Mastère Spécialisé
Direction de la Cybersécurité Avancée

tech université technologique

tech université technologique

Mastère Spécialisé
Direction de la Cybersécurité Avancée

- 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-direction-cybersecurite-avancee

Sommaire

01

Présentation

Le monde d'aujourd'hui évolue vers une numérisation complète. De plus en plus de processus de base, d'opérations et de tâches de toutes sortes sont réalisés via un appareil électronique. Mais ce progrès s'accompagne aussi de certains risques, car les ordinateurs, *les smartphones*, *les tablettes* et toutes sortes d'applications numériques peuvent être exposés à des cyberattaques. C'est pourquoi de nombreuses entreprises recherchent des experts capables de diriger et de gérer efficacement la cybersécurité de leurs services. Ce nouveau profil professionnel est très demandé, c'est pourquoi ce programme a été conçu pour fournir les dernières connaissances et techniques à l'informaticien, qui sera préparé à être le directeur de la cybersécurité dans toute entreprise qui le demande.

Ce programme vous préparera intensivement à vous spécialiser dans la gestion de la cybersécurité, le profil professionnel le plus demandé dans le domaine de l'informatique"

Ces dernières années, le processus de numérisation s'est accéléré, sous l'effet des progrès constants des technologies de l'information. Ainsi, ce n'est pas seulement la technologie qui a bénéficié d'améliorations majeures, mais aussi les outils numériques mêmes avec lesquels de nombreuses tâches sont effectuées aujourd'hui. Par exemple, ces progrès ont rendu possible la réalisation de nombreuses opérations bancaires à partir d'une application mobile. Des évolutions ont également eu lieu dans le secteur de la santé, dans les systèmes de rendez-vous ou dans l'accès aux dossiers médicaux. En outre, grâce à ces technologies, il est possible de consulter des factures ou de demander des services à des entreprises dans des domaines tels que la téléphonie.

Mais ces progrès ont également entraîné une augmentation des vulnérabilités informatiques. Ainsi, bien que les possibilités de réaliser diverses activités et tâches se soient élargies, les attaques contre la sécurité des appareils, des applications et des sites web ont augmenté proportionnellement. C'est pourquoi de plus en plus d'entreprises recherchent des professionnels spécialisés dans la cybersécurité, capables de leur fournir une protection adéquate contre tous les types d'attaques informatiques.

Ainsi, le profil de directeur de la cybersécurité est l'un des plus recherchés par les entreprises qui opèrent sur Internet ou qui ont des services dans l'environnement numérique. Et pour répondre à cette demande, TECH a conçu ce Mastère Spécialisé en Direction de la Cybersécurité Avancée, qui fournira à l'informaticien tous les outils nécessaires pour exercer cette fonction de manière efficace et en tenant compte des derniers développements en matière de protection et de vulnérabilité dans ce domaine technologique.

Ce programme vous permettra d'approfondir des aspects tels que la sécurité dans le développement et la conception de systèmes, les meilleures techniques cryptographiques ou la sécurité dans les environnements de *Cloud Computing*. Pour ce faire, vous utiliserez une méthodologie 100% en ligne qui vous permettra de combiner votre travail professionnel et vos études, sans horaires rigides ni trajets inconfortables vers un centre universitaire. En outre, vous bénéficierez de nombreuses ressources pédagogiques multimédias, dispensées par le corps enseignant le plus prestigieux et le plus spécialisé dans le domaine de la cybersécurité.

Ce **Mastère Spécialisé en Direction de la Cybersécurité Avancée** le programme éducatif le plus complet et le plus actuel du marché. Ses principales caractéristiques sont:

- Le développement d'études de cas présentées par des experts en informatique cybersécurité
- Les contenus graphiques, schématiques et éminemment pratiques avec lesquels ils sont conçus fournissent des informations scientifiques et sanitaires essentielles à la pratique professionnelle
- Des exercices où le processus d'auto-évaluation peut être réalisé pour améliorer l'apprentissage
- Il met l'accent sur les méthodologies innovantes
- Leçons théoriques, questions à l'expert, forums de discussion sur des sujets controversés et travail de réflexion individuel
- La possibilité d'accéder au contenu à partir de n'importe quel appareil fixe ou portable doté d'une connexion internet

Apprenez, de première main, les meilleures techniques de sécurité appliquées aux environnements de Cloud Computing ou à la technologie Blockchain"

Vous bénéficierez de nombreux contenus multimédias pour accélérer votre apprentissage, tout en recevant le soutien d'un corps professoral de grand prestige dans le domaine de la cybersécurité"

La méthodologie en ligne de TECH vous permettra de choisir le moment et le lieu où étudier, sans entraver votre travail professionnel.

Vous pourrez devenir le directeur de la cybersécurité des meilleures entreprises de votre région.

Le corps enseignant du programme englobe des spécialistes réputés dans le domaine et qui apportent à ce programme l'expérience de leur travail, ainsi que des spécialistes reconnus dans de grandes sociétés et des universités prestigieuses.

Grâce à son contenu multimédia développé avec les dernières technologies éducatives, les spécialistes bénéficieront d'un apprentissage situé et contextuel. Ainsi, ils se formeront dans un environnement simulé qui leur permettra d'apprendre en immersion et de s'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 cours académique. Pour ce faire, l'étudiant sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.

02

Objectifs

Le développement rapide des technologies informatiques a entraîné de grandes avancées, offrant de nombreux services à l'ensemble de la population. Cependant, le nombre de vulnérabilités et de cyberattaques a également augmenté. C'est pourquoi l'objectif principal de ce Mastère Spécialisé est de faire de l'informaticien un véritable spécialiste de la gestion de la cybersécurité, garantissant une progression professionnelle énorme et immédiate. Ainsi, vos nouvelles connaissances vous donneront la possibilité d'accéder à de grandes entreprises qui opèrent de manière numérique dans divers secteurs.

L'objectif de ce programme est de faire de vous un professionnel prêt à diriger le département de cybersécurité d'une grande entreprise"

Objectifs généraux

- Générer des connaissances spécialisées sur un système d'information, les types et les aspects de sécurité à prendre en compte. les aspects de sécurité à prendre en compte
- Identifier les vulnérabilités d'un système d'information
- Développer les réglementations légales et la typification de la criminalité en s'attaquant à un système d'information
- Évaluer les différents modèles d'architecture de sécurité afin d'établir le modèle le plus approprié pour l'organisation
- Identifier les cadres réglementaires d'application et leurs bases réglementaires
- Analyser la structure organisationnelle et fonctionnelle d'un secteur de sécurité de l'information (le bureau du CISO)
- Analyser et développer le concept de risque, d'incertitude dans l'environnement dans lequel nous vivons
- Examiner le modèle de gestion des risques basé sur la norme ISO 31.000
- Examiner la science de la cryptologie et la relation avec ses branches: cryptographie, cryptanalyse, stéganographie et stégoanalyse
- Analyser les types de cryptographie en fonction du type d'algorithme et en fonction de son utilisation
- Examiner les certificats numériques
- Examiner l'infrastructure à clé publique (ICP)
- Développer le concept de gestion de l'identité
- Identifier les méthodes d'authentification
- Générer des connaissances spécialisées sur l'écosystème de la sécurité informatique
- Évaluer les connaissances en matière de cybersécurité
- Identifier les domaines de sécurité dans le *Cloud*
- Analyser les services et les outils dans chacun des domaines de sécurité
- Développer les spécifications de sécurité de chaque technologie LPWAN
- Analyse comparative de la sécurité des technologies LPWAN

Vos objectifs professionnels sont désormais à votre portée grâce à ce Mastère Spécialisé, qui offre les connaissances les plus avancées en matière de cybersécurité"

Objectifs spécifiques

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

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

Module 2. Architectures et modèles de sécurité de l'information

- Aligner le Plan Directeur de Sécurité sur les objectifs stratégiques de l'organisation
- Établir un cadre permanent de gestion des risques faisant partie intégrante du plan directeur de sécurité
- Déterminer les indicateurs appropriés pour le suivi de la mise en œuvre du SGSI
- Établir une stratégie de sécurité basée sur des politiques
- Analyser les objectifs et les procédures associés au plan de sensibilisation des employés, des fournisseurs et des partenaires
- Identifier, dans le cadre réglementaire, les règlements, les certifications et les lois applicables dans chaque organisation
- Développer les éléments clés requis par la norme ISO 27001:2013
- Mettre en œuvre un modèle de gestion de la confidentialité conforme au règlement européen GDPR/RGPD

Module 3. Gestion de la sécurité IT

- Identifier les différentes structures que peut avoir un secteur de sécurité de l'information
- Développez un modèle de sécurité basé sur trois lignes de défense
- Présenter les différents comités périodiques et extraordinaires dans lesquels le domaine de la cybersécurité intervient
- Spécifier les outils technologiques qui soutiennent les principales fonctions de l'équipe des opérations de sécurité (SOT)
- Évaluer les mesures de contrôle de la vulnérabilité appropriées à chaque scénario
- Développer le cadre des opérations de sécurité sur la base du NIST CSF
- Préciser la portée des différents types de contrôles (*Red Team*, *Pentesting*, *Bug Bounty*, etc.)
- Proposer les activités à mener après un incident de sécurité
- Mettre en place un centre de commandement de la sécurité de l'information englobant tous les acteurs concernés (autorités, clients, fournisseurs, etc.)

Module 4. Analyse des risques et environnement de la sécurité informatique

- Examiner, avec une vision holistique, l'environnement dans lequel nous opérons
- Identifier les principaux risques et opportunités qui peuvent affecter la réalisation de nos objectifs. de nos objectifs
- Analyser les risques sur la base des meilleures pratiques dont nous disposons
- Évaluer l'impact potentiel de ces risques et opportunités
- Développer des techniques pour traiter les risques et les opportunités de manière à maximiser la contribution à la valeur
- Développer des techniques pour traiter les risques et les opportunités de manière à maximiser la contribution à la valeur
- Examiner en profondeur les différentes techniques de transfert de risques et de valeurs
- Examiner les résultats pour proposer des améliorations continues de la gestion des projets et des processus sur la base de modèles de gestion axés sur les risques ou les *Risk-Driven*
- Innover et transformer des données générales en informations pertinentes pour la prise de décision fondée sur le risque

Module 5. Cryptographie en informatique

- Compiler les opérations fondamentales (XOR, grands nombres, substitution et transposition) et les différents composants (fonctions à sens unique, Hash, générateurs de nombres aléatoires)
- Analyser les techniques cryptographiques
- Développer différents algorithmes cryptographiques
- Démontrer l'utilisation des signatures numériques et leur application dans les certificats numériques
- Évaluer les systèmes de gestion des clés et l'importance de la longueur des clés cryptographiques
- Examiner les algorithmes de dérivation de clés
- Analyser le cycle de vie des clés
- Évaluer les modes de chiffrement par blocs et de chiffrement par flux
- Déterminer les générateurs de nombres pseudo-aléatoires
- Développer des cas réels d'applications cryptographiques, comme Kerberos, PGP ou les cartes à puce
- Examinez les associations et organismes connexes, tels que l'ISO, le NIST ou le NCSC
- Déterminer les défis de la cryptographie de l'informatique quantique

Module 6. Gestion des identités et des accès dans la sécurité informatique

- Développer le concept d'identité numérique
- Évaluation du contrôle de l'accès physique aux informations
- Principes fondamentaux de l'authentification biométrique et de l'authentification MFA
- Évaluer les attaques contre la confidentialité des informations
- Analyser la fédération d'identité
- Établir un contrôle d'accès au réseau

Module 7. Sécurité des communications et de l'exploitation du software

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

Module 8. Sécurité dans les environnements *Cloud*

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

Module 9. Sécurité des communications des dispositifs IoT

- Présenter l'architecture IoT simplifiée
- Expliquer les différences entre les technologies de connectivité généralistes et les technologies de connectivité IoT
- Établir le concept du triangle de fer de la connectivité IoT
- Analyser les spécifications de sécurité de la technologie LoRaWAN, de la technologie NB-IoT et de la technologie WiSUN
- Justifier le choix de la technologie IoT appropriée pour chaque projet

Module 10. Plan de continuité des activités associé à la sécurité

- Présenter les éléments clés de chaque phase et analyser les caractéristiques du plan de continuité des activités (PCA). Plan de continuité des activités (PCA)
- Justifier la nécessité d'un plan de continuité des activités
- Déterminer les cartes de réussite et de risque de chaque phase du plan de Continuité des Activités
- Préciser comment établir un plan d'action pour la mise en œuvre
- Évaluer l'exhaustivité d'un plan de continuité des activités (PCA)
- Développer le plan pour une mise en œuvre réussie d'un plan de continuité des activités

03

Compétences

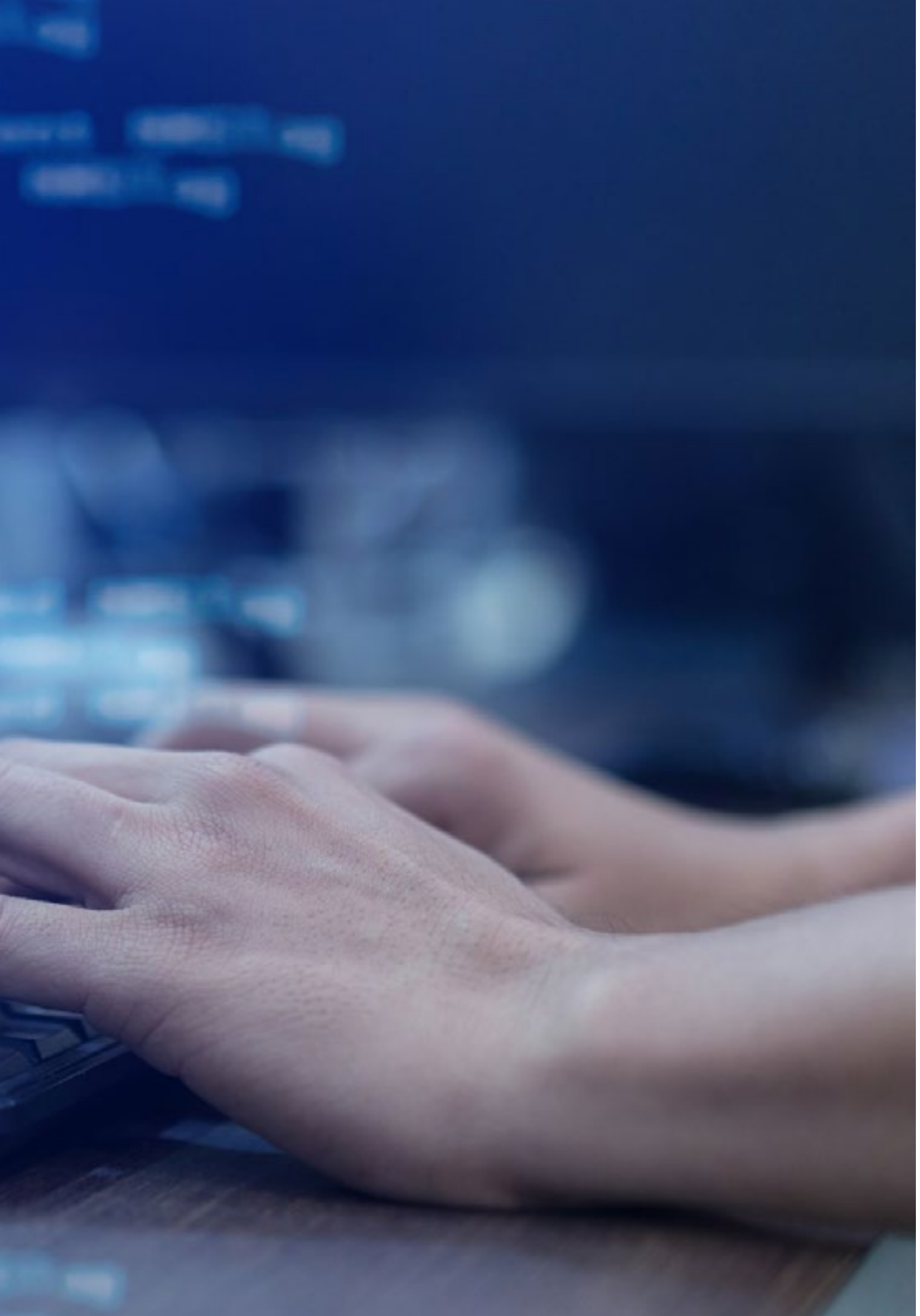
Grâce à ce Mastère Spécialisé, le professionnel acquerra de nombreuses nouvelles compétences dans le domaine de la cybersécurité. L'émergence, ces dernières années, de technologies telles que *Blockchain*, le *Cloud Computing* et l'intelligence artificielle a conduit au développement de nouveaux domaines de cybersécurité. C'est pourquoi ce programme a été spécialement conçu pour fournir aux professionnels toutes les compétences nécessaires pour s'adapter à ces technologies en plein essor.

Les compétences que ce Mastère Spécialisé vous apportera vous permettront de vous mettre à jour et de vous adapter au nouvel environnement informatique, où des technologies telles que la Blockchain ou l'intelligence artificielle ont fait irruption sur la scène"

Compétences générales

- Appliquer les mesures de sécurité les plus appropriées en fonction des menaces
- Déterminer la politique et le plan de sécurité dans le système d'information d'une entreprise, achever la conception et la mise en œuvre du plan d'urgence
- Établir un programme d'audits pour couvrir les besoins d'auto-évaluation de l'organisation en matière de cybersécurité
- Développer un programme d'analyse et de surveillance des vulnérabilités et un plan de réponse aux incidents de cybersécurité
- Maximiser les opportunités présentées et éliminer l'exposition à tous les risques potentiels par la conception
- Compiler les systèmes de gestion des clés
- Évaluer la sécurité de l'information d'une entreprise
- Analyser les systèmes d'accès à l'information
- Développer les meilleures pratiques en matière de développement sécurisé
- Présenter les risques pour les entreprises de ne pas avoir mis en place un environnement de sécurité informatique

Non seulement vous améliorerez vos compétences en matière de cybersécurité, mais vous vous préparerez également à diriger ce département dans toute grande entreprise Internet ou numérique ou dans la sphère numérique"



Compétences spécifiques

- Développez un Systèmes de Gestion de Sécurité de l'Information (SGSI)
- Identifier les éléments clés qui composent un SMSI
- Appliquer la méthodologie MAGERIT pour faire évoluer le modèle et le faire progresser
- Concevoir de nouvelles méthodologies de gestion des risques basées sur le concept de *agile Risk Management*
- Identifier, analyser, évaluer et traiter les risques auxquels le professionnel est confronté dans une nouvelle perspective commerciale fondée sur un modèle *Risk-Driven* qui permet non seulement de survivre dans son propre environnement, mais aussi de stimuler sa propre contribution à la valeur
- Examiner le processus de conception d'une stratégie de sécurité lors du déploiement de services de *Cloud* d'entreprise
- Évaluer les différences dans les implémentations spécifiques des différents fournisseurs de *Cloud* publics
- Évaluer les options de connectivité IoT pour répondre à un projet, en mettant l'accent sur les technologies LPWAN
- Présenter les spécifications de base des principales technologies LPWAN pour l'IoT

04

Direction de la formation

L'énorme complexité de la cybersécurité d'aujourd'hui exige un processus d'apprentissage complet et détaillé. C'est pourquoi TECH a réuni les meilleurs enseignants spécialisés dans ce domaine Ainsi, le professionnel bénéficiera de l'accompagnement et de l'encadrement d'un corps enseignant au fait des dernières avancées en la matière, afin qu'il puisse intégrer les meilleures techniques de cybersécurité dans son travail quotidien, tout en acquérant les compétences de gestion nécessaires dans ce domaine.

Vous aurez à votre disposition de véritables spécialistes de la cybersécurité. C'est l'opportunité que vous recherchiez"

Direction

M. Olalla Bonal, Martín

- Spécialiste technique client Blockchain chez IBM
- Architecte *Blockchain*
- Architecte d'infrastructure dans le secteur bancaire
- Gestion de projet et mise en œuvre de solutions en production
- Technicien en Électronique Numérique
- Professeurs: Formation *Hyperledger Fabric* pour les entreprises
- Professeur: Formation *Blockchain* en entreprise

Professeurs

M. Gonzalo Alonso, Félix

- Directeur général et fondateur de Smart REM Solutions
- Associé fondateur et responsable de l'ingénierie des risques et de l'innovation Dynargy
- Directeur général et associé fondateur Risknova (Bureau d'experts spécialisés en technologie)
- Diplôme d'ingénieur en organisation industrielle de l'Universidad Pontificia de Comillas ICAI
- Diplômé en ingénierie technique industrielle, spécialisé en électronique industrielle, Universidad Pontificia de Comillas ICAI
- Master en gestion des assurances de l'ICEA (Institut pour la collaboration entre les compagnies d'assurances)

Dr entraîner, Alejandro

- Entelgy Innotec
- Innovery Espagne
- Atos Spain
- Diplôme d'ingénieur technique en systèmes informatiques de l'université de Cordoba
- Master en gestion de la sécurité de l'information de l'Université polytechnique de Madrid

Dr Nogales Avila, Javier

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

Dr Gómez Rodríguez, Antonio

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

Dr del Valle Arias, Jorge

- Smart Cities Business Growth Manager Spain en Itron Inc
- Consultant IoT
- Directeur de la division IoT chez Diode Espagne
- Sales Manager IoT & Celular en Aicox Soluciones
- Fondateur et PDG de Sensor Intelligence
- Directeur des Opérations chez Codium Networks
- Chef du secteur électronique chez Aitemin
- Ingénieur en Télécommunications de l'Université Polytechnique de Madrid
- Executive MBA de l'International Graduate School de La Salle à Madrid

Dr Fernandez, Juan Luis

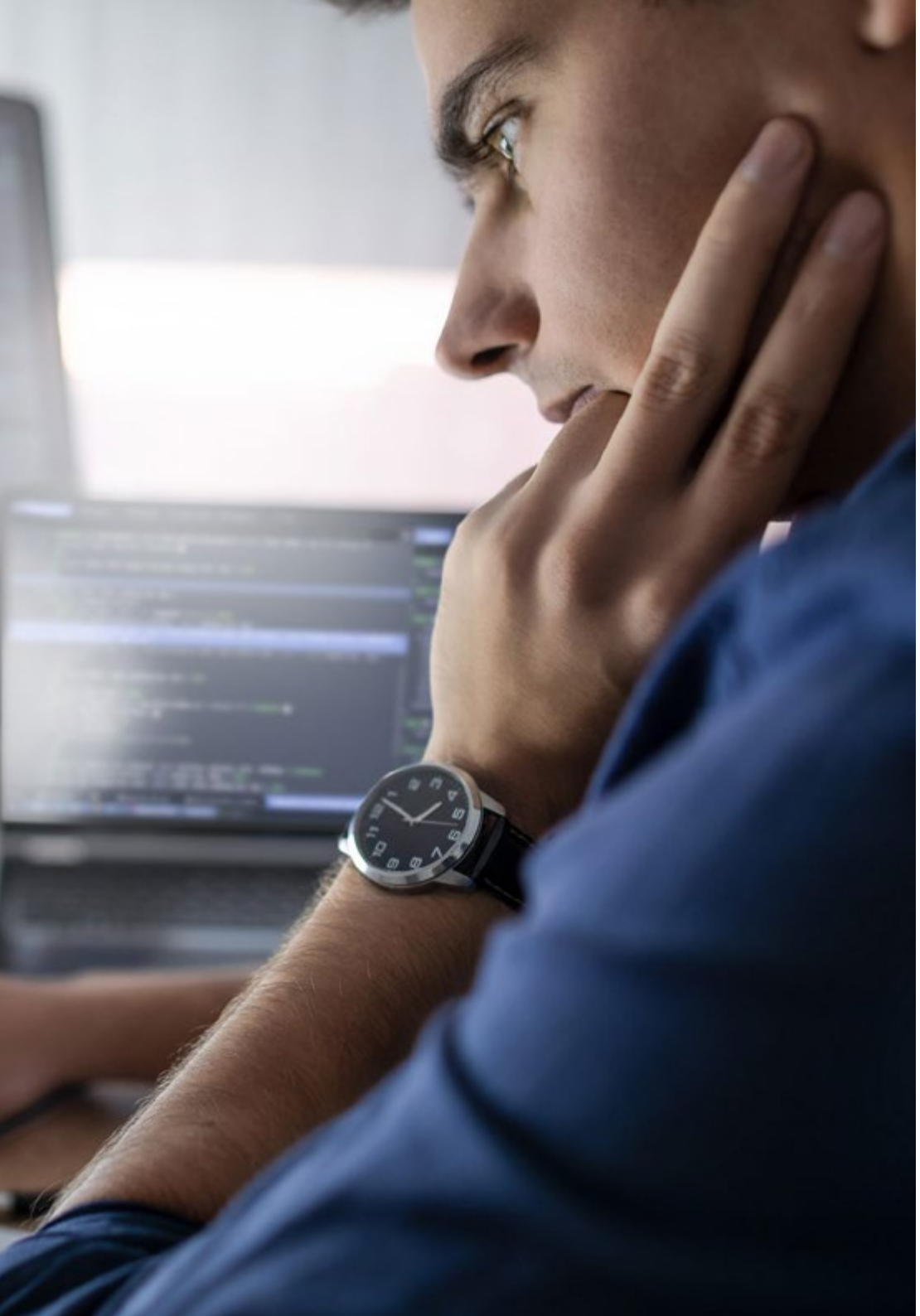
- Ingénieur en informatique
- Directeur de Blockchain DevOps chez Alastria
- Directeur du développement des applications mobiles Tinkerlink chez Cronos Telecom
- Directeur informatique à la Banque Santander
- Directeur de la Technologie de Gestion des Services Informatiques à la Barclays Bank Espagne
- Diplôme d'ingénieur en informatique de l'Université Nationale d'Éducation à Distance (UNED)

Dr Jurado Jabonero, Lorena

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

M. Ortega, Octavio

- Programmeur d'applications informatiques et développement Web
- Conception de sites web et d'APPS pour des clients, CRDS pour les recherches menées par l'Instituto de Salud Carlos III, boutiques en ligne, applications Android, etc.
- Professeur de Sécurité Informatique
- Diplôme de psychologie de l'Universitat Oberta de Catalunya (UOC)
- Technicien Supérieur Universitaire en Analyse, Conception et Solutions Software
- Technicien Supérieur Universitaire en Programmation Avancée



M. Embid Ruiz, Mario

- Avocat spécialisé dans le droit des TIC et de la protection des données
- Responsable juridique de Branddocs, SL, une entreprise technologique entreprise de solutions technologiques de confiance
- Diplôme de Droit et d'Administration des Activités de l'Université Rey Juan Carlos, Madrid
- Master en droit des nouvelles technologies, de l'Internet et de l'audiovisuel du Centre d'études Universitaires Villanueva et Cremades & Calvo Sotelo

M. Rodrigo, Juan Manuel

- Fondateur d'ISMET TECH S.L
- Diplôme en Ingénierie de l'Université de Valladolid
- Master en Systèmes de Gestion Intégrée par CFE-CEU
- ISO 27001 Lead Auditor (IMQ)
- ISO 27001 Lead Implementor (IMQ)
- NATO Standards HPS (OTAN)

Vous serez en mesure de répondre de manière appropriée à tous les types de menaces en matière de cybersécurité. Inscrivez-vous et devenez un grand spécialiste"

05

Structure et contenu

Ce programme est structuré en 10 modules spécialisés qui permettront au professionnel d'étudier en profondeur des aspects tels que l'identification numérique, les systèmes de contrôle d'accès, l'architecture de la sécurité de l'information, la structure du domaine de la sécurité, les systèmes de gestion de la sécurité de l'information dans l'exploitation des communications et des softwares ou le développement du plan de continuité des activités associé à la sécurité. Cela donnera à l'informaticien une compréhension complète de toutes les questions pertinentes en matière de cybersécurité aujourd'hui.

Vous ne trouverez pas de contenu plus complet et innovant que celui-ci pour vous spécialiser dans la gestion avancée de la cybersécurité"

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

1.1. Systèmes d'information
- 1.1.1. Domaines de systèmes d'information
- 1.1.2. Composants de systèmes d'information
- 1.1.3. Activités de systèmes d'information
- 1.1.4. Cycle de vie de systèmes d'information
- 1.1.5. Ressources de systèmes d'information

1.2. Systèmes d'information. Typologie
- 1.2.1. Types des systèmes d'information
  - 1.2.1.1. Entreprise
  - 1.2.1.2. Stratégiques
  - 1.2.1.3. Selon le champ d'application
  - 1.2.1.4. Spécifiques
- 1.2.2. Systèmes d'information. Exemples concrets
- 1.2.3. Évolution des systèmes d'information: étapes
- 1.2.4. Méthodologies des systèmes d'information

1.3. Sécurité des systèmes d'information. Implications juridiques
- 1.3.1. Accès aux données
- 1.3.2. Menaces pour la sécurité: vulnérabilités
- 1.3.3. Implications juridiques: infractions pénales
- 1.3.4. Procédures de maintenance des systèmes d'information

1.4. Sécurité des systèmes d'information. Protocole de sécurité
- 1.4.1. Sécurité de systèmes d'information
  - 1.4.1.1. Intégration
  - 1.4.1.2. Confidentialité
  - 1.4.1.3. Disponibilité
  - 1.4.1.4. Authentification
- 1.4.2. Services de sécurité
- 1.4.3. Protocoles de sécurité de l'information. Typologie
- 1.4.4. Sensibilité de systèmes d'information

1.5. Sécurité des systèmes d'information Mesures et systèmes de contrôle d'accès
- 1.5.1. Mesures de sécurité
- 1.5.2. Type de mesures de sécurité
  - 1.5.2.1. Prévention
  - 1.5.2.2. Détection
  - 1.5.2.3. Correction
- 1.5.3. Systèmes de contrôle de Accès Typologie
- 1.5.4. Cryptographie

1.6. Sécurité des réseaux et de l'internet
- 1.6.1. Firewalls
- 1.6.2. Identification numérique
- 1.6.3. Virus et vers
- 1.6.4. *Hacking*
- 1.6.5. Exemples et cas réels

1.7. Délits informatiques
- 1.7.1. Délit informatique
- 1.7.2. Délits informatiques Typologie
- 1.7.3. Délit informatique Ataque. Typologies
- 1.7.4. Le cas de la réalité virtuelle
- 1.7.5. Profils des délinquants et des victimes. Qualification pénale de l'infraction
- 1.7.6. Délits informatiques Exemples et cas réels

1.8. Plan de sécurité d'un système d'information
- 1.8.1. Plan de sécurité. Objectifs
- 1.8.2. Plan de sécurité. Planification
- 1.8.3. Plan de risques. Analyse
- 1.8.4. Politique de sécurité. Mise en œuvre dans l'organisation
- 1.8.5. Plan de sécurité. Mise en œuvre dans l'organisation
- 1.8.6. Procédures de sécurité. Types
- 1.8.7. Plan de sécurité. Exemples

1.9. Plan d'urgence
- 1.9.1. Plan d'urgence. Fonctions
- 1.9.2. Plans d'urgence: Éléments et objectifs
- 1.9.3. Plans des imprévu dans l'organisation. Mise en œuvre
- 1.9.4. Plans d'intervention. Exemples

1.10. Gouvernance de la sécurité de systèmes d' information
- 1.10.1. Réglementation juridique
- 1.10.2. Normes
- 1.10.3. Certifications
- 1.10.4 Technologies

Module 2. Architectures et modèles de sécurité de l'information

2.1. Architecture de sécurité de l'information
- 2.1.1. SGSI/PDS
- 2.1.2. Alignement stratégique
- 2.1.3. Gestion des risques
- 2.1.4. Mesure de la performance

2.2. Modèles de sécurité de l'information
- 2.2.1. Modèles de sécurités basé sur des politiques
- 2.2.2. Basés sur des politiques, les modèles de sécurité
- 2.2.3. Basés sur des outils de protection

2.3. Modèle de sécurité. Principaux éléments
- 2.3.1. Identification des risques
- 2.3.2. Définition des contrôles
- 2.3.3. Évaluation continue des niveaux de risque
- 2.3.4. Plan de sensibilisation des employés, fournisseurs, partenaires, etc.

2.4. Processus de gestion des risques
- 2.4.1. Identification des actifs
- 2.4.2. Identification des menaces
- 2.4.3. Évaluation des risques
- 2.4.4. Priorité des contrôles
- 2.4.5. Réévaluation et risque résiduel

2.5. Processus d'entreprise et sécurité de l'information
- 2.5.1. Processus d'activité
- 2.5.2. Évaluation des risques sur la base de paramètres commerciaux
- 2.5.3. Analyse de l'impact des activités
- 2.5.4. Les opérations d'entreprise et sécurité de l'information

2.6. Processus d'amélioration continue
- 2.6.1. Le cycle de Deming
  - 2.6.1.1. Planification
  - 2.6.1.2. Faire
  - 2.6.1.3. Vérifier
  - 2.6.1.4. Agir

2.7. Architectures de sécurité
- 2.7.1. Sélection et homogénéisation des technologies
- 2.7.2. Gestion de l'identité. Authentification
- 2.7.3. Gestion de l'accès. Autorisation
- 2.7.4. Sécurité de l'infrastructure des réseaux
- 2.7.5. Technologies et solutions de cryptage
- 2.7.6. Sécurité des dispositifs terminaux (EDR)

2.8. Le cadre réglementaire
- 2.8.1. Réglementations sectorielles
- 2.8.2. Certifications
- 2.8.3. Législation

2.9. La norme ISO 27001
- 2.9.1. Mise en œuvre
- 2.9.2. Certification
- 2.9.3. Contrôles et tests de pénétration
- 2.9.4. Gestion continue des risques
- 2.9.5. classification des informations

2.10. Législation sur la protection de la vie privée. RGPD (GDPR)
- 2.10.1. Portée du Règlement Général sur la Protection des Données (RGPD)
- 2.10.2. Données personnelles
- 2.10.3. Rôles dans le traitement des données personnelles
- 2.10.4 Droits d'ARCO
- 2.10.5 Le DPD. Fonctions

Module 3. Gestion de la sécurité IT

3.1. Gestion de la sécurité
- 3.1.1. Opérations de sécurité
- 3.1.2. Aspect juridique et réglementaire
- 3.1.3. Soutien aux entreprises
- 3.1.4. Gestion des risques
- 3.1.5. Gestion des identités et des accès

3.2. Structure de la zone de sécurité. Le bureau du CISO
- 3.2.1. Structure organisationnelle Position du CISO dans la structure
- 3.2.2. Les lignes de défense
- 3.2.3. Organigramme du bureau du CISO
- 3.2.4. Gestion du budget

3.3. Gouvernance de la sécurité
- 3.3.1. Comité de sécurité
- 3.3.2. Comité de suivi des risques
- 3.3.3. Comité de contrôle
- 3.3.4. Comité de crise

3.4. Gouvernance de la sécurité. Fonctions
- 3.4.1. Politiques et normes
- 3.4.2. Plan directeur de sécurité
- 3.4.3. Tableaux de bord
- 3.4.4. Sensibilisation et formation
- 3.4.5. Sécurité de la chaîne d'approvisionnement

3.5. Opérations de sécurité
- 3.5.1. Gestion des identités et des accès
- 3.5.2. Configuration des règles de sécurité du réseau. *Firewalls*
- 3.5.3. Gestion de la plateforme IDS/IPS
- 3.5.4. Analyse de vulnérabilité

3.6. Cadre de cybersécurité. NIST CSF
- 3.6.1. Méthodologie NIST
  - 3.6.1.1. Identifier
  - 3.6.1.2. Protéger
  - 3.6.1.3. Détecter
  - 3.6.1.4. Répondre
  - 3.6.1.5. Récupérer

3.7. Centre des opérations de sécurité (SOC). Fonctions
- 3.7.1. Protection. *Red Team, pentesting, threat intelligence*
- 3.7.2. Détection. SIEM, *user behavior analytics, fraud prevention*
- 3.7.3. Réponse

3.8. Contrôles de sécurité
- 3.8.1. Tests d'intrusion
- 3.8.2. Exercices de *red team*
- 3.8.3. Contrôles du code source. Développement sécurisé
- 3.8.4. Sécurité des composants (*software supply chain*)
- 3.8.5. Analyse médico-légale

3.9. Réponse aux incidents
- 3.9.1. Préparation
- 3.9.2. Détection, analyse et rapports
- 3.9.3. Confinement, éradication et récupération
- 3.9.4. Activité après l'incident
  - 3.9.4.1. Conservation des preuves
  - 3.9.4.2. Analyse médico-légale
  - 3.9.4.3. Gestion des lacunes
- 3.9.5. Lignes directrices officielles pour la gestion des cyberincidents

3.10. Gestion des vulnérabilités
- 3.10.1. Analyse de vulnérabilité
- 3.10.2 Évaluation de vulnérabilité
- 3.10.3 Base des systèmes
- 3.10.4 Les vulnérabilités de type "zero-day" *Zero-day*

Module 4. Analyse des risques et environnement de la sécurité informatique

4.1. Analyse de l'entourage
- 4.1.1. Analyse de la situation extérieure
  - 4.1.1.1. Environnement VUCA
    - 4.1.1.1.1. Volatile
    - 4.1.1.1.2. Incertain
    - 4.1.1.1.3. complexe
    - 4.1.1.1.4. Ambiguës
  - 4.1.1.2. Environnement BANI
    - 4.1.1.2.1. Fragile
    - 4.1.1.2.2. Anxieux
    - 4.1.1.2.3. Non-linéaire
    - 4.1.1.2.4. Incompréhensible
- 4.1.2. Analyse de l'environnement général PESTEL
  - 4.1.2.1. Politique
  - 4.1.2.2. Économique
  - 4.1.2.3. Social
  - 4.1.2.4. Technologique
  - 4.1.2.5. Écologique/Environnemental
  - 4.1.2.6. Legal
- 4.1.3. Analyse de la situation interne. SWOT
  - 4.1.3.1. Objectifs
  - 4.1.3.2. Menaces
  - 4.1.3.3. Opportunités
  - 4.1.3.4. Points forts

4.2. Risque et incertitude
- 4.2.1. Risque
- 4.2.2. Gestion des risques
- 4.2.3. Normes de gestion des risques

4.3. Lignes directrices pour le management du risque ISO 31.000:2018
- 4.3.1. Objet
- 4.3.2. Principes
- 4.3.3. Cadre de référence
- 4.3.4. Processus

4.4. Méthodologie d'analyse et de gestion des risques liés aux systèmes d'information (MAGERIT)
- 4.4.1. Méthodologie MAGERIT
  - 4.4.1.1. Objectifs
  - 4.4.1.2. Méthode
  - 4.4.1.3. Éléments
  - 4.4.1.4. Techniques
  - 4.4.1.5. Outils disponibles (PILAR)

4.5. Transfert du risque cybernétique
- 4.5.1. Transfert de risques
- 4.5.2. Cyber risques. Typologie
- 4.5.3. Assurance contre les cyberrisques

4.6. Méthodologies agiles pour la gestion de risques
- 4.6.1. Méthodologie agile
- 4.6.2. Scrum pour la gestion de risque
- 4.6.3. *Agile risk management*

4.7. TTechnologies pour la gestion du risque
- 4.7.1. L'intelligence artificielle appliquée à la gestion des risques
- 4.7.2. *Blockchain* et cryptographie. Méthodes de préservation de la valeur
- 4.7.3. L'informatique quantique Opportunité ou menace

4.8. Cartographie des risques informatiques basée sur les méthodologies Agile
- 4.8.1. Représentation de la vraisemblance et de l'impact dans les environnements agiles
- 4.8.2. Le risque comme menace pour la valeur
- 4.8.3. Réévolution dans la gestion de projet et les processus agiles basés sur les KRIs

4.9. *Risk driven* axée sur le risque
- 4.9.1. *Risk driven*
- 4.9.2. *Risk driven* axée sur le risque
- 4.9.3. Développement d'un modèle de gestion d'entreprise axé sur le risque

4.10. Innovation et transformation numérique dans la gestion des risques informatiques
- 4.10.1. La gestion agile des risques comme source d'innovation commerciale
- 4.10.2. Transformation des données en informations utiles à la prise de décision
- 4.10.3. Vision holistique de l'entreprise à travers le risque

Module 5. Cryptographie en informatique

5.1. Cryptographie
- 5.1.1. Cryptographie
- 5.1.2. Bases mathématiques

5.2. Cryptologie
- 5.2.1. Cryptologie
- 5.2.2. Cryptanalyse
- 5.2.3. Stéganographie et stégananalyse

5.3. Protocoles cryptographiques
- 5.3.1. Blocs de base
- 5.3.2. Protocoles de base
- 5.3.3. Protocoles intermédiaires
- 5.3.4. Protocoles avancés
- 5.3.5. Protocoles exotériques

5.4. Techniques cryptographiques
- 5.4.1. Longueur de la clé
- 5.4.2. Manipulation des clés
- 5.4.3. Types d'algorithmes
- 5.4.4. Résumé des fonctions. *Hash*
- 5.4.5. Générateurs de nombres pseudo-aléatoires
- 5.4.6. Utilisation d'algorithmes

5.5. Cryptographie symétrique
- 5.5.1. Blocs de chiffrement
- 5.5.2. DES (*Data Encryption Standard*)
- 5.5.3. Algorithme RC4
- 5.5.4. AES (*Advance Encryption Standard*)
- 5.5.5. Combinaison de chiffrements par blocs
- 5.5.6. Dérivation de la clé

5.6. Cryptographie asymétrique
- 5.6.1. Diffie-Hellman
- 5.6.2. DSA (*Digital Signature Algorithm*)
- 5.6.3. RSA (Rivest, Shamir y Adleman)
- 5.6.4. Courbe elliptique
- 5.6.5. Cryptographie asymétrique Typologie

5.7. Certificats numériques
- 5.7.1. Signature numérique
- 5.7.2. Certificats X509
- 5.7.3. Infrastructure à clé publique(PKI)

5.8. Implémentations
- 5.8.1. Kerberos
- 5.8.2. IBM CCA
- 5.8.3. *Pretty Good Privacy* (PGP)
- 5.8.4. ISO *Authentication Framework*
- 5.8.5. SSL et TLS
- 5.8.6. Cartes à puce dans les moyens de paiement (EMV)
- 5.8.7. Protocoles de téléphonie mobile
- 5.8.8. *Blockchain*

5.9. Stéganographie
- 5.9.1. Stéganographie
- 5.9.2. Steganoanalyse
- 5.9.3. Applications et utilisations

5.10. Cryptographie quantique
- 5.10.1. Algorithmes quantiques
- 5.10.2. Protection des algorithmes contre l'informatique quantique
- 5.10.3. Distribution de clés quantiques

Module 6. Gestion des identités et des accès dans la sécurité informatique

6.1. Gestion des identités et des accès (IAM)
- 6.1.1. Identité numérique
- 6.1.2. Gestion de l'identité
- 6.1.3. Fédération d'identité

6.2. contrôle d'accès physique
- 6.2.1. Systèmes de protection
- 6.2.2. Sécurité de la zone
- 6.2.3. Installations de récupération

6.3. Contrôle d'accès logique
- 6.3.1. Authentification: typologie
- 6.3.2. Protocoles d'authentification
- 6.3.3. Attaques d'authentification

6.4. Contrôle d'accès logique Authentification MFA
- 6.4.1. Contrôle d'accès logique Authentification MFA
- 6.4.2. Mots de passe. Importance
- 6.4.3. Attaques d'authentification

6.5. Contrôle d'accès logique Authentification biométrique
- 6.5.1. Contrôle d'accès logique Authentification biométrique
  - 6.5.1.1. Authentification biométrique Exigences
- 6.5.2. Fonctionnement
- 6.5.3. Modèles et techniques

6.6. Systèmes de gestion de l'authentification
- 6.6.1. *Single sign on*
- 6.6.2. Kerberos
- 6.6.3. Systèmes AAA

6.7. Systèmes de gestion de l'authentification: Systèmes AAA
- 6.7.1. TACACS
- 6.7.2. RADIUS
- 6.7.3. DIAMETER

6.8. Services de contrôle d'accès
- 6.8.1. FW-Pare-feu
- 6.8.2. VPN-Réseaux privés virtuels
- 6.8.3. Systèmes de contrôle d'accès au réseau

6.9. Systèmes de contrôle d'accès au réseau
- 6.9.1. NAC
- 6.9.2. Architecture et éléments
- 6.9.3. Fonctionnement et normalisation

6.10. Accès aux réseaux sans fil
- 6.10.1. Types de réseaux sociaux
- 6.10.2. Sécurité dans les réseaux sans fil
- 6.10.3. Attaques contre les réseaux sans fil

Module 7. Sécurité des communications et de l'exploitation du software

7.1. Sécurité informatique dans les communications et l'exploitation des logiciels
- 7.1.1. Sécurité informatique
- 7.1.2. Cybersécurité
- 7.1.3. Sécurité du cloud

7.2. Sécurité informatique dans les communications et l'exploitation des logiciels. Typologie
- 7.2.1. Sécurité physique
- 7.2.2. Sécurité logique

7.3. Sécurité des communications
- 7.3.1. Principaux éléments
- 7.3.2. Sécurité des réseaux
- 7.3.3. Meilleures pratiques

7.4. Cyber intelligence
- 7.4.1. Ingénierie sociale
- 7.4.2. *Deep web*
- 7.4.3. *Phishing*
- 7.4.4. *Malware*

7.5. Développement Sécurité des communications et de l'exploitation du software
- 7.5.1. Développement sécurisé Protocole HTTP
- 7.5.2. Développement sécurisé Cycle de vie
- 7.5.3. Développement sécurisé Sécurité PHP
- 7.5.4. Développement sécurisé Sécurité NET
- 7.5.5. Développement sécurisé Meilleures pratiques

7.6. Systèmes de gestion de la sécurité de l'information des communications et de l'exploitation du software
- 7.6.1. RGPD
- 7.6.2. ISO 27021
- 7.6.3. ISO 27017/18

7.7. Technologies SIEM
- 7.7.1. Technologies SIEM
- 7.7.2. Fonctionnement du SOC
- 7.7.3. SIEM *Vendors*

7.8. Le rôle de la sécurité dans les organisations
- 7.8.1. Rôles dans les organisations
- 7.8.2. Rôle des spécialistes de l'IdO dans les entreprises
- 7.8.3. Certifications reconnues sur le marché

7.9. Analyse médico-légale
- 7.9.1. Analyse médico-légale
- 7.9.2. Analyse médico-légale Méthodologie
- 7.9.3. Analyse médico-légale Outils et mise en œuvre

7.10. La Cybersécurité aujourd'hui
- 7.10.1. Cyberattaques majeures
- 7.10.2. Prévisions d'employabilité
- 7.10.3. Défis

Module 8. Sécurité dans les environnements *Cloud*

8.1. Sécurité dans les environnements *Cloud computing*
- 8.1.1. Sécurité dans les environnements *Cloud computing*
- 8.1.2. Sécurité dans les environnements *Cloud Computing*. Menaces et risques pour la sécurité
- 8.1.3. Sécurité dans les environnements *Cloud Computing*. Principaux aspects de la sécurité

8.2. Types d'infrastructures en *Cloud*
- 8.2.1. Public
- 8.2.2. Privé
- 8.2.3. Hybride

8.3. Modèle de gestion partagée
- 8.3.1. Éléments de sécurité gérés par le fournisseur
- 8.3.2. Éléments gérés par le client
- 8.3.3. Définition de la stratégie de sécurité

8.4. Mécanismes de prévention
- 8.4.1. Systèmes de gestion de l'authentification
- 8.4.2. Système de gestion des autorisations: politiques d'accès
- 8.4.3. Systèmes de gestion des clés

8.5. Securitisation du système
- 8.5.1. Sécurisation des systèmes de stockage
- 8.5.2. Sécurisation des systèmes de bases de données
- 8.5.3. Sécuriser les données en transit

8.6. Protection des infrastructures
- 8.6.1. Conception et mise en œuvre de réseaux sécurisés
- 8.6.2. Sécurité des ressources informatiques
- 8.6.3. Outils et ressources pour la protection des infrastructures

8.7. Détection des menaces et des attaques
- 8.7.1. Systèmes de contrôle, *Logging* d'enregistrement et de surveillance
- 8.7.2. Systèmes de événements et d'alarmes
- 8.7.3. Systèmes SIEM

8.8. Réponse aux incidents
- 8.8.1. Plan de réponse aux incidents
- 8.8.2. Continuité des activités
- 8.8.3. Analyse médico-légale et remédiation d'incidents de même nature

8.9. La sécurité en *Clouds* publics
- 8.9.1. AWS (Amazon Web Services)
- 8.9.2. Microsoft Azure
- 8.9.3. Google &GCP
- 8.9.4. Oracle Cloud

8.10. Réglementation et conformité
- 8.10.1. Conformité en matière de sécurité
- 8.10.2. Gestion des risques
- 8.10.3. Personnes et processus dans les organisations

Module 9. Sécurité des communications des dispositifs IoT

9.1. De la télémétrie à l'IdO
- 9.1.1. Télémétrie
- 9.1.2. Connectivité M2M
- 9.1.3. Démocratisation de la télémétrie

9.2. Modèles de référence de l'IdO
- 9.2.1. Modèles de référence de l'IdO
- 9.2.2. Architecture IoT simplifiée

9.3. Vulnérabilités de la sécurité de l'IdO
- 9.3.1. Dispositifs IoT
- 9.3.2. Dispositifs IoT Études de cas d'utilisation
- 9.3.3. Dispositifs IoT Vulnérabilités

9.4. Connectivité IoT
- 9.4.1. Réseaux PAN, LAN, WAN
- 9.4.2. Technologies sans fil non IoT
- 9.4.3. Technologies sans fil LPWAN

9.5. Technologies LPWAN
- 9.5.1. Le triangle de fer des LPWAN
- 9.5.2. Bandes de fréquences libres vs. Bandes sous licence
- 9.5.3. Options technologiques LPWAN

9.6. Technologie LoRaWAN
- 9.6.1. Technologie LoRaWAN
- 9.6.2. Cas d'utilisation de LoRaWAN. Écosystème
- 9.6.3. Sécurité dans LoRaWAN

9.7. Technologie Sigfox
- 9.7.1. Technologie Sigfox
- 9.7.2. Cas d'utilisation de Sigfox. Écosystème
- 9.7.3. Sécurité dans Sigfox

9.8. IoT Technologie cellulaire
- 9.8.1. Technologie cellulaire IoT (NB-IoT et LTE-M)
- 9.8.2. Cas d'utilisation de l'IoT cellulaire. Écosystème
- 9.8.3. Sécurité de l'IdO cellulaire

9.9. Technologie WiSUN
- 9.9.1. Technologie WiSUN
- 9.9.2. Cas d'utilisation du WiSUN. Écosystème
- 9.9.3. Sécurité dans le WiSUN

9.10. Autres technologies IoT
- 9.10.1. Autres technologies IoT
- 9.10.2. Cas d'utilisation et écosystème des autres technologies IoT
- 9.10.3. Sécurité dans d'autres technologies IoT

Module 10. Plan de continuité des activités associé à la sécurité

10.1. Plan de continuité des activités
- 10.1.1. Planification de la continuité des activités (PCA)
- 10.1.2. Plan de continuité des activités (PCA). Aspects clés
- 10.1.3. Plan de continuité des activités (PCA) pour l'évaluation de l'entreprise

10.2. Mesures dans un plan de continuité des activités (PCA)
- 10.2.1. *Recovery Time Objective* (RTO) et *Recovery Point Objective* (RPO)
- 10.2.2. Durée maximale tolérable (DMT)
- 10.2.3. Niveaux de récupération minimum (ROL)
- 10.2.4. Objectif de point de récupération (RPO)

10.3. Projets de continuité. Typologie
- 10.3.1. Plan de continuité des activités (PCA)
- 10.3.2. Plan d' Continuité des PCTIC)
- 10.3.3. Plan de reprise après sinistre (PRS)

10.4. Gestion des risques associés au PCA
- 10.4.1. Analyse de l'impact des activités
- 10.4.2. Avantages de la mise en œuvre d'un PCA
- 10.4.3. Réflexion sur les risques

10.5. Cycle de vie d'un plan de continuité des activités
- 10.5.1. Phase 1: Analyse organisationnelle
- 10.5.2. Phase 2: Détermination de la stratégie de continuité
- 10.5.3. Phase 3: Réponse aux situations d'urgence
- 10.5.4. Phase 4: Tests, maintenance et révision

10.6. Phase d'analyse organisationnelle d'un PCA
- 10.6.1. Identification des processus dans le champ d'application du PCA
- 10.6.2. Identification des domaines d'activité critiques
- 10.6.3. Identification des dépendances entre les domaines et les processus
- 10.6.4. Détermination des MTD appropriées
- 10.6.5. Produits livrables Création d'un plan

10.7. Phase d'analyse Stratégie d' de continuité un PCA
- 10.7.1. Rôles dans la phase de détermination de la stratégie
- 10.7.2. Tâches de la phase de détermination de la stratégie
- 10.7.3. Produits livrables

10.8. Phase d'intervention d'urgence d'un PCA
- 10.8.1. Rôles dans la phase de réponse
- 10.8.2. Tâches dans cette phase
- 10.8.3. Produits livrables

10.9. Phase de test, de maintenance et de révision d'un PCA
- 10.9.1. Rôles dans la phase de test, de maintenance et de révision
- 10.9.2. Tâches de la phase de test, de maintenance et de révision
- 10.9.3. Produits livrables

10.10. Normes ISO associées aux plans de continuité des activités (PCA)
- 10.10.1. ISO 22301: 2019
- 10.10.2. ISO 22313: 2020
- 10.10.3. Autres normes ISO et internationales connexes

La meilleure équipe d'enseignants et un système d'enseignement innovant, combinés au programme d'études le plus complet et le plus récent: c'est une excellente occasion de progresser en tant qu'informaticien"

06

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

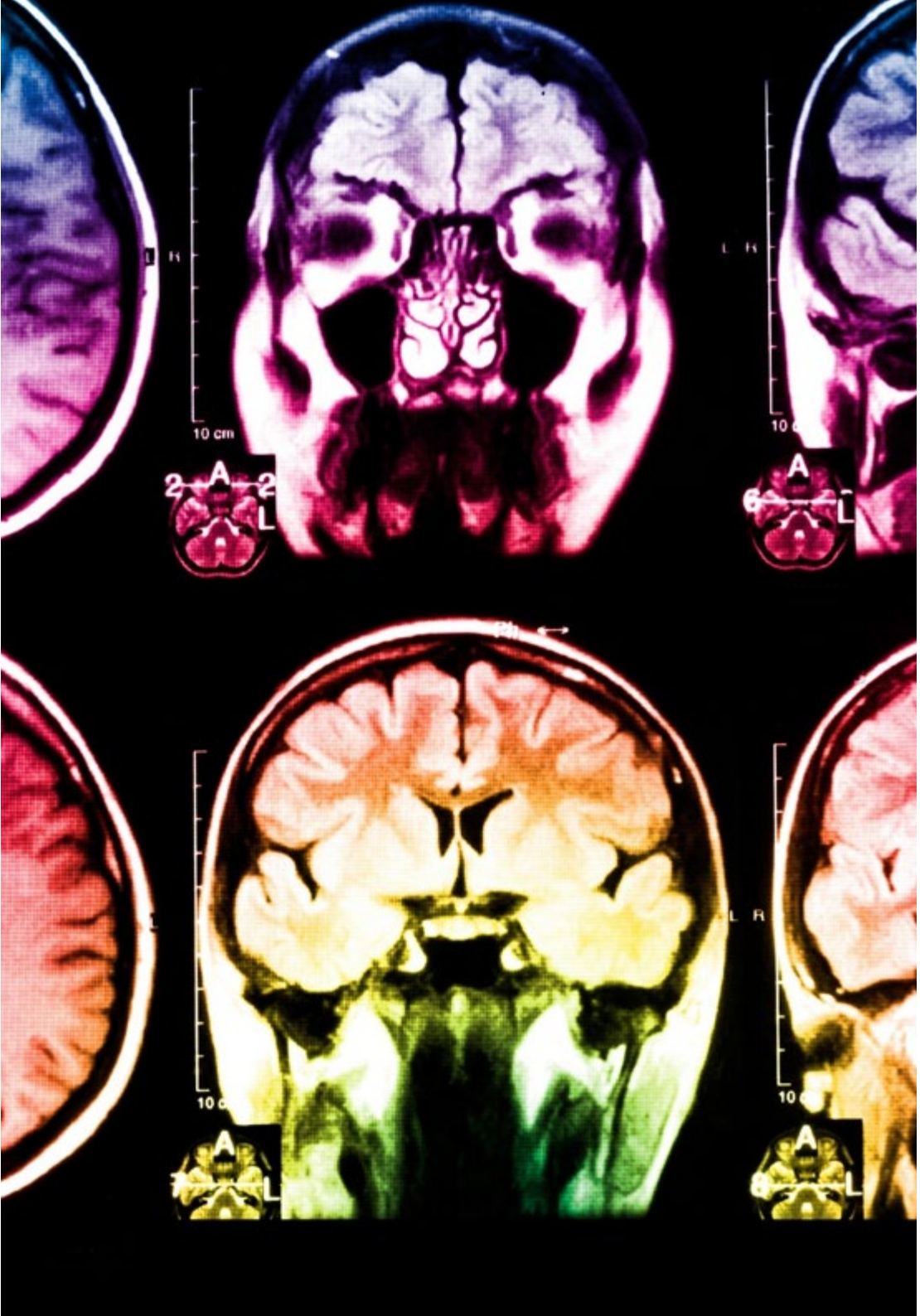
TECH combine efficacement la méthodologie des Études de Cas avec un système d'apprentissage 100% en ligne basé sur la répétition, qui associe différents éléments didactiques dans chaque leçon.

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.

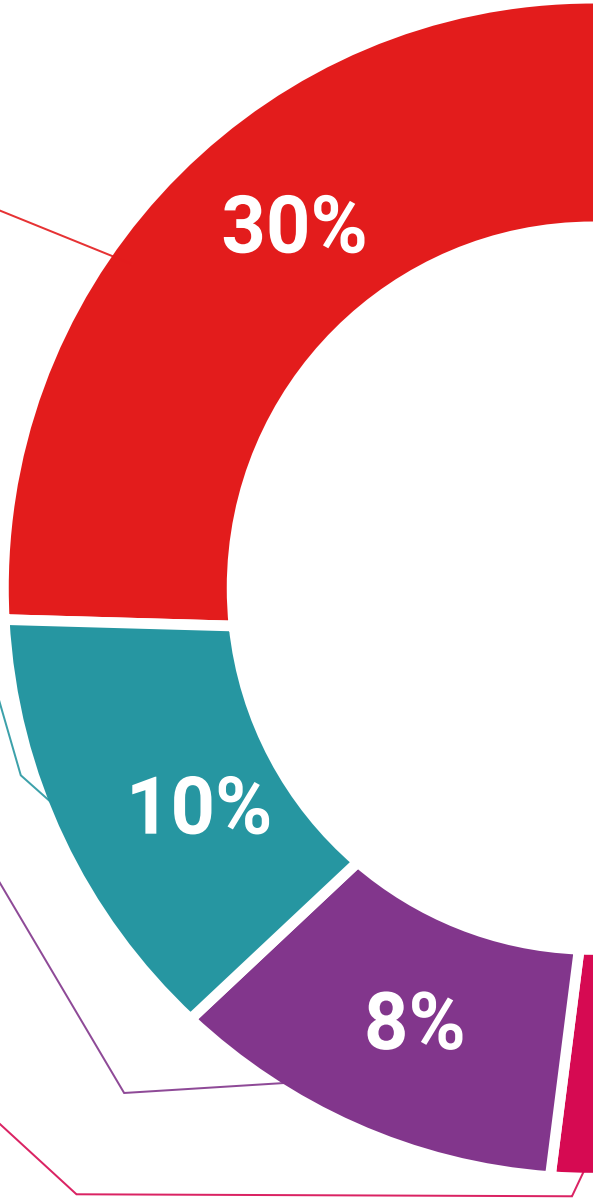
La méthode "Learning from an Expert" renforce les connaissances et la mémoire, et donne confiance dans les futures décisions difficiles.

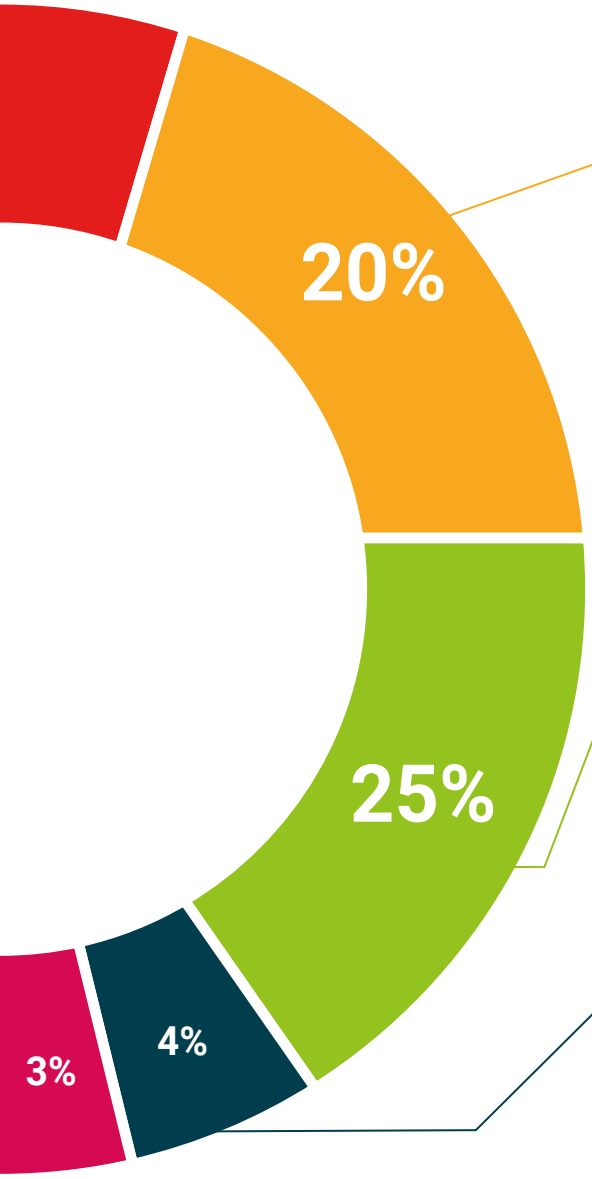
Pratiques en compétences et aptitudes

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.

07

Diplôme

Le Mastère Spécialisé en Direction de la Cybersécurité Avancée 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.

Finalisez cette formation avec succès et recevez votre diplôme sans avoir à vous soucier des déplacements ou des démarches administratives"

Ce **Mastère Spécialisé en Direction de la Cybersécurité Avancée** 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 Direction de la Cybersécurité Avancée**

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

Direction de la Cybersécurité Avancée

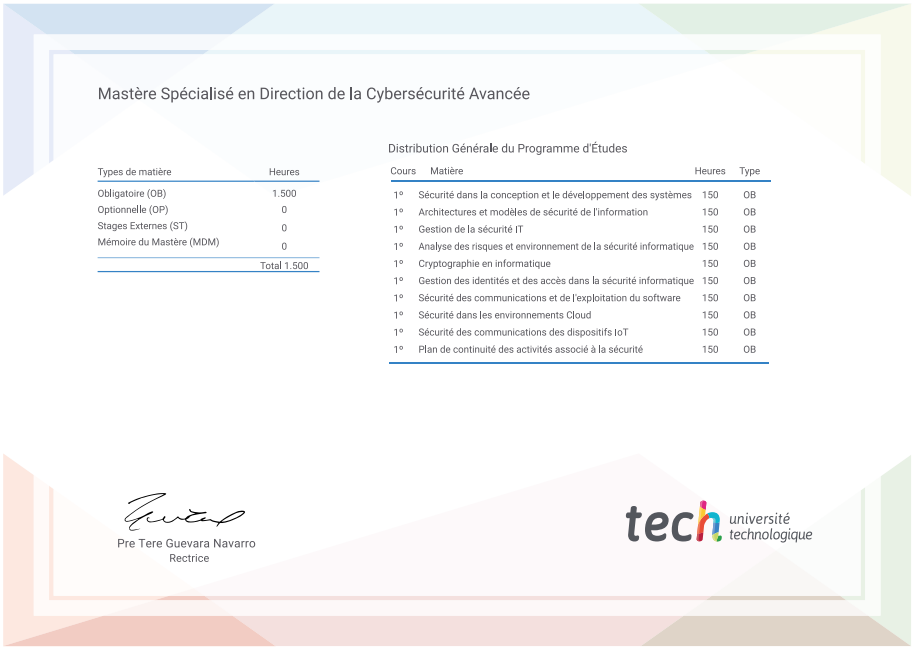
Il s'agit d'un diplôme spécialisé octroyé par cette Université d'une durée de 1.500 heures, débutant le dd/mm/aaaa et finalisant le dd/mm/aaaa.

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

Ce diplôme doit être impérativement accompagné d'un diplôme universitaire reconnu par les autorités compétantes pour exercer la profession dans chaque pays. Code Unique TECH: AFWOR23S techtitute.com/diplômes



Mastère Spécialisé en Direction de la Cybersécurité Avancée

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	Sécurité dans la conception et le développement des systèmes	150	OB
1º	Architectures et modèles de sécurité de l'information	150	OB
1º	Gestion de la sécurité IT	150	OB
1º	Analyse des risques et environnement de la sécurité informatique	150	OB
1º	Cryptographie en informatique	150	OB
1º	Gestion des identités et des accès dans la sécurité informatique	150	OB
1º	Sécurité des communications et de l'exploitation du software	150	OB
1º	Sécurité dans les environnements Cloud	150	OB
1º	Sécurité des communications des dispositifs IoT	150	OB
1º	Plan de continuité des activités associé à la sécurité	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
Direction de la Cybersécurité Avancée

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

Mastère Spécialisé
Direction de la Cybersécurité Avancée

tech université technologique