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 — 2022-2023

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 les modules 63-12 et 63-13
☐ Pas de prérequis
☐ Autres :

4. Compétences visées / Objectifs généraux d'apprentissage

L'étudiante ou l'étudiant doit être capable, en fin de module, de justifier des compétences professionnelles suivantes :

- Comprendre comment mener une évaluation des risques dans une entreprise.
- Être capable de mettre en place des mesures de sécurité comme les permissions, le chiffrement, les signatures digitales, les firewalls ou l'Active Directory.
- Connaissances des cyber-attaques sur l'Internet.

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.
- Maitriser les étapes de la gestion des risques du SI d'entreprise.
- Être capable d'élaborer une Politique de Sécurité des Systèmes d'Information.
- Comprendre la nature des principales cyber-attaques.
- 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.

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 (PCA / PRA)
- Politique de Sécurité du Système d'Information (PSSI)
- 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 Directory.
- Le Social Engineering
- L'anonymat
- Les firewalls et les systèmes de détection d'intrusions.
- Norme ISO 27xxx, Système de Management de la Sécurité de l'Information
- Norme ISO 22301, - Continuité d'activité
- Méthode d'analyse des risques EBIOS – EBIOS-RM
- Règlement européen RGPD

6. Forme du cours et méthodes pédagogiques

Un cours de deux heures sur la gouvernance de la sécurité a lieu chaque semaine.

Un cours d'une heure sur les techniques de sécurité pour les systèmes d'information a lieu toutes les semaines.

Un laboratoire de 3 heures a lieu chaque semaine. Ce labo permet à l'étudiant de mettre en œuvre des mécanismes de sécurité abordés dans le cours. Notamment, on apprend à sécuriser un serveur Linux et Windows Server, ainsi qu'un serveur Web.

Dans la dernière partie du semestre, l'étudiant.e réalisera un projet de groupe autour de l'analyse des risques dans une entreprise, avec la proposition d'une politique de sécurité et d'une architecture de sécurité.

7. 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 : 100%	**Il n'y a pas d'examen pour ce module**
3 contrôles continus individuels — coefficient 1 chacun 1 projet de groupe — coefficient 1	