

Certificat Avancé

Gestion des Menaces de Sécurité Informatique



Certificat Avancé Gestion des Menaces de Sécurité Informatique

- » 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-gestion-menaces-securite-informatique

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

Une enquête du Forum Économique Mondial révèle que les attaques de *Ransomware* contre les entreprises ont augmenté de 150% en 2021, par rapport à l'année précédente. Une menace qui touche aussi bien les grandes entreprises, les institutions que les petites entreprises opérant en ligne. Ce contexte nécessite la mise en œuvre correcte d'un Système de Gestion de la Sécurité de l'Information (SGSI). Ce programme 100% en ligne fournit aux professionnels de l'informatique des connaissances spécifiques dans le domaine de la sécurité, tout son développement dans le cadre d'une application correcte du cadre juridique existant. Ce programme est enseigné par un corps enseignant ayant une grande expérience dans le domaine de la cybersécurité, et est accessible à tout moment et en tout lieu à partir d'un appareil doté d'une connexion internet.



“

Transformez toute entreprise en un environnement sécurisé, à l'abri des cybermenaces, grâce à ce programme"

La sécurité sur Internet est devenue l'un des principaux problèmes des grandes entreprises et des gouvernements qui investissent des sommes importantes pour éviter le vol de données et d'informations particulièrement sensibles. Ce problème est traité par des professionnels de l'informatique capables de détecter et d'anticiper les hackers, même si, pour ce faire, ils ont besoin d'une connaissance approfondie, tant de la technique que des concepts les plus avancés et les plus applicables d'un Système de Gestion de Sécurité Internet (SGSI).

Ce Certificat Avancé en Gestion des Menaces de Sécurité Informatique permet aux étudiants d'acquérir une connaissance approfondie des piliers sur lesquels repose le SGSI, des documents et modèles à mettre en œuvre, ainsi que des réglementations et normes en vigueur. Une équipe pédagogique, expérimentée en Droit de l'informatique et de la cybersécurité, fournira les lignes directrices essentielles pour gérer la sécurité dans l'entreprise en application de la norme ISO/IEC 27.000, qui établit le cadre des meilleures pratiques en matière de sécurité de l'information.

C'est une excellente opportunité pour les professionnels de l'informatique qui souhaitent développer leur carrière en offrant une sécurité maximale aux entreprises qui font appel à leurs services. Le modèle en ligne de TECH permet de combiner travail et vie personnelle en facilitant l'accès à l'ensemble du programme dès le premier jour, sans horaires et avec la possibilité de télécharger le contenu pour le visionner sur un appareil doté d'une connexion Internet.

Ce **Certificat Avancé en Gestion des Menaces de Sécurité Informatique** contient le programme académique le plus complet et le plus actuel du marché. Les principales caractéristiques sont les suivantes:

- ◆ Le développement d'études de cas présentées par des experts en Sécurité Informatique
- ◆ Les contenus graphiques, schématiques et éminemment pratiques avec lesquels il est conçu, fournissent des informations pratiques sur les disciplines essentielles à la pratique professionnelle
- ◆ Les exercices pratiques d'auto-évaluation pour améliorer l'apprentissage
- ◆ 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
- ◆ La possibilité d'accéder aux contenus depuis tout appareil fixe ou portable doté d'une simple connexion à internet



Découvrez les avantages des normes ISO/IEC 27.000 et appliquez-les pour assurer la sécurité informatique"

“

Progresser dans le domaine de la Sécurité Informatique. Chaque jour, des millions d'entreprises sont touchées par des cyber-attaques. Inscrivez-vous à ce Certificat Avancé”

Planifiez et concevez un SGSI transparent pour les entreprises. Devenez le professionnel de la sécurité informatique qu'elles recherchent.

Les entreprises exigent des professionnels de l'informatique capables de protéger leurs données les plus sensibles. Devenez un expert en Sécurité Informatique.

Le programme comprend un corps enseignant, formé de professionnels du domaine, qui apportent à cette formation l'expérience de leur travail, ainsi que des spécialistes reconnus de grandes sociétés et d'universités prestigieuses.

Son contenu multimédia qui est développé avec les dernières technologies éducatives, permettra aux professionnels d'apprendre de manière située et contextuelle, c'est-à-dire dans un environnement simulé qui offrira une formation en immersion programmée pour s'entraîner aux situations de la vie réelle.

La conception de ce programme est axée sur l'Apprentissage Par les Problèmes, grâce offre des de résoudre les différentes situations de pratique professionnelle qui se présentent tout au long du programme. Pour ce faire, il sera assisté d'un système vidéo interactif innovant créé par des experts reconnus.



02 Objectifs

Ce Certificat Avancé offre aux étudiants l'opportunité d'approfondir les concepts clés de la sécurité de l'information, ainsi que de réaliser une implantation correcte d'un SGSI selon les normes de base et les réglementations existantes, afin d'obtenir une spécialisation qui facilitera le développement de leur carrière professionnelle. Les études de cas, qui placeront les professionnels de l'informatique dans une situation réelle, et le système de *Relearning*, basé sur la répétition du contenu, faciliteront la réalisation de ces objectifs.





“

Obtenez les clés pour mettre en place un SMSI en conformité avec les réglementations existantes. Devenez un grand professionnel de la sécurité informatique”

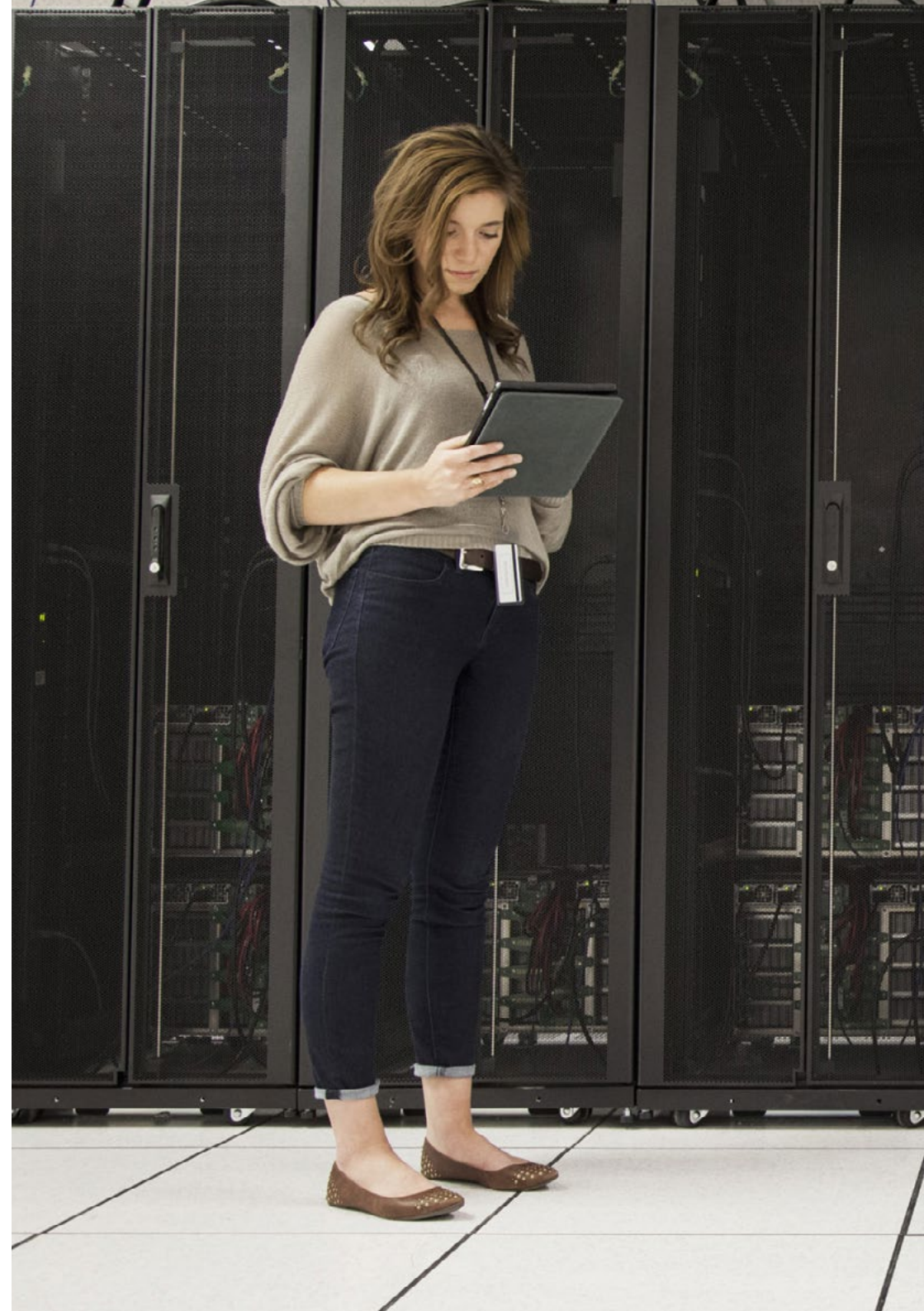


Objectifs généraux

- ◆ Approfondir la compréhension des concepts clés de la sécurité de l'information
- ◆ Développer les mesures nécessaires pour assurer de bonnes pratiques en matière de sécurité de l'information
- ◆ Développer les différentes méthodologies pour effectuer une analyse exhaustive des menaces
- ◆ Installer et apprendre les différents outils utilisés dans le traitement et la prévention des incidents



Appliquez les contre-mesures de sécurité les plus efficaces grâce à ce Certificat Avancé. Cliquez et inscrivez-vous dès maintenant"





Objectifs spécifiques

Module 1. Systèmes de Gestion de Sécurité de Information (SGSI)

- ◆ Analyser les réglementations et les normes actuellement applicables aux SGSI
- ◆ Développer les phases nécessaires à la mise en œuvre d'un SGSI dans une entreprise
- ◆ Analyser les procédures de gestion et de mise en œuvre des incidents de sécurité de l'information

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

- ◆ Implanter un SGSI dans l'entreprise
- ◆ Déterminer les départements concernés par la mise en œuvre du système de gestion de la sécurité
- ◆ Mettre en œuvre les contre-mesures de sécurité nécessaires dans les opérations

Module 3. Politiques de Sécurité pour l'Analyse de la Menace des Systèmes Informatiques

- ◆ Analyser la signification des menaces
- ◆ Déterminer les phases de la gestion préventive des menaces
- ◆ Comparer différentes méthodologies de gestion des menaces

03

Direction de la formation

Les professionnels qui composent le corps enseignant de ce Certificat Avancé possèdent un haut niveau de qualification académique et une grande expérience dans le secteur de la Cybersécurité. C'est précisément leur participation à des projets de sécurité informatique qui permettra aux étudiants de connaître la réalité du secteur technologique, les principaux problèmes détectés dans les protocoles d'action, ainsi que leur correction afin d'offrir des garanties et une tranquillité d'esprit aux entreprises. Pendant cette formation de six mois, les enseignants accompagneront les étudiants dans un enseignement de qualité, qui améliorera leurs compétences tout au long du processus d'apprentissage.



“

Les experts en Cybersécurité et en protection des données vous feront bénéficier de leur précieuse expérience dans le cadre de ce Certificat Avancé”

Direction



Mme Fernández Sapena, Sonia

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

Professeurs

M. Oropesiano Carrizosa, Francisco

- ◆ Ingénieur informatique
- ◆ Technicien en Micro-informatique, Réseaux et Sécurité à Cas-Training
- ◆ Développeur de Services Web, CMS, e-Commerce, UI et UX à Fersa Reparaciones
- ◆ Gestionnaire de Services Web, de Contenu, de Courrier et de DNS à Oropesia Web & Network
- ◆ Designer Graphique et d'Applications Web à Xarxa Sakai Projectes
- ◆ Diplôme en Systèmes Informatiques de l'Université d'Alcalá de Henares
- ◆ Master en DevOps: Docker and Kubernetes por Cyber Business Center
- ◆ Technicien en Réseau et Sécurité Informatique de l'Université des Iles Baléares
- ◆ Certificat en Design Graphique de l'Université Polytechnique de Madrid

M. Ortega López, Alfonso

- ◆ Consultant en Sécurité (Gestion de l'Identité) à SIA Group
- ◆ Consultant en TIC et Sécurité en tant qu'indépendant
- ◆ Enseignant Formateur en TI
- ◆ Diplôme en Génie Technique Industriel à l'Université d'Alcalá de Henares
- ◆ Master en Enseignement par l'UNIR
- ◆ MBA en Gestion et Administration des Entreprises de l'IDE-CESEM
- ◆ Master en Direction et Gestion des Technologies de l'Information par l'IDE-CESEM
- ◆ Certified Information Security Management (CISM) par ISACA

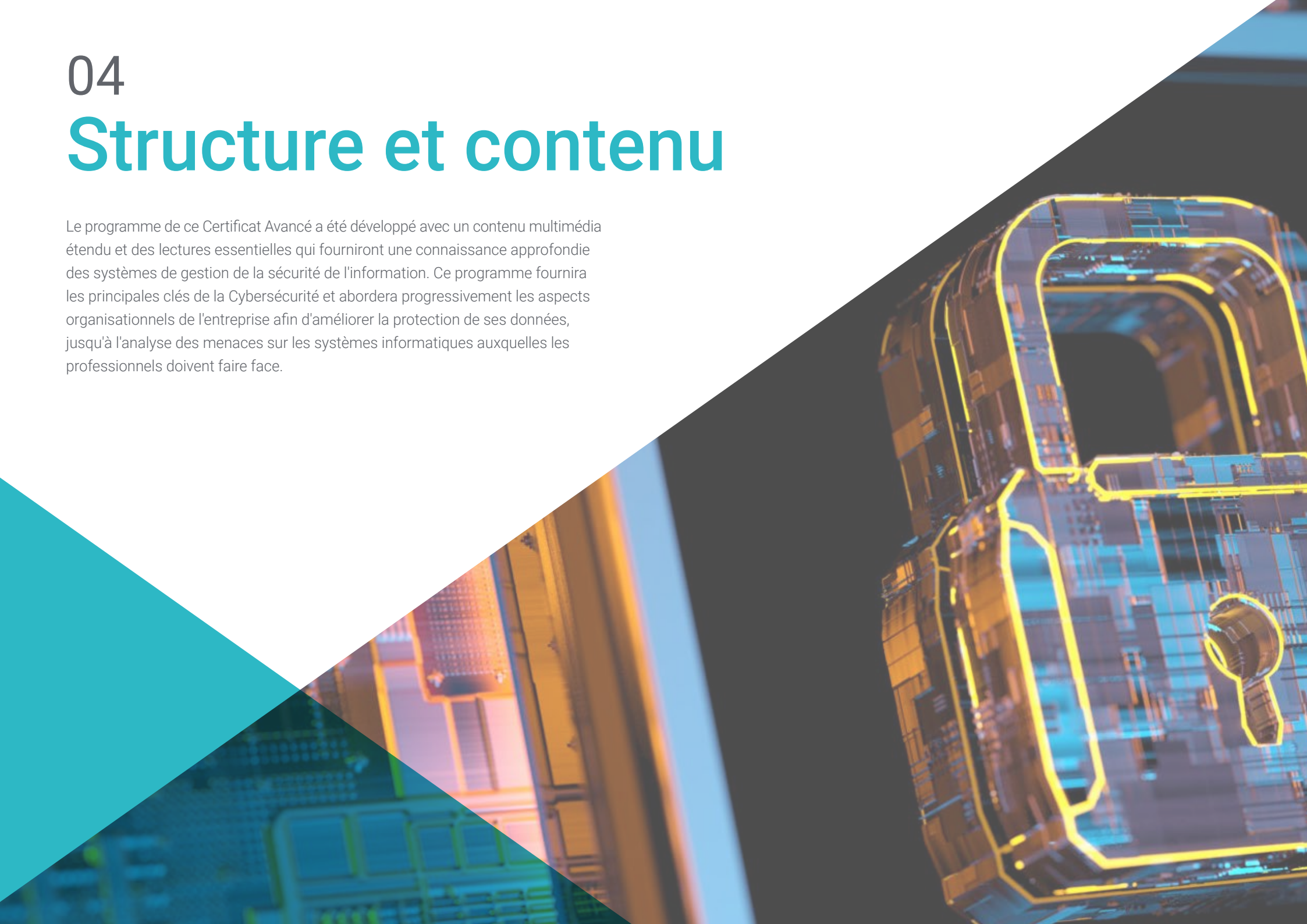
M. Peralta Alonso, Jon

- ◆ Consultant Senior - Protection des Données et Cybersécurité Altia
- ◆ vocat / Conseiller juridique Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- ◆ Conseiller juridique / Stagiaire Cabinet d'avocats: Oscar Padura
- ◆ Licence en Droit Université Public du Pays Basque
- ◆ Master en Protection des Données Délégué EIS Innovative School
- ◆ Master Universitaire en Droit Université Public du Pays Basque
- ◆ Master en Pratique du Contentieux Civil Université internationale Isabel I de Castille
- ◆ Professeur du Master en Protection des Données Personnelles, Cybersécurité et Droit des TIC

04

Structure et contenu

Le programme de ce Certificat Avancé a été développé avec un contenu multimédia étendu et des lectures essentielles qui fourniront une connaissance approfondie des systèmes de gestion de la sécurité de l'information. Ce programme fournira les principales clés de la Cybersécurité et abordera progressivement les aspects organisationnels de l'entreprise afin d'améliorer la protection de ses données, jusqu'à l'analyse des menaces sur les systèmes informatiques auxquelles les professionnels doivent faire face.



“

Un programme d'études qui vous donnera les directives pour mettre en œuvre des politiques de sécurité efficaces dans n'importe quelle entreprise"

Module 1. Systèmes de Gestion de Sécurité de 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. Systèmes 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/CEI 27.000
 - 1.4.1. Objectif et domaines d'application
 - 1.4.2. Structure de la norme
 - 1.4.3. Certification
 - 1.4.4. Étapes de l'accréditation
 - 1.4.5. Avantages des Normes ISO/CEI 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 normes



- 1.7. Phase II: Préparation
 - 1.7.1. Contexte organisationnel
 - 1.7.2. Analyse des règles de sécurité applicables
 - 1.7.3. Champ d'application du système général de sécurité de l'information
 - 1.7.4. Politique du système général de sécurité de l'information
 - 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 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 projets
- 2.2. Gestion des biens
 - 2.2.1. Responsabilité des actifs
 - 2.2.2. Classification des informations
 - 2.2.3. Traitement des supports de stockage

- 2.3. Politiques de sécurité dans les processus d'entreprise
 - 2.3.1. Analyse des processus opérationnels vulnérables
 - 2.3.2. Analyse de l'impact sur les activités
 - 2.3.3. Classement des processus en fonction de leur impact sur les activités
- 2.4. Politiques de sécurité liées aux Ressources Humaines
 - 2.4.1. Avant le recrutement
 - 2.4.2. Pendant le recrutement
 - 2.4.3. Fin de contrat ou changement de poste
- 2.5. Politiques de sécurité de la direction
 - 2.5.1. Directives de gestion sur la sécurité de l'information
 - 2.5.2. BIA - analyse de l'impact
 - 2.5.3. Le plan de reprise en tant que politique de sécurité
- 2.6. Acquisition et maintenance des systèmes d'information
 - 2.6.1. Exigences d'une Sécurité des systèmes d'information
 - 2.6.2. Sécurité des données de développement et soutien
 - 2.6.3. Données de l'essai
- 2.7. Sécurité avec les fournisseurs
 - 2.7.1. Sécurité informatique avec les fournisseurs
 - 2.7.2. Gestion de la prestation du service avec garantie
 - 2.7.3. Sécurité de la chaîne d'approvisionnement
- 2.8. Sécurité des opérations
 - 2.8.1. Responsabilités opérationnelles
 - 2.8.2. Protection contre les codes malveillants
 - 2.8.3. Copies de sécurité
 - 2.8.4. Registres d'activité et de suivi
- 2.9. Gestion de la sécurité et de la réglementation
 - 2.9.1. Respect des exigences légales
 - 2.9.2. Examens de la sécurité de l'information
- 2.10. Sécurité dans la gestion de la continuité des activités
 - 2.10.1. Continuité de la sécurité de l'information
 - 2.10.2. Redondances

Module 3. Politiques de Sécurité pour l'Analyse des Menaces des Systèmes Informatiques

- 3.1. Gestion de Menaces dans les Politiques de Sécurité
 - 3.1.1. Gestion des risques
 - 3.1.2. Risque de sécurité
 - 3.1.3. Méthodes de gestion des menaces
 - 3.1.4. Implémentation des méthodologies
- 3.2. Phases de la gestion des menaces
 - 3.2.1. Identification
 - 3.2.2. Analyses
 - 3.2.3. Localisation
 - 3.2.4. Mesures de sauvegarde
- 3.3. Systèmes d'audit 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 du risque
 - 3.5.1. Implémentation des mesures de sauvegarde
 - 3.5.2. Transfert ou prise en charge
- 3.6. Maîtrise des risques
 - 3.6.1. Processus continu de gestion des risques
 - 3.6.2. Implémentation de mesures de sécurité
 - 3.6.3. Modèle stratégique de mesures de la sécurité de l'information
- 3.7. Méthodes pratiques d'analyse et de surveillance des menaces
 - 3.7.1. Catalogue des menaces
 - 3.7.2. Catalogue des mesures de contrôle
 - 3.7.3. Catalogue des mesures de protection



- 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, incidences et 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 dans 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 des impacts et des risques
 - 3.10.4. Méthodologie

“

Les études de cas de ce Certificat Avancé vous mettront dans des situations réelles de cyberattaques. Les connaissances acquises vous aideront à y parvenir”

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

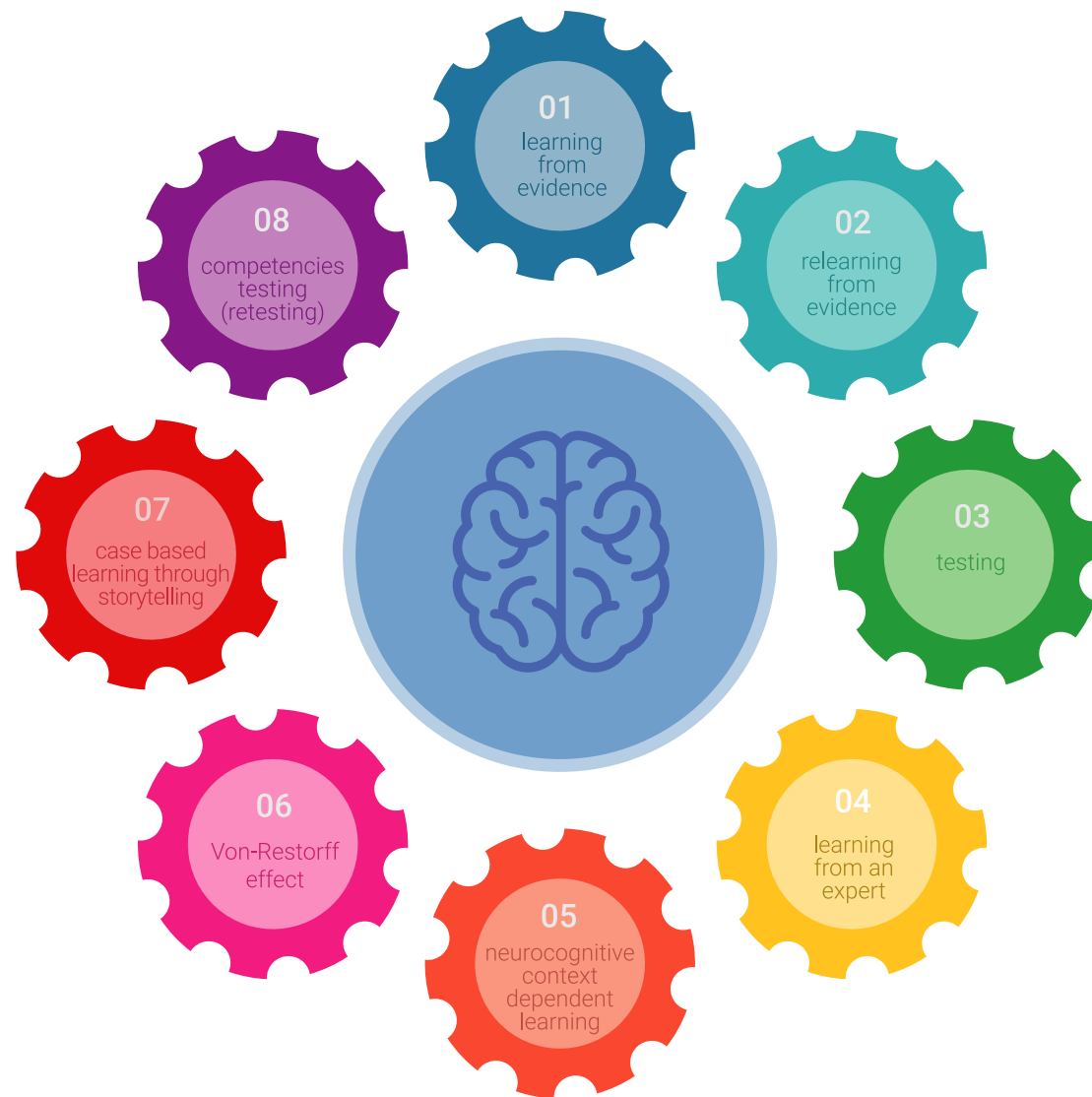
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.



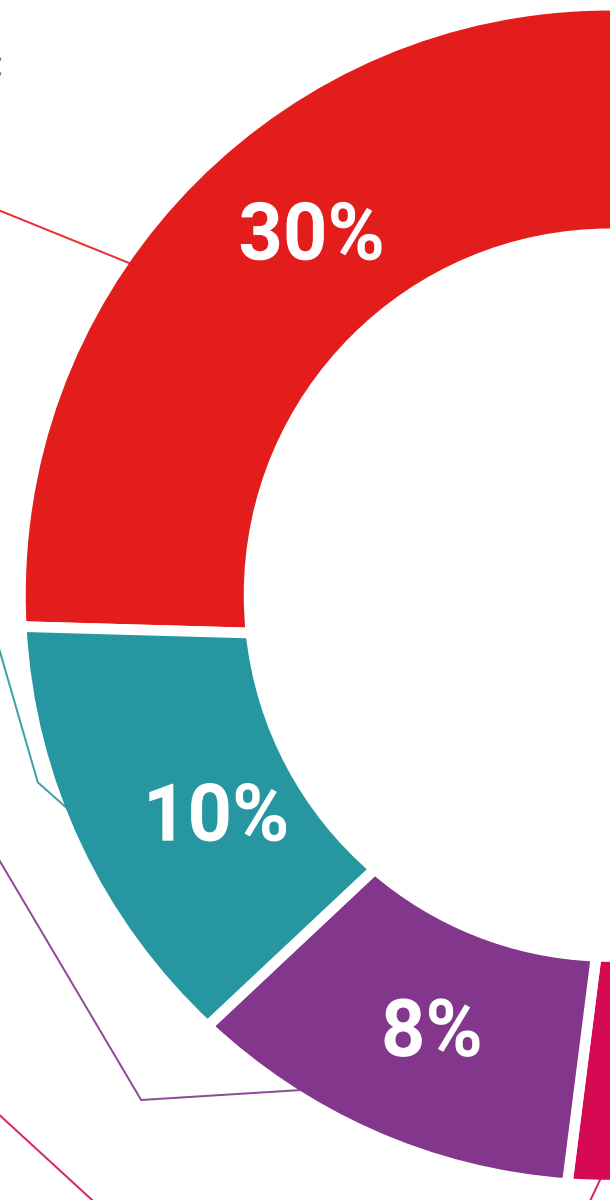
Pratiques en compétences et aptitudes

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 Gestion des Menaces de Sécurité Informatique 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.



“

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

Ce **Certificat Avancé en Gestion des Menaces de Sécurité Informatique** contient le programme le plus complet et le plus à jour 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 Gestion des Menaces de Sécurité Informatique**

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.



Certificat Avancé
Gestion des Menaces
de Sécurité Informatique

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

Certificat Avancé

Gestion des Menaces de Sécurité Informatique

