Mastère Spécialisé

Gestion des Politiques de Cybersécurité dans l'Entreprise

tech université technologique

tech université technologique

Mastère Spécialisé
Gestion des Politiques de Cybersécurité dans l'Entreprise

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

Accès web: **www.techtitute.com/fr/informatique/master/master-gestion-politiques-cybersecurite-entreprise**

Sommaire

01

Présentation

La dépendance accrue de nombreuses entreprises et industries vis-à-vis des environnements virtuels a, à son tour, entraîné la prolifération de la cybercriminalité et des cyberattaques contre tous les types d'organisations. Quelle que soit leur taille ou leur localisation, les menaces de cybersécurité représentent un réel danger qui peut entraîner de nombreuses pertes de temps, d'argent et de données. C'est pourquoi la figure de l'informaticien ayant des connaissances spécifiques en gestion des politiques de cybersécurité prend de plus en plus d'importance dans le secteur des entreprises, avec de nombreuses possibilités de développement professionnel et personnel. Ce diplôme offre aux professionnels de l'informatique une occasion unique de donner un coup de fouet à leur carrière, en s'appuyant sur une équipe de professionnels ayant une grande expérience dans le domaine. Le format 100% en ligne du diplôme en fait également une option totalement compatible avec toutes sortes d'activités ou de responsabilités.

Inscrivez-vous dès maintenant et accédez à un contenu spécialisé sur les politiques de gestion des incidents, la sécurité des logiciels et des matériels et la reprise après sinistre pratique en matière de sécurité"

Des milliers de cybercriminels attaquent chaque jour les entreprises du monde entier, même à des milliers de kilomètres de distance, ce qui a fait de la cybersécurité une préoccupation majeure dans le paysage commercial moderne. Les vulnérabilités des organisations qui reposent sur des environnements virtuels peuvent être exploitées par des criminels de toutes sortes, qui volent des données sensibles ou en empêchent l'accès en échange d'une rançon.

C'est pourquoi une gestion correcte des politiques de cybersécurité dans l'entreprise implique une grande responsabilité, cette position de responsabilité étant d'un grand prestige et d'une projection économique pour l'informaticien spécialisé. Par conséquent, franchir le pas et se pencher sur des questions telles que les systèmes d'audit pour localiser les menaces ou les protocoles de communication sécurisés, c'est se donner un coup de pouce direct pour accéder à un poste clé dans toute organisation.

Pour ce Mastère Spécialisé, un groupe d'enseignants soigneusement sélectionnés par TECH a préparé un contenu didactique de premier ordre. Tout au long de 10 modules complets, l'informaticien développera ses compétences dans la mise en œuvre des politiques de sécurité physique et environnementale, du système de gestion de la sécurité de l'information, des outils de surveillance et de nombreuses autres compétences qui feront de lui un atout précieux dans toute institution.

Tout cela avec l'avantage indéniable de ne pas avoir à assister à des cours en face à face ou à des horaires fixes, puisque l'ensemble du programme est enseigné en ligne. Le contenu didactique peut être téléchargé depuis n'importe quel appareil doté d'une connexion Internet et peut même être utilisé comme guide de référence une fois le diplôme obtenu. L'informaticien aura la liberté d'adapter la charge d'enseignement à son propre rythme, pouvant la combiner avec son activité professionnelle habituelle ou ses responsabilités plus exigeantes.

Ce **Mastère Spécialisé en Gestion des Politiques de Cybersécurité dans l'Entreprise** contient le programme le plus complet et le plus actualisé du marché. Ses principales caractéristiques sont :

- Le développement d'études de cas présentées par des experts en cybersécurité informatique.
- Le contenu graphique, schématique et éminemment pratique de l'ouvrage fournit des informations techniques et pratiques sur les disciplines essentielles à la pratique professionnelle.
- Des exercices pratiques où le processus d'auto-évaluation peut être utilisé pour améliorer l'apprentissage.
- Il met l'accent sur les méthodologies innovantes
- Des cours théoriques, des questions à l'expert, des forums de discussion sur des sujets controversés et un travail de réflexion individuel
- La possibilité d'accéder aux contenus depuis n'importe quel appareil fixe ou portable doté d'une connexion internet

Positionnez-vous comme un responsable de la politique de cybersécurité solvable, s'adaptant à toutes sortes de situations et d'événements imprévus en matière de sécurité informatique"

Intégrez dans votre travail quotidien les pratiques les plus efficaces de la politique de sécurité contre les attaques, mises au point par une équipe pédagogique spécialisée dans le domaine"

Accédez à un syllabus riche en contenu multimédia, renforcé par des sujets spécifiques sur les politiques de gestion de la sécurité, la classification des risques informatiques et le détournement.

Vous pourrez choisir quand, où et comment suivre l'ensemble des cours, avec la liberté totale de progresser à votre propre rythme dans le programme.

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

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

La conception de ce programme est basée sur l'Apprentissage par Problèmes. Ainsi l'étudiant devra essayer de résoudre les différentes situations de pratique professionnelle qui se présentent à lui tout au long du Mastère Spécialisé. Pour ce faire, l'étudiant sera assisté d'un innovant système de vidéos interactives, créé par des experts reconnus.

02

Objectifs

La cybersécurité étant une question si importante dans le monde des affaires d'aujourd'hui, ce diplôme suppose que l'informaticien joue un rôle central dans la résolution de ces problèmes. C'est pourquoi les objectifs poursuivis tout au long du cursus sont diversifiés, la priorité étant d'offrir un contenu théorique actualisé basé sur les dernières avancées en matière de sécurité informatique.

Vous aurez à votre disposition un guide de référence sur la gestion des politiques de cybersécurité qui vous aidera à dynamiser votre carrière d'informaticien expert en sécurité numérique"

Objectifs généraux

- Approfondir leur connaissance des concepts clés de la sécurité de l'information.
- Développer les mesures nécessaires pour assurer de bonnes pratiques en matière de sécurité de l'information.
- Développer les différentes méthodologies pour réaliser une analyse exhaustive des menaces.
- Installez et découvrez les différents outils utilisés dans le traitement et la prévention des incidents.

La méthodologie pédagogique de TECH vous permettra d'atteindre vos objectifs les plus ambitieux encore plus rapidement que vous ne le pensez"

Objectifs spécifiques

Module 1 Système de gestion de la sécurité de l'information (SGSI)

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

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

- Mettre en œuvre un SMSI dans l'entreprise
- Déterminer les départements que la mise en œuvre du système de gestion de la sécurité doit couvrir.
- Mettre en œuvre les contre-mesures de sécurité nécessaires dans l'opération.

Module 3. Politiques de sécurité pour l'analyse des menaces dans les systèmes informatiques

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

Module 4. Mise en œuvre pratique des politiques de sécurité logicielle et matérielle

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

existent pour le bastionnement des systèmes.

Module 5. Politiques de gestion des incidents de sécurité

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

Module 6. Mise en œuvre de politiques de sécurité physique et environnementale dans l'entreprise

- Analyser les termes "zone sécurisée" et "périmètre sécurisé".
- Examiner la biométrie et les systèmes biométriques
- Mise en œuvre de politiques de sécurité correctes pour la sécurité physique
- Développer les réglementations actuelles sur les zones sécurisées des systèmes informatiques

Module 7. Politiques de communications sécurisées dans l'entreprise

- Sécuriser un réseau de communication en le partitionnant
- Analyser les différents algorithmes de cryptage utilisés dans les réseaux de communication.
- Mise en œuvre de diverses techniques de cryptage dans le réseau telles que TLS, VPN ou SSH

Module 8. Mise en œuvre pratique des politiques de sécurité face aux attaques

- Déterminer les différentes attaques réelles sur notre système d'information
- Évaluer les différentes politiques de sécurité pour atténuer les attaques.
- Mettre en œuvre techniquement des mesures pour atténuer les principales menaces.

Module 9. Outils de surveillance des politiques de sécurité des systèmes d'information

- Développer le concept de suivi et de mise en œuvre des métriques
- Configurer des pistes d'audit sur les systèmes et surveiller les réseaux
- Compilation des meilleurs outils de surveillance du système actuellement disponibles sur le marché

Module 10. Politique pratique de sécurité en cas de catastrophe

- Générer des connaissances spécialisées sur le concept de continuité de la sécurité de l'information
- Élaborer un plan de continuité des activités
- Analyser un plan de continuité des TIC
- Conception d'un plan de reprise après sinistre

03

Compétences

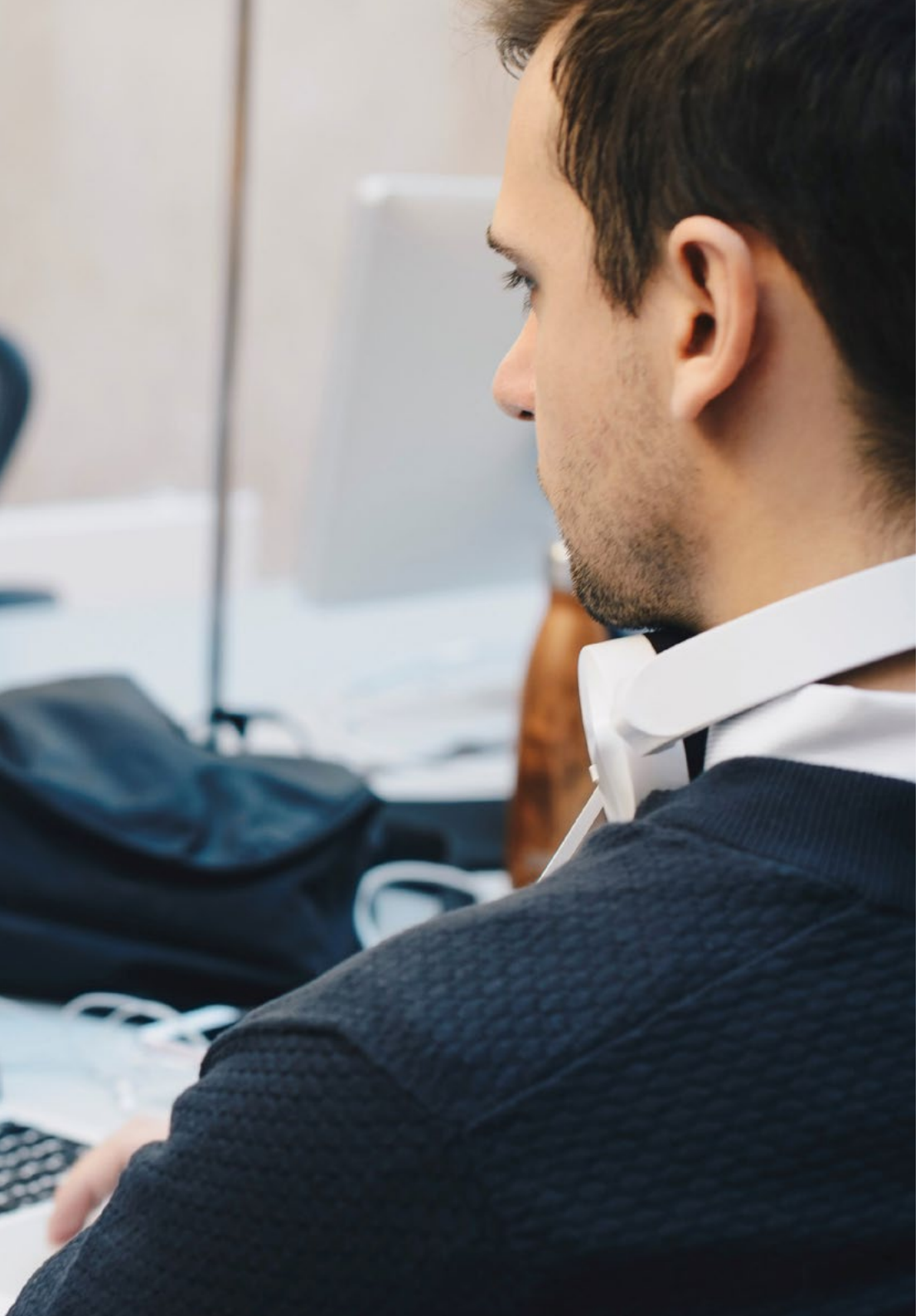
Afin de développer les compétences renforcées et spécialisées que doit posséder un informaticien spécialisé dans la politique de cybersécurité, TECH s'est appuyé sur un corps enseignant exceptionnel. Grâce à une combinaison pratique de leur expérience professionnelle et des derniers développements en matière de sécurité numérique, l'informaticien obtiendra une contextualisation beaucoup plus grande de chaque sujet abordé, avec de nombreux exemples et des ressources multimédia à l'appui.

Vous acquerrez un ensemble de compétences qui souligneront votre importance clé dans tout plan de cyber-stratégie dans votre organisation"

Compétences générales

- Mettre en œuvre et développer un plan de continuité des activités en fonction de chaque type d'entité et de ses besoins.
- Développer une analyse des processus d'affaires
- Analyser les méthodologies d'audit
- Évaluer la nécessité d'une analyse médico-légale de l'ordinateur pour une étude approfondie des incidents enregistrés.

Vous pourrez augmenter votre projection d'emploi et de salaire grâce à une spécialisation dans le sujet le plus préoccupant actuellement, la cybersécurité"



Compétences spécifiques

- Déterminer l'implication d'un SMSI dans l'organisation interne de l'entité, ainsi que son statut.
- Établir les politiques de sécurité dans l'entreprise
- Déterminer les mesures que nous devons mettre en œuvre avec les fournisseurs et la maintenance des systèmes d'information.
- Générer des connaissances spécialisées sur le contrôle des menaces
- Déterminer les phases de la gestion préventive des menaces
- Développer des méthodologies pour l'analyse des menaces informatiques
- Classer les menaces en fonction de leur impact et de leur gravité
- Concevoir une méthodologie propre pour l'analyse et le contrôle préventif des menaces
- Mettre en œuvre une politique de contrôle d'accès correcte pour les réseaux et les services.
- Analyser l'importance d'un traitement correct des incidents de sécurité.
- Compiler les différents systèmes biométriques disponibles
- Examiner la biométrie et les systèmes biométriques
- Mettre en œuvre les bonnes politiques de sécurité physique et les systèmes de contrôle d'accès physique dans les centres de traitement des données.
- Mise en œuvre d'un réseau sécurisé
- Examiner les vulnérabilités des plateformes mobiles et IoT et comment les prévenir.
- Établir les types d'ingénierie sociale et apprendre à les atténuer.
- Analyser le concept de suivi et de mise en œuvre des métriques.
- Déterminer le besoin de continuité de la sécurité de l'information

04

Direction de la formation

Tous les professionnels que TECH a sélectionnés pour ce Mastère Spécialisé ont une grande expérience dans le domaine de la gestion des services informatiques, en mettant toujours l'accent sur la cybersécurité et la bonne exécution des protocoles. C'est précisément cette expérience qui confère une qualité supérieure à l'ensemble du programme, car sa nature éminemment pratique signifie que l'informaticien peut adopter immédiatement toutes les nouvelles connaissances, améliorant ainsi ses compétences avant même d'avoir obtenu son diplôme.

Vous aurez le soutien et l'aide d'un groupe d'enseignants engagés au maximum dans votre perfectionnement professionnel vers la gestion des politiques de cybersécurité"

Direction

Mme Fernández Sapena, Sonia

- Formateur en sécurité informatique et Ethical Hacking au Centre National de Référence pour l'informatique et les télécommunications. de Madrid
- Instructeur certifié E-Council
- Formateur dans les certifications suivantes : EXIN Ethical Hacking Foundation y EXIN Cyber & IT Security Foundation. Madrid
- Formateur expert accrédité par le CAM pour les certificats de professionnalisme suivants : Sécurité informatique (IFCT0190), Gestion des réseaux voix et données (IFCM0310), Administration des réseaux départementaux (IFCT0410), Gestion des alarmes dans les réseaux de télécommunications (IFCM0410), Opérateur de réseaux voix et données (IFCM0110), et Administration des services Internet (IFCT0509).
- Collaborateur externe CSO/SSA (Chief Security Officer/Senior Security Architect) à l'Université des Baléares.
- Diplôme d'ingénieur en informatique de l'université d'Alcalá de Henares à Madrid.
- Master en DevOps : Docker et Kubernetes. Cas-Training
- Technologies de sécurité Microsoft Azure. E-Council

Professeurs

- Maîtrise en gestion des technologies de l'information par IDE-CESEM
- Gestion certifiée de la sécurité de l'information (CISM) par l'ISACA

M. Solana Villarias, Fabián

- Consultant en technologie de l'information
- Développeur et administrateur de services d'enquête chez Investigación, Planificación y Desarrollo, S.A.
- Spécialiste des marchés financiers et de la maintenance des systèmes informatiques chez Iberia Financial Software.
- Développeur web et spécialiste de l'accessibilité chez Indra
- Diplôme en ingénierie des systèmes supérieurs à l'Université du Pays de Galles/ CESINE
- Diplôme d'ingénieur technique en ingénierie des systèmes informatiques de l'Université du Pays de Galles/ CESINE

Mme López García, Rosa María

- Spécialiste de l'information de gestion
- Conférencier au Linux Professional Institute
- Collaborateur de l'Incibe Hacker Academy
- Capitaine des talents en cybersécurité chez Teamciberhack
- Responsable administratif, comptable et financier chez Integra2Transportes
- Assistante administrative en charge des achats de ressources au centre éducatif Cardenal Marcelo Espínola.
- Technicien supérieur en cybersécurité et piratage éthique
- Membre de Ciberpatrulla

M. Oropesiano Carrizosa, Francisco

- Ingénieur en informatique
- Technicien en micro-informatique, réseaux et sécurité chez Cas-Training
- Développeur de services Web, CMS, e-Commerce, UI et UX chez Fersa Reparaciones
- Gestionnaire de services Web, de contenu, de courrier et de DNS dans Oropesia Web & Network
- Concepteur d'applications graphiques et web chez Xarxa Sakai Projectes
- Diplômé en systèmes informatiques à l'Université d'Alcalá de Henares
- Master en DevOps : Docker et Kubernetes par le Cyber Business Center
- Technicien en réseaux et sécurité informatique de l'Université des Baléares
- Expert en design graphique de l'Université polytechnique de Madrid

M. Ortega López, Florencio

- Consultant en sécurité (gestion des identités) chez SIA Group
- Consultant en TIC et sécurité en tant que professionnel indépendant
- Formateur d'enseignants dans le secteur de l'informatique
- Diplômé en ingénierie technique industrielle de l'université d'Alcalá de Henares
- Maîtrise pour les enseignants de l'UNIR (UNIR)
- MBA en gestion et administration des affaires de l'IDE-CESEM

M. Peralta Alonso, Jon

- Consultant senior - Protection des données et cybersécurité. Altia
- Avocat / Conseiller juridique. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Conseiller juridique / Stagiaire. Bureau professionnel : Oscar Padura
- Diplôme en droit. Université publique du Pays basque
- Master en protection des données Délégué. EIS Innovative School
- Maîtrise en droit. Université publique du Pays basque
- Maîtrise spécialisée en pratique du contentieux civil. Université internationale Isabel I de Castille
- Chargé de cours pour le Master en protection des données personnelles, cybersécurité et droit des TIC

Profitez de l'occasion pour découvrir les dernières avancées dans ce domaine et les appliquer à votre pratique quotidienne”

05

Structure et contenu

TECH a utilisé la méthodologie *Relearning* pour développer tous les contenus de ce programme. Cela signifie que les clés et les concepts les plus importants dans le domaine de la gestion des politiques de cybersécurité sont donnés progressivement tout au long du syllabus, ce qui permet un enseignement beaucoup plus efficace et rapide. L'informaticien aura accès à de nombreuses vidéos détaillées, à des exercices d'autocontrôle et à des lectures complémentaires faites et sélectionnées spécifiquement pour chaque thème du programme.

Tout le matériel multimédia contenu dans ce Mastère Spécialisé vous aidera à vous spécialiser de manière beaucoup plus profonde, rapide et exhaustive"

Module 1 Système de gestion de la sécurité de l'information

1.1. Sécurité de l'information. Aspects clés
- 1.1.1. Sécurité de l'information
  - 1.1.1.1. Confidentialité
  - 1.1.1.2. Intégration
  - 1.1.1.3. Disponibilité
  - 1.1.1.4. Mesures de sécurité de l'information

1.2. Système de gestion de la sécurité de l'information
- 1.2.1. Modèles de gestion de la sécurité de l'information
- 1.2.2. Documents pour la mise en œuvre d'un SGSI
- 1.2.3. Niveaux et contrôles d'un SGSI

1.3. Normes et standards internationaux
- 1.3.1. Normes internationales en matière de sécurité de l'information
- 1.3.2. Origine et évolution de la norme
- 1.3.3. Normes internationales de gestion de la sécurité de l'information
- 1.3.4. Autres normes de référence

1.4. Normes ISO/IEC 27000
- 1.4.1. Objectif et champ d'application
- 1.4.2. Structure de la norme
- 1.4.3. Certification
- 1.4.4. Phases de l'accréditation
- 1.4.5. Avantages des normes ISO/IEC 27.000

1.5. Conception et mise en œuvre d'un système général de sécurité de l'information
- 1.5.1. Conception et mise en œuvre d'un système général de sécurité de l'information
- 1.5.2. Phases de mise en œuvre d'un système général de sécurité de l'information
- 1.5.3. Plan de continuité des activités

1.6. Phase I : diagnostic
- 1.6.1. Diagnostic préliminaire
- 1.6.2. Identification du niveau de stratification
- 1.6.3. Niveau de conformité aux standards/normes

1.7. Phase II : Préparation
- 1.7.1. Contexte organisationnel
- 1.7.2. Analyse des règlements de sécurité applicables
- 1.7.3. Portée du système global de sécurité de l'information
- 1.7.4. Politique générale du système de sécurité des informations
- 1.7.5. Objectifs du système général de sécurité de l'information

1.8. Phase III : Planification
- 1.8.1. Classification des actifs
- 1.8.2. Évaluation des risques
- 1.8.3. Identification des menaces et des risques

1.9. Phase IV : Mise en œuvre et suivi
- 1.9.1. Analyse des résultats
- 1.9.2. Attribution des responsabilités
- 1.9.3. Calendrier du plan d'action
- 1.9.4. Suivi et Vérification

1.10. Politiques de sécurité en matière de gestion des incidents
- 1.10.1. Phases
- 1.10.2. Catégorisation des incidents
- 1.10.3. Procédures et gestion des incidents

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

2.1. Organisation interne
- 2.1.1. Attribution des responsabilités
- 2.1.2. Séparation des tâches
- 2.1.3. Contacts avec les autorités
- 2.1.4. Sécurité de l'information dans la gestion de projet

2.2. Gestion des actifs
- 2.2.1. Responsabilité des biens
- 2.2.2. Classification des informations
- 2.2.3. Manipulation des supports de stockage

2.3. Politiques de sécurité dans les processus d'entreprise
  2.3.1. Analyse des processus commerciaux vulnérables
  2.3.2. Analyse de l'impact sur les affaires
  2.3.3. Classement des processus en fonction de leur impact sur l'entreprise
2.4. Politiques de sécurité liées aux ressources humaines
  2.4.1. Pré-embauche
  2.4.2. Pendant le recrutement
  2.4.3. Cessation ou changement de poste
2.5. Politiques de sécurité au niveau de la direction
  2.5.1. Lignes directrices en matière de gestion de la sécurité de l'information
  2.5.2. BIA - Analyse de l'impact
  2.5.3. Le plan de reprise comme politique de sécurité
2.6. Acquisition et maintenance des systèmes d'information
  2.6.1. Exigences de sécurité des systèmes d'information
  2.6.2. Développement et soutien de la sécurité des données
  2.6.3. Données d'essai
2.7. Sécurité avec les fournisseurs
  2.7.1. Sécurité informatique avec les fournisseurs
  2.7.2. Gestion de la fourniture du service avec garantie
  2.7.3. Sécurité de la chaîne d'approvisionnement
2.8. Sécurité opérationnelle
  2.8.1. Responsabilités opérationnelles
  2.8.2. Protection contre les codes malveillants
  2.8.3. Copies de sauvegarde
  2.8.4. Journaux d'activité et suivi
2.9. Gestion et réglementation de la sécurité
  2.9.1. Gestion et réglementation de la sécurité
  2.9.2. Respect des exigences légales
  2.9.3. Examens de la sécurité de l'information
2.10. La sécurité dans la gestion de la continuité des activités
  2.10.1. La sécurité dans la gestion de la continuité des activités
  2.10.2. Continuité de la sécurité de l'information
  2.10.3. Licenciements

Module 3. Politiques de sécurité pour l'analyse des menaces dans les systèmes d'information

3.1. Gestion des menaces dans les politiques de sécurité
  3.1.1. Gestion des risques
  3.1.2. Risque de sécurité
  3.1.3. Méthodologies de gestion des menaces
  3.1.4. Mise en œuvre des méthodologies
3.2. Phases de la gestion des menaces
  3.2.1. Identification
  3.2.2. Analyse
  3.2.3. Localisation
  3.2.4. Mesures de sauvegarde
3.3. Audit des systèmes pour la localisation des menaces
  3.3.1. Systèmes d'audit de la localisation des menaces
  3.3.2. Classification et flux d'informations
  3.3.3. Analyse des processus vulnérables
3.4. Classification des risques
  3.4.1. Types de risques
  3.4.2. Calcul de la probabilité de la menace
  3.4.3. Risque résiduel
3.5. Traitement des risques
  3.5.1. Traitement du risque
  3.5.2. Mise en œuvre des mesures de sauvegarde
  3.5.3. Transfert ou reprise

3.6. Contrôle des risques
- 3.6.1. Processus continu de gestion des risques
- 3.6.2. Mise en œuvre des mesures de sécurité
- 3.6.3. Modèle stratégique des mesures de sécurité de l'information

3.7. Méthodologies pratiques pour l'analyse et le contrôle des menaces
- 3.7.1. Catalogue des menaces
- 3.7.2. Catalogue des mesures de contrôle
- 3.7.3. Catalogue des mesures de sauvegarde

3.8. Norme ISO 27005
- 3.8.1. Identification des risques
- 3.8.2. Analyse des risques
- 3.8.3. Évaluation des risques

3.9. Matrice des risques, des impacts et des menaces
- 3.9.1. Données, systèmes et personnel
- 3.9.2. Probabilité de la menace
- 3.9.3. Ampleur des dommages

3.10. Phases et processus de conception de l'analyse des risques
- 3.10.1. Identification des éléments critiques de l'organisation
- 3.10.2. Détermination des menaces et des impacts
- 3.10.3. Analyse d'impact et de risque
- 3.10.4 Méthodologies

Module 4. Mise en œuvre pratique des politiques de sécurité des logiciels et des matériels

4.1. Mise en œuvre pratique des politiques de sécurité des logiciels et des matériels
- 4.1.1. Mise en œuvre de l'identification et de l'autorisation
- 4.1.2. Mise en œuvre des techniques d'identification
- 4.1.3. Mesures techniques d'autorisation

4.2. Technologies d'identification et d'autorisation
- 4.2.1. Identifiant et OTP
- 4.2.2. *Clé USB* ou carte à puce PKI
- 4.2.3. La touche "Confidentiel Défense".
- 4.2.4. RFID active

4.3. Politiques de sécurité d'accès aux logiciels et aux systèmes
- 4.3.1. Mise en œuvre des politiques de contrôle d'accès
- 4.3.2. Mise en œuvre des politiques d'accès aux communications
- 4.3.3. Types d'outils de sécurité pour le contrôle d'accès

4.4. Gestion de l'accès des utilisateurs
- 4.4.1. Gestion des droits d'accès
- 4.4.2. Séparation des rôles et des fonctions d'accès
- 4.4.3. Mise en œuvre des droits d'accès dans les systèmes

4.5. Contrôle de l'accès aux systèmes et aux applications
- 4.5.1. Règle d'accès minimal
- 4.5.2. Technologies de connexion sécurisée
- 4.5.3. Politiques de sécurité des mots de passe

4.6. Technologies des systèmes d'identification
- 4.6.1. Active Directory
- 4.6.2. OTP
- 4.6.3. PAP, CHAP
- 4.6.4. KERBEROS, DIAMETER, NTLM

4.7. Contrôles CIS pour le bastioning du système
- 4.7.1. Contrôles de base du CIS
- 4.7.2. Contrôles fondamentaux du CIS
- 4.7.3. Contrôles organisationnels CIS

4.8. Sécurité opérationnelle
- 4.8.1. Protection contre les codes malveillants
- 4.8.2. Copies de sauvegarde
- 4.8.3. Enregistrement et suivi des activités

4.9. Gestion des vulnérabilités techniques
- 4.9.1. Vulnérabilités techniques
- 4.9.2. Gestion des vulnérabilités techniques
- 4.9.3. Restrictions relatives à l'installation du logiciel

4.10. Mise en œuvre des pratiques de la politique de sécurité
- 4.10.1. Mise en œuvre des pratiques de la politique de sécurité
- 4.10.2. Vulnérabilités logiques
- 4.10.3. Mise en œuvre des politiques de défense

Module 5. Politiques de gestion des incidents de sécurité

5.1. Politiques de gestion de Incidence sécurité de l'information des améliorations
- 5.1.1. Gestion des incidents
- 5.1.2. Responsabilités et procédures
- 5.1.3. Notification d'événement

5.2. Systèmes de détection et de prévention des Intrusion: (IDS/IPS)
- 5.2.1. Données de fonctionnement du système
- 5.2.2. Types de systèmes de détection d'intrusion
- 5.2.3. Critères de placement des IDS/IPS

5.3. Réponse aux incidents de sécurité
- 5.3.1. Procédure de collecte d'informations
- 5.3.2. Processus de vérification des intrusions
- 5.3.3. Organismes CERT

5.4. Processus de notification et de gestion des tentatives d'intrusion
- 5.4.1. Responsabilités dans le processus de notification
- 5.4.2. Classification des incidents
- 5.4.3. Processus de résolution et de récupération

5.5. L'analyse médico-légale comme politique de sécurité
- 5.5.1. Preuves volatiles et non volatiles
- 5.5.2. Analyse et collecte de preuves électroniques
  - 5.5.2.1. Analyse des preuves électroniques
  - 5.5.2.2. Collecte de preuves électroniques

5.6. Outils de systèmes de détection et de prévention des intrusions (IDS/IPS)
- 1.7.1. *Snort*
- 5.6.2. Suricata
- 5.6.3. Solar-Winds

5.7. Outils de centralisation des événements
- 5.7.1. SIM
- 5.7.2. SEM
- 5.7.3. SIEM

5.8. Guide de sécurité CCN-STIC 817
- 5.8.1. Guide de sécurité CCN-STIC 817
- 5.8.2. Gestion des cyberincidents
- 5.8.3. Métriques et indicateurs

5.9. NIST SP800-61
- 5.9.1. Capacité de réponse aux incidents de sécurité informatique
- 5.9.2. Traitement des incidents
- 5.9.3. Coordination et partage d'informations

5.10. Norme ISO 27035
- 5.10.1. ISO 27035. Principes de la gestion des incidents
- 5.10.2. Lignes directrices pour l'élaboration d'un plan de gestion des incidents
- 5.10.3. Lignes directrices pour les opérations de réponse aux incidents

Module 6. Mettre en œuvre des politiques de sécurité physique et environnementale dans l'entreprise

6.1. Zones sécurisées
- 6.1.1. Périmètre de sécurité physique
- 6.1.2. Travailler dans des zones sécurisées
- 6.1.3. Sécurité des bureaux, des locaux et des ressources

6.2. Contrôles physiques d'entrée
- 6.2.1. Contrôles physiques d'entrée
- 6.2.2. Politiques de contrôle d'accès physique
- 6.2.3. Systèmes de contrôle des entrées physiques

6.3. Vulnérabilités de l'accès physique
- 6.3.1. Vulnérabilités de l'accès physique
- 6.3.2. Principales vulnérabilités physiques
- 6.3.3. Mise en œuvre des mesures de sauvegarde

6.4. Systèmes biométriques physiologiques
- 6.4.1. Empreinte digitale
- 6.4.2. Reconnaissance faciale
- 6.4.3. Reconnaissance de l'iris et de la rétine
- 6.4.4. Autres systèmes biométriques physiologiques

6.5. Systèmes biométriques comportementaux
- 1.7.1. Reconnaissance de la signature
- 6.5.2. Reconnaissance des écrivains
- 6.5.3. Reconnaissance vocale
- 6.5.4. Autres systèmes biométriques comportementaux

6.6. Gestion du risque en biométrie
- 6.6.1. Gestion du risque en biométrie
- 6.6.2. Mise en œuvre des systèmes biométriques
- 6.6.3. Vulnérabilités des systèmes biométriques

6.7. Mise en œuvre des politiques d' *Hosts*
- 6.7.1. Installation du câblage Provisionnement et sécurité
- 6.7.2. Emplacement de l'équipement
- 6.7.3. Sortie de l'équipement à l'extérieur des locaux
- 6.7.4. Politique relative aux équipements informatiques non surveillés et aux postes clairs

6.8. Protection de l'environnement
- 6.8.1. Systèmes de protection contre l'incendie
- 6.8.2. Systèmes de protection contre les tremblements de terre
- 6.8.3. Systèmes de protection contre les tremblements de terre

6.9. Sécurité du centre de traitement des données
- 6.9.1. Portes de sécurité
- 6.9.2. Systèmes de vidéosurveillance (CCTV)
- 6.9.3. Contrôle de sécurité

6.10. Règlement international sur la sécurité physique
- 6.10.1. IEC 62443-2-1 (européen)
- 6.10.2. NERC CIP-005-5 (U.S.A.)
- 6.10.3. NERC CIP-014-2 (U.S.A.)

Module 7. Politiques de communications sécurisées dans l'entreprise

7.1. Gestion de la sécurité des réseaux
- 7.1.1. Surveillance et contrôle du réseau
- 7.1.2. Ségrégation des réseaux
- 7.1.3. Systèmes de sécurité des réseaux

7.2. Protocoles de communication sécurisés
- 7.2.1. Modèle TCP/IP
- 7.2.2. Protocole IPSEC
- 7.2.3. Protocole TLS

7.3. Protocole TLS 1,3
- 7.3.1. Phases d'un processus TLS1.3
- 7.3.2. Protocole *Handshake*
- 7.3.3. Protocole d'enregistrement
- 7.3.4. Différences avec TLS 1.2

7.4. Algorithmes cryptographiques
- 7.4.1. Algorithmes cryptographiques utilisés dans les communications
- 7.4.2. *Suites à ciphers*
- 7.4.3. Algorithmes cryptographiques autorisés pour TLS 1.3

7.5. Fonctions *Digest*
- 7.5.1. Fonctions *Digest*
- 7.5.2. MD6
- 7.5.3. SHA

7.6. PKI. Infrastructure à clé publique
- 7.6.1. PKI et ses entités
- 7.6.2. Certificat numérique
- 7.6.3. Types de certificats numériques

7.7. Communications dans les tunnels et les transports
- 7.7.1. Tunnel de communication
- 7.7.2. Communications de transport

7.7.3. Mise en œuvre du tunnel crypté
7.8. SSH *Secure Shell*
7.8.1. SSH Secure Shell
7.8.2. Opération SSH
7.8.3. Outils de SSH
7.9. Vérification des systèmes cryptographiques
7.9.1. Vérification des systèmes cryptographiques
7.9.2. Test d'intégrité
7.9.3. Test de systèmes cryptographiques
7.10. Systèmes cryptographiques
7.10.1. Systèmes cryptographiques
7.10.2. Vulnérabilités des systèmes cryptographiques
7.10.3. Garanties cryptographiques

Module 8. Mise en œuvre pratique des politiques de sécurité contre les attaques

8.1. *System Hacking*
8.1.1. *System Hacking*
8.1.2. Risques et vulnérabilités
8.1.3. Contre-mesures
8.2. DoS dans les services
8.2.1. DoS dans les services
8.2.2. Risques et vulnérabilités
8.2.3. Contre-mesures
8.3. *Session Hijacking*
1.7.1. *Session Hijacking*
8.3.2. Le processus de *Hijacking*
8.3.3. Contre-mesures au *Hijacking*
8.4. Évasion des IDS, *Firewalls and Honeypots*
8.4.1. Évasion des IDS, *Firewalls and Honeypots*
8.4.2. Techniques d'évasion
8.4.3. Mise en œuvre de contre-mesures
8.5. *Piratage des serveurs Web*
8.5.1. *Piratage des serveurs Web*
8.5.2. Attaques contre les serveurs web
8.5.3. Mise en œuvre des mesures de défense
8.6. *Piratage des applications Web*
8.6.1. *Piratage des applications Web*
8.6.2. Attaques contre les applications Web
8.6.3. Mise en œuvre des mesures de défense
8.7. *Hacking Wireless Networks*
8.7.1. *Hacking Wireless Networks*
8.7.2. Vulnérabilités du réseau Wifi
8.7.3. Mise en œuvre des mesures de défense
8.8. *Hacking Mobile Platforms*
8.8.1. *Hacking Mobile Platforms*
8.8.2. Vulnérabilités des plates-formes mobiles
8.8.3. Mise en œuvre de contre-mesures
8.9. *Ramsonware*
8.9.1. *Ramsonware*
8.9.2. Vulnérabilités causant le *Ramsonware*
8.9.3. Mise en œuvre de contre-mesures
8.10. Ingénierie sociale
8.10.1. Ingénierie sociale
8.10.2. Types d'ingénierie sociale

8.10.3. Contre-mesures à l'ingénierie sociale

Module 9. Outils de surveillance des politiques de sécurité des systèmes d'information

9.1. Politiques de surveillance des systèmes d'information
- 9.1.1. Surveillance du système
- 9.1.2. Métriques
- 9.1.3. Types de mesures

9.2. Vérification et enregistrement dans les systèmes
- 9.2.1. Audit et journalisation dans les systèmes
- 9.2.2. Audit et journalisation de Windows
- 9.2.3. Journalisation et audit de Linux

9.3. Protocole SNMP. *Protocole de gestion de réseau simple*
- 9.3.1. Protocole SNMP
- 9.3.2. Opération SNMP
- 9.3.3. Outils de SNMP

9.4. Surveillance du réseau
- 9.4.1. Surveillance du réseau
- 9.4.2. Surveillance du réseau dans les systèmes de contrôle
- 9.4.3. Outils de surveillance des systèmes de contrôle

9.5. Nagios. Système de surveillance du réseau
- 9.5.1. Nagios
- 9.5.2. Fonctionnement de Nagios
- 9.5.3. Installation de Nagios

9.6. Zabbix. Système de surveillance du réseau
- 9.6.1. Zabbix
- 9.6.2. Fonctionnement de Zabbix
- 9.6.3. Installation de Zabbix

9.7. Cacti. Système de surveillance du réseau
- 9.7.1. Cacti.
- 9.7.2. Fonctionnement de Cacti

9.7.3. Installation de Cacti
9.8. Pandora Système de surveillance du réseau
9.8.1. Pandora
9.8.2. Fonctionnement de Pandora
9.8.3. Installation de Pandora
9.9. *SolarWinds*. Système de surveillance du réseau
9.9.1. *SolarWinds*.
9.9.2. Fonctionnement de *SolarWinds*
9.9.3. Installation de *SolarWinds*
9.10. Suivi des règlements
9.10.1. Suivi des règlements
9.10.2. Contrôles CIS sur l'audit et l'enregistrement
9.10.3. NIST 800-123 (ÉTATS-UNIS)

Module 10. Politique pratique de sécurité en cas de catastrophe

10.1. DRP Plan de reprise après sinistre
1.7.1. Objectif d'un DRP
10.1.2. Avantages d'un DRP
10.1.3. Conséquences de ne pas avoir de PRA et de ne pas le tenir à jour
10.2. Guide pour la définition d'un DRP (plan de reprise après sinistre)
10.2.1. Portée et objectifs
10.2.2. Conception de la stratégie de récupération
10.2.3. Répartition des rôles et des responsabilités
10.2.4. Inventaire du matériel, des logiciels et des services
10.2.5. Tolérance aux temps d'arrêt et aux pertes de données
10.2.6. Déterminer les types spécifiques de DRP requis
10.2.7. Mise en œuvre d'un plan de formation, de sensibilisation et de communication
10.3. Portée et objectifs d'un DRP (Disaster Recovery Plan)
10.3.1. Assurer la réponse
10.3.2. Composants technologiques
10.3.3. Champ d'application de la politique de continuité
10.4. Conception d'une stratégie de reprise après sinistre (DRP)
10.4.1. Stratégie de reprise après sinistre
10.4.2. Budget
10.4.3. Ressources humaines et physiques
1.7.4. Postes de direction à risque
10.4.5. Technologie
10.4.6. Données
10.5. Continuité des processus d'information
10.5.1. Planification de la continuité
10.5.2. Mise en œuvre de la continuité
10.5.3. Vérification et évaluation de la continuité
10.6. Portée d'un PCA (Plan de continuité des activités)
10.6.1. Détermination des processus les plus critiques
10.6.2. Approche fondée sur les actifs
10.6.3. Approche par processus
10.7. Mise en œuvre de processus d'affaires assurés
10.7.1. Activités prioritaires (AP)
10.7.2. Temps de récupération idéal (TRI)
10.7.3. Stratégies de survie
10.8. Analyse organisationnelle
10.8.1. Collecte d'informations
10.8.2. Analyse de l'impact sur les entreprises (BIA)
10.8.3. Analyse des risques organisationnels
10.9. Réponse aux situations d'urgence
10.9.1. Plan de crise
10.9.2. Plans de rétablissement de l'environnement opérationnel
10.9.3. Procédures techniques de travail ou d'incident
10.10. Norme internationale ISO 27031 BCP
10.10.1. Objectifs
10.10.2. 2015 : références, normes et champ d'application
10.10.3. Opération

06

Méthodologie

Cette formation vous propose une manière différente d'apprendre. Notre méthodologie est développée à travers un mode d'apprentissage cyclique: ***Le Relearning***.
Ce système d'enseignement s'utilise, notamment, dans les Écoles de Médecine les plus prestigieuses du monde. De plus il a été considéré comme l'une des Méthodes les plus efficaces par des magazines scientifiques de renom comme par exemple le ***New England Journal of Medicine.***

Découvrez Relearning, un système qui abandonne 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 contextualiser tout le contenu.

Notre programme propose une approche révolutionnaire du développement des compétences et des connaissances. Notre objectif est de renforcer les compétences dans un contexte changeant, compétitif et très exigeant.

Avec TECH, vous ferez l'expérience d'une méthode d'apprentissage qui ébranle les fondements des universités traditionnelles du monde entier"

Vous accéderez à un système d'apprentissage basé sur la répétition, avec un enseignement naturel et progressif tout au long du cursus.

L'étudiant apprendra, par le biais d'activités collaboratives et de cas réels, à résoudre des situations complexes dans des environnements commerciaux réels.

Une méthode d'apprentissage innovante et différente

Ce Mastère Spécialisé de TECH est un programme d'enseignement intensif, créé de toutes pièces, offrir aux managers des défis et des décisions d'affaires au plus haut niveau, que ce soit au niveau national ou international. Grâce à cette méthodologie, l'épanouissement personnel et professionnel est stimulé, faisant ainsi un pas décisif vers la réussite. La méthode des cas, une technique qui jette les bases de ce contenu, garantit que la réalité économique, sociale et professionnelle la plus actuelle est suivie.

> *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 de Sciences informatique du monde et ce depuis leur fondement. Développée en 1912 à Harvard pour que les étudiants en Droit n'apprennent pas uniquement sur la base d'un contenu théorique, la méthode des cas consistait à leur présenter des situations réelles complexes pour que les apprenants s'entraînent à les résoudre et à prendre des décisions. Elle a été établie comme méthode d'enseignement standard à Harvard en 1924.

Face à une situation donnée, que doit faire un professionnel? C'est la question à laquelle nous vous confrontons dans la méthode des cas, une méthode d'apprentissage orientée vers l'action. Tout au long du programme, vous serez confronté à de multiples cas réels. Ils devront intégrer toutes leurs connaissances, faire des recherches, argumenter et défendre leurs idées et leurs décisions.

Relearning Methodology

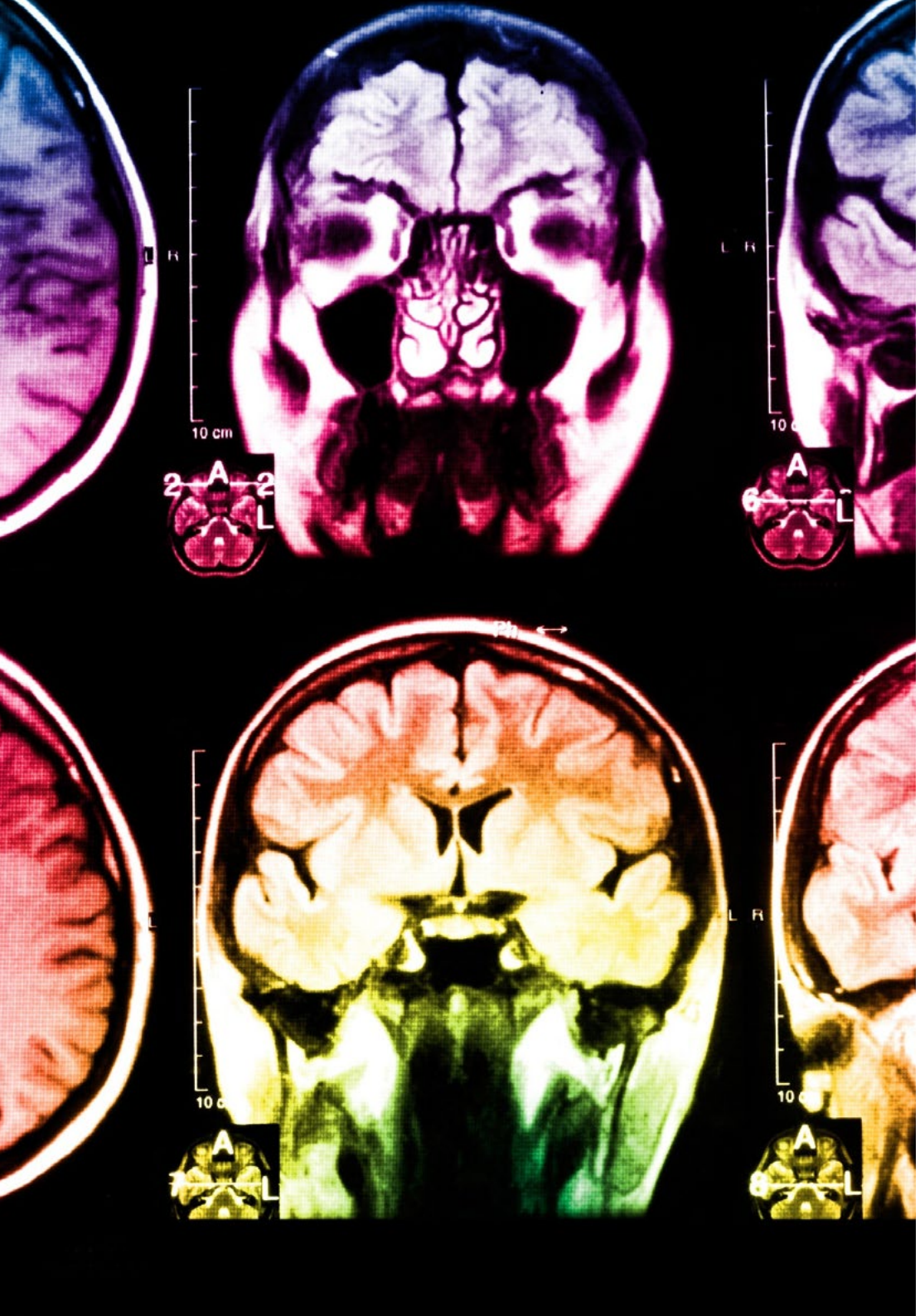
TECH est la première Université au monde à combiner les case studies avec un système d'apprentissage 100% en ligne basé sur la répétition, qui combine éléments didactiques différents dans chaque leçon.

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 serez formé 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 efficace. 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 Mastère Spécialisé, 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. Grâce à cette méthodologie, nous avons formé 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 matière de gestion, les sciences du sport, la philosophie, le droit, l'ingénierie, le journalisme, l'histoire ou les marchés et instruments financiers. Le tout 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 plus facilement et de manière plus productive tout en développant un esprit critique, en défendant des arguments et en contrastant des opinions : une équation directe vers le succès.

D'après les dernières données 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 façon, et dans ce que l'on appelle Neurocognitive context-dependent elearning les différents éléments de notre programme sont liés au contexte dans lequel le participant développe sa pratique professionnelle.

Ce programme offre les meilleurs matériels éducatifs, préparés à l'intention des professionnels :

Support d'étude

Tous les contenus didactiques sont créés par les spécialistes qui enseignent les cours. Ils ont été conçus en exclusivité pour le programme 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 online. Ils sont élaborés à l'aide des dernières techniques ce qui nous permet de vous offrir une grande qualité dans chacun des supports que nous partageons avec vous.

Cours magistraux

Il existe de nombreux faits scientifiques prouvant l'utilité de l'observation par un tiers expert.

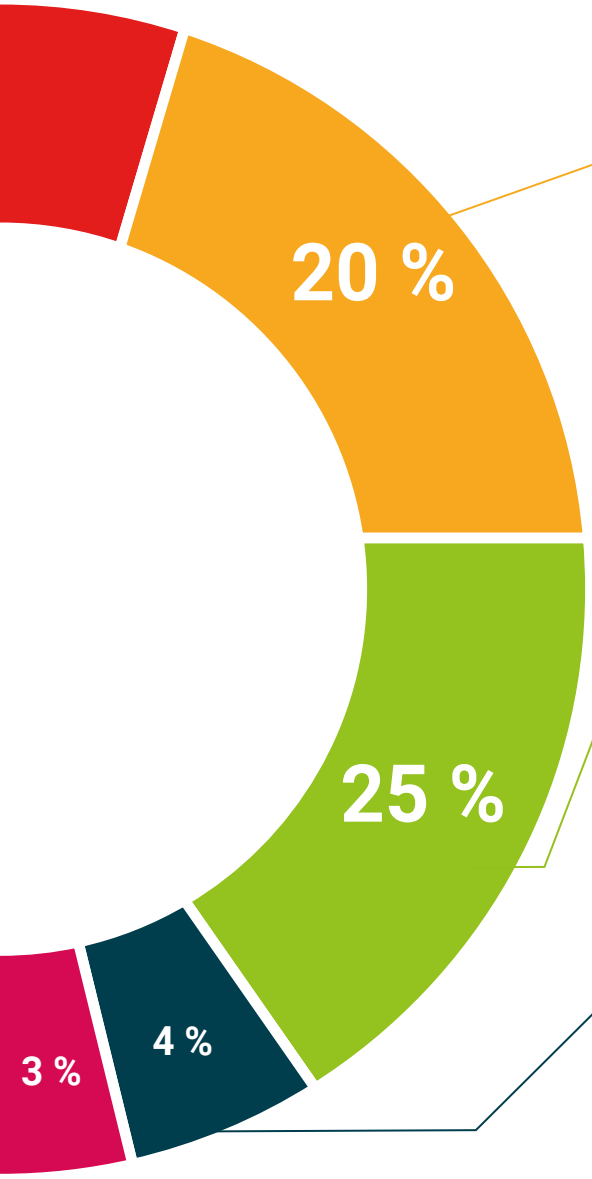
La méthode Learning from an Expert renforce les connaissances et la mémoire, et génère de la confiance dans les futures décisions difficiles.

Pratique des aptitudes et des compétences

Ils réaliseront des activités visant à développer des compétences et des aptitudes spécifiques dans chaque domaine. Pratiques et dynamiques pour acquérir et développer les compétences et les capacités 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 notre bibliothèque virtuelle TECH, vous aurez accès à tout ce dont vous avez besoin pour compléter votre 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

Nous présentons les contenus de manière attrayante et dynamique dans des dossiers multimédias comprenant des fichiers audios, des vidéos, des images, des diagrammes et des cartes conceptuelles afin de consolider les connaissances.

Ce système unique de formation à 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 Gestion des Politiques de Cybersécurité dans l'Entreprise garantit, outre la formation la plus rigoureuse et la plus actuelle, l'accès à un Mastère Spécialisé délivré par TECH Université Technologique.

Terminez ce programme avec succès et recevez votre diplôme sans avoir à vous soucier des voyages ou de la paperasserie"

Ce **Mastère Spécialisé en Gestion des Politiques de Cybersécurité dans l'Entreprise** contient le programme le plus complet et le plus actualisé du marché.

Après avoir réussi les évaluations, l'étudiant recevra par courrier postal avec accusé de réception le diplôme de **Mastère Spécialisé** délivré par **TECH Université Technologique.**

Le diplôme délivré par **TECH Université Technologique** attestera de la qualification obtenue dans le cadre du Mastère Spécialisé TECH répond aux exigences communément demandées par les bourses d'emploi, les concours et les commissions d'évaluation des carrières professionnelles.

Diplôme: **Mastère Spécialisé en Gestion des Politiques de Cybersécurité dans l'Entreprise**

N.º d'Heures Officielles : **1.500 h.**


tech universidad tecnológica

Otorga la presente

CONSTANCIA

a

C. _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

MÁSTER TÍTULO PROPIO

en

Gestión de Políticas de Ciberseguridad en la Empresa

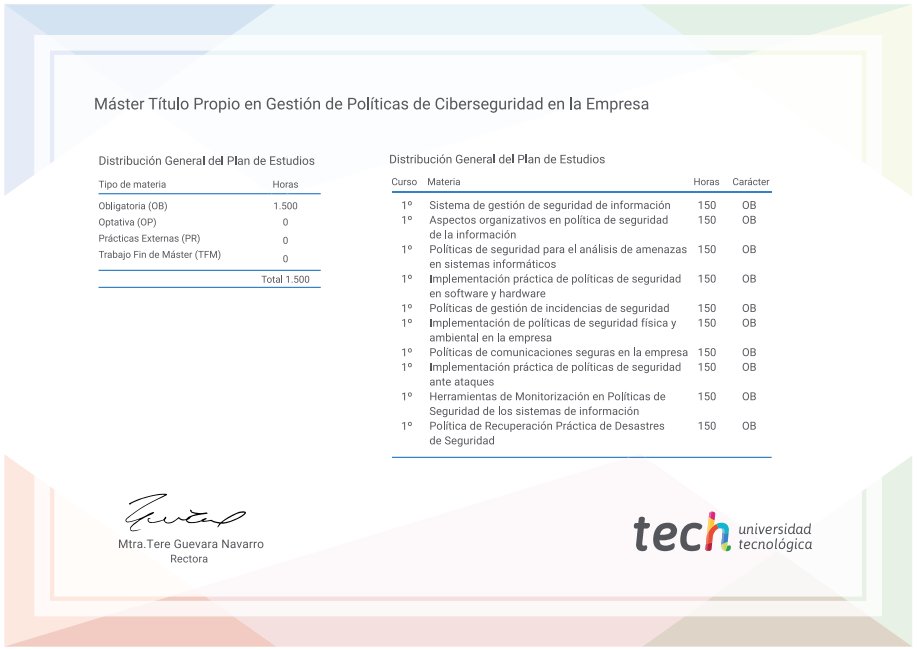
Se trata de un título propio de esta Universidad con una duración de 1.500 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH es una Institución Particular de Educación Superior reconocida por la Secretaría de Educación Pública a partir del 28 de junio de 2018.

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

código único TECH: AFWOR23S techtitute.com/titulos


Máster Título Propio en Gestión de Políticas de Ciberseguridad en la Empresa

Distribución General del Plan de Estudios

Tipo de materia	Horas
Obligatoria (OB)	1.500
Optativa (OP)	0
Prácticas Externas (PR)	0
Trabajo Fin de Máster (TFM)	0
	Total 1.500

Distribución General del Plan de Estudios

Curso	Materia	Horas	Carácter
1º	Sistema de gestión de seguridad de información	150	OB
1º	Aspectos organizativos en política de seguridad de la información	150	OB
1º	Políticas de seguridad para el análisis de amenazas en sistemas informáticos	150	OB
1º	Implementación práctica de políticas de seguridad en software y hardware	150	OB
1º	Políticas de gestión de incidencias de seguridad	150	OB
1º	Implementación de políticas de seguridad física y ambiental en la empresa	150	OB
1º	Políticas de comunicaciones seguras en la empresa	150	OB
1º	Implementación práctica de políticas de seguridad ante ataques	150	OB
1º	Herramientas de Monitorización en Políticas de Seguridad de los sistemas de información	150	OB
1º	Política de Recuperación Práctica de Desastres de Seguridad	150	OB

Mtra.Tere Guevara Navarro
Rectora

tech universidad tecnológica

*Apostille de la Haye Si l'étudiant souhaite que son diplôme version papier celui-ci doit posséder l'Apostille de La Haye, TECH EDUCATION fera les démarches nécessaires pour son obtention moyennant un coût supplémentaire.

tech université technologique

Mastère Spécialisé
Gestion des Politiques de Cybersécurité dans l'Entreprise

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

Mastère Spécialisé

Gestion des Politiques de Cybersécurité dans l'Entreprise

tech université technologique