Certificat Avancé

Implémentation des Politiques de Sécurité Informatique

tech université technologique

tech université technologique

Certificat Avancé

Implémentation des Politiques 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-implementation-politiques-securite-informatique

Sommaire

01

Présentation

Les entreprises se concentrent sur la sécurité des ordinateurs et du Cloud pour éviter le vol ou la perte de données précieuses, mais négligent d'autres aspects de la sécurité qui sont tout aussi importants dans une entreprise, tels que la protection des équipements physiques et environnementaux. Dans ce programme 100% en ligne, les professionnels de l'informatique se pencheront sur le renforcement des systèmes avec des méthodes de sécurité avancées, pour maintenir le contrôle d'accès et l'autorisation pour chaque utilisateur. Tout cela avec un contenu de qualité basé sur des résumés vidéo, des lectures spécifiques et des études de cas qui permettront de se spécialiser dans un domaine de l'informatique qui a besoin de professionnels hautement qualifiés.

Découvrez les principales technologies d'identification et d'autorisation et mettez en place des systèmes informatiques plus sûrs grâce à ce Certificat Avancé"

Les investissements dans la Sécurité Informatique sont essentiels pour les entreprises et les institutions, mais beaucoup se concentrent sur les cyber-attaques externes potentielles et négligent d'élaborer une politique de sécurité physique et environnementale adéquate pour contrôler l'accès aux systèmes informatiques. Dans ce Certificat Avancé, le professionnel de l'informatique se penchera sur les principaux aspects à prendre en compte pour mettre en pratique cette tâche qui n'est pas du tout facile.

Le programme, dispensé par des experts en Sécurité Informatique, explique comment vérifier le niveau de sécurité d'un système informatique par le biais des contrôles CIS, comment analyser tous les systèmes de contrôle d'accès biométriques existants, leur mise en œuvre et la gestion des risques. De plus, il aborde la mise en œuvre de la cryptographie dans les réseaux de communication avec les protocoles actuels les plus répandus, tant symétriques qu'asymétriques.

De même, l'authentification et l'identification occuperont une place importante dans ce programme, dans lequel vous développerez une PKI, apprendrez sa structure et l'utilisation de cette infrastructure pour protéger le réseau grâce à l'utilisation de certificats numériques.

Cette excellente opportunité offerte par TECH permet de se spécialiser dans un secteur qui requiert des professionnels dotés de connaissances actualisées et innovantes dans le domaine de la Sécurité Informatique. Le modèle d'enseignement 100% en ligne permet aux étudiants de combiner l'apprentissage avec d'autres aspects de leur vie personnelle, puisqu'ils n'ont besoin que d'un appareil doté d'une connexion internet pour accéder à tous les contenus multimédias de qualité mis à leur disposition.

Ce **Certificat Avancé en Implémentation des Politiques 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

Actualisez vos connaissances en matière de sécurité informatique en cas d'incendie ou de tremblement de terre. Inscrivez-vous à ce Certificat Avancé"

Découvrez les derniers développements en matière de reconnaissance des empreintes digitales, du visage, de l'iris et de la rétine commee mesures de sécurité informatique"

Découvrez les protocoles de communication sécurisés et prévenez le vol de données de grande valeur. Inscrivez-vous maintenant.

Maîtriser l'outil Secure Shell pour perfectionner et prévenir les fuites d'informations de l'entreprise.

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

02

Objectifs

A l'issue de ce Certificat Avancé, les professionnels en informatique seront en mesure de mettre en œuvre des politiques de sécurité dans les logiciels et le matériel ou d'examiner la biométrie et les systèmes biométriques. De plus, les étudiants seront capables d'appliquer différentes techniques de cryptage réseau telles que TLS, VPN ou SSH et de contrôler les meilleurs outils de surveillance du système actuellement disponibles sur le marché. Le large éventail de ressources et d'études de cas fournira une expérience d'apprentissage très proche de la réalité à laquelle vous serez confronté dans votre environnement de travail.

Obtenez une spécialisation dans le domaine de la Sécurité Informatique grâce à ce Certificat Avancé. Inscrivez-vous dès maintenant"

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

Objectifs spécifiques

Module 1. Implémentation des Politiques de Sécurité de Software et Hardware

- Déterminer ce que sont l'authentification et l'identification
- Analyser les différentes méthodes d'authentification existantes et leur mise en œuvre pratique
- Mettre en œuvre une politique de contrôle d'accès correcte pour les logiciels et les systèmes
- Établir les principales technologies d'identification actuelles
- Générer des connaissances spécialisées sur les différentes méthodologies existantes pour le bastioning des systèmes

Module 2. Implémentation des Politiques de Sécurité Physique et Environnementale dans l'Entreprise

- Analyser les termes "zone sécurisée" et "périmètre sécurisé"
- Examiner la biométrie et les systèmes biométriques
- Mettre en œuvre de bonnes politiques de sécurité physique
- Élaborer les réglementations en vigueur sur les zones sécurisées des systèmes informatiques

Module 3. Politiques de Communications Sécurisées dans l'Entreprise

- Sécuriser un réseau de communication en le cloisonnant
- Analyser les différents algorithmes de cryptage utilisés dans les réseaux de communication
- Mettre en œuvre différentes techniques de cryptage dans le réseau telles que TLS, VPN ou SSH

Module 4. 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

Ce programme vous fournira les outils nécessaires pour examiner la biométrie et les systèmes biométriques dans une entreprise"

03

Direction de la formation

Ce Certificat Avancé dispose d'un corps enseignant expérimenté dans la gestion des sites web et la sécurité des réseaux et systèmes de services. Leurs connaissances approfondies dans ce domaine de l'informatique ont été déterminantes dans ce choix. De cette manière, les étudiants ont la garantie d'être guidés pendant les six mois, par des enseignants qui ont la formation académique nécessaire et la pratique quotidienne de l'application des outils, des systèmes et des protocoles de sécurité dans les entreprises. Tout cela dans le but ultime de fournir un apprentissage de qualité qui permette aux professionnels de l'informatique de progresser dans ce domaine.

Une équipe enseignante dotée d'une grande expérience en Sécurité Informatique sera votre garantie de réussite dans ce programme d'apprentissage"

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 Techonologies E-Council

Professeurs

Mme López García, Rosa María

- Spécialiste en information de Gestion
- Professeur à l'Institut Professionnel Linux
- Collaboratrice à l'Incibe Hacker Academy
- Capitaine des Talents de la Cybersécurité à Teamciberhack
- Responsable Administratif, Comptable et Financier à Integra2Transportes
- Assistante Administrative en Ressources des Achats au Centre d'Education Cardinal Marcelo Espínola
- Technicienne Supérieure en Cybersécurité et Piratage Ethique
- Membre de Ciberpatrol

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

04

Structure et contenu

Le corps enseignant de ce Certificat Avancé a développé un programme qui intègre toutes les connaissances sur la mise en œuvre pratique des politiques de sécurité dans les logiciels et le matériel, en consacrant l'un de ses modules à l'étude approfondie des systèmes biométriques et la protection contre les facteurs environnementaux, tels que les incendies ou les tremblements de terre. De plus, ce programme d'études accorde une attention particulière aux outils de surveillance des systèmes et aux algorithmes cryptographiques. Le système de *Relearning*, basé sur la répétition du contenu, et les cas éminemment pratiques permettront aux étudiants d'acquérir un apprentissage solide de manière simple.

Adaptez la charge d'enseignement de ce programme à vos besoins. Accédez au contenu à tout moment et de n'importe où. Inscrivez-vous en un clic"

Module 1. Implémentation des Politiques de Sécurité de Software et Hardware

1.1. Implémentation des Politiques de Sécurité de Software et Hardware
- 1.1.1. Implémentation de l'identification et de l'autorisation
- 1.1.2. Implémentation des techniques d'identification
- 1.1.3. Mesures techniques d'autorisation

1.2. Technologies d'identification et d'autorisation
- 1.2.1. Identificateur et OTP
- 1.2.2. *Token* USB oou carte intelligente PKI
- 1.2.3. La clé « Secret Défense »
- 1.2.4. RFID actif

1.3. Politiques de sécurité d'accès aux logiciels et aux systèmes
- 1.3.1. Implémentation des politiques de contrôle d'accès
- 1.3.2. Implémentation des politiques d'accès aux communications
- 1.3.3. Types d'outils de sécurité pour le contrôle d'accès

1.4. Gestion des accès des utilisateurs
- 1.4.1. Gestion des droits d'accès
- 1.4.2. Séparation des rôles et des fonctions d'accès
- 1.4.3. Mise en œuvre des droits d'accès dans les systèmes

1.5. Contrôle d'accès aux systèmes et applications
- 1.5.1. Règle d'accès minimum
- 1.5.2. Technologies de connexion sécurisée
- 1.5.3. Politiques de sécurité des mots de passe

1.6. Technologies des systèmes d'identification
- 1.6.1. Active Directory
- 1.6.2. OTP
- 1.6.3. PAP, CHAP
- 1.6.4. KERBEROS, DIAMETER, NTLM

1.7. Contrôles CIS pour la base du système
- 1.7.1. Contrôles CIS de base
- 1.7.2. Contrôles fondamentaux du SID
- 1.7.3. Contrôles organisationnels du SID

1.8. Sécurité opérationnelle
- 1.8.1. Protection contre les codes malveillants
- 1.8.2. Copies de sécurité
- 1.8.3. Enregistrement et surveillance des activités

1.9. Gestion des vulnérabilités techniques
- 1.9.1. Vulnérabilités techniques
- 1.9.2. Gestion des vulnérabilités techniques
- 1.9.3. Restrictions en Installation logiciel

1.10. Restrictions relatives à l'installation de logiciels
- 1.10.1. Vulnérabilités logiques
- 1.10.2. Implémentation des politiques de défense

Module 2. Implémentation des Politiques de Sécurité Physique et Environnementale dans l'Entreprise

2.1. Zones sécurisées
- 2.1.1. Périmètre de sécurité physique
- 2.1.2. Travailler dans des zones sécurisées
- 2.1.3. Sécurité des bureaux, des locaux et des ressources

2.2. Contrôles physiques des entrées
- 2.2.1. Politiques de contrôle d'accès physique
- 2.2.2. Systèmes de contrôle des entrées physiques

2.3. Vulnérabilités de l'accès physique
- 2.3.1. Principales vulnérabilités physiques
- 2.3.2. Implémentation des mesures de sauvegarde

2.4. Systèmes biométriques physiologiques
- 2.4.1. Empreintes digitales
- 2.4.2. Reconnaissance faciale
- 2.4.3. Reconnaissance de l'iris et de la rétine
- 2.4.4. Autres Systèmes biométriques physiologiques

2.5. Systèmes biométriques du comportement
- 2.5.1. Reconnaissance de la signature
- 2.5.2. Reconnaissance du scripteur
- 2.5.3. Reconnaissance de la voix
- 2.5.4. Autres systèmes comportementaux biométriques

2.6. Gestion des risques de la biométrie
- 2.6.1. Implémentation des systèmes biométriques
- 2.6.2. Vulnérabilités des systèmes biométriques

2.7. Implémentation des politiques des *Hosts*
- 2.7.1. Installation du câblage, approvisionnement et sécurité
- 2.7.2. Emplacement de l'équipement
- 2.7.3. Sortie du matériel en dehors des locaux
- 2.7.4. Matériel informatique non surveillé et politique claire en matière d'étalage

2.8. Protection de l'environnement
- 2.8.1. Systèmes de protection contre l'incendie
- 2.8.2. Systèmes de protection face aux tremblements de terre
- 2.8.3. Systèmes de protection antisismique

2.9. Sécurité du centre de traitement des données
- 2.9.1. Portes de sécurité
- 2.9.2. Systèmes de vidéosurveillance (CCTV)
- 2.9.3. Contrôle de sécurité

2.10. Règlements internationaux en matière de sécurité physique
- 2.10.1. IEC 62443-2-1 (europe)
- 2.10.2. NERC CIP-005-5 USA
- 2.10.3. NERC CIP-014-2 USA

Module 3. Politiques de Communications Sécurisées dans l'Entreprise

3.1. Gestion de la sécurité des réseaux
- 3.1.1. Contrôle et surveillance du réseau
- 3.1.2. Séparation des réseaux
- 3.1.3. Systèmes de sécurité du réseau

3.2. Protocoles de communication sécurisés
- 3.2.1. Modèle TCP/IP
- 3.2.2. Protocole IPSEC
- 3.2.3. Protocole TLS

3.3. Protocole TLS 1.3
- 3.3.1. Phases d'un processus TLS 1.3
- 3.3.2. Protocole Handshake
- 3.3.3. Protocole d'enregistrement
- 3.3.4. Différences avec TLS 1.2

3.4. Algorithmes cryptographiques
- 3.4.1. Algorithmes cryptographiques utilisés dans les communications
- 3.4.2. *Cipher-suites*
- 3.4.3. Algorithmes cryptographiques autorisés pour TLS 1.3

3.5. Functions *Digest*
- 3.5.1. MD6
- 3.5.2. SHA

3.6. PKI Infrastructure à clé publique
- 3.6.1. PKI et ses entités
- 3.6.2. Certificat numérique
- 3.6.3. Types de certificats numériques

3.7. Communications par tunnel et transport
- 3.7.1. Communications par tunnel
- 3.7.2. Communications de transport
- 3.7.3. Implémentation d'un tunnel crypté

3.8. SSH. *Secure Shell*
- 3.8.1. SSH Capsule sécurisée
- 3.8.2. Fonctionnement de SSH
- 3.8.3. Outils de SSH

3.9. Audit des systèmes cryptographiques
- 3.9.1. Tests d'intégration
- 3.9.2. Test des systèmes cryptographiques

3.10. Systèmes cryptographiques
- 3.10.1. Vulnérabilités des systèmes cryptographiques
- 3.10.2. Sauvegardes en cryptographie

Module 4. Les outils de Contrôle dans les Politiques de Sécurité des Systèmes d'Information

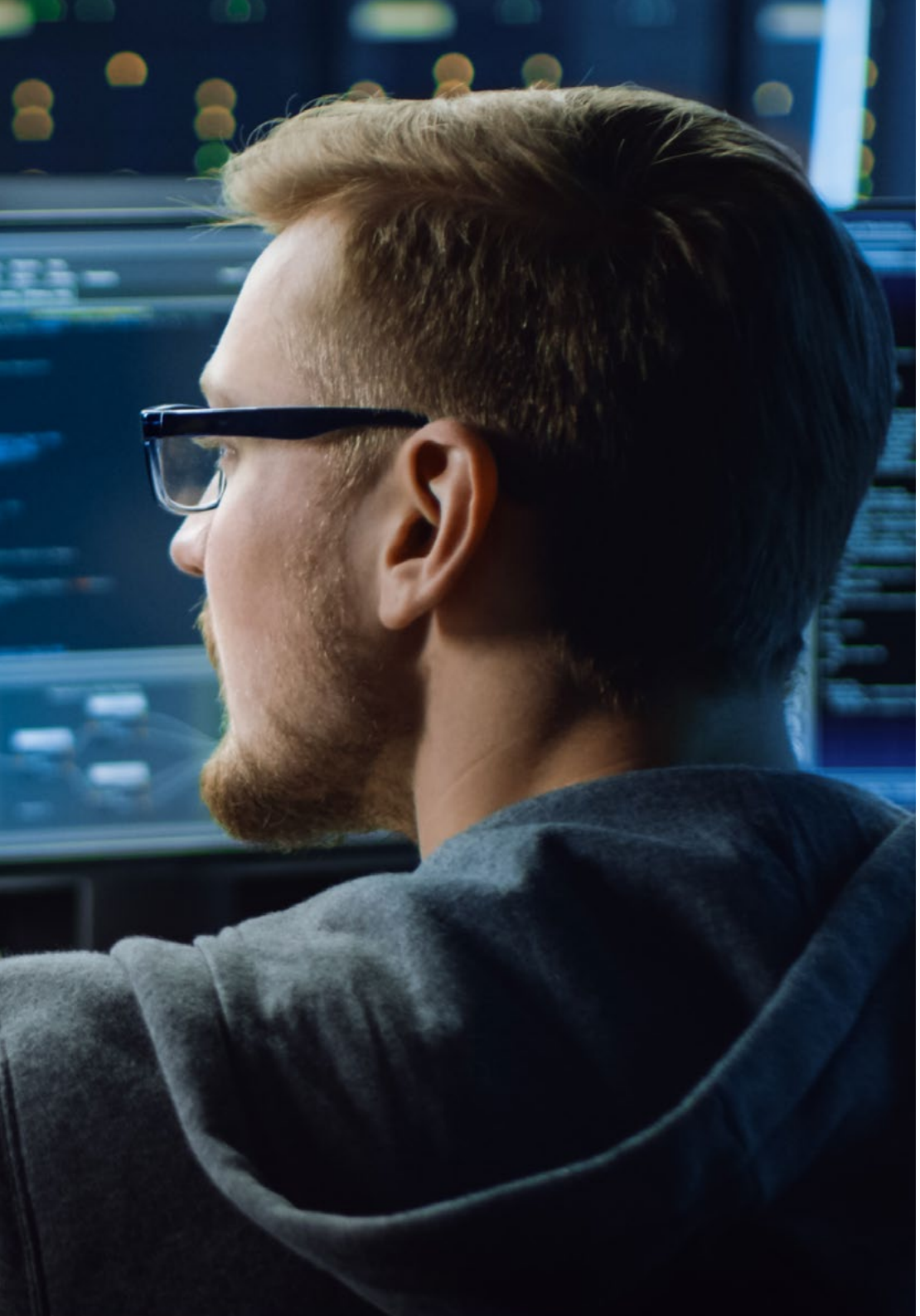
4.1. Politiques de contrôle des systèmes d'information
- 4.1.1. Surveillance des systèmes
- 4.1.2. Métriques
- 4.1.3. Types de mesures

4.2. Audit et registre des systèmes
- 4.2.1. Audit et registre de Windows
- 4.2.2. Audit et registre de Linux

4.3. Protocole SNMP *Simple Network Management Protocol*
- 4.3.1. Protocole SNMP
- 4.3.2. Fonctionnement du SNMP
- 4.3.3. Outils de SNMP

4.4. Surveillance du réseau
- 4.4.1. Surveillance du réseau dans les systèmes de contrôle
- 4.4.2. Outils de surveillance des systèmes de contrôle

4.5. Nagios Système de surveillance du réseau
- 4.5.1. Nagios
- 4.5.2. Fonctionnement de Nagios
- 4.5.3. Installation de Nagios



4.6. Zabbix Système de surveillance du réseau
- 4.6.1. Zabbix
- 4.6.2. Fonctionnement de Zabbix
- 4.6.3. Installation de Zabbix

4.7. Cacti Système de surveillance du réseau
- 4.7.1. Cacti
- 4.7.2. Fonctionnement de Cacti
- 4.7.3. Installation de Cacti

4.8. Pandora Système de surveillance du réseau
- 4.8.1. Pandora
- 4.8.2. Fonctionnement de Pandora
- 4.8.3. Installation de Pandora

4.9. SolarWinds Système de surveillance du réseau
- 4.9.1. SolarWinds
- 4.9.2. Fonctionnement de SolarWinds
- 4.9.3. Installation de SolarWinds

4.10. Réglementation en matière de contrôle
- 4.10.1. Contrôles CIS en matière d' Audits et d'enregistrement
- 4.10.2. NIST 800-123 USA

Les résumés interactifs et les études de cas élaborés par le corps enseignant vous fourniront le contenu dont vous avez besoin pour développer votre carrière"

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***.

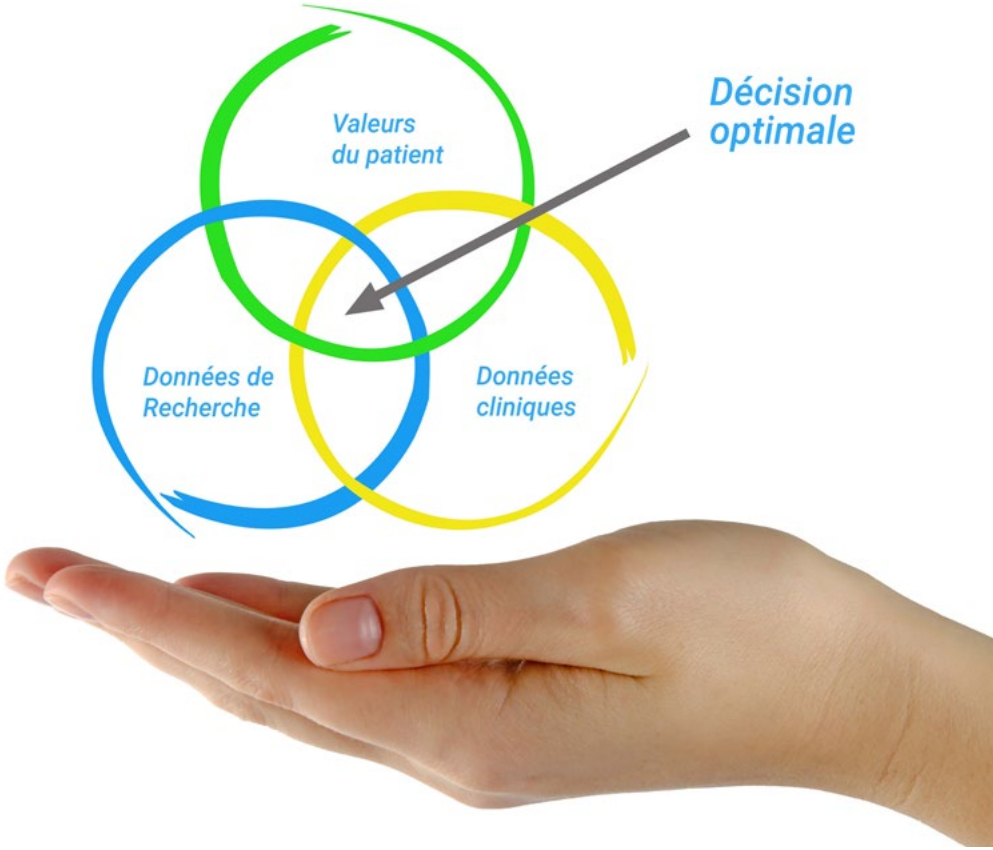
Ce système d'enseignement est utilisé, par exemple, dans les écoles de médecine les plus prestigieuses du monde et a été considéré comme l'un des plus efficaces par des publications de premier plan telles que le ***New England Journal of Medicine.***

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

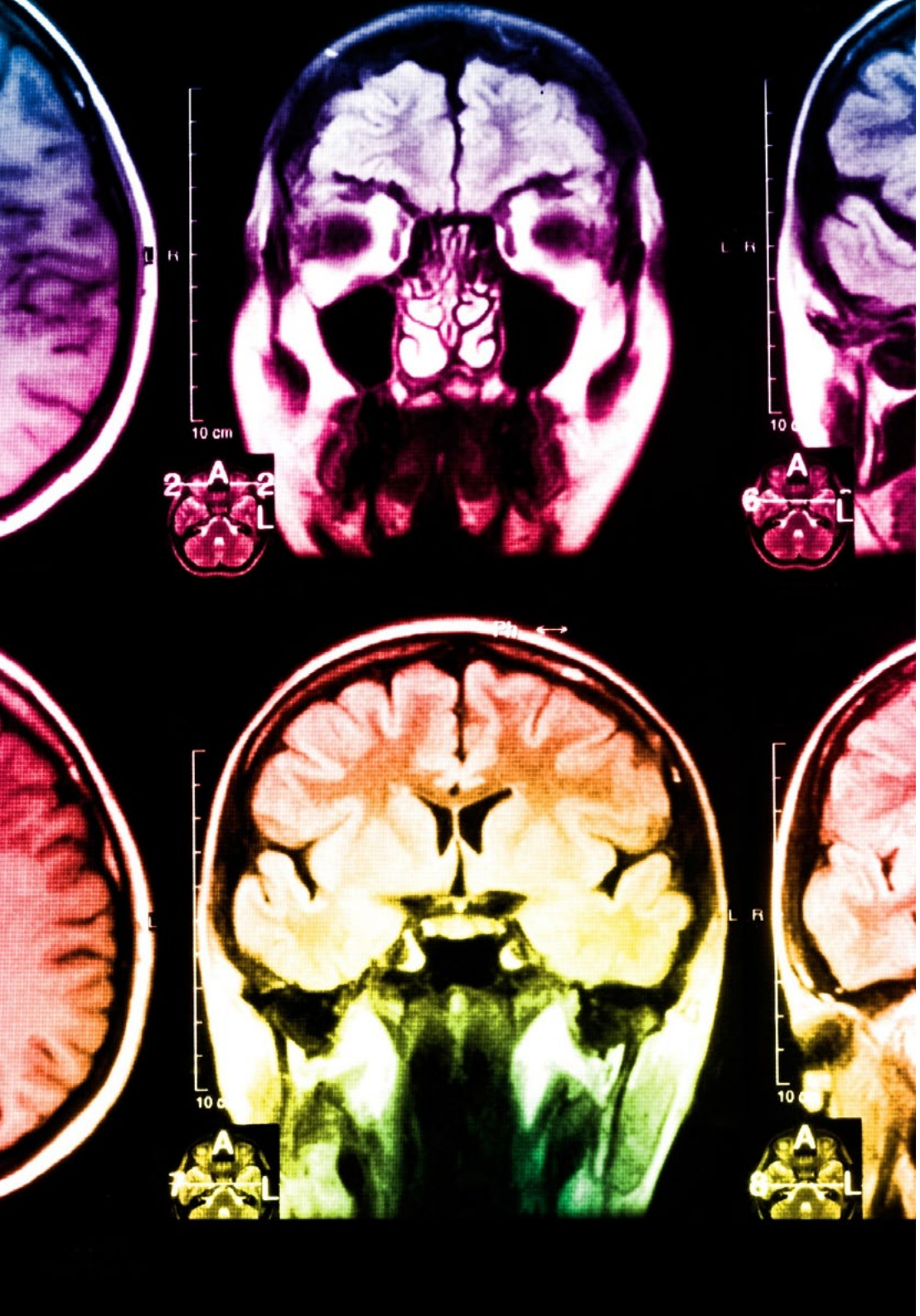
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

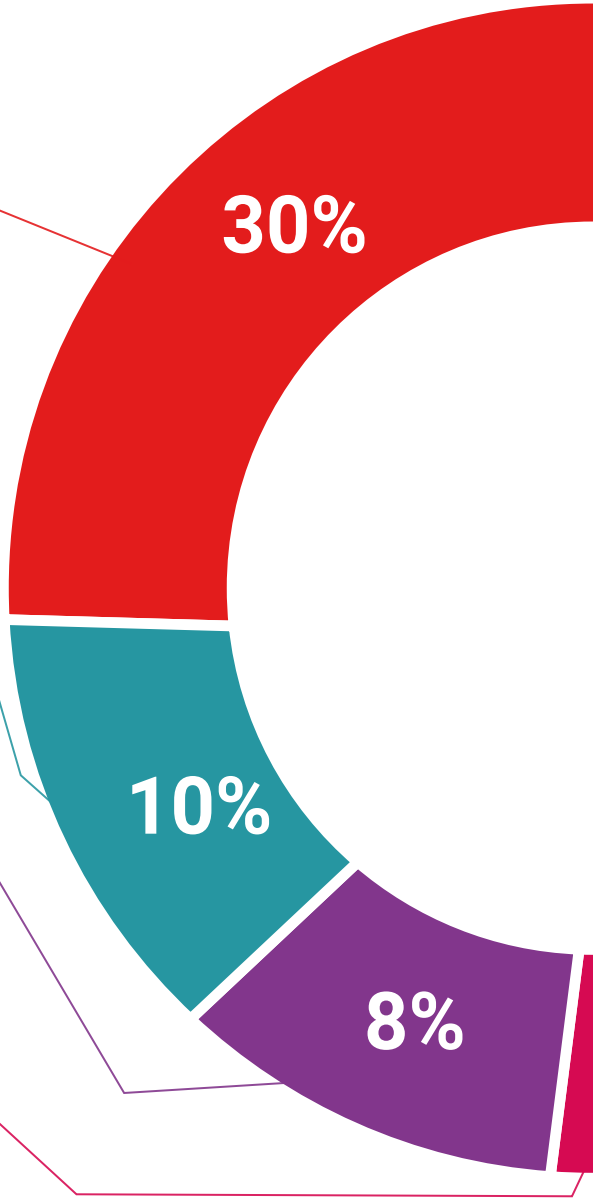
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

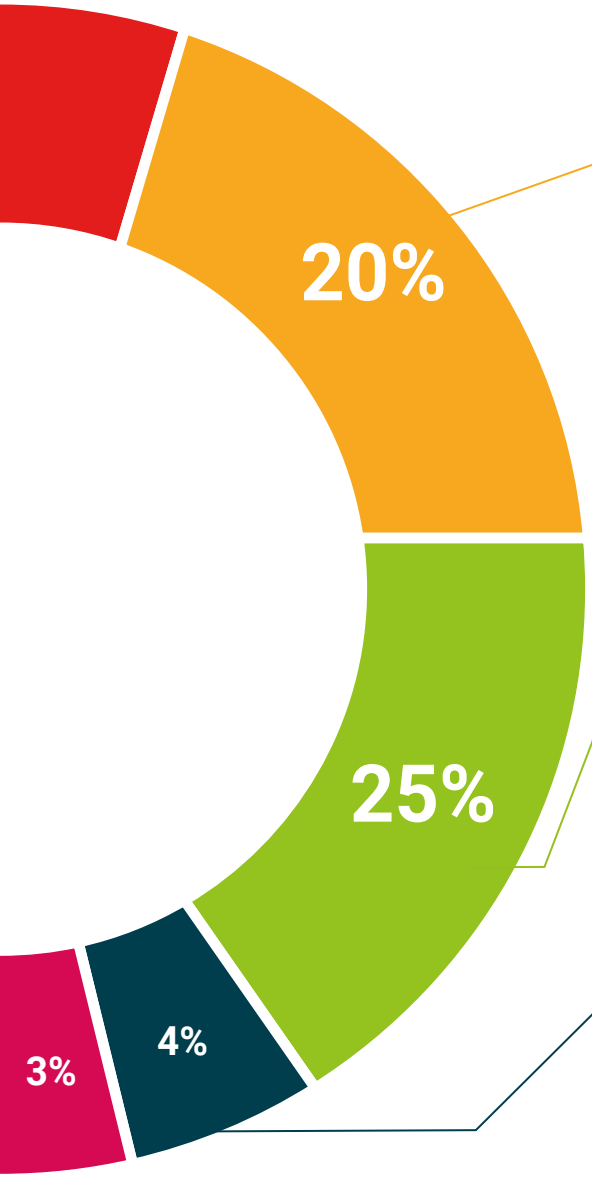
Pratiques en compétences et aptitudes

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 Implémentation des Politiques 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.

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

Ce **Certificat Avancé en Implémentation des Politiques 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 Implémentation des Politiques de Sécurité Informatique**
N.º 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

Implémentation des Politiques de Sécurité Informatique

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

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

Implémentation des Politiques 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

Implémentation des Politiques de Sécurité Informatique

tech université technologique