

Descriptif de module 63-22

Domaine : Economie & Service
Filière : Informatique de gestion

1. Intitulé de module	Sécurité informatique	2026-2027
Code : 63-22 Niveau : ☐ Module de base ☒ Module d'approfondissement ☐ Module avancé ☐ Module spécialisé ☐ Autres : Type : ☒ Module principal ☐ Module lié au module principal ☐ Module facultatif ou complémentaire ☐ Autres :	Type de formation : ☒ Bachelor ☐ Master ☐ MAS ☐ DAS ☐ CAS ☐ Autres : Caractéristique : ☒ Module dont l'échec peut entraîner l'exclusion définitive de la filière selon l'art.15, al.1 des directives cadres "statut des étudiants-e-s" 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 | ☐ Italien |
| ☐ Allemand | ☒ Anglais |
| ☐ Autres : | |

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

À l'issue du module, l'étudiant-e est capable de :

- Analyser les menaces, vulnérabilités et attaques affectant les systèmes d'information, en tenant compte des dimensions techniques, humaines et organisationnelles.
- Évaluer les risques et impacts d'incidents de sécurité pour une organisation, et justifier des mesures de protection et de défense adaptées.
- Appliquer des techniques de sécurité informatique afin d'identifier des vulnérabilités et de mettre en œuvre des mesures élémentaires de défense dans des environnements contrôlés et encadrés.

5. Objectifs détaillés des enseignements

- Identifier les risques auxquels sont exposés les systèmes d'information et les actifs numériques d'une organisation.
- Décrire les principaux concepts, normes et méthodes mobilisés en sécurité des systèmes d'information.
- Analyser les étapes d'une démarche de gestion des risques appliquée à un système d'information d'entreprise.
- Être capable d'élaborer une Politique de Sécurité des Systèmes d'Information.
- Examiner les composantes d'une politique et d'une architecture de sécurité en mettant en relation les mécanismes de protection (permissions, chiffrement, clés publiques, pare-feu) et les menaces associées.
- Distinguer les principales catégories de cyber-attaques en fonction des vulnérabilités exploitées et des impacts potentiels.
- Mettre en pratique, de manière encadrée, des techniques élémentaires d'attaque et de défense afin d'illustrer les concepts étudiés.

6. Plan et chapitres des cours

- Introduction à la sécurité des systèmes d'information
- Fondements techniques de la sécurité
- Gouvernance et organisation de la sécurité
- Gestion de risques (ISO 27005 – EBIOS – EBIOS-RM – NIST)
- Continuité d'activité
- Politique de Sécurité du SI (PSSI)
- Normes et standards d'un Système de Management de la Sécurité de l'Information (SMSI)
- Facteur humain
- Principes de la cryptographie appliquée
- Sécurité des réseaux
- Attaques par injection et exploitation de vulnérabilités
- Défense et protection des systèmes
- Dimensions éthiques, légales et professionnelles

Dans le cadre du cours, la durabilité est traitée via la résilience des systèmes et l'intégration des dimensions éthiques et professionnelles de la sécurité, assurant des solutions robustes et adaptables à long terme.

7. Forme du cours et méthodes pédagogiques

Le module est dispensé sur un semestre et repose sur une articulation entre enseignements théoriques, enseignements pratiques et apports en gouvernance de la sécurité.

Enseignements théoriques (3h par semaine, sauf semaines 5-10)

Ces enseignements portent sur les fondements techniques de la sécurité informatique, les mécanismes d'attaque et les principes de protection et de défense des systèmes, réseaux et applications

Enseignements liés à la gouvernance de la sécurité (3h par semaine, semaines 5-10)

Ces enseignements abordent les enjeux organisationnels, les risques, les responsabilités et le cadre réglementaire liés à la sécurité des systèmes

Enseignements pratiques (3h par semaine)

Les travaux pratiques et laboratoires sont réalisés en environnement contrôlé. Ils permettent d'expérimenter des situations d'attaque, d'analyser les vulnérabilités observées et de mettre en œuvre des mesures élémentaires de défense en lien avec les enseignements théoriques.

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.

Utilisation de l'IA dans le cadre du module

☒ Dans le cadre du cours

Description : L'utilisation de l'IA est déconseillée, sauf comme outil d'apprentissage et de brainstorming pour clarifier des concepts ou générer des idées.

☒ Dans le cadre des laboratoires

Description : L'utilisation de l'IA est déconseillée, sauf à des fins d'exploration (par exemple, pour comprendre des scénarios d'attaques ou analyser du code).

☒ Dans le cadre des évaluations

Description : Non autorisé. Sauf si explicitement communiqué avec des règles d'utilisation.

8. Modalités d'évaluation et de validation

Présence :

La présence à toutes les activités d'enseignement est obligatoire et constitue une condition de validation du module. Tout absence doit être justifiée au près du secrétariat dans les 48 heures suivant l'absence. Les points bonus sont attribués au CC3 sous condition d'une participation active, avec plus de 90 % des travaux pratiques validés pendant les ateliers.

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

Contrôle continu : 100% CC1 – Sécurité : prévu en principe en semaine 3 – 15% CC2 – Gouvernance : prévu en principe en semaine 10 – 20% CC3 – Sécurité applicative : prévu en principe en semaine 13 – 35% CC4 – Projet de groupe début semaine 10 Rapport en anglais à remettre semaine 14 Présentation orale en anglais semaine 15 — 30%	Il n'y a pas d'examen pour ce module
---	---

Acquis : A-E
Remédiation : Fx
Répétition : F

Remédiation / Fx :

Un module pour lequel l'étudiant-e obtiendrait une note entre 3.5 et 3.9 peut faire l'objet d'une remédiation, conformément à l'art. 29 al. 1 du Règlement sur la Formation de base en HES-SO.

Si la remédiation est validée la note de 4 sera attribuée.

Si la remédiation n'est pas validée le module sera répété.

Répétition / F :

Un module pour lequel l'étudiant-e obtiendrait une note inférieure ou égale à 3.4 doit être répété.

L'étudiant-e qui n'obtient pas les crédits attribués à un module doit le répéter dès que possible, conformément à l'art. 30 al. 1 du Règlement sur la formation de base en HES-SO.