h e g

Haute école de gestion
Genève

Descriptif de module 63-22

Domaine : Economie & Services
Filière : Informatique de gestion

1. Intitulé de module — Sécurité informatique — 2020-2021

Code :
63-22

Type de formation :
☒ Bachelor ☐ Master ☐ MAS ☐ DAS ☐ CAS ☐ Autres :

Niveau :
☒ Module de base
☐ Module d'approfondissement
☐ Module avancé
☐ Module spécialisé
☐ Autres :

Caractéristique :
☒ Module dont l'échec peut entrainer l'exclusion définitive de la filière selon l'art.15, al.1 des directives cadres "statut des étudiants-e-s"

Type :
☒ Module principal
☐ Module lié au module principal
☐ Module facultatif ou complémentaire
☐ Autres :

Organisation temporelle :
☒ Module sur 1 semestre
☐ Module sur 2 semestres
☐ Semestre d'automne
☒ Semestre de printemps
☐ Autres :

2. Organisation

Crédits ECTS
5

Langue principale d'enseignement :
☒ Français
☐ Allemand
☐ Autres :
☐ Italien
☐ Anglais

3. Prérequis

☐ Avoir validé le module
☐ Avoir suivi le module
☐ Pas de prérequis
☐ Autres :

4. Compétences visées / Objectifs généraux d'apprentissage

À la fin du module l'étudiant-e devra :

- Savoir exposer les principales normes de sécurité
- Pouvoir identifier et répondre aux menaces de sécurité
- Être capable de concevoir et appliquer la sécurité

5. Objectifs détaillés des enseignements

- Acquérir les bases nécessaires à la compréhension des risques encourus par les systèmes d'information
- Connaître les concepts, normes et méthodes liés à la sécurité des SI
- Maîtriser les étapes de la gestion des risques du SI d'entreprise
- Être capable d'élaborer une Politique de Sécurité des Systèmes d'information
- Comprendre et mettre en place une architecture de sécurité autour des concepts tels que les permissions, le chiffrement, les clés publiques, l'Active Directory, les firewalls
- Mettre en œuvre des solutions de sécurité en Linux et Windows, ainsi que pour les serveurs Web

6. Plan et chapitres des cours

- Définition du Système d'information
- Menaces et objectifs de sécurité
- Gestion des risques
- Normes et méthodes
- Sensibilisation
- Plan de Continuité/Reprise des Activités
- Les permissions en Linux et Windows
- La sécurisation des serveurs Web
- Les mots de passe, les *hash functions* et le chiffrement
- Les systèmes des clés publiques
- La sécurisation des serveurs Linux et Windows
- Active Directoy
- Le Social Engineering
- L'anonymat
- Les firewalls et les systèmes de détection d'intrusions

7. Forme du cours et méthodes pédagogiques

Cours en salle de théorie et travail de recherche personnel. Un atelier pour les aspects pratiques.

8. Modalités d'évaluation et de validation

Acquis : A-E
Remédiation : Fx
Répétition : F

L'évaluation du module se fera en principe de la manière suivante :

Contrôle continu : 50%	**Examen : 50%**
1 contrôle continu 90' – coeff 1 1 contrôle continu 60' – coeff 1 1 contrôle continu 120' – coeff 1 1 présentation en groupe – coeff 1	Pas d'examen