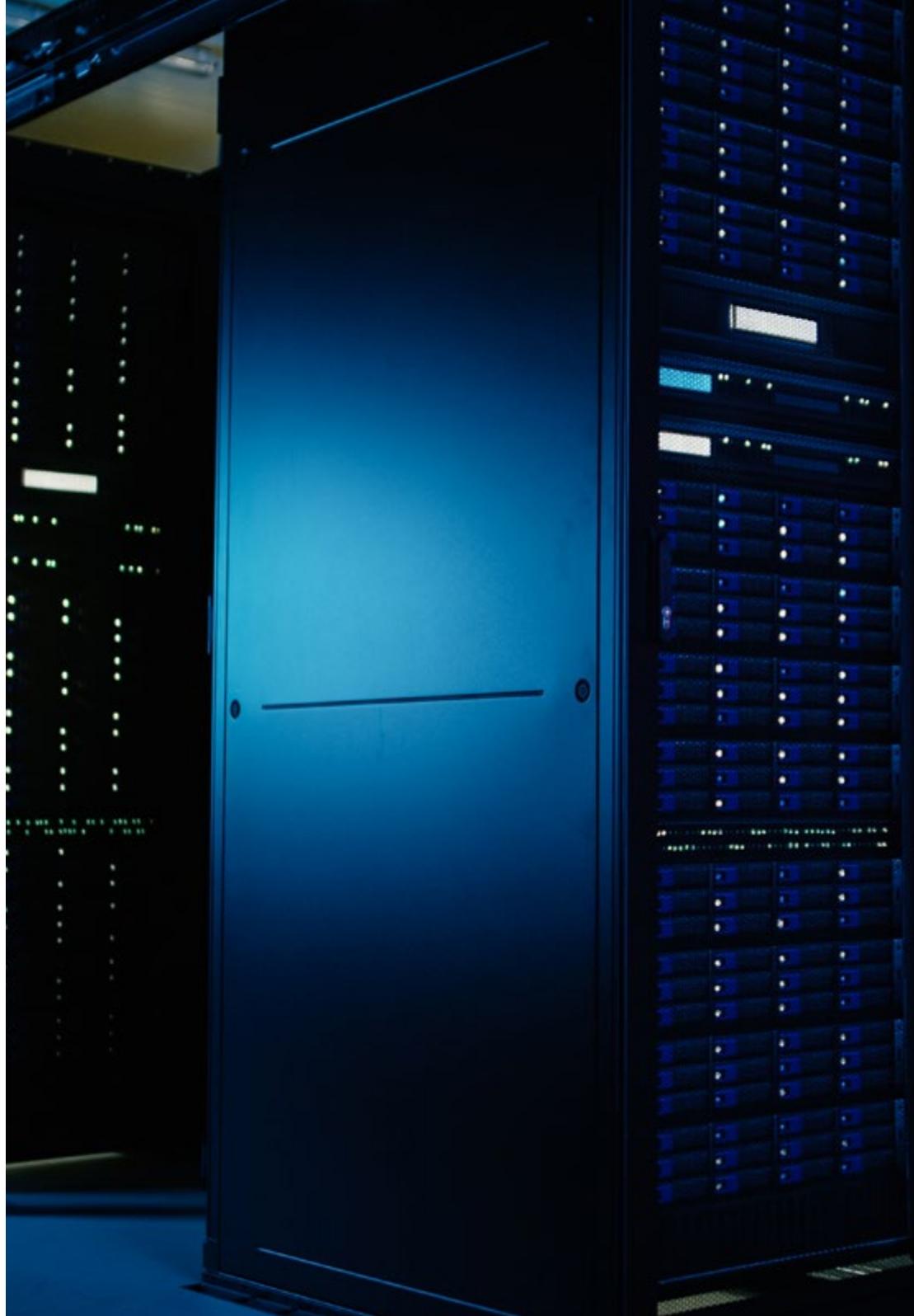
## Module 2. Sécurité des communications et de l'exploitation du software

- 2.1. Sécurité informatique dans les communications et l'exploitation des logiciels
  - 2.1.1. Sécurité informatique
  - 2.1.2. Cybersécurité
  - 2.1.3. Sécurité du cloud
- 2.2. Sécurité informatique dans les communications et l'exploitation des logiciels. Typologie
  - 2.2.1. Sécurité physique
  - 2.2.2. Sécurité logique
- 2.3. Sécurité des communications
  - 2.3.1. Principaux éléments
  - 2.3.2. Sécurité des réseaux
  - 2.3.3. Meilleures pratiques
- 2.4. Cyber intelligence
  - 2.4.1. Ingénierie sociale
  - 2.4.2. *Deep web*
  - 2.4.3. *Phishing*
  - 2.4.4. *Malware*

- 2.5. Développement Sécurité des communications et de l'exploitation du software
  - 2.5.1. Développement sécurisé Protocole HTTP
  - 2.5.2. Développement sécurisé Cycle de vie
  - 2.5.3. Développement sécurisé Sécurité PHP
  - 2.5.4. Développement sécurisé Sécurité NET
  - 2.5.5. Développement sécurisé Meilleures pratiques
- 2.6. Systèmes de gestion de la sécurité de l'information des communications et de l'exploitation du software
  - 2.6.1. RGPD
  - 2.6.2. ISO 27021
  - 2.6.3. ISO 27017/ 18
- 2.7. Technologies SIEM
  - 2.7.1. Technologies SIEM
  - 2.7.2. Fonctionnement du SOC
  - 2.7.3. SIEM *Vendors*
- 2.8. Le rôle de la sécurité dans les organisations
  - 2.8.1. Rôles dans les organisations
  - 2.8.2. Rôle des spécialistes de l'IdO dans les entreprises
  - 2.8.3. Certifications reconnues sur le marché
- 2.9. Analyse médico-légale
  - 2.9.1. Analyse médico-légale
  - 2.9.2. Analyse médico-légale Méthodologie
  - 2.9.3. Analyse médico-légale Outils et mise en œuvre
- 2.10. La Cybersécurité aujourd'hui
  - 2.10.1. Cyberattaques majeures
  - 2.10.2. Prévisions d'employabilité
  - 2.10.3. Défis

### Module 3. Sécurité dans les environnements *Cloud*

- 3.1. Sécurité dans les environnements *Cloud computing*
  - 3.1.1. Sécurité dans les environnements *Cloud Computing*
  - 3.1.2. Sécurité dans les environnements *Cloud computing*. Menaces et risques pour la sécurité
  - 3.1.3. Sécurité dans les environnements *Cloud computing*. Principaux aspects de la sécurité
- 3.2. Types d'infrastructures en *Cloud*
  - 3.2.1. Public
  - 3.2.2. Privé
  - 3.2.3. Hybride
- 3.3. Modèle de gestion partagée
  - 3.3.1. Éléments de sécurité gérés par le fournisseur
  - 3.3.2. Éléments gérés par le client
  - 3.3.3. Définition de la stratégie de sécurité
- 3.4. Mécanismes de prévention
  - 3.4.1. Systèmes de gestion de l'authentification
  - 3.4.2. Système de gestion des autorisations: politiques d'accès
  - 3.4.3. Systèmes de gestion des clés
- 3.5. Sécurisation du système
  - 3.5.1. Sécurisation des systèmes de stockage
  - 3.5.2. Sécurisation des systèmes de bases de données
  - 3.5.3. Sécuriser les données en transit
- 3.6. Protection des infrastructures
  - 3.6.1. Conception et mise en œuvre de réseaux sécurisés
  - 3.6.2. Sécurité des ressources informatiques
  - 3.6.3. Outils et ressources pour la protection des infrastructures



- 3.7. Détection des menaces et des attaques
  - 3.7.1. Systèmes de contrôle, *Logging* d'enregistrement et de surveillance
  - 3.7.2. Systèmes de événements et d'alarmes
  - 3.7.3. Systèmes SIEM
- 3.8. Réponse aux incidents
  - 3.8.1. Plan de réponse aux incidents
  - 3.8.2. Continuité des activités
  - 3.8.3. Analyse médico-légale et remédiation d'incidents de même nature
- 3.9. La sécurité en *Clouds* publics
  - 3.9.1. AWS(Amazon Web Services)
  - 3.9.2. Microsoft Azure
  - 3.9.3. Google &GCP
  - 3.9.4. Oracle Cloud
- 3.10. Réglementation et conformité
  - 3.10.1. Conformité en matière de sécurité
  - 3.10.2. Gestion des risques
  - 3.10.3. Personnes et processus dans les organisations

“ *Le programme d'études le plus complet et le plus récent du marché est désormais à votre portée. Inscrivez-vous, vous ne le regretterez pas*”

# 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.*

t

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.



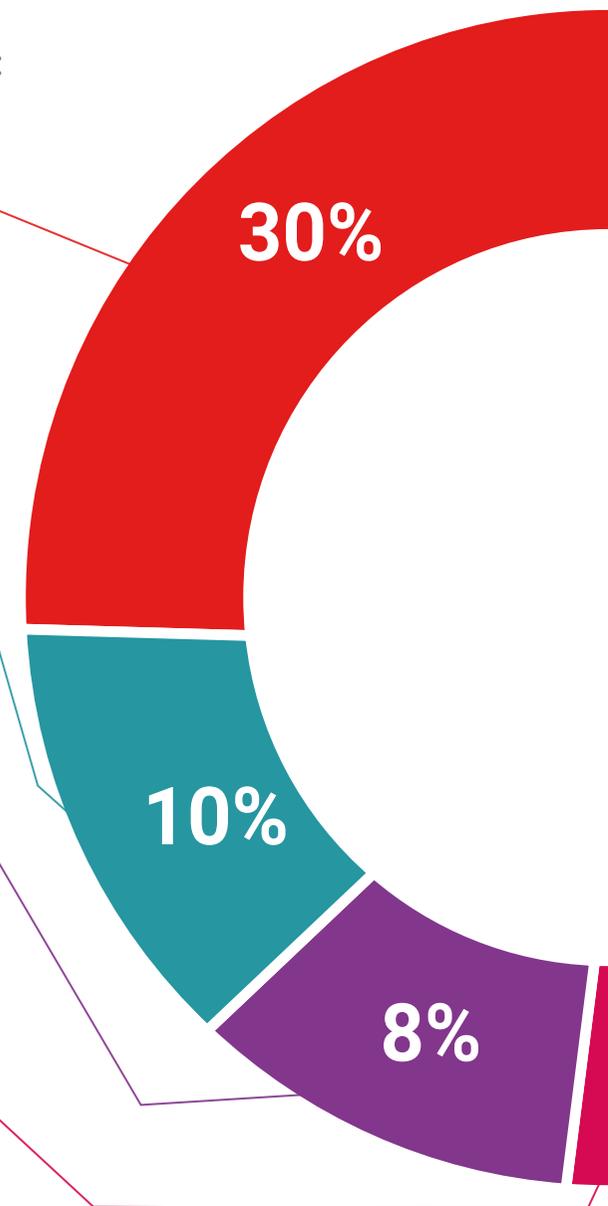
#### Pratiques en compétences et aptitudes

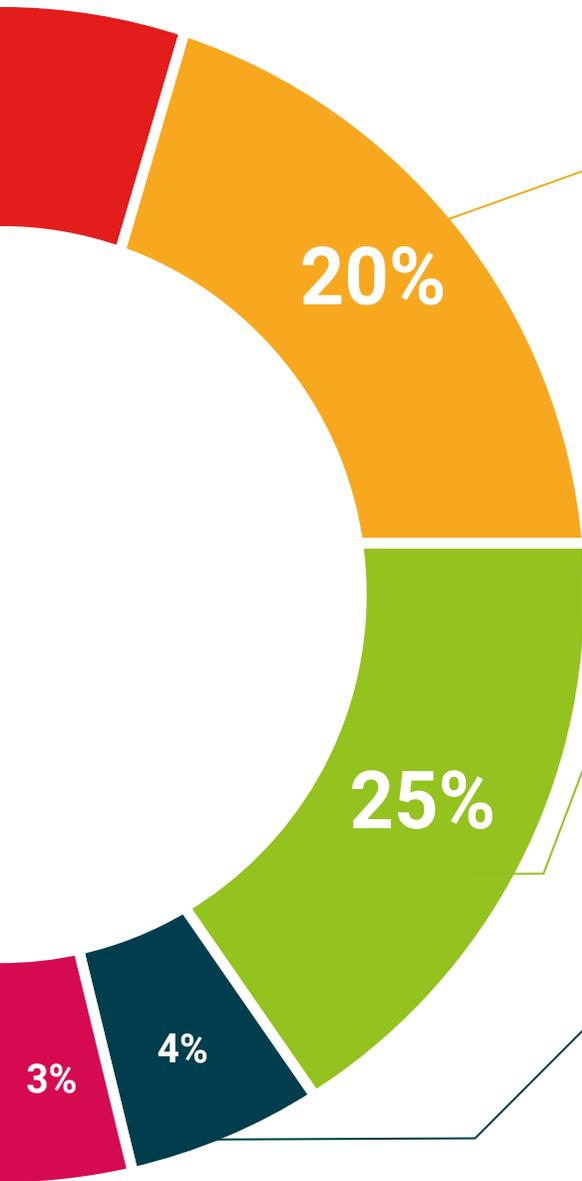
Les étudiants réaliseront des activités visant à développer des compétences et des aptitudes spécifiques dans chaque domaine. Des activités pratiques et dynamiques pour acquérir et développer les compétences et aptitudes qu'un spécialiste doit développer dans le cadre de la mondialisation dans laquelle 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 Sécurité IT, 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 Sécurité IT** 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 en Sécurité IT** délivré par **TECH Université Technologique**.

Le diplôme délivré par **TECH Université Technologique** indiquera la qualification obtenue dans le 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 Sécurité IT**

N.º d'heures Officielles: **450 h.**



\*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.

future  
santé confiance personnes  
éducation information tuteurs  
garantie accréditation enseignement  
institutions technologie apprentissage  
communauté engagement  
service personnalisé innovation  
connaissance présent qualité  
en ligne formation  
développement institutions  
classe virtuelle langues

**tech** université  
technologique

Certificat Avancé

Sécurité IT

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

# Certificat Avancé

## Sécurité IT