

# Certificat Avancé

## Gestion des Incidents de Sécurité Informatique



## Certificat Avancé Gestion des Incidents 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-incidents-securite-informatique](http://www.techtitute.com/fr/informatique/diplome-universite/diplome-universite-gestion-incidents-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

Les entreprises savent qu'elles sont exposées à un grand nombre de cyber-attaques, c'est pourquoi la mise en place de politiques de sécurité est aujourd'hui indispensable pour garantir la protection des données sensibles. Dans ce contexte, les professionnels de l'informatique doivent réagir aux incidents prévisibles et prendre des mesures préventives pour éviter d'autres attaques. Ce programme 100% en ligne fournit aux étudiants tous les outils nécessaires pour gérer la sécurité informatique. L'équipe d'enseignants experts dans ce domaine et la vaste bibliothèque dotée de ressources multimédias favoriseront l'apprentissage et la spécialisation des professionnels dans un domaine qui exige un haut niveau de qualification.



“

*Vous serez prêt à faire face à tout incident de Sécurité Informatique subi par une entreprise. Inscrivez-vous à ce Certificat Avancé”*

La sécurité informatique devient de plus en plus nécessaire compte tenu du volume important de données sensibles détenues par les entreprises et les institutions. Cependant, certaines mauvaises pratiques de la part du personnel ou le manque de connaissances dans ce domaine technologique entraînent des fissures et des incidents. Ceux-ci peuvent parfois générer des pertes ou affecter gravement l'image d'une organisation.

Ce Certificat Avancé offre une formation spécialisée qui permet d'analyser et de gérer les incidents, depuis leur détection par les systèmes IDS/IPS et leur traitement ultérieur dans le SIEM, jusqu'au processus de notification et d'escalade vers le service correspondant. Cette procédure nécessite l'intervention d'informaticiens experts qui maîtrisent les outils utiles au contrôle des systèmes d'information.

Ce programme, à l'approche éminemment pratique, mettra les étudiants en situation de confrontation avec une attaque de *Ransomware*, afin qu'ils puissent parfaire leurs connaissances dans l'adoption de mesures d'action et de protocoles de récupération.

Ce programme 100% en ligne permet aux professionnels de l'informatique d'accéder à un contenu multimédia de qualité dès le premier jour, sans horaires fixes et à partir de n'importe quel dispositif doté d'un accès Internet. TECH facilite l'apprentissage pour les étudiants qui souhaitent combiner leur vie professionnelle et personnelle avec une éducation accessible à tous.

Ce **Certificat Avancé en Gestion des Incidents 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



*Grâce à ce Certificat Avancé, vous maîtriserez parfaitement les logiciels de surveillance de réseau tels que Nagios, Zabbix ou Pandora en gardant un œil sur vos équipements"*

“

*Donnez un élan à votre carrière professionnelle. Spécialisez-vous et apportez des réponses aux problèmes de sécurité informatique des entreprises et des institutions. Inscrivez-vous dès maintenant”*

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.

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 programme universitaire. Pour ce faire, il sera assisté d'un système vidéo interactif innovant créé par des experts reconnus.

*Découvrez la norme ISO 27035 et évitez les failles de sécurité qui pourraient menacer les entreprises. Inscrivez-vous à cette qualification.*

*Exploitez à la perfection les protocoles et les outils SNMP grâce à ce Certificat Avancé.*



# 02

## Objectifs

Pendant les six mois de cette formation, les professionnels de l'informatique approfondiront leurs connaissances en matière de sécurité informatique, ce qui les amènera à développer au cours du programme, des mesures efficaces pour assurer de bonnes pratiques de sécurité dans les entreprises. Ces derniers seront en mesure d'effectuer correctement des pistes d'audit sur les systèmes et de surveiller les réseaux à l'aide des outils technologiques les plus récents. À l'issue du programme, ils seront en mesure de mettre en œuvre un plan parfait de politique de sécurité en cas de catastrophe. Les vidéos résumant chaque sujet et les lectures complémentaires faciliteront la réalisation de ces objectifs.



“

*Élaborez le meilleur plan de Sécurité Informatique et devenez l'expert dont les entreprises ont besoin pour se protéger”*



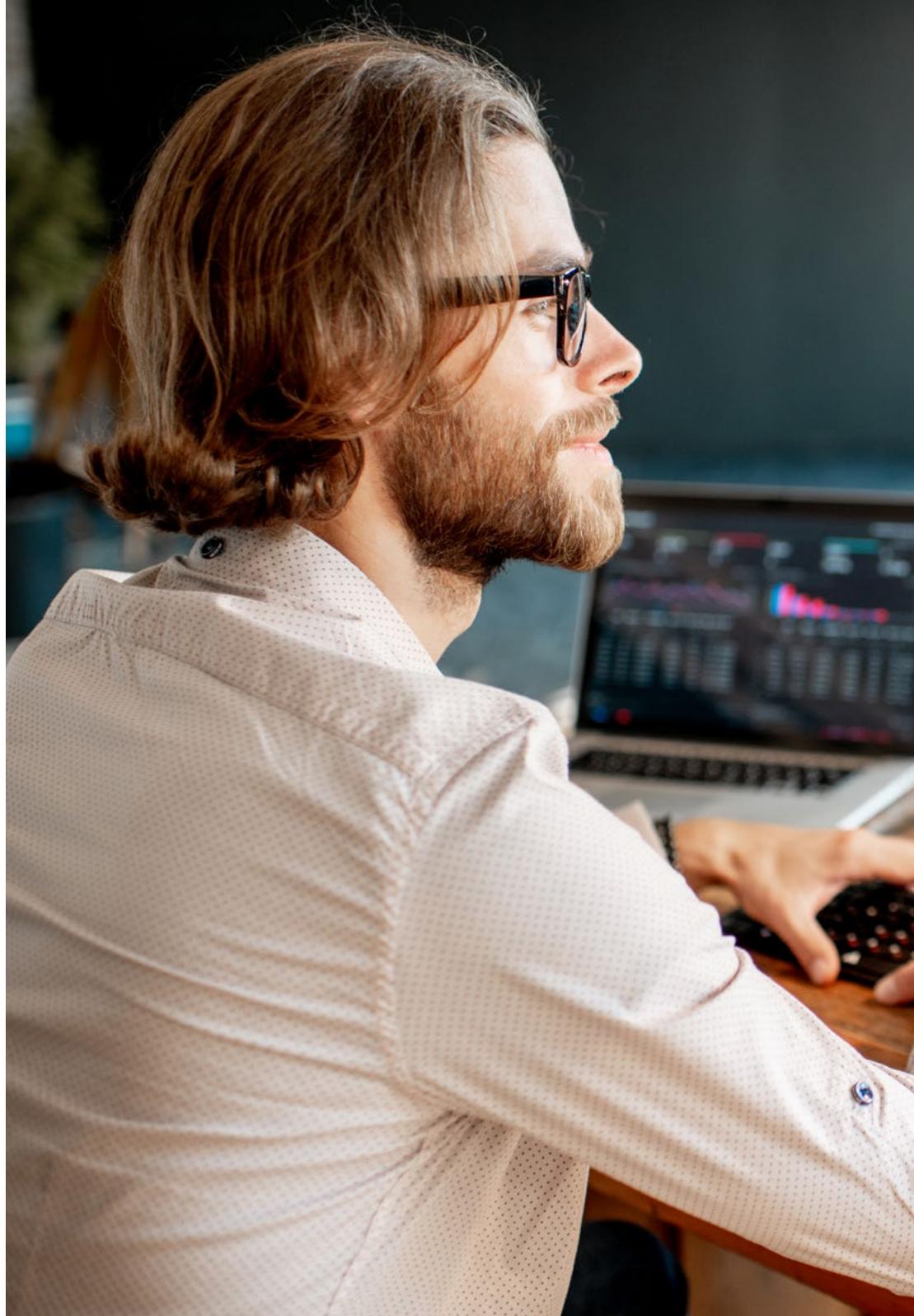
## Objectifs généraux

---

- ◆ 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

“

*La méthodologie pédagogique de TECH vous permettra d'atteindre vos objectifs les plus ambitieux plus tôt que vous ne l'espérez"*





## Objectifs spécifiques

---

### **Module 1. Politiques de Gestion des Incidents de Sécurité**

- ◆ Développer des connaissances spécialisées sur la manière de gérer les incidents causés par des événements liés à la sécurité informatique
- ◆ Déterminer le fonctionnement d'une équipe de traitement des incidents de sécurité
- ◆ Analyser les différentes phases de la gestion des événements de sécurité informatique
- ◆ Examiner les protocoles standardisés pour le traitement des incidents de sécurité

### **Module 2. Les outils de Contrôle dans les Politiques de Sécurité des Systèmes d'Information**

- ◆ Développer le concept de surveillance et mettre en place des métriques
- ◆ Configurer des pistes d'audit sur les systèmes et surveiller les réseaux
- ◆ Compiler les meilleurs outils de surveillance des systèmes actuellement disponibles sur le marché

### **Module 3. Politique de Récupération Pratique de la Sécurité en cas de Désastre**

- ◆ Générer des connaissances spécialisées sur le concept de continuité de la sécurité de l'information
- ◆ Développer un plan de continuité des activités
- ◆ Analyser un plan de continuité des TIC
- ◆ Concevoir un plan de reprise après le sinistre

# 03

## Direction de la formation

TECH offre aux étudiants une formation de qualité conforme aux dernières évolutions du secteur, dont la Sécurité Informatique. Ce Certificat Avancé offre au professionnel en informatique des connaissances approfondies, grâce au savoir d'une équipe enseignante ayant une grande expérience de la Cybersécurité et travaillant actuellement dans ce domaine. Ainsi, les étudiants disposeront d'un enseignement proche de la réalité que les professionnels vivent au quotidien face aux cyberattaques.



“

*Ces experts de la sécurité dans les entreprises publiques et privées vous donneront les clés pour booster votre carrière professionnelle dans ce domaine”*

## 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

# 04

## Structure et contenu

Le programme de Certificat Avancé a été conçu pour aborder en trois modules les points clés de la gestion des incidents de sécurité informatique. Ainsi, les étudiants apprendront les politiques de gestion et les systèmes de détection et de prévention des instructions, et ils découvriront tout au long du programme les outils, les protocoles et les audits dans le domaine de la sécurité. Par ailleurs, la sécurité et de la récupération en cas de catastrophe auront également un rôle important dans le cadre de ce diplôme. Les études de cas et le système de *Relearning*, basé sur la répétition du contenu, permettront aux étudiants de consolider plus facilement et plus rapidement toutes les connaissances de ce diplôme.



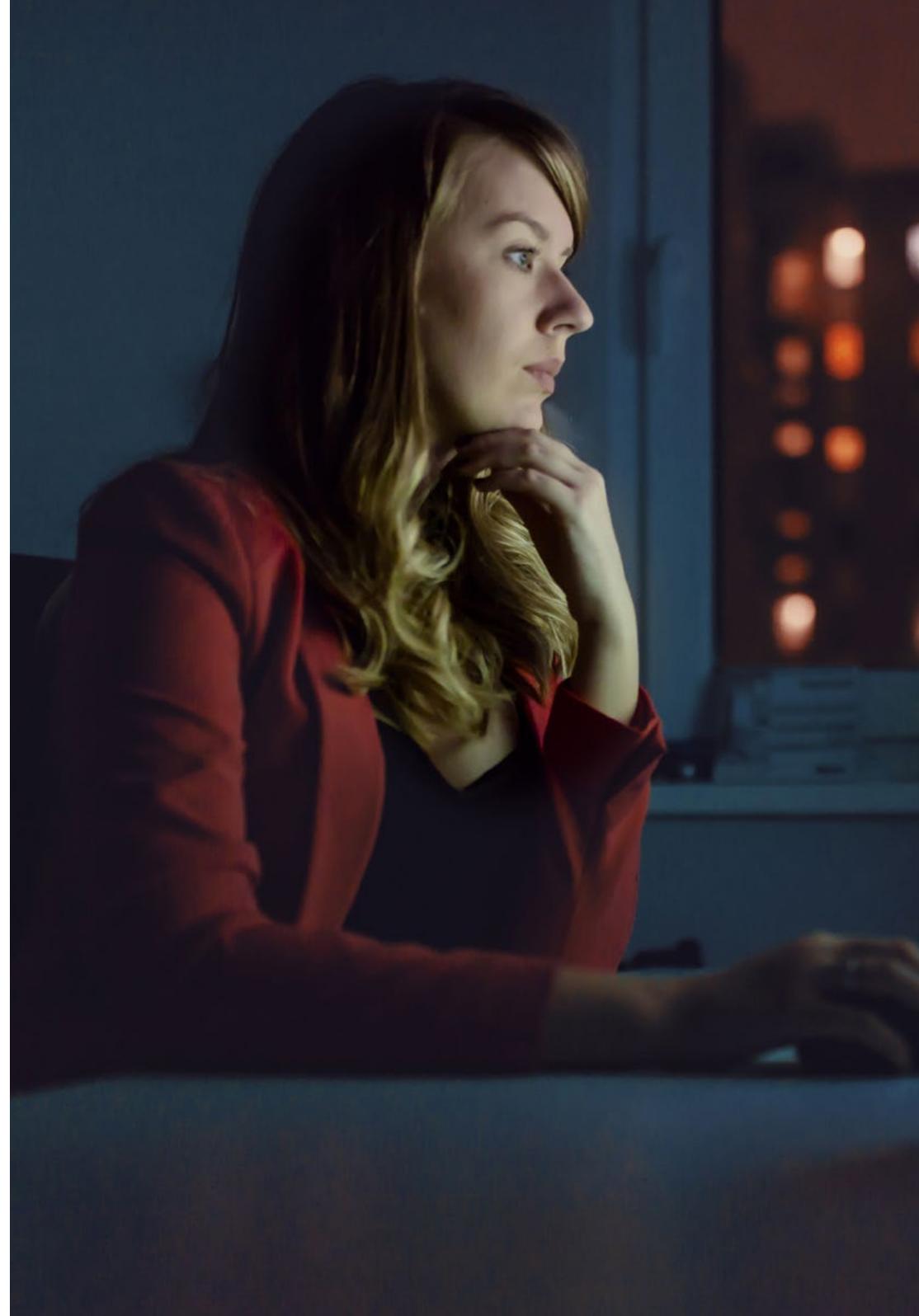


“

*Le large éventail de ressources multimédias enrichit ce programme élaboré par des experts dans le domaine de la Sécurité Informatique"*

## Module 1. Politiques de Gestion des Incidents de Sécurité

- 1.1. Politiques de Gestion des Incidents de Sécurité Informatique et leurs avancées
  - 1.1.1. Gestion des Incidents
  - 1.1.2. Responsabilités et procédures
  - 1.1.3. Notification des événements
- 1.2. Systèmes de détection et prévention des intrusions (IDS/IPS)
  - 1.2.1. Données relatives au fonctionnement du système
  - 1.2.2. Types de systèmes de détection d'intrusion
  - 1.2.3. Critères de localisation des IDS/IPS
- 1.3. Réponse aux incidents de sécurité
  - 1.3.1. Procédure de collecte d'informations
  - 1.3.2. Procédure de vérification des intrusions
  - 1.3.3. Organismes CERT
- 1.4. Processus de notification et gestion des tentatives d'intrusion
  - 1.4.1. Responsabilité sur le processus de notification
  - 1.4.2. Classification des incidents
  - 1.4.3. Processus de résolution et de rétablissement
- 1.5. L'analyse criminalistique en tant que politique de sécurité
  - 1.5.1. Preuves volatiles et non volatiles
  - 1.5.2. Analyse et collecte de preuves électroniques
    - 1.5.2.1. Analyse des preuves électroniques
    - 1.5.2.2. Collecte de preuves électroniques
- 1.6. Outils de détection et prévention des intrusions (IDS/IPS)
  - 1.6.1. Snort
  - 1.6.2. Suricata
  - 1.6.3. SolarWinds
- 1.7. Outils de centralisation des événements
  - 1.7.1. SIM
  - 1.7.2. SEM
  - 1.7.3. SIEM



- 1.8. Guide de sécurité CCN-STIC 817
  - 1.8.1. Gestion des cyberincidents
  - 1.8.2. Mesures et indicateurs
- 1.9. NIST SP800-61
  - 1.9.1. Capacité de réponse aux incidents de sécurité Informatique
  - 1.9.2. Gestion d'un incident
  - 1.9.3. Coordination et partage d'informations
- 1.10. Norme ISO 27035
  - 1.10.1. Norme ISO 27035 Principes de gestion des incidents
  - 1.10.2. Lignes directrices pour l'élaboration d'un plan de gestion des incidents
  - 1.10.3. Lignes directrices pour une réponse aux incidents

## Module 2. Les outils de Contrôle dans les Politiques de Sécurité des Systèmes d'Information

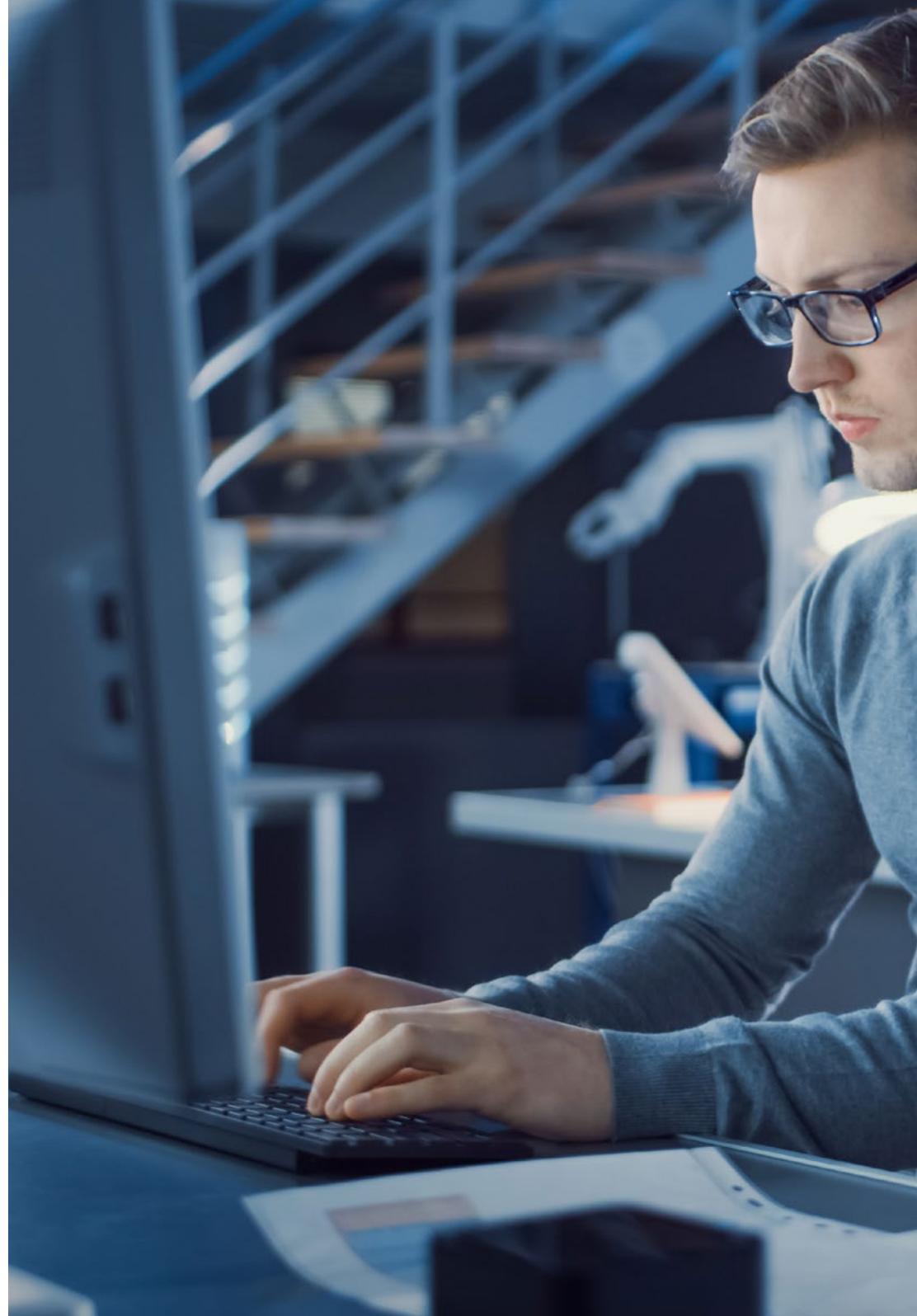
- 2.1. Politiques de contrôle des systèmes d'information
  - 2.1.1. Surveillance des systèmes
  - 2.1.2. Métriques
  - 2.1.3. Types de mesures
- 2.2. Audit et registre des systèmes
  - 2.2.1. Audit et registre des systèmes
  - 2.2.2. Audit et registre de Windows
  - 2.2.3. Audit et registre de Linux
- 2.3. Protocole SNMP *Simple Network Management Protocol*
  - 2.3.1. Protocole SNMP
  - 2.3.2. Fonctionnement du SNMP
  - 2.3.3. Outils du SNMP
- 2.4. Surveillance du réseau
  - 2.4.1. Surveillance du réseau dans les systèmes de contrôle
  - 2.4.2. Outils de surveillance des systèmes de contrôle
- 2.5. Nagios Système de surveillance du réseau
  - 2.5.1. Nagios
  - 2.5.2. Fonctionnement de Nagios
  - 2.5.3. Installation de Nagios

- 2.6. Zabbix Système de surveillance du réseau
  - 2.6.1. Zabbix
  - 2.6.2. Fonctionnement de Zabbix
  - 2.6.3. Installation de Zabbix
- 2.7. Cacti Système de surveillance du réseau
  - 2.7.1. Cacti
  - 2.7.2. Fonctionnement de Cacti
  - 2.7.3. Installation de Cacti
- 2.8. Pandora Système de surveillance du réseau
  - 2.8.1. Pandora
  - 2.8.2. Fonctionnement de Pandora
  - 2.8.3. Installation de Pandora
- 2.9. SolarWinds Système de surveillance du réseau
  - 2.9.1. SolarWinds
  - 2.9.2. Fonctionnement de SolarWinds
  - 2.9.3. Installation de SolarWinds
- 2.10. Réglementation en matière de contrôle
  - 2.10.1. Contrôles CIS en matière d'audit et d'enregistrement
  - 2.10.2. NIST 800-123 USA

## Module 3. Politique de Récupération Pratique de la Sécurité en cas de Sinistre

- 3.1. DRP Plan de Récupération après un sinistre
  - 3.1.1. Objectif d'un DRP
  - 3.1.2. Avantages d'un DRP
  - 3.1.3. Conséquences de l'absence d'un DRP et sans mise à jour
- 3.2. Orientations pour la définition d'un plan de reprise après sinistre (DRP)
  - 3.2.1. Champ d'application et objectifs
  - 3.2.2. Conception de la stratégie de reprise
  - 3.2.3. Attribution des rôles et des responsabilités
  - 3.2.4. Inventaire du matériel, des logiciels et des services
  - 3.2.5. Tolérance des temps d'arrêt et des pertes de données
  - 3.2.6. Déterminer les types spécifiques d'ARP qui sont nécessaires
  - 3.2.7. Réalisation d'un plan de formation, de sensibilisation et de communication

- 3.3. Portée et objectifs d'un DRP (Plan de Reprise après Sinistre)
  - 3.3.1. Garantie de réponse
  - 3.3.2. Composants technologiques
  - 3.3.3. Champ d'application de la politique de continuité
- 3.4. Conception de la stratégie d'un DRP (Plan de Reprise après Sinistre)
  - 3.4.1. Stratégie de Plan de Reprise après Sinistre
  - 3.4.2. Budget
  - 3.4.3. Ressources humaines et matérielles
  - 3.4.4. Postes d'encadrement à risque
  - 3.4.5. Technologie
  - 3.4.6. Les données
- 3.5. Continuité des processus d'information
  - 3.5.1. Planification de la continuité
  - 3.5.2. Implantation de la continuité
  - 3.5.3. Vérification de l'évaluation de la continuité
- 3.6. Champ d'application d'un PCA (Plan de Continuité des Affaires)
  - 3.6.1. Détermination des processus les plus critiques
  - 3.6.2. Approche basée sur les actifs
  - 3.6.3. Approche par processus
- 3.7. Implémentation de procédures commerciales sécurisées
  - 3.7.1. Activités prioritaires (AP)
  - 3.7.2. Temps de récupération idéal (IRT)
  - 3.7.3. Stratégies de survie





- 3.8. Analyse organisationnelle
  - 3.8.1. Collecte d'informations
  - 3.8.2. Analyse d'impact sur l'entreprise (BIA)
  - 3.8.3. Analyse des risques organisationnels
- 3.9. Réponse aux imprévus
  - 3.9.1. Plan de crise
  - 3.9.2. Plans de rétablissement de l'environnement opérationnel
  - 3.9.3. Procédures techniques de travail ou d'incident
- 3.10. Norme Internationale ISO 27031 BCP
  - 3.10.1. Objectifs
  - 3.10.2. Conditions et définitions
  - 3.10.3. Opération

“

*Le système de réapprentissage  
et la modalité 100% en ligne  
vous permettront de réaliser un  
apprentissage très utile dans votre  
domaine professionnel”*

# 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 Incidents 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 délivré par TECH Université Technologique.



“

*Complétez ce programme et recevez  
votre diplôme sans avoir à vous  
soucier des déplacements ou des  
démarches administratives inutiles”*

Ce **Certificat Avancé en Gestion des Incidents 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 Incidents de Sécurité Informatique**  
N.º 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 Gestion des Incidents 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 Incidents de Sécurité Informatique

