Mastère Spécialisé
Télématique

tech université technologique

tech université technologique

Mastère Spécialisé

Télématique

- Modalité: **en ligne**
- Durée: **12 mois**
- Qualification: **TECH Université Technologique**
- Intensité: **16h/semaine**
- Horaire: **à votre rythme**
- Examens: **en ligne**

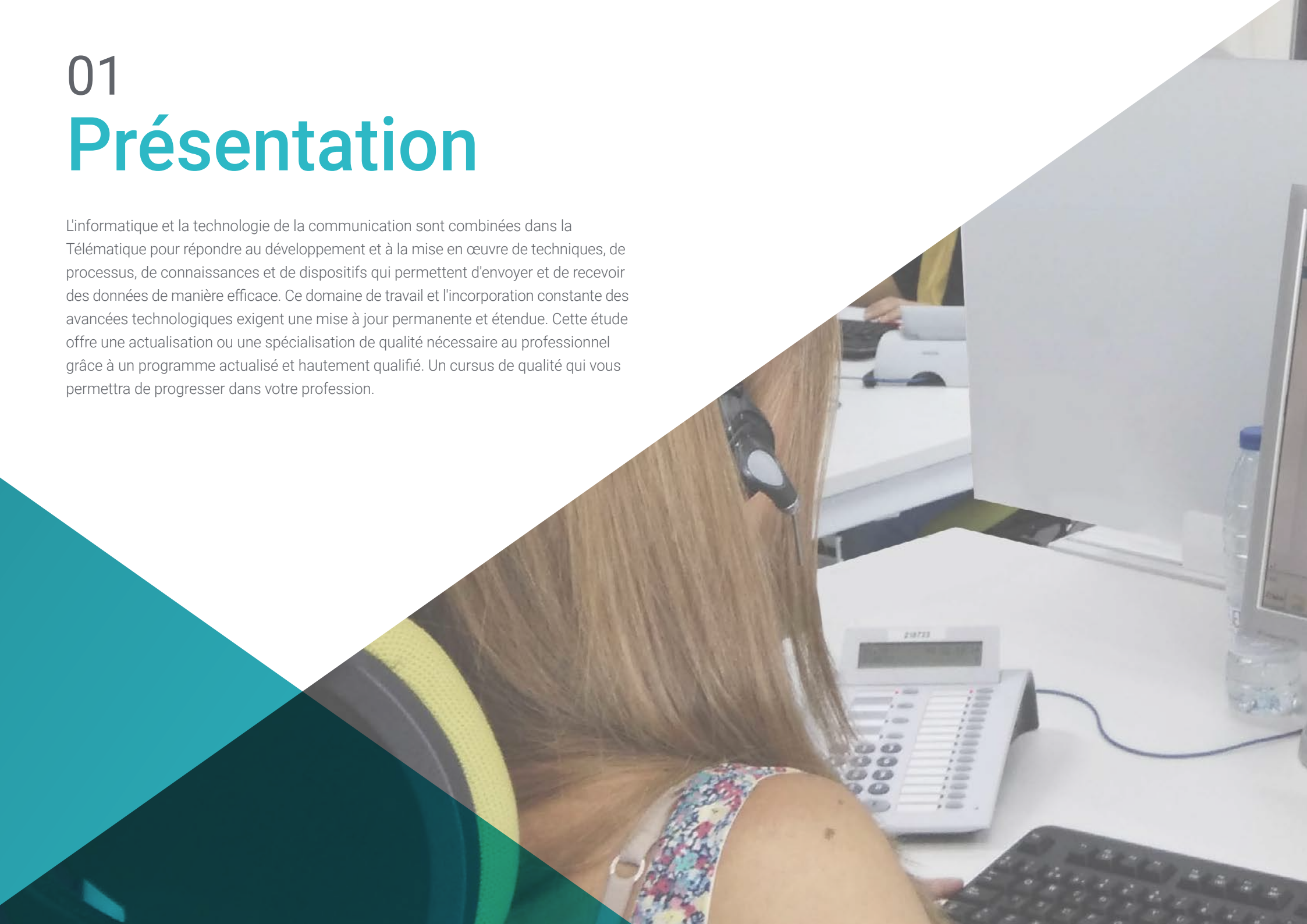
Accès au site web: www.techtitute.com/fr/informatique/master/master-telematique

Sommaire

01

Présentation

L'informatique et la technologie de la communication sont combinées dans la Télématique pour répondre au développement et à la mise en œuvre de techniques, de processus, de connaissances et de dispositifs qui permettent d'envoyer et de recevoir des données de manière efficace. Ce domaine de travail et l'incorporation constante des avancées technologiques exigent une mise à jour permanente et étendue. Cette étude offre une actualisation ou une spécialisation de qualité nécessaire au professionnel grâce à un programme actualisé et hautement qualifié. Un cursus de qualité qui vous permettra de progresser dans votre profession.



Complet, actualisé et adaptable à vos disponibilités, ce programme est un outil de grande qualité pour l'informaticien désireux d'élargir ses compétences"

Les progrès dans le domaine des télécommunications sont constants, car il s'agit de l'un des domaines qui évolue le plus rapidement. Par conséquent, il est nécessaire de disposer d'experts en informatique capables de s'adapter à ces changements et d'avoir une connaissance de première main des nouveaux outils et techniques qui émergent dans ce domaine.

Le programme en Télématique couvre toutes les matières impliquées dans ce domaine. Ce programme permet aux étudiants de connaître l'interrelation avec d'autres domaines inclus dans le champ multidisciplinaire des télécommunications, en offrant une vision plus large qui incorpore les compétences complémentaires d'autres domaines d'intérêt. L'équipe pédagogique de ce programme a réalisé une sélection minutieuse de chacun des thèmes de ce programme, pour offrir aux étudiants une opportunité d'étude la plus complète possible et toujours en lien avec l'actualité.

Ce programme s'adresse à ceux qui souhaitent atteindre un niveau supérieur de connaissances en Télématique. L'objectif principal est de permettre aux étudiants d'appliquer les connaissances acquises dans ce diplôme dans le monde réel, dans un environnement de travail qui reproduit les conditions qu'ils pourraient rencontrer dans leur avenir, de manière rigoureuse et réaliste.

De plus, comme il s'agit d'un programme 100% en ligne, l' étudiant n'aura aucunes contraintes horaires ou de déplacements, et accédera aux contenus à tout moment, en combinant sa vie personnelle avec sa vie académique.

Ce **Mastère Spécialisé en Télématique** contient le programme académique le plus complet et le plus actuel du marché. Les principales caractéristiques sont les suivantes:

- Le développement de cas pratiques présentés par des experts en Télématique
- Son contenu graphique, schématique et éminemment pratique est destiné à fournir des informations scientifiques et sanitaires sur les disciplines médicales indispensables à la pratique professionnelle
- Des exercices pratiques où le processus d'autoévaluation peut être réalisé pour améliorer l'apprentissage
- Il met l'accent sur les méthodologies innovantes en Télématique
- Les cours théoriques, des questions à l'expert, des forums de discussion sur des sujets controversés ainsi que des travaux de réflexion individuels
- La disponibilité de l'accès aux contenus à partir de tout appareil fixe ou portable avec connexion internet

Vous pourrez inclure dans vos compétences la capacité d'intervenir dans les différents domaines de la télématique, grâce à un parcours d'apprentissage qui stimulera votre développement professionnel"

Ce programme est le meilleur investissement que vous puissiez faire, en choisissant un programme de remise à niveau pour actualiser vos connaissances en Télématique"

Le matériel didactique utilisé pour l'étude est un recueil de grande qualité qui vous permettra d'avancer de manière simple et confortable.

Ce programme 100% en ligne vous permettra de combiner vos études avec votre travail professionnel.

Son corps enseignant comprend des professionnels du domaine Informatique des télécommunications, qui apportent leur expérience professionnelle à cette formation, ainsi que des spécialistes reconnus par des sociétés de premier plan et des universités prestigieuses.

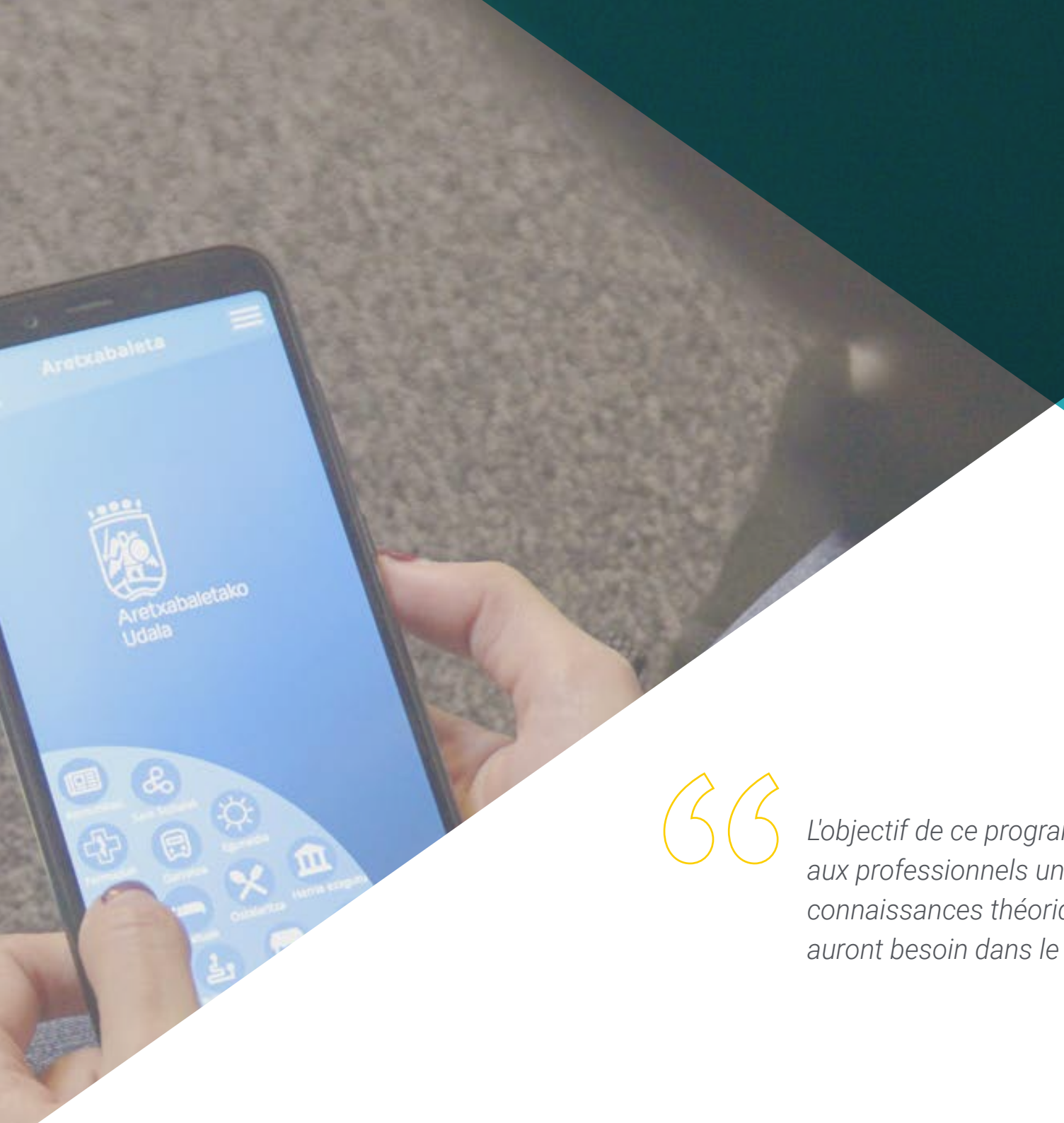
Grâce à son contenu multimédia développé avec les dernières technologies éducatives, les spécialistes bénéficieront d'un apprentissage situé et contextuel. Ainsi, ils se formeront dans un environnement simulé qui leur permettra d'apprendre en immersion et de s'entrainer dans des situations réelles.

La conception de ce programme est basée sur l'Apprentissage par les Problèmes, grâce auquel le professionnel devra essayer de résoudre les différentes situations de pratique professionnelle qui se présentent tout au long de la formation. À cette fin, le professionnel sera assisté d'un système vidéo interactif innovant créé par des experts reconnus et expérimentés en Télématique.

02

Objectifs

Le programme en Télématique vise à offrir aux professionnels de l'Informatique une étude complète et actualisée de tous les domaines d'intervention de ce domaine, avec la sécurité et la qualité d'un programme créé selon un critère d'excellence totale.



L'objectif de ce programme est de fournir aux professionnels un aperçu complet des connaissances théoriques et pratiques dont ils auront besoin dans le domaine de la Télématique"

Objectif général

- Former des étudiants à développer des applications télématiques, à analyser des données ou à effectuer des tâches de sécurité numérique

Une opportunité créée pour les professionnels qui recherchent un cours intensif et efficace pour donner un élan significatif à leur carrière"

Objectifs spécifiques

Module 1. Réseaux informatiques

- Acquérir les connaissances essentielles des réseaux informatiques sur Internet
- Comprendre le fonctionnement des différentes couches qui définissent un système en réseau, telles que les couches d'application, de transport, de réseau et de liaison
- Connaître la composition des réseaux locaux, leur topologie, les éléments de réseau et d'interconnexion
- Apprendre le fonctionnement de l'adressage et du sous-réseau IP
- Comprendre la structure des réseaux sans fil et mobiles, y compris le nouveau réseau 5G
- Connaître les différents mécanismes de sécurité des réseaux, ainsi que les différents protocoles de sécurité Internet

Module 2. Systèmes distribués

- Contrôler les principes de base des systèmes distribués
- Apprendre à caractériser et à classer les systèmes distribués en fonction d'un certain nombre de paramètres de base
- Comprendre les différents types de modèles utilisés dans les systèmes distribués
- Comprendre les architectures actuelles qui mettent en œuvre le concept de systèmes de fichiers distribué
- Analyser les algorithmes de synchronisation des processus et des objets, la définition des horloges logiques et la cohérence temporelle des informations
- Comprendre le système de dénomination utilisé sur Internet, connu sous le nom de DNS (Domain Name System)
- Apprendre le fonctionnement de l'adressage IP et le *Subnetting*

Module 3. Sécurité des systèmes et réseaux de communication

- Acquérir une perspective globale sur la sécurité, la cryptographie et la cryptanalyse classique
- Comprendre les principes fondamentaux de la cryptographie symétrique et de la cryptographie asymétrique, ainsi que leurs principaux algorithmes
- Analyser la nature des attaques de réseaux et les différents types d'architectures de sécurité
- Comprendre les différentes techniques de protection des systèmes et de développement de codes sécurisés
- Comprendre les composantes essentielles des réseaux de zombies et du spam, ainsi que des logiciels et des codes malveillants
- Établir les bases de l'analyse criminalistique dans le monde des logiciels et des audits informatiques

Module 4. Réseaux et infrastructures d'entreprise

- Maîtriser les aspects avancés de l'interconnexion des infrastructures, essentiels lors de la conception et de la planification des réseaux à grande vitesse
- Connaître les principales caractéristiques et technologies des réseaux de transport
- Comprendre les architectures WAN classiques, All-Ethernet, MPLS, VPN
- Analyser les aspects fondamentaux de l'évolution des réseaux vers les NGN (réseaux de prochaine génération)
- Compréhension des exigences avancées en matière de qualité de service, de routage, de contrôle de la congestion et de fiabilité
- Connaître et savoir appliquer les normes internationales en matière de réseaux

Module 5. Architectures de sécurité

- Comprendre les principes de base de la sécurité informatique
- Maîtriser les normes de sécurité informatique et les processus de certification
- Analyser les fondements organisationnels et cryptographiques sur lesquels reposent les technologies de sécurité
- Identifier les principales menaces et vulnérabilités des différents éléments impliqués dans les TIC, ainsi que leurs causes
- Acquérir une connaissance approfondie des outils de sécurité des réseaux et de leurs fonctions spécifiques
- Appliquer les technologies qui composent l'architecture de sécurité des TIC, dans ses différentes perspectives

Module 6. Centres de données, exploitation de réseaux et services

- Pouvoir concevoir, exploiter, gérer et entretenir des réseaux, des services et des contenus fournis par l'intermédiaire d'un Data Center
- Comprendre tous les éléments essentiels qui composent un Data Center et les normes et certifications existantes
- Analyser l'impact économique d'une infrastructure de Data Center en termes de performance et d'efficacité
- Identifier dans des infrastructures réelles les éléments matériels d'un Data Center
- Comprendre les implications en matière de sécurité des différentes solutions d'offre de services par les fournisseurs du marché
- Comprendre le fonctionnement du processus de virtualisation
- Comprendre les avantages, les bénéfices et les modèles d'adoption de l'informatique dématérialisée (Cloud)

Module 7. Programmation Avancée

- Approfondir les connaissances en matière de programmation, notamment en ce qui concerne la programmation par objet, et les différents types de relations entre les classes existantes
- Connaître les différents modèles de conception pour les problèmes concernant l'objet
- Apprendre la programmation événementielle et le développement d'interfaces utilisateurs avec Qt
- Acquérir les connaissances essentielles de la programmation concurrente, des processus et des fils d'exécution
- Apprendre à gérer l'utilisation des threads et de la synchronisation, ainsi que la résolution des problèmes courants de la programmation concurrente
- Comprendre l'importance de la documentation et des tests dans le développement de logiciels

Module 8. Ingénierie des systèmes et des services de réseau

- Maîtriser les concepts fondamentaux de l'ingénierie des services
- Comprendre les principes de base de la gestion de la configuration des systèmes logiciels en évolution
- Connaître les technologies et les outils pour la fourniture de services télématiques
- Connaître les différents styles d'architecture d'un système logiciel, comprendre leurs différences et savoir choisir le plus approprié en fonction des exigences du système
- Comprendre les processus de validation et de vérification et leurs relations avec les autres phases du cycle de vie

- Être capable d'intégrer des systèmes de capture, de représentation, de traitement, de stockage, de gestion et de présentation de l'information multimédia pour la construction de services de télécommunication et d'applications télématiques
- Connaître les éléments communs pour la conception détaillée d'un système logiciel
- Acquérir des compétences en matière de programmation, de simulation et de validation pour les services et les applications télématiques, en réseau et distribués
- Comprendre le processus et les activités de transition, de configuration, de déploiement et d'exploitation
- Comprendre les processus de gestion, d'automatisation et d'optimisation des réseaux

Module 9. Audits des Systèmes d' Information

- Connaître les principaux concepts, normes et méthodologies de l'audit des systèmes
- Connaître les éléments organisationnels et le cadre juridique des audits
- Obtenir un guide de référence pour la conception de nouveaux systèmes de contrôle interne des technologies de l'information
- Comprendre et identifier les risques liés au développement technologique
- Détecter comment les différents systèmes d'information répondent ou non aux exigences de sécurité souhaitées
- Pouvoir mettre en œuvre un processus d'amélioration continue de la cybersécurité

Module 10. Gestion de Projets

- Connaître les concepts fondamentaux et le cycle de vie de la gestion de projets
- Comprendre les différentes étapes de la Gestion de Projets, telles que le lancement, la planification, la gestion des *Stakeholders* et le champ d'action
- Élaborer un calendrier pour la gestion du temps, l'élaboration d'un budget et la réponse aux risques
- Comprendre le fonctionnement de la gestion de la qualité dans les projets, la planification, l'assurance, le contrôle, les concepts statistiques et les outils disponibles
- Comprendre le fonctionnement des processus de passation de marchés, d'exécution, de suivi, de contrôle et la clôture d'un projet
- Acquérir les connaissances essentielles liées à la responsabilité professionnelle découlant de la Gestion de Projets

03

Compétences

À l'issue des évaluations du programme Télématique, vous aurez acquis les compétences nécessaires pour intervenir de manière sûre et actualisée dans les différents domaines de travail développés par la Télématique. Un processus de développement des compétences qui marquera la différence dans votre carrière professionnelle.

Acquérez les compétences d'un spécialiste en Télématique et intervenez dans ce domaine avec la vision d'un professionnel de pointe"

Compétence générale

- Développer des applications télématiques et effectuer des tâches de sécurité numérique

Spécialisez-vous avec les meilleurs et soyez à la pointe de l'intervention professionnelle"

Compétences spécifiques

- Connaître l'ensemble de la structure des réseaux informatiques
- Maîtriser les systèmes distribués et savoir les classer
- Effectuer des tâches de sécurité sur les systèmes et réseaux de communication
- Appliquer les normes internationales pour les réseaux
- Maîtriser toutes les procédures de sécurité informatique
- Concevoir et gérer des centres de données
- Effectuer des tâches de programmation, détecter les problèmes éventuels et les résoudre
- Connaître l'ensemble du processus de conception des systèmes
- Réaliser des audits de systèmes et améliorer la cybersécurité
- Connaître toutes les étapes de la gestion de projet et son cycle de vie afin de savoir les gérer

04

Structure et contenu

La structure des contenus a été conçue par les meilleurs professionnels du secteur de l'informatique de télécommunications. Ce programme intensif et complet comprend tous les aspects que l'informaticien travaillant dans le domaine de la Télématique doit gérer en toute confiance, de manière structurée et efficace pour l'étudiant.

Nous disposons du programme le plus complet et le plus récent du marché. Nous visons l'excellence académique et nous voulons que vous l'atteigniez également"

Module 1. Réseaux informatiques

1.1. Réseaux informatiques sur Internet
- 1.1.1. Réseaux et Internet
- 1.1.2. Architecture du protocole

1.2. La couche d'application
- 1.2.1. Modèle et protocoles
- 1.2.2. Services FTP et SMTP
- 1.2.3. Service DNS
- 1.2.4. Modèle d'opération HTTP
- 1.2.5. Formats des messages HTTP
- 1.2.6. Interaction avec les méthodes avancées

1.3. La couche de transport
- 1.3.1. Communication interprocessus
- 1.3.2. Transport orienté vers la connexion: TCP et SCTP

1.4. La couche réseau
- 1.4.1. Commutation de circuits et de paquets
- 1.4.2. Le protocole IP (v4 et v6)
- 1.4.3. Algorithmes de routage

1.5. La couche de liaison
- 1.5.1. Couche de liaison et techniques de détection et de correction d'erreurs
- 1.5.2. Liens et protocoles d'accès multiple
- 1.5.3. Adressage au niveau des liaisons

1.6. Réseaux LAN
- 1.6.1. Topologies de réseau
- 1.6.2. Éléments de réseau et d'interconnexion

1.7. Adressage IP
- 1.7.1. Adressage IP et *Subnetting*
- 1.7.2. Vue d'ensemble: une requête HTTP

1.8. Réseaux sans fil et mobiles
- 1.8.1. Réseaux et services mobiles 2G, 3G et 4G
- 1.8.2. Réseaux 5G

1.9. Sécurité des réseaux
- 1.9.1. Principes fondamentaux de la sécurité des communications
- 1.9.2. Contrôle d'accès
- 1.9.3. Sécurité des systèmes
- 1.9.4. Principes fondamentaux de la cryptographie
- 1.9.5. Signature numérique

1.10. Protocoles de sécurité Internet
- 1.10.1. Sécurité IP et Réseaux Privés Virtuels (VPN)
- 1.10.2. Sécurité du Web avec SSL/TLS

Module 2. Systèmes distribués

2.1. Introduction à l'informatique distribuée
- 2.1.1. Concepts de base
- 2.1.2. Informatique monolithique, distribuée, parallèle et coopérative
- 2.1.3. Avantages, inconvénients et défis des systèmes distribués
- 2.1.4. Concepts préliminaires sur les systèmes d'exploitation: processus et concurrence
- 2.1.5. Concepts préliminaires du réseau
- 2.1.6. Concepts préliminaires sur le génie logiciel
- 2.1.7. Organisation du manuel

2.2. Paradigmes informatiques distribués et communication entre processus
- 2.2.1. Communication interprocessus
- 2.2.2. Synchronisation des événements
  - 2.2.2.1. Situation 1 : envoi synchrone et réception synchrone
  - 2.2.2.2. Situation 2 : envoi asynchrone et réception synchrone
  - 2.2.2.3. Situation 3 : envoi synchrone et réception asynchrone
  - 2.2.2.4. Situation 4 : envoi asynchrone et réception asynchrone
- 2.2.3. Verrouillages et temporisations
- 2.2.4. Représentation et codage des données
- 2.2.5. Classification et description des paradigmes informatiques distribués
- 2.2.6. Java en tant qu'environnement de développement des systèmes distribués

2.3. API de *Sockets*
- 2.3.1. API Sockets, types et différences
- 2.3.2. Sockets de type datagramme
- 2.3.3. Sockets de type *Stream*
- 2.3.4. Solution aux interblocages: temporisations et événements non bloquants
- 2.3.5. Sécurité des *Sockets*

2.4 Paradigme de communication client-serveur
- 2.4.1. Caractéristiques et concepts fondamentaux des systèmes distribués client-serveur
- 2.4.2. Processus de conception et de mise en œuvre d'un système client-serveur
- 2.4.3. Problèmes d'adressage non orienté connexion avec des clients anonymes
- 2.4.4. Serveurs itératifs et simultanés
- 2.4.5. Informations sur les états et les sessions
  - 2.4.5.1. Informations sur les sessions
  - 2.4.5.2. Informations sur l'état global
- 2.4.6. Clients complexes recevant des réponses asynchrones du côté serveur
- 2.4.7. Serveurs complexes agissant comme intermédiaires entre plusieurs clients

2.5. Communication de groupe
- 2.5.1. Introduction à la multidiffusion et à ses utilisations courantes
- 2.5.2. Fiabilité et ordonnancement dans les systèmes de multidiffusion
- 2.5.3. Implémentation Java des systèmes de multidiffusion
- 2.5.4. Exemple d'utilisation de la communication de groupe poste
- 2.5.5. Implémentations fiables de la multidiffusion
- 2.5.6. Multidiffusion au niveau de l'application

2.6. Objets distribués
- 2.6.1. Introduction aux objets distribués
- 2.6.2. Architecture d'une application basée sur des objets distribués
- 2.6.3. Technologies des systèmes d'objets distribués
- 2.6.4. Couches logicielles Java RMI côté client et côté serveur
- 2.6.5. API Java RMI pour les objets distribués
- 2.6.6. Étapes de construction d'une application RMI
- 2.6.7. Utilisation de *Callback* en RMI
- 2.6.8. Déchargement dynamique des caches d'objets distants et du gestionnaire de sécurité RMI

2.7. Applications Internet I: HTML, XML, HTTP
- 2.7.1. Introduction aux Applications Internet I
- 2.7.2. Langage HTML
- 2.7.3. Langage XML
- 2.7.4. Protocole Internet HTTP
- 2.7.5. Utilisation de contenu dynamique: traitement des formulaires et CGI
- 2.7.6. Traitement des données d'état et de session sur l'internet

2.8. CORBA
- 2.8.1. Introduction à CORBA
- 2.8.2. Architecture du CORBA
- 2.8.3. Langage de description d'interface dans CORBA
- 2.8.4. Protocoles d'interopérabilité GIOP
- 2.8.5. Références d'objets distants IOR
- 2.8.6. Service de dénomination CORBA
- 2.8.7. Exemple IDL Java
- 2.8.8. Étapes de conception, de compilation et d'exécution en IDL Java

2.9. Applications Internet II: Applets, Servlets et SOA
- 2.9.1. Introduction aux Applications Internet II
- 2.9.2. Applets
- 2.9.3. Introduction aux Servlets
- 2.9.4. Servlets HTTP et leur fonctionnement
- 2.9.5. Maintien des informations d'état dans les Servlets
  - 2.9.5.1. Champs de formulaire cachés
  - 2.9.5.2. *Cookies*
  - 2.9.5.3. Variables de Servlet
  - 2.9.5.4. Objet Session
- 2.9.6. Services Web
- 2.9.7. Protocole SOAP
- 2.9.8. Bref aperçu de l'architecture REST

2.10. Paradigmes avancés
- 2.10.1. Introduction aux paradigmes avancés
- 2.10.2. Paradigme MOM
- 2.10.3. Paradigme de l'agent logiciel mobile
- 2.10.4. Paradigme de l'espace objet
- 2.10.5. Informatique collaborative
- 2.10.6. Tendances futures de l'informatique distribuée

Module 3. Sécurité des systèmes et réseaux de communication

3.1. Un aperçu de la sécurité, de la cryptographie et des cryptanalyses classiques.
- 3.1.1. Sécurité informatique: perspective historique
- 3.1.2. Mais qu'est-ce que la sécurité exactement?
- 3.1.3. Histoire de la cryptographie
- 3.1.4. Chiffres de substitution
- 3.1.5. Étude de cas: la machine Enigma

3.2. Cryptographie symétrique
- 3.2.1. Introduction et terminologie de base
- 3.2.2. Cryptage symétrique
- 3.2.3. Modes de fonctionnement
- 3.2.4. DES
- 3.2.5. La nouvelle norme AES
- 3.2.6. Cryptage de flux
- 3.2.7. Cryptanalyse

3.3. Cryptographie asymétrique
- 3.3.1. Origines de la cryptographie à clé publique
- 3.3.2. Concepts de base et fonctionnement
- 3.3.3. L'algorithme RSA
- 3.3.4. Certificats numériques
- 3.3.5. Stockage et gestion des clés

3.4. Attaques de réseau
- 3.4.1. Menaces et attaques contre les réseaux
- 3.4.2. Énumération
- 3.4.3. Interception du trafic *Sniffers*
- 3.4.4. Attaques par déni de service
- 3.4.5. Attaques par empoisonnement ARP

3.5. Architectures de sécurité
- 3.5.1. Architectures de sécurité traditionnelles
- 3.5.2. Secure Socket Layer: SSL
- 3.5.3. Protocole SSH
- 3.5.4. Réseaux privés virtuels (VPN)
- 3.5.5. Mécanismes de protection des unités de stockage externes
- 3.5.6. Mécanismes de protection du matériel

3.6. Techniques de protection des systèmes et développement de code sécurisé
- 3.6.1. Sécurité des opérations
- 3.6.2. Ressources et contrôle
- 3.6.3. Monitoring
- 3.6.4. Systèmes de détection d'intrusion
- 3.6.5. IDS de *Host*
- 3.6.6. IDS réseau
- 3.6.7. IDS basé sur les signatures
- 3.6.8. Systèmes de leurres
- 3.6.9. Principes de base de la sécurité dans le développement du code
- 3.6.10. Gestion des pannes
- 3.6.11. Ennemi public numéro 1 : le dépassement de tampon
- 3.6.12. Botches cryptographiques

3.7. Botnets et *Spam*
- 3.7.1. Origine du problème
- 3.7.2. Processus de spam
- 3.7.3. Envoi de spam
- 3.7.4. Affinement des listes de diffusion

3.7.5. Techniques de protection
3.7.6. Service *Antispam* offert par des tiers
3.7.7. Étude de cas
3.7.8. Spam exotique
3.8. Audit et attaques du Web
3.8.1. Collecte d'informations
3.8.2. Techniques d'attaque
3.8.3. Outils
3.9. Malware et code malveillant
3.9.1. Qu'est-ce qu'un malware?
3.9.2. Types de malware
3.9.3. Virus
3.9.4. Cryptovirus
3.9.5. Vers
3.9.6. *Adware*
3.9.7. *Spyware*
3.9.8. *Hoaxes*
3.9.9. *Pishing*
3.9.10. Cheval de Troie
3.9.11. L'économie des malware
3.9.12. Solutions possibles
3.10. Analyse médico-légale
3.10.1. Collecte des preuves
3.10.2. Analyse des preuves
3.10.3. Techniques anti-médico-légal
3.10.4. Étude de cas pratique

Module 4. Réseaux et infrastructures d'entreprise

4.1. Réseaux de transport
4.1.1. Architecture fonctionnelle des réseaux de transport
4.1.2. Interface de nœud de réseau en SDH
4.1.3. Élément de réseau
4.1.4. Qualité et disponibilité du réseau
4.1.5. Gestion du réseau de transmission
4.1.6. Évolution des réseaux de transmission
4.2. Architectures WAN classiques
4.2.1. Réseaux étendus WAN
4.2.2. Normes WAN
4.2.3. Encapsulation WAN
4.2.4. Dispositifs WAN
4.2.4.1. Router
4.2.4.2. Modem
4.2.4.3. *Switch*
4.2.4.4. Serveurs de communication
4.2.4.5. *Gateway*
4.2.4.6. *Firewall*
4.2.4.7. *Proxy*
4.2.4.8. NAT
4.2.5. Types de connexion
4.2.5.1. Liaisons point à point
4.2.5.2. Commutation de circuits
4.2.5.3. Commutation de paquets
4.2.5.4. Circuits virtuels WAN
4.3. Réseaux basés sur l'ATM
4.3.1. Introduction, caractéristiques et modèle de couche
4.3.2. Couche d'accès physique ATM
4.3.2.1. Sous-couche dépendante du support physique PM
4.3.2.2. Sous-couche de convergence de transmission, TC

4.3.3. Cellule ATM
4.3.3.1. En-tête
4.3.3.2. Connexion virtuelle
4.3.3.3. Nœud de Switching ATM
4.3.3.4. Contrôle de flux (Link Loading)
4.3.4. Adaptation des cellules AAL
4.3.4.1. Types de services AAL
4.4. Modèles avancés de file d'attente
4.4.1. Introduction
4.4.2. Fondements de la théorie des files d'attente
4.4.3. Théorie des files d'attente - systèmes de base
4.4.3.1. Systèmes M/M/1, M/M/m et M/M/∞
4.4.3.2. Systèmes M/M/1/k et M/M/m/m/m
4.4.4. Théorie des files d'attente - systèmes avancés
4.4.4.1. Système M/G/1
4.4.4.2. Système M/G/1 avec priorités
4.4.4.3. Réseaux de file d'attente
4.4.4.4. Modélisation des réseaux de communication
4.5. Qualité de service dans les réseaux d'entreprise
4.5.1. Principes fondamentaux
4.5.2. Facteurs de QoS dans les réseaux convergents
4.5.3. Concepts de QoS
4.5.4. Politiques de QoS
4.5.5. Méthodes de mise en œuvre du QoS
4.5.6. Modèles de QoS
4.5.7. Mécanismes de déploiement pour la QoS DiffServ
4.5.8. Exemple d'application
4.6. Réseaux d'entreprise et infrastructures All-Ethernet
4.6.1. Topologies des Réseaux Ethernet
4.6.1.1. Topologie en bus
4.6.1.2. Topologie en étoile
4.6.2. Format de trame Ethernet et IEEE 802.3
4.6.3. Réseau Ethernet Commuté

4.6.3.1. Réseaux virtuels (VLAN)
4.6.3.2. Agrégation de ports
4.6.3.3. Redondance de connexion
4.6.3.4. Gestion de QoS
4.6.3.5. Fonctions de sécurité
4.6.4. Fast Ethernet
4.6.5. Gigabit Ethernet
4.7. Infrastructures MPLS
4.7.1. Introduction
4.7.2. MPLS
4.7.2.1. Historique et évolution de MPLS
4.7.2.2. Architecture du MPLS
4.7.2.3. Réexpédition de paquets étiquetés
4.7.2.4. Protocole de distribution d'étiquettes (LDP)
4.7.3. VPN MPLS
4.7.3.1. Définition d'un VPN
4.7.3.2. Modèles VPN
4.7.3.3. Modèle VPN MPLS
4.7.3.4. Architecture VPN MPLS
4.7.3.5. *Virtual Routing Forwarding* (VRF)
4.7.3.6. RD
4.7.3.7. Route Target (RT)
4.7.3.8. Propagation des routes VPNv4 dans un VPN MPLS
4.7.3.9. Transfert de paquets dans un réseau VPN MPLS
4.7.3.10. BGP
4.7.3.11. Communauté étendue BGP: RT
4.7.3.12. Transport d'étiquettes BGP
4.7.3.13. Route Reflector (RR
4.7.3.14. Groupe RR
4.7.3.15. Sélection de route BGP
4.7.3.16. Transfert de paquets

4.7.4. Protocoles de *Routing* courants des environnements MPLS
4.7.4.1. Protocoles de routage à Distance Vectorielle
4.7.4.2. Protocoles de routage de l'État de Liaison
4.7.4.3. OSPF
4.7.4.4. ISIS
4.8. Services aux opérateurs et VPN
4.8.1. Introduction
4.8.2. Exigences de base de VPN
4.8.3. Types de VPN
4.8.3.1. VPN d'accès à distance
4.8.3.2. VPN point à point
4.8.3.3. VPN interne (over LAN)
4.8.4. Protocoles utilisés dans les VPN
4.8.5. Implémentations et types de connexion
4.9. NGN (Next Generation Networks)
4.9.1. Introduction
4.9.2. Contexte
4.9.2.1. Définition et caractéristiques du réseau NGN
4.9.2.2. Migration vers les réseaux de prochaine génération
4.9.3. Architecture du NGN
4.9.3.1. Couche de connectivité primaire
4.9.3.2. Couche d'accès
4.9.3.3. Couche de service
4.9.3.4. Couche de gestion
4.9.4. IMS
4.9.5. Organismes de normalisation
4.9.6. Tendances réglementaires
4.10. Examen des normes de l'UIT et de l'IETF
4.10.1. Introduction
4.10.2. Normalisation
4.10.3. Quelques organismes types
4.10.4. Protocoles et normes de la couche physique du WAN
4.10.5. Exemples de protocoles axés sur le support

Module 5. Architectures de sécurité

5.1. Principes de base de la sécurité informatique
5.1.1. Qu'entend-on par sécurité informatique?
5.1.2. Objectifs de la sécurité informatique
5.1.3. Services de sécurité informatique
5.1.4. Conséquences d'un manque de sécurité
5.1.5. Principe de défense de la sécurité
5.1.6. Politiques, plans et procédures de sécurité
5.1.6.1. Gestion des comptes utilisateurs
5.1.6.2. Identification et authentification des utilisateurs
5.1.6.3. Contrôle d'accès logique et autorisation
5.1.6.4. Surveillance du serveur
5.1.6.5. Protection des données
5.1.6.6. Sécurité des connexions à distance
5.1.7. L'importance du facteur humain
5.2. Normalisation et certification de la sécurité des TI
5.2.1. Normes de sécurité
5.2.1.1. Objectif des normes
5.2.1.2. Organismes responsables
5.2.2. Normes aux États-Unis
5.2.2.1. TCSEC
5.2.2.2. Federal Criteria
5.2.2.3. FISCAM
5.2.2.4. NIST SP 800
5.2.3. Normes européennes
5.2.3.1. ITSEC
5.2.3.2. ITSEM
5.2.3.3. Agence Européenne pour la Sécurité des Réseaux et de l'Information
5.2.4. Normes internationales
5.2.5. Processus de certification

5.3. Menaces pour la sécurité informatique: vulnérabilités et logiciels malveillants
- 5.3.1. Introduction
- 5.3.2. Vulnérabilités des systèmes
  - 5.3.2.1. Incidents de sécurité dans les réseaux
  - 5.3.2.2. Causes de la vulnérabilité des systèmes informatiques
  - 5.3.2.3. Types de vulnérabilités
  - 5.3.2.4. Responsabilités des fabricants de logiciels
  - 5.3.2.5. Outils d'évaluation de la vulnérabilité
- 5.3.3. Menaces pour la sécurité informatique
  - 5.3.3.1. Classification des intrus dans les réseaux
  - 5.3.3.2. Motivations des attaquants
  - 5.3.3.3. Phases d'une attaque
  - 5.3.3.4. Types d'attaques
- 5.3.4. Virus informatiques
  - 5.3.4.1. Caractéristiques générales
  - 5.3.4.2. Types de virus
  - 5.3.4.3. Dommages causés par des virus
  - 5.3.4.4. Comment lutter contre les virus

5.4. Cyberterrorisme et réponse aux incidents
- 5.4.1. Introduction
- 5.4.2. La menace du cyberterrorisme et des cyberguerres
- 5.4.3. Conséquences des défaillances et attaques sur les entreprises
- 5.4.4. Espionnage dans les réseaux informatiques

5.5. Identification des utilisateurs et systèmes biométriques
- 5.5.1. Introduction à l'authentification, l'autorisation et l'enregistrement des utilisateurs
- 5.5.2. Modèle de sécurité AAA
- 5.5.3. Contrôle d'accès
- 5.5.4. Identification de l'utilisateur
- 5.5.5. Vérification du mot de passe
- 5.5.6. Authentification par certificats numériques
- 5.5.7. Identification de l'utilisateur à distance
- 5.5.8. Accès unique
- 5.5.9. Gestionnaires de mots de passe
- 5.5.10. Systèmes biométriques
  - 5.5.10.1. Caractéristiques générales
  - 5.5.10.2. Types des systèmes biométriques
  - 5.5.10.3. Implémentation des systèmes

5.6. Principes fondamentaux de la cryptographie et des protocoles cryptographiques
- 5.6.1. Introduction à la cryptographie
  - 5.6.1.1. Cryptographie, cryptanalyse et cryptologie
  - 5.6.1.2. Fonctionnement d'un système cryptographique
  - 5.6.1.3. Histoire des systèmes cryptographiques
- 5.6.2. Cryptanalyse
- 5.6.3. Classification des systèmes cryptographiques
- 5.6.4. Systèmes cryptographiques symétriques et asymétriques
- 5.6.5. Authentification avec des systèmes cryptographiques
- 5.6.6. Signature électronique
  - 5.6.6.1. Qu'est-ce qu'une signature électronique?
  - 5.6.6.2. Caractéristiques de la signature électronique
  - 5.6.6.3. Autorités de certification
  - 5.6.6.4. Certificats numériques
  - 5.6.6.5. Systèmes basés sur des tiers de confiance
  - 5.6.6.6. Utilisation de la signature électronique
  - 5.6.6.7. Identité électronique
  - 5.6.6.8. Facture électronique

5.7. Outils de sécurité des réseaux
- 5.7.1. Le problème de la sécurité des connexions Internet
- 5.7.2. Sécurité dans le réseau externe
- 5.7.3. Le rôle des serveurs *Proxy*
- 5.7.4. Le rôle des pare-feu
- 5.7.5. Serveurs d'authentification pour les connexions à distance
- 5.7.6. L'analyse des registres d'activité
- 5.7.7. Systèmes de détection d'intrusion
- 5.7.8. Les ameçons

5.8. Sécurité des réseaux privés virtuels et des réseaux sans fil
- 5.8.1. Sécurité des réseaux privés virtuels
  - 5.8.1.1 Le rôle des VPN
  - 5.8.1.2 Protocoles des VPN
- 5.8.2. Sécurité traditionnelle dans les réseaux sans fil
- 5.8.3. Attaques potentielles des réseaux sans fil
- 5.8.4. Le protocole WEP
- 5.8.5. Normes de sécurité des réseaux sans fil
- 5.8.6. Recommandations pour renforcer la sécurité

5.9. Sécurité dans l'utilisation des services internet
- 5.9.1. Navigation sûre sur le web
  - 5.9.1.1. Le service www
  - 5.9.1.2. Problèmes de sécurité sur www
  - 5.9.1.3. Recommandations de sécurité
  - 5.9.1.4. Protection de la vie privée sur Internet
- 5.9.2. Sécurité du courrier électronique
  - 5.9.2.1. Caractéristiques du courrier électronique
  - 5.9.2.2. Problèmes de sécurité du courrier électronique
  - 5.9.2.3. Recommandations en sécurité du courrier électronique
  - 5.9.2.4. Services avancés de courrier électronique
  - 5.9.2.5. Utilisation du courrier électronique par les employés
- 5.9.3. Le SPAM
- 5.9.4. Le *Phising*

5.10. Contrôle des contenus
- 5.10.1. La distribution des contenus sur l'internet
- 5.10.2. Mesures juridiques pour lutter contre les contenus illicites
- 5.10.3. Filtrage, catalogage et blocage des contenus
- 5.10.4. Atteinte à l'image et la réputation

Module 6. Centres de données, exploitation de réseaux et services

6.1. Data Center: concepts et composants de base
- 6.1.1. Introduction
- 6.1.2. Concepts de base
  - 6.1.2.1. Définition d'un DC
  - 6.1.2.2. Classification et importance
  - 6.1.2.3. Catastrophes et pertes
  - 6.1.2.4. Tendance évolutive
  - 6.1.2.5. Coûts de la complexité
  - 6.1.2.6. Piliers et couches de redondance
- 6.1.3. Philosophie de conception
  - 6.1.3.1. Objectifs
  - 6.1.3.2. Choix de l'emplacement
  - 6.1.3.3. Disponibilité
  - 6.1.3.4. Éléments critiques
  - 6.1.3.5. Évaluation et analyse des coûts
  - 6.1.3.6. Budgétisation de la TI
- 6.1.4. Composants de base
  - 6.1.4.1. Plancher technique
  - 6.1.4.2. Types de dalles
  - 6.1.4.3. Considérations générales
  - 6.1.4.4. Taille du CD
  - 6.1.4.5. *Racks*
  - 6.1.4.6. Serveurs et équipements de communication
  - 6.1.4.7. Surveillance

6.2. *Data Center*: systèmes de contrôle
- 6.2.1. Introduction
- 6.2.2. Alimentation électrique
  - 6.2.2.1. Réseau électrique
  - 6.2.2.2. Puissance électrique

6.2.2.3. Stratégies de distribution de l'électricité
6.2.2.4. UPS
6.2.2.5. Générateurs
6.2.2.6. Problèmes électriques
6.2.3. Contrôle de l'environnement
6.2.3.1. Température
6.2.3.2. Humidité
6.2.3.3. Climatisation
6.2.3.4. Estimation des calories
6.2.3.5. Stratégies de refroidissement
6.2.3.6. Conception des couloirs Circulation de l'air
6.2.3.7. Capteurs et maintenance
6.2.4. Sécurité et prévention des incendies
6.2.4.1. Sécurité physique
6.2.4.2. Le feu et sa classification
6.2.4.3. Classification et types de systèmes d'extinction
6.3. *Data Centers*: conception et organisation
6.3.1. Introduction
6.3.2. Conception du réseau
6.3.2.1. Typologies
6.3.2.2. Câblage structuré
6.3.2.3. Backbone
6.3.2.4. Câbles de réseau UTP y STP
6.3.2.5. Câbles téléphoniques
6.3.2.6. Éléments terminaux
6.3.2.7. Câbles à fibres optiques
6.3.2.8. Câbles coaxiaux
6.3.2.9. Transmission sans fil
6.3.2.10. Recommandations et étiquetage
6.3.3. Organisation
6.3.3.1. Introduction
6.3.3.2. Mesures basiques
6.3.3.3. Stratégies de gestion des câbles
6.3.3.4. Politiques et procédures
6.3.4. Gestion de CD
6.3.5. Normes dans le *Data Center*
6.4. *Data Center*: modèles de continuité d'activité
6.4.1. Introduction
6.4.2. Optimisation
6.4.2.1. Techniques d'optimisation
6.4.2.2. *Data Centers* écologiques
6.4.2.3. Défis actuels
6.4.2.4. *Data Centers* modulaires
6.4.2.5. Housing
6.4.2.6. Consolidation des *Data Centers*
6.4.2.7. Monitoring
6.4.3. Continuité des activités
6.4.3.1. BCP Plan de continuité des activités Points clés
6.4.3.2. DR Plan de récupération après un sinistre
6.4.3.3. Mise en œuvre du DR
6.4.3.4. *Backup* et stratégies
6.4.3.5. *Data Center* de sauvegarde
6.4.4. Meilleures pratiques
6.4.4.1. Recommandations
6.4.4.2. Utilisation de la méthodologie ITIL
6.4.4.3. Mesures de disponibilité
6.4.4.4. Contrôle de l'environnement
6.4.4.5. Gestion des risques
6.4.4.6. Responsable du CD
6.4.4.7. Outils
6.4.4.8. Conseils de mise en œuvre
6.4.4.9. Caractérisation

6.5. *Cloud Computing*: introduction et concepts de base
- 6.5.1. Introduction
- 6.5.2. Concepts et terminologie de base
- 6.5.3. Objectifs et avantages
  - 6.5.3.1. Disponibilité
  - 6.5.3.2. Fiabilité
  - 6.5.3.3. Évolutivité
- 6.5.4. Risques et défis
- 6.5.5. Rôles Provider Consumer
- 6.5.6. Caractéristiques du Cloud
- 6.5.7. Modèles de fourniture de services
  - 6.5.7.1. IaaS
  - 6.5.7.2. PaaS
  - 6.5.7.3. SaaS
- 6.5.8. Types de Cloud
  - 6.5.8.1. Publique
  - 6.5.8.2. Privé
  - 6.5.9.3. Hybride
- 6.5.9. Technologies habilitantes du cloud
  - 6.5.9.1. Architectures de réseau
  - 6.5.9.2. Réseaux à bande large Interconnectivité
  - 6.5.9.3. Technologies des Data Center
    - 6.5.9.3.1. *Computing*
    - 6.5.9.3.2. *Storage*
    - 6.5.9.3.3. *Networking*
    - 6.5.9.3.4. Haute disponibilité
    - 6.5.9.3.5. Systèmes de *Backup*
    - 6.5.9.3.6. Balances
  - 6.5.9.4. Virtualisation
  - 6.5.9.5. Technologies Web
  - 6.5.9.6. Technologie Multitenant

6.5.9.7. Technologie des services
6.5.9.8. Sécurité du Cloud
6.5.9.8.1. Termes et concepts
6.5.9.8.2. Intégrité et authentification
6.5.9.8.3. Mécanismes de sécurité
6.5.9.8.4. Menaces pour la sécurité
6.5.9.8.5. Attaques de sécurité du cloud
6.5.9.8.6. Études de cas

6.6. *Cloud Computing*: technologie et sécurité dans le nuage
6.6.1. Introduction
6.6.2. Mécanismes de l'infrastructure Cloud
6.6.2.1. Périmètre du réseau
6.6.2.2. Stockage
6.6.2.3. Environnement du serveur
6.6.2.4. Monitoring du Cloud
6.6.2.5. Haute disponibilité
6.6.3. Mécanismes de Sécurité du Cloud (Partie I)
6.6.3.1. Automatisation
6.6.3.2. Équilibreurs de charge
6.6.3.3. Moniteur SLA
6.6.3.4. Mécanismes de paiement d'utilisation
6.6.4. Mécanismes de Sécurité du Cloud (Partie II)
6.6.4.1. Systèmes de traçabilité et audit
6.6.4.2. Systèmes de Failover
6.6.4.3. Hyperviseur
6.6.4.4. Regroupement
6.6.4.5. Systèmes Multitenant

6.7. *Cloud Computing*: Infrastructure Mécanismes de contrôle et sécurité
6.7.1. Introduction aux mécanismes de gestion du cloud
6.7.2. Systèmes d'administration à distance
6.7.3. Systèmes de gestion des ressources
6.7.4. Systèmes de gestion des accords de niveau de service
6.7.5. Systèmes de gestion de la facturation
6.7.6. Mécanismes de Sécurité du Cloud
6.7.6.1. Cryptage
6.7.6.2. *Hashing*
6.7.6.3. Signature numérique
6.7.6.4. PKI
6.7.6.5. Gestion des accès et identifiants
6.7.6.6. SSO
6.7.6.7. Groupes de sécurité basés sur le cloud
6.7.6.8. Systèmes de bastion

6.8. *Cloud Computing*: Architectures Cloud
6.8.1. Introduction
6.8.2. Architectures basiques du Cloud
6.8.2.1. Architectures de répartition de la charge de travail
6.8.2.2. Architectures d'utilisation des ressources
6.8.2.3. Architectures graduelles
6.8.2.4. Architectures d'équilibrage des charges
6.8.2.5. Architectures redondantes
6.8.2.6. Exemples
6.8.3. Architectures cloud avancées
6.8.3.1. Architectures de clusters d'hyperviseurs
6.8.3.2. Architectures d'équilibrage de charge virtuelle
6.8.3.3. Architectures *non-stop*
6.8.3.4. Architectures de haute disponibilité
6.8.3.5. Architectures Bare metal
6.8.3.6. Architectures redondantes
6.8.3.7. Architectures hybrides

6.8.4. Architectures cloud spécialisées
6.8.4.1. Architectures à accès direct I/O
6.8.4.2. Architectures à accès direct LUN
6.8.4.3. Architectures de réseau élastique
6.8.4.4. Architectures SDDC
6.8.4.5. Architectures spéciales
6.8.4.6. Exemples
6.9. *Cloud Computing*: modèles de prestation de services
6.9.1. Introduction
6.9.2. Provision des services Cloud
6.9.3. Perspective du fournisseur de services
6.9.4. Perspective du consommateur de ces services
6.9.5. Étude de cas
6.10. *Cloud Computing*: modèles contractuels, mesures et fournisseurs de services
6.10.1. Introduction aux modèles et métriques de facturation
6.10.2. Modèles de facturation
6.10.3. Mesures de paiement à l'utilisation
6.10.4. Considérations relatives à la gestion des coûts
6.10.5. Introduction aux mesures de qualité de service et SLA
6.10.6. Mesures de la qualité des services
6.10.7. Mesures de performance des services
6.10.8. Mesures d'évolutivité des services
6.10.9. SLA du modèle de service
6.10.10. Étude de cas

Module 7. Programmation Avancée

7.1. Introduction à la programmation des objets
7.1.1. Introduction à la programmation des objets
7.1.2. Conception des classes
7.1.3. Introduction à UML pour la modélisation des problèmes
7.2. Relations entre les classes
7.2.1. Abstraction et héritage
7.2.2. Concepts avancés d'héritage
7.2.3. Polymorphisme
7.2.4. Composition et agrégation
7.3. Introduction aux modèles de conception pour les problèmes orientés objet
7.3.1. Que sont les patrons de conception?
7.3.2. Modèle Factory
7.3.3. Modèle Singleton
7.3.4. Modèle Observer
7.3.5. Modèle Composite
7.4. Exceptions
7.4.1. Qu'est-ce qu'une exception?
7.4.2. Capture et gestion des exceptions
7.4.3. Lancer des exceptions
7.4.4. Création d'une exception
7.5. Interfaces utilisateur
7.5.1. Introduction à Qt
7.5.2. Positionnement
7.5.3. Qu'est-ce qu'un événement?
7.5.4. Événements: définition et capture
7.5.5. Développement d'interfaces utilisateurs
7.6. Introduction à la programmation simultanée
7.6.1. Introduction à la programmation simultanée
7.6.2. Le concept de processus et de thread
7.6.3. Interaction entre processus ou threads
7.6.4. Les threads en C++
7.6.5. Avantages et inconvénients de la programmation concurrente
7.7. Gestion des threads et synchronisation
7.7.1. Cycle de vie des threads
7.7.2. La classe Thread
7.7.3. L'ordonnancement des threads
7.7.4. Les groupes de threads
7.7.5. Fils de type démon
7.7.6. Synchronisation

7.7.7. Mécanismes de verrouillage
7.7.8. Mécanismes de communication
7.7.9. Moniteurs
7.8. Problèmes courants dans la programmation concurrente
7.8.1. Le problème du producteur-consommateur
7.8.2. Le problème des lecteurs et des écrivains
7.8.3. Le problème du dîner des philosophes
7.9. Documentation et tests de logiciels
7.9.1. Pourquoi est-il important de documenter les logiciels?
7.9.2. Documentation de la conception
7.9.3. Utilisation d'outils pour la documentation
7.10. Tests de logiciels
7.10.1. Introduction aux tests de logiciels
7.10.2. Types de tests
7.10.3. Tests unitaires
7.10.4. Tests d'intégration
7.10.5. Test de validation
7.10.6. Test du système

Module 8. Ingénierie des systèmes et des services de réseau

8.1. Introduction à l'ingénierie des systèmes et aux services de réseau
8.1.1. Concept de système informatique et ingénierie informatique
8.1.2. Les logiciels et leurs caractéristiques
8.1.2.1. Caractéristiques des logiciels
8.1.3. L'évolution des logiciels
8.1.3.1. L'aube du développement des logiciels
8.1.3.2. La crise du logiciel
8.1.3.3. Génie logiciel
8.1.3.4. La tragédie des logiciels
8.1.3.5. L'actualité des logiciels
8.1.4. Les mythes du logiciel
8.1.5. Les nouveaux défis du logiciel
8.1.6. L'éthique professionnelle dans l'ingénierie logicielle
8.1.7. SWEBOK Le corps de connaissances du génie logiciel
8.2. Le processus de développement
8.2.1. Processus de résolution de problèmes
8.2.2. Le processus de développement des logiciels
8.2.3. Processus logiciel et cycle de vie
8.2.4. Cycles de vie. Modèles de processus (traditionnels)
8.2.4.1. Modèle en cascade
8.2.4.2. Modèles basés sur des prototypes
8.2.4.3. Modèle de développement incrémentiel
8.2.4.4. Développement rapide d'applications (RAD)
8.2.4.5. Modèle en spirale
8.2.4.6. Processus de développement unifié ou Rational Unified Process (RUP)
8.2.4.7. Développement de logiciels à base de composants
8.2.5. Le manifeste agile Méthodes agiles
8.2.5.1. Programmation extrême (XP)
8.2.5.2. Scrum
8.2.5.3. Développement piloté par les fonctionnalités (FDD)
8.2.6. Normes de processus logiciel
8.2.7. Définition d'un processus logiciel
8.2.8. Maturité des processus logiciels
8.3. Planification et gestion de projets agiles
8.3.1 Qu'est-ce que la méthode Agile?
8.3.1.1. Histoire d'Agile
8.3.1.2. Manifeste Agile
8.3.2. Principes fondamentaux de la méthode Agile
8.3.2.1. La mentalité Agile
8.3.2.2. L'ajustement Agile
8.3.2.3. Cycle de vie du développement du produit
8.3.2.4. Le triangle de fer
8.3.2.5. Travailler avec l'incertitude et la volatilité

8.3.2.6. Processus définis et processus empiriques
8.3.2.7. Les mythes de l'Agile
8.3.3. L'environnement Agile
8.3.3.1. Modèle d'exploitation
8.3.3.2. Rôles agiles
8.3.3.3. Techniques agiles
8.3.3.4. Pratiques agiles
8.3.4. Cadres agiles
8.3.4.1. e-Xtreme Programming (XP)
8.3.4.2. Scrum
8.3.4.3. Méthode de développement de systèmes dynamiques (DSDM)
8.3.4.4. Gestion de projet Agile
8.3.4.5. Kanban
8.3.4.6. Lean software Development
8.3.4.7. Lean Start-up
8.3.4.8. Scaled Agile Framework (SAFe)
8.4. Gestion de la configuration et référentiels collaboratifs
8.4.1. Principes de base de la gestion de la configuration logicielle
8.4.1.1. Qu'est-ce que la gestion de la configuration logicielle?
8.4.1.2. Configuration du logiciel et éléments de configuration du logiciel
8.4.1.3. Lignes de base
8.4.1.4. Versions, révisions, variantes et *Releases*
8.4.2. Activités de gestion de la configuration
8.4.2.1. Identification de la configuration
8.4.2.2. Contrôle des changements de configuration
8.4.2.3. Génération de rapports d'état
8.4.2.4. Audit de la configuration
8.4.3. Le plan de gestion de la configuration
8.4.4. Outils de gestion de la configuration
8.4.5. Gestion de la configuration dans la méthodologie Metric v.3
8.4.6. Gestion de la configuration dans SWEBOK

8.5. Test des systèmes et des services
- 8.5.1. Concepts généraux de test
  - 8.5.1.1. Vérifier et valider
  - 8.5.1.2. Définition des tests
  - 8.5.1.3. Principes d'essai
- 8.5.2. Approches en matière de tests
  - 8.5.2.1. Tests en boîte blanche
  - 8.5.2.2. Tests en boîte noire
- 8.5.3. Tests statiques ou révisions
  - 8.5.3.1. Revues techniques formelles
  - 8.5.3.2. *Walkthroughs*
  - 8.5.3.3. Inspections du code
- 8.5.4. Essais dynamiques
  - 8.5.4.1. Tests unitaires
  - 8.5.4.2. Tests d'intégration
  - 8.5.4.3. Test du système
  - 8.5.4.4. Test d'acceptation
  - 8.5.4.5. Tests de régression
- 8.5.5. Test alpha et test bêta
- 8.5.6. Le processus d'essai
- 8.5.7. Erreur, défaut et défaillance
- 8.5.8. Outils de tests automatisés
  - 8.5.8.1. Junit
  - 8.5.8.2. LoadRunner

8.6. Modélisation et conception d'architectures de réseaux
- 8.6.1. Introduction
- 8.6.2. Caractéristiques du système
  - 8.6.2.1. Description des systèmes
  - 8.6.2.2. Description et caractéristiques des services
  - 8.6.2.3. Exigences d'opérabilité

8.6.3. Analyse des besoins
8.6.3.1. Besoins des utilisateurs
8.6.3.2. Conditions d'application
8.6.3.3. Exigences en matière de réseau
8.6.4. Conception d'architectures de réseau
8.6.4.1. Architecture de référence et composants
8.6.4.2. Modèles d'architecture
8.6.4.3. Architectures de systèmes et de réseaux
8.7. Modélisation et conception de systèmes distribués
8.7.1. Introduction
8.7.2. Architecture d'adressage et de *routage*
8.7.2.1. Stratégie d'adressage
8.7.2.2. Stratégie de routage
8.7.2.3. Considérations sur la conception
8.7.3. Concepts de conception de réseaux
8.7.4. Processus de conception
8.8. Plateformes et environnements de déploiement
8.8.1. Introduction
8.8.2. Systèmes informatiques distribués
8.8.2.1. Concepts de base
8.8.2.2. Modèles de calcul
8.8.2.3. Avantages, inconvénients et défis
8.8.2.4. Les bases des systèmes d'exploitation
8.8.3. Déploiements de réseaux virtualisés
8.8.3.1. Besoin de changement
8.8.3.2. Transformation des réseaux: du "tout-IP" au Cloud
8.8.3.3. Déploiement de réseaux dans le nuage
8.8.4. Exemple: Architecture réseau dans Azure
8.9. Performances E2E: le délai et la largeur de bande QoS
8.9.1. Introduction
8.9.2. Analyse des performances
8.9.3. QoS
8.9.4. Priorité et gestion du trafic
8.9.5. Accords de niveau de service
8.9.6. Considérations sur la conception
8.9.6.1. Évaluation de la performance
8.9.6.2. Relations et interactions
8.10. Automatisation et optimisation des réseaux
8.10.1 Introduction
8.10.2. Gestion du réseau
8.10.2.1. Protocoles de gestion et de configuration
8.10.2.2. Architectures de gestion de réseau
8.10.3 Orchestration et automatisation
8.10.3.1. Architecture du ONAP
8.10.3.2. Contrôleurs et fonctions
8.10.3.3. Politiques
8.10.3.4. Inventaire du réseau
8.10.4 Optimisation

Module 9. Audits des Systèmes d' Information

9.1. Audits des Systèmes d' Information Normes de bonne pratique
9.1.1. Introduction
9.1.2. L'audit et COBIT
9.1.3. Audits des systèmes de gestion des TIC
9.1.4. Certifications
9.2. Concepts et méthodologies de l'audit des systèmes
9.2.1. Introduction
9.2.2. Méthodes d'évaluation des systèmes: quantitatives et qualitatives
9.2.3. Méthodologies d'audit informatique
9.2.4. Le plan d'audit
9.3. Le contrat d'audit
9.3.1. Nature juridique de la mission
9.3.2. Parties prenantes à une mission d'audit

9.3.3. Objet de la mission d'audit
9.3.4. Le rapport d'audit
9.4. Éléments organisationnels des audits
9.4.1. Introduction
9.4.2. Mission du service d'audit
9.4.3. Planification de l'audit
9.4.4. Méthodologie d'audit des SI
9.5. Cadre juridique des audits
9.5.1. Protection des données à caractère personnel
9.5.2. Protection juridique des logiciels
9.5.3. Infractions technologiques
9.5.4. Contrat, signature et identité électronique
9.6. Audit de sous-traitance et cadres de référence
9.6.1. Introduction
9.6.2. Concepts de base de l'outsorcing
9.6.3. Audit de l'outsorcing de TI
9.6.4. Cadre de référence: CMMI, ISO27001, ITIL
9.7. Audit de sécurité
9.7.1. Introduction
9.7.2. Sécurité physique et logique
9.7.3. Sécurité de l'environnement
9.7.4. Planification et exécution de l'audit de sécurité physique
9.8. Audit des réseaux et de l'internet
9.8.1. Introduction
9.8.2. Vulnérabilités des réseaux
9.8.3. Principes et droits d'internet
9.8.4. Contrôle et traitement des données
9.9. Audit des applications et systèmes informatiques
9.9.1. Introduction
9.9.2. Modèles de référence
9.9.3. Évaluer la qualité des applications
9.9.4. Audit de l'organisation et la gestion des aires de développement et d'entretien
9.10. Audit des données à caractère personnel
9.10.1. Introduction
9.10.2. Lois et règlements sur la protection des données
9.10.3. Réalisation de l'audit
9.10.4. Infractions et sanctions

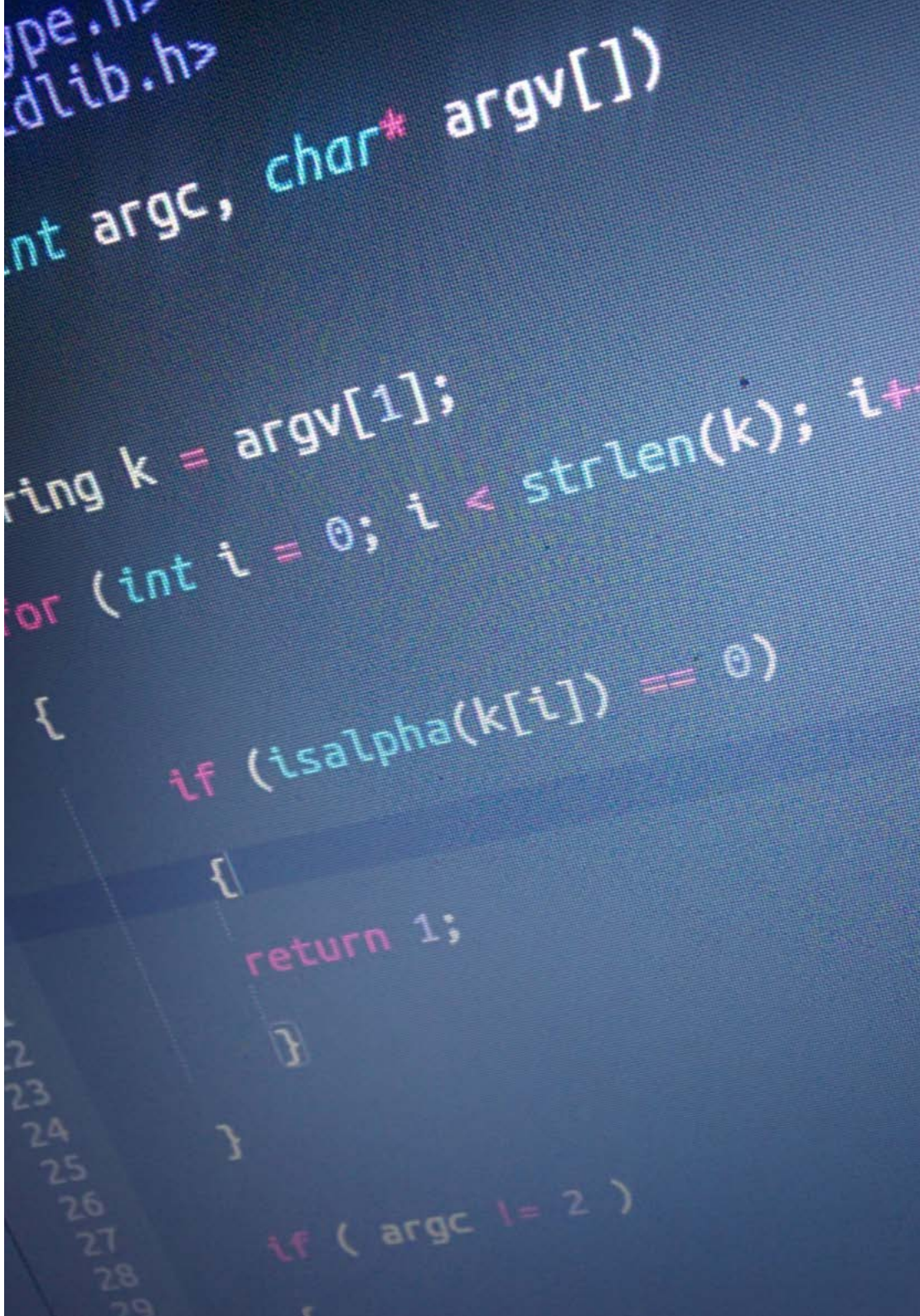
Module 10. Gestion de projets

10.1. Concepts fondamentaux de la conduite de projet et du cycle de vie de la Gestion de Projets
10.1.1. Qu'est-ce qu'un projet?
10.1.2. Méthodologie commune
10.1.3. Qu'est-ce que la gestion de projet?
10.1.4. Qu'est-ce qu'un plan de projet?
10.1.5. Avantages
10.1.6. Cycles de vie d'un projet
10.1.7. Groupes de processus ou cycle de vie de la gestion de projet
10.1.8. La relation entre les groupes de processus et les domaines de connaissances
10.1.9. Les relations entre le produit et le cycle de vie du projet
10.2. Initiation et planification
10.2.1. De l'idée au projet
10.2.2. Élaboration de la charte du projet
10.2.3. Réunion de lancement du projet
10.2.4. Tâches, connaissances et compétences dans le processus de démarrage
10.2.5. Le plan du projet
10.2.6. Élaboration du plan de base Étapes
10.2.7. Tâches, connaissances et compétences dans le processus de planification

10.3. Gestion des *Stakeholders* et du champ d'application
- 10.3.1. Identifier les parties prenantes
- 10.3.2. Élaborer le plan de gestion des parties prenantes
- 10.3.3. Gérer l'engagement des parties prenantes
- 10.3.4. Contrôler l'engagement des parties prenantes
- 10.3.5. L'objectif du projet
- 10.3.6. La gestion du champ d'application et son plan
- 10.3.7. Recueil des conditions
- 10.3.8. Définir l'énoncé du champ d'application
- 10.3.9. Créer l'organigramme des tâches WBS
- 10.3.10. Vérifier et contrôler le champ d'application

10.4. Élaborer le calendrier
- 10.4.1. La gestion du temps et son plan
- 10.4.2. Définir les activités
- 10.4.3. Séquencement des activités
- 10.4.4. Estimation des ressources des activités
- 10.4.5. Estimation de la durée des activités
- 10.4.6. Élaboration du calendrier et calcul du chemin critique
- 10.4.7. Contrôle du calendrier

10.5. Élaboration du budget et réponse aux risques
- 10.5.1. Estimation des coûts
- 10.5.2. Élaborer le budget et la courbe en S
- 10.5.3. Contrôle des coûts et méthode de la valeur acquise
- 10.5.4. Les concepts de risque
- 10.5.5. Comment faire une analyse des risques
- 10.5.6. Élaboration du plan d'intervention



10.6. Gestion de la qualité
- 10.6.1. Planification de la qualité
- 10.6.2. Assurance de la qualité
- 10.6.3. Contrôle de la qualité
- 10.6.4. Concepts statistiques de base
- 10.6.5. Outils de gestion de la qualité

10.7. La communication et les ressources humaines
- 10.7.1. Planifier la gestion de la communication
- 10.7.2. Analyse les besoins en communication
- 10.7.3. Technologie de la communication
- 10.7.4. Modèles de communication
- 10.7.5. Méthodes de communication
- 10.7.6. Plan de gestion de la communication
- 10.7.7. Gestion de la communication
- 10.7.8. Gestion des ressources humaines
- 10.7.9. Les principaux acteurs et leurs rôles dans les projets
- 10.7.10. Types d'organisations
- 10.7.11. Organisation du projet
- 10.7.12. L'équipe de travail

10.8. Approvisionnement
- 10.8.1. La procédure de passation de marchés
- 10.8.2. Planification
- 10.8.3. Recherche de fournisseurs et appels d'offres
- 10.8.4. Attribution du marché
- 10.8.5. Gestion des contrats
- 10.8.6. Contrats
- 10.8.7. Types de contrats
- 10.8.8. Négociation des contrats

10.9. Exécution, suivi, contrôle et clôture
- 10.9.1. Les groupes de processus
- 10.9.2. Réalisation du projet
- 10.9.3. Suivi et contrôle du projets
- 10.9.4. Clôture du projet

10.10. Responsabilité professionnelle
- 10.10.1. Responsabilité professionnelle
- 10.10.2. Caractéristiques de la responsabilité sociale et professionnelle
- 10.10.3. Code d'éthique du chef de projet
- 10.10.4. Responsabilité vs. PMP®
- 10.10.5. Exemples de responsabilité
- 10.10.6. Avantages de la professionnalisation

Un parcours de croissance professionnelle et personnelle qui se traduira par un énorme renforcement de votre compétitivité"

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***.

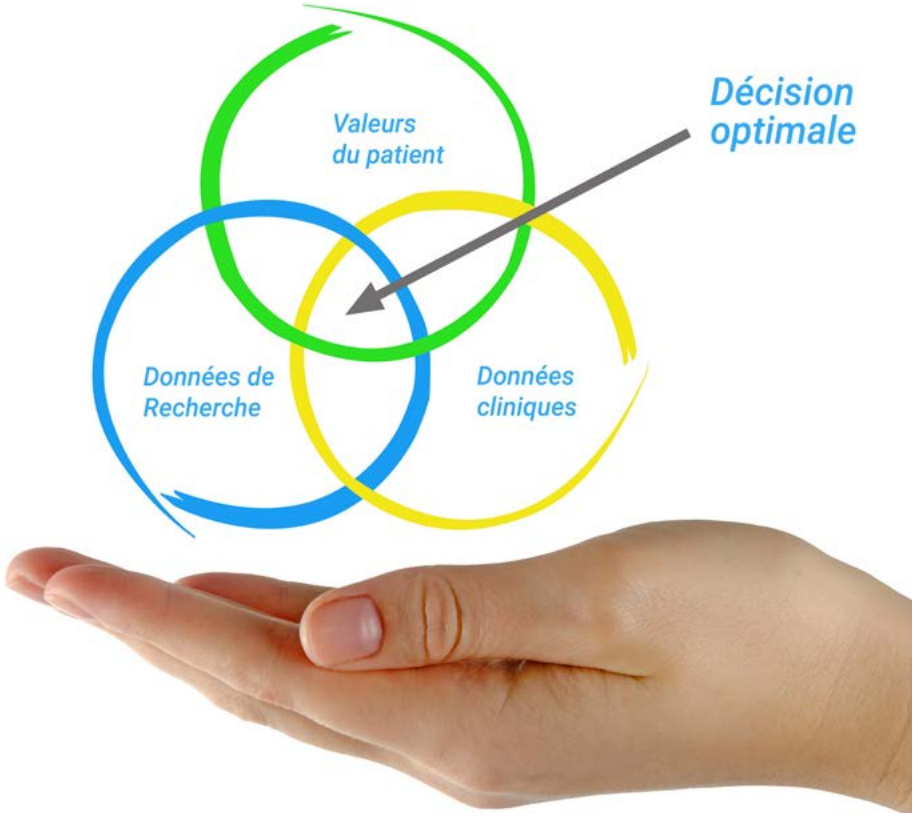
Ce système d'enseignement est utilisé, par exemple, dans les écoles de médecine les plus prestigieuses du monde et a été considéré comme l'un des plus efficaces par des publications de premier plan telles que le ***New England Journal of Medicine.***

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

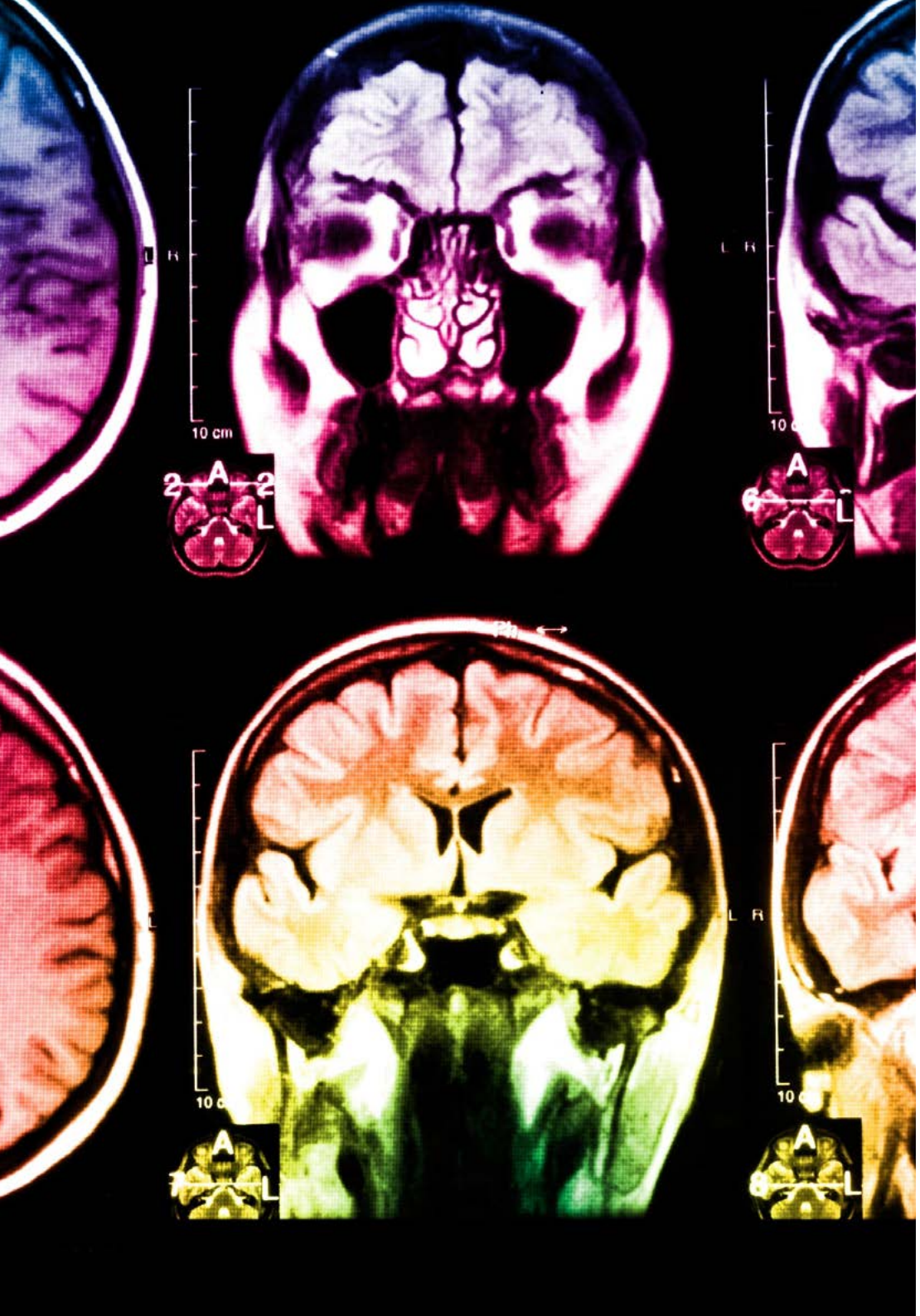
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

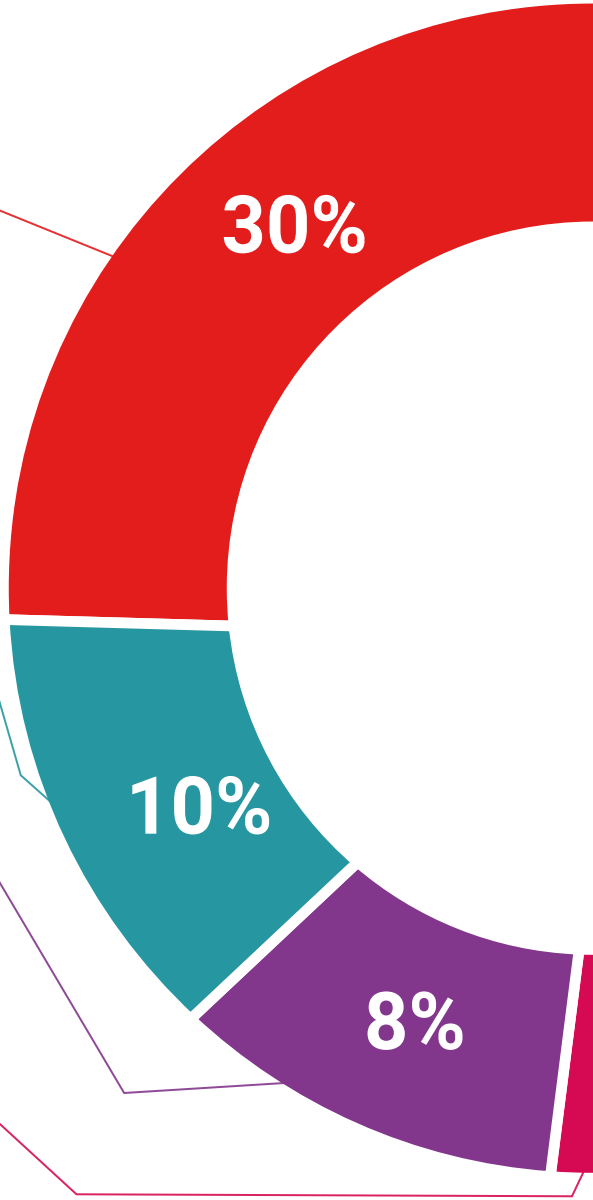
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

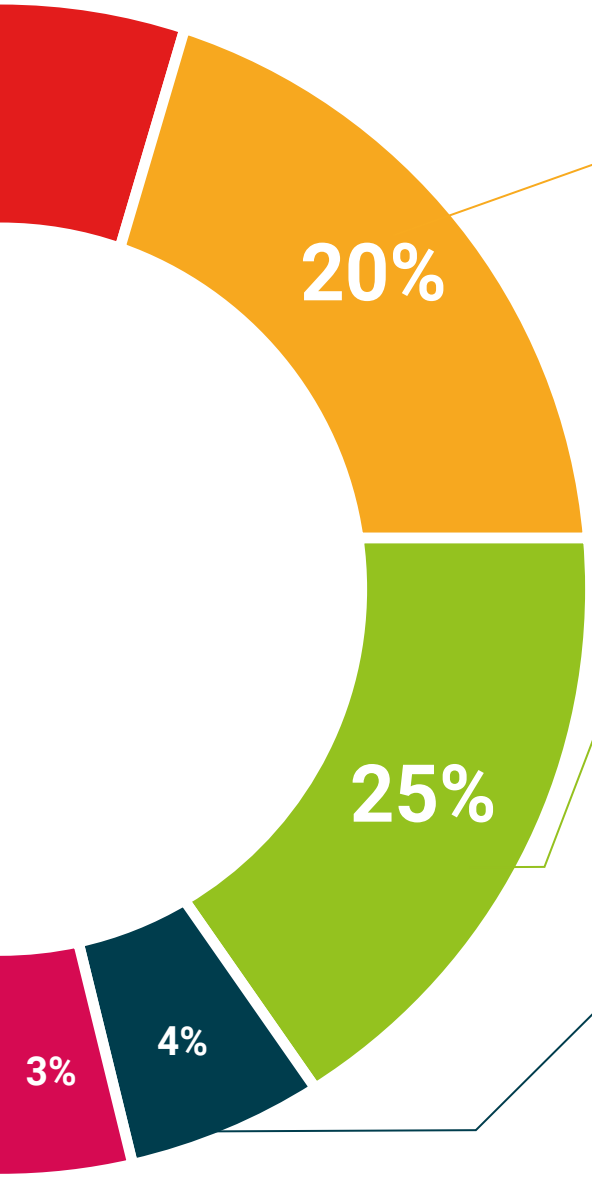
Pratiques en compétences et aptitudes

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 Mastère Spécialisé en Télématique garantit, en plus vous garantit, en plus de la formation la plus rigoureuse et la plus actuelle, l'accès à un diplôme universitaire de Mastère Spécialisé délivré par TECH Université Technologique.

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

Ce **Mastère Spécialisé en Télématique** 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 **Mastère Spécialisé** délivré par **TECH Université Technologique.**

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

Diplôme: **Mastère Spécialisé en Télématique**
N.º d'Heures Officielles: **1.500 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

MASTÈRE SPÉCIALISÉ

en

Télématique

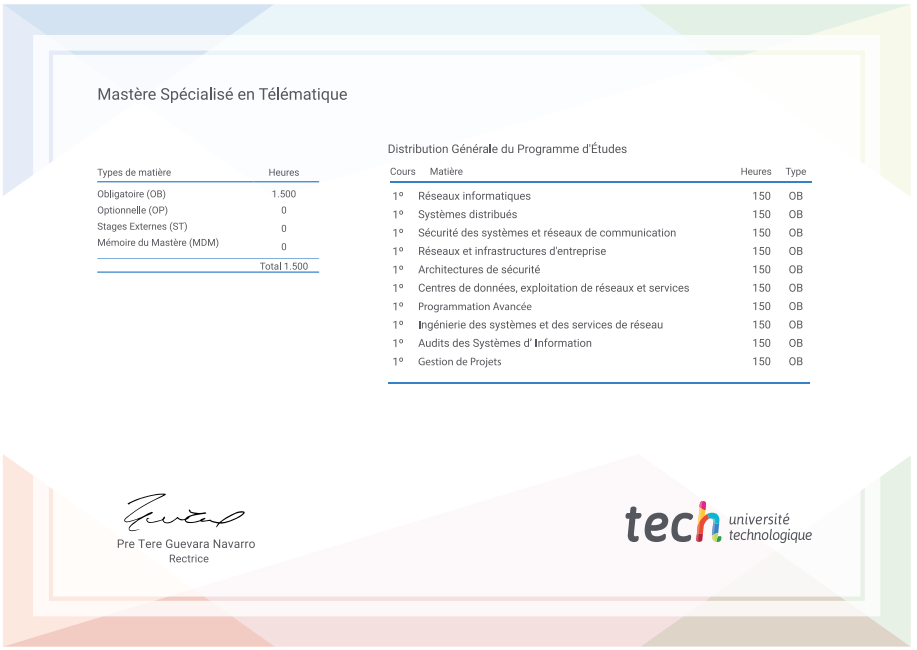
Il s'agit d'un diplôme spécialisé octroyé par cette Université d'une durée de 1.500 heures, débutant le dd/mm/aaaa et finalisant le dd/mm/aaaa.

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


Mastère Spécialisé en Télématique

Types de matière	Heures
Obligatoire (OB)	1.500
Optionnelle (OP)	0
Stages Externes (ST)	0
Mémoire du Mastère (MDM)	0
	Total 1.500

Distribution Générale du Programme d'Études

Cours	Matière	Heures	Type
1º	Réseaux informatiques	150	OB
1º	Systèmes distribués	150	OB
1º	Sécurité des systèmes et réseaux de communication	150	OB
1º	Réseaux et infrastructures d'entreprise	150	OB
1º	Architectures de sécurité	150	OB
1º	Centres de données, exploitation de réseaux et services	150	OB
1º	Programmation Avancée	150	OB
1º	Ingénierie des systèmes et des services de réseau	150	OB
1º	Audits des Systèmes d' Information	150	OB
1º	Gestion de Projets	150	OB

Pre Tere Guevara Navarro
Rectrice

tech université technologique

*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

Mastère Spécialisé

Télématique

- Modalité: **en ligne**
- Durée: **12 mois**
- Qualification: **TECH Université Technologique**
- Intensité: **16h/semaine**
- Horaire: **à votre rythme**
- Examens: **en ligne**

Mastère Spécialisé
Télématique

tech université technologique