Université de Sherbrooke

Centre de formation en technologie de l'information

INF 801 – Concepts de base de la sécurité en TI

Plan d'activité pédagogique

Hiver 2026

Enseignants	Aboudoulaye Fofana	Dominic Brodeur
Courriel :	aboudoulaye.fofana@usherbrooke.ca	dominic.brodeur@usherbrooke.ca
Local :		
Téléphone :		+1 514 205-5131
Disponibilités :	Enseignant : Dominic Brodeur : Délai de 3 jours pour répondre aux courriels Chargé d'exercice / laboratoire : Jim Morrison Lafrenière : Délai de 3 jours pour répondre aux courriels	

Site web du cours : https ://moodle.usherbrooke.ca

Horaire Exposé magistral : Mardi 18 h 30 à 21 h 50 salle Réunion Microsoft Teams

Description officielle de l'activité pédagogique[1]

Cibles de formation :	Comprendre les fondements de la sécurité informatique, dont la cryptologie, la cybersécurité et l'authentification. Comprendre et maîtriser les technologies de la sécurité.
Contenu :	La sécurité en TI aujourd'hui ; sécurisation de la base avant les attaques trop avancées ; analyse et gestion de la sécurité et du risque ; authentification. Sécurité dans le développement logiciel, sensibilisation à l'hameçonnage et à l'ingénierie sociale téléphonique ; notions de système d'exploitation et de réseau ; les vulnérabilités et les menaces communes, les attaques communes, les bonnes pratiques de base pour l'authentification, la segmentation réseau ; introduction à la cryptographie ; sécurité des mobiles ; sécurité dans l'approche « prenez vos appareils personnels » (PAP) (bring your own device) ; sécurité des systèmes opérationnels (OT) ; sécurité des systèmes de contrôle industriels (ICS) ; modélisation de menaces.
Crédits	3
Organisation	3 heures d'exposé magistral par semaine 6 heures de travail personnel par semaine
Particularités	Aucune

[1] https ://www.usherbrooke.ca/admission/fiches-cours/inf801

1 Présentation

Cette section présente les cibles de formation spécifiques et le contenu détaillé de l'activité pédagogique. Cette section, non modifiable sans l'approbation du comité de programme du Centre de formation en technologie de l'information, constitue la version officielle.

1.1 Mise en contexte

1.2 Cibles de formation spécifiques

Le Microprogramme en sécurité informatique - volet prévention permet à l'étudiante ou à l'étudiant de :

- maîtriser les tenants et aboutissants de la sécurité informatique contemporaine ;
- maîtriser la nature des surfaces d'attaque exposées par une infrastructure de TI ;
- savoir concevoir, mettre en œuvre et documenter une stratégie efficace pour protéger et défendre ces surfaces d'attaque, en tenant compte d'un budget de ressources donné ;
- pouvoir critiquer une telle stratégie telle que mise en place dans une organisation, de manière à en corriger les faiblesses.

1.3 Contenu détaillé

Thème	Contenu	Nbr. d'heures	Objectifs
1	Séance 1 : Introduction à la cybersécurité : • Présentation du cours • Sécurité – sécurité de l'information –cybersécurité • Dépendance technologique • État actuel de la cybersécurité	3	
2	Séance 2 : Concepts de base en cybersécurité : • Par où commencer ? • Modèles • Agent de menace • Actif informationnel • Classification des actifs • Sécurité physique, logique • Veille Quiz Séance 1 et 2	3	
3	Séance 3 : Vulnérabilités et menaces communes : • Impacts des brèches de sécurité • Type d'attaques • Types de menaces • Vulnérabilités les plus communes • Comment se protéger, périmètre • Défense active Quiz Séance 3	3	
4	Séance 4 : Aspects humains : • Sensibilisation • Piratage psychologique • Facteurs de motivation Quiz Séance 4	3	

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs
5	Séance 5 : Modélisation des menaces : • Différence méthode de modélisation • Analyse comportementale • Gestion des événements de sécurité de l'information • Pattern d'attaque • Cycle de vie d'une attaque • Types de contrôles • Un exemple réel Quiz Séance 5	3	
6	Séance 6 : Cryptologie : • Historique • Principes • Algorithmes classiques • Protocoles • Informatique quantique Quiz Séance 6	3	
7	Séance 7 : Analyse et gestion du risque de cybersécurité : • Gouvernance en gestion de la sécurité • Processus de gestion de la sécurité • Modèle de gestion du risque • Investissements en sécurité, ROSI Quiz Séance 7	3	
8	Séance 8 : Notions de base pour les systèmes d'exploitation et les réseaux : EXAMEN INTRA, séance 1 à 7 • Couches logicielles • Architecture de variantes populaires (Android, iOS, Linux, MacOS, Windows) • Couches OSI • Protocole TCP/IP • Composants d'un réseau	3	
9	Séance 9 : Gestion des identités et des accès : • Processus / cycle de vie • Sécurité en profondeur • Gestion des accès modèle cloud et vue holistique, Chaîne de confiance • IAAA • Biométrie, MFA • Contrôles d'accès • Les modèles de gestion des accès • Vulnérabilités et types d'attaque	3	
10	Séance 10 : Sécurité des appareils mobiles : • Sécurité physique • Authentification • BYOD Quiz Séance 9	3	
11	Séance 11 : Protection des systèmes : • Architecture entreprise • Modélisation réseau • Segmentation de réseau • Durcissement d'un système • Pare-feu • Sécurité en profondeur • Architecture cloud IaaS, PaaS, SaaS • Sécurité avant et après le Cloud • CASB Courtiers de sécurité d'accès au nuage • Menaces et contrôle de l'environnement cloud Remise Laboratoire en ligne de CrypTool Quiz Séance 10	3	

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs
12	Séance 12 : Sécurité dans le développement logiciel : • Cycle de vie de développement d'un logiciel • Définition des besoins et exigences en sécurité • Analyse des exigences • Architecture de sécurité • Développement sécuritaire • Tests • Mises à jour • Retour sur OWASP top 10 Quiz Séance 11	3	
13	Séance 13 : Technologies émergentes : • Systèmes opérationnels • Appareils intelligents, assistant vocal • Internet des objets • Intelligence artificielle Quiz Séance 12	3	
14	Séance 14 : Infrastructures nationales critiques : • Définition • Systèmes de type SCADA • Systèmes en grille • Mesures gouvernementales Quiz Séance 13	3	
15	Séance 15 : Examen final : Examen final sur Moodle	3	

2 Organisation

Cette section propre à l'approche pédagogique de chaque enseignante ou enseignant présente la méthode pédagogique, le calendrier, le barème et la procédure d'évaluation ainsi que l'échéancier des travaux. Cette section doit être cohérente avec le contenu de la section précédente.

2.1 Méthode pédagogique

Les 3 crédits équivalent à 135 heures, soit 45 heures de rencontres collectives et 90 heures de travail personnel, réparties de la façon suivante : (distinguer le temps de lecture personnelle, le temps de travail sur le site, le temps de réalisation des travaux, etc.)

Enseignement magistral	39 heures
Laboratoire	6 heures
Lecture personnelle	45 heures
Activités de consolidation	45 heures
TOTAL	135 heures

2.2 Calendrier

Date	Thème	
2026-01-06	1	• Présentation du cours • Sécurité – sécurité de l'information – cybersécurité • Dépendance technologique • État actuel de la cybersécurité
2026-01-13	2	• Par où commencer ? • Modèles • Agent de menace • Actif informationnel • Classification des actifs • Sécurité physique, logique • Veille Quiz Séance 1 et 2
2026-01-20	3	• Impacts des brèches de sécurité • Type d'attaques • Types de menaces • Vulnérabilités les plus communes • Comment se protéger, périmètre • Défense active Quiz Séance 3
2026-01-27	4	• Sensibilisation • Piratage psychologique • Facteurs de motivation Quiz Séance 4

Table 2 :

Date	Thème	
2026-02-03	5	• Différence méthode de modélisation • Analyse comportementale • Gestion des événements de sécurité de l'information • Pattern d'attaque • Cycle de vie d'une attaque • Types de contrôles • Un exemple réel Quiz Séance 5
2026-02-10	6	• Historique • Principes • Algorithmes classiques • Protocoles • Informatique quantique Quiz Séance 6
2026-02-17	7	• Gouvernance en gestion de la sécurité • Processus de gestion de la sécurité • Modèle de gestion du risque • Investissements en sécurité, ROSI Quiz Séance 7
2026-02-24	8	**EXAMEN INTRA, séance 1 à 7** • Couches logicielles • Architecture de variantes populaires (Android, iOS, Linux, MacOS, Windows) • Couches OSI • Protocole TCP/IP • Composants d'un réseau
2026-03-03	Relâche	
2026-03-10	9	• Processus / cycle de vie • Sécurité en profondeur • Gestion des accès modèle cloud et vue holistique, Chaîne de confiance • IAAA • Biométrie, MFA • Contrôles d'accès • Les modèles de gestion des accès • Vulnérabilités et types d'attaque
2026-03-17	10	• Sécurité physique • Authentification • BYOD Quiz Séance 9

Table 2 :

Date	Thème	
2026-03-24	11	• Architecture entreprise • Modélisation réseau • Segmentation de réseau • Durcissement d'un système • Pare-feu • Sécurité en profondeur • Architecture cloud IaaS, PaaS, SaaS • Sécurité avant et après le Cloud • CASB Courtiers de sécurité d'accès au nuage • Menaces et contrôle de l'environnement cloud Remise Laboratoire en ligne de CrypTool Quiz Séance 10
2026-03-31	12	• Cycle de vie de développement d'un logiciel • Définition des besoins et exigences en sécurité • Analyse des exigences • Architecture de sécurité • Développement sécuritaire • Tests • Mises à jour • Retour sur OWASP top 10 Quiz Séance 11
2026-04-07	13	• Systèmes opérationnels • Appareils intelligents, assistant vocal • Internet des objets • Intelligence artificielle Quiz Séance 12
2026-04-14	14	• Définition • Systèmes de type SCADA • Systèmes en grille • Mesures gouvernementales Quiz Séance 13
2026-04-21	Semaine des examens finals	
2026-04-28	Semaine des examens finals	

2.3 Évaluation

Type de l'évaluation	Pondération	Utilisation des IAG[1]
11 quiz (les 10 meilleurs) de 3 points chacun	30 %	Interdite
Laboratoire en ligne de CrypTool (15%)	15 %	Interdite
Examen intra	20 %	Interdite
Examen final	35 %	Interdite

[1] Référez-vous à la page "Balises d'utilisation des outils d'intelligence artificielle générative" à la fin du document.

11 quiz de 3 pts chacun seront distribués suite à chaque séance (presque chaque séance). Les quiz sont de 15 mins chacun et comportent 3 questions à choix multiple. Les étudiants auront 5 jours pour les faire chacun. Aucune possibilité de reprise de quiz possible. Les 10 meilleurs quiz vont compter sur les 10 pour un total de 30 points sur la note finale.

2.3.1 Qualité de la langue et de la présentation

Conformément à l'article 17 du Règlement facultaire d'évaluations des apprentissages[2] l'enseignante ou l'enseignant peut retourner à l'étudiante ou à l'étudiant tout travail non conforme aux exigences quant à la qualité de la langue et aux normes de présentation.

2.3.2 Plagiat

Le plagiat consiste à utiliser des résultats obtenus par d'autres personnes afin de les faire passer pour sien et dans le dessein de tromper l'enseignante ou l'enseignant. Vous trouverez en annexe un document d'information relatif à l'intégrité intellectuelle qui fait état de l'article 9.4.1 du Règlement des études[3]. Lors de la correction de tout travail individuel ou de groupe une attention spéciale sera portée au plagiat. Si une preuve de plagiat est attestée, elle sera traitée en conformité, entre autres, avec l'article 9.4.1 du Règlement des études de l'Université de Sherbrooke. L'étudiante ou l'étudiant peut s'exposer à de graves sanctions qui peuvent être soit l'attribution de la note E ou de la note zéro (0) pour un travail, un examen ou une activité évaluée, soit de reprendre un travail, un examen ou une activité pédagogique. Tout travail suspecté de plagiat sera transmis au Secrétaire de la Faculté des sciences. Ceci n'indique pas que vous n'ayez pas le droit de coopérer entre deux équipes, tant que la rédaction finale des documents et la création du programme restent le fait de votre équipe. En cas de doute de plagiat, l'enseignante ou l'enseignant peut demander à l'équipe d'expliquer les notions ou le fonctionnement du code qu'elle ou qu'il considère comme étant plagié. En cas d'incertitude, ne pas hésiter à demander conseil et assistance à l'enseignante ou l'enseignant afin d'éviter toute situation délicate par la suite.

2.4 Échéancier des travaux

Laboratoire en ligne de CrypTool

Travail individuel

Compétence mobilisée : Comprendre les fondements de la sécurité informatique (C1), dont la cryptologie (C2)

Description : Réaliser différents essais en cryptographie pour ensuite rapporter le résultat de ces observations.

Critères d'évaluation : Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle, une section sera prévue pour présenter le travail à faire et la grille d'évaluation.

[2] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/2017-10-27_Reglement_facultaire_-_evaluation_des_apprentissages.pdf

[3] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

2.5 Utilisation d'appareils électroniques et du courriel

Selon le règlement complémentaire des études, section 4.2.3 [4], l'utilisation d'ordinateurs, de cellulaires ou de tablettes pendant une prestation est interdite à condition que leur usage soit explicitement permise dans le plan de cours.

Dans ce cours, l'usage de téléphones cellulaires, de tablettes ou d'ordinateurs est autorisé. Cette permission peut être retirée en tout temps si leur usage entraîne des abus.

Tel qu'indiqué dans le règlement universitaire des études, section 4.2.3[5], toute utilisation d'appareils de captation de la voix ou de l'image exige la permission de la personne enseignante.

Note : Je réponds aux questions posées par courriel à l'extérieur des périodes de cours.

3 Matériel nécessaire pour l'activité pédagogique

Obligatoire

Fernando Maymi & Shon Harris, CISSP All-in-One Exam Guide, 9th edition, McGraw Hill Education, Dec 2021.

[4] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/Sciences_Reglement_complementaire.pdf

[5] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

Faculté des sciences UdS

Délits relatifs aux études

Extrait du règlement des études (Règlement 2575-009)

Sont notamment considérés comme un délit relatif aux études les faits suivants :

a) commettre un plagiat, soit faire passer ou tenter de faire passer pour sien, dans une production évaluée, le travail d'une autre personne, des passages ou idées tirés de l'œuvre d'autrui ou du contenu, de toute forme, généré par un système d'intelligence artificielle (ce qui inclut notamment le fait de ne pas indiquer la source et la référence adéquate);
b) commettre un autoplagiat, soit soumettre, sans autorisation préalable, une même production, en tout ou en partie, à plus d'une activité pédagogique ou dans une même activité pédagogique (notamment en cas de reprise);
c) usurper l'identité d'une autre personne ou procéder à une substitution de personne lors d'une production évaluée ou de toute autre prestation obligatoire;
d) fournir ou obtenir toute forme d'aide non autorisée, qu'elle soit collective ou individuelle (incluant l'assistance provenant d'un système d'intelligence artificielle), pour une production faisant l'objet d'une évaluation;
e) obtenir par vol ou toute autre manœuvre frauduleuse, posséder ou utiliser du matériel non autorisé de toute forme (incluant le matériel numérique et celui généré par un système d'intelligence artificielle) avant ou pendant une production faisant l'objet d'une évaluation;
f) copier, contrefaire ou falsifier un document pour l'évaluation d'une activité pédagogique;
k) posséder ou avoir à sa portée un appareil électronique ou numérique interdit durant une activité d'évaluation;

[...]

Un guide sur l'intégrité intellectuelle vous est rendu disponible par le service des bibliothèques et des archives de l'Université de Sherbrooke, afin de bien comprendre les différents délits et ainsi éviter d'être aux prises avec un dossier disciplinaire et une ou des sanctions.

Les mesures pouvant être imposées à titre de sanctions disciplinaires sont les suivantes :

a) la réprimande simple ou sévère consignée au dossier étudiant pour la période fixée par l'autorité disciplinaire ou à défaut, définitivement. En cas de réprimande fixée pour une période déterminée, la décision rendue demeure au dossier de la personne aux seules fins d'attester de l'existence du délit en cas de récidive;
b) l'obligation de reprendre une production ou une activité pédagogique, dont la note pourra être établie en tenant compte du délit survenu antérieurement;
c) la diminution de la note ou l'attribution de la note E ou 0;

[...]

UDS Faculté des sciences

Balises d'utilisation des outils d'intelligence artificielle générative

Autorisés ou pas dans les situations d'apprentissage et d'évaluation ?

NIVEAU 0	NIVEAU 1	NIVEAU 2	NIVEAU 3	NIVEAU 4
L'utilisation des outils d'intelligence artificielle générative (IAg) est limitée, voire complètement interdite parce que la personne enseignante considère que l'usage de ces outils nuit au développement de compétences essentielles. Ces compétences peuvent être disciplinaires, comme elles peuvent être d'ordre méthodologique, rédactionnel ou informationnel. Considérant que l'utilisation des IAg requiert un esprit critique, il peut s'agir d'une situation d'apprentissage ou d'évaluation sans IAg qui vise à développer celui-ci. Dans ces situations, **la personne étudiante produit le travail**.			L'utilisation prononcée des IAg est permise parce que la personne enseignante considère que les personnes étudiantes sont en mesure d'exercer un esprit critique et sont capables de juger de la qualité des contenus produits par les IAg. Ou encore, l'utilisation est encouragée parce que la situation d'apprentissage ou d'évaluation proposée contribue à développer leur esprit critique. Dans ces situations, l'IAg produit le travail préliminaire, alors que **la personne étudiante s'assure de sa qualité en l'améliorant**.	
				
Utilisation interdite	**Utilisation limitée**	**Utilisation guidée**	**Utilisation balisée**	**Utilisation libre**
Le **NIVEAU 0** signifie que l'**utilisation est interdite**. Ceci signifie que si la personne enseignante a un motif de croire qu'il y a eu l'utilisation d'une IAg dans une situation d'évaluation, elle doit dénoncer les faits auprès de la personne responsable des dossiers disciplinaires universitaires. Il s'agit d'un délit relatif aux études tel que stipulé dans le Règlement des études.	Le **NIVEAU 1 D'UTILISATION** signifie que l'**utilisation est autorisée uniquement pour assister l'apprentissage dans le domaine disciplinaire ou des langues**. Dans ce contexte, la personne étudiante **est tenue de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation peut être considérée comme un délit. Par exemple : Domaine disciplinaire : - S'inspirer - Générer des idées - Explorer un sujet pour mieux le comprendre - Générer du matériel pour apprendre Domaine des langues : - Identifier ses erreurs et se les faire expliquer - Reformuler un texte - Générer un plan pour aider à structurer un texte - Traduire un texte	Le **NIVEAU 2 D'UTILISATION** signifie que l'**utilisation est autorisée pour améliorer un travail produit par la personne étudiante**. Dans ce contexte, la personne étudiante **est tenue de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Par exemple : - Analyser des contenus - Obtenir une rétroaction - Évaluer la qualité de son travail à partir de critères - Demander à être confronté relativement à ses idées, à sa démarche - Diriger les processus de résolution de problèmes	Le **NIVEAU 3 D'UTILISATION** signifie que l'**utilisation est autorisée pour produire un travail qui sera amélioré.** Dans ce contexte, la personne étudiante **est tenue de citer selon les normes[1] le contenu généré par l'IAg** ou **de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Par exemple : - Résumer ou rédiger des parties d'un texte - Générer un texte ou un modèle d'une production et l'adapter - Réaliser des calculs mathématiques - Produire du code informatique - Résoudre des problèmes complexes - Répondre à une question - Générer des images, ou autres contenus multimédias	Le **NIVEAU 4 D'UTILISATION** signifie qu'**aucune restriction spécifique n'est imposée**. Dans ce contexte, la personne étudiante **est tenue de citer selon les normes[1] le contenu généré par l'IAg** ou **de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Ce niveau inclut tout ce qui précède, de l'exploration à la production, ainsi que toute autre tâche particulière jugée complexe.

UDS Faculté des sciences

À considérer avant l'utilisation d'outils d'intelligence artificielles génératives

Si, en tant que personne étudiante envisagez d'utiliser un outil d'intelligence artificielle générative (IAG) lorsque l'évaluation autorise les niveaux 1 à 4 d'utilisation mentionnés précédemment.

Dans ce cas, gardez à l'esprit les éléments clés suivants.

- Vous assumez la responsabilité de tout le contenu produit, avec ou sans IAG, et intégré à votre production.
- Les produits des outils d'IAG peuvent très souvent comporter **des erreurs ou des faussetés** (hallucinations) : on doit donc impérativement valider tout contenu généré par ces outils.
- Dans l'état actuel de la Loi sur le droit d'auteur du Canada, les **productions faites par l'IAG sont du domaine public,** puisque les outils d'IAG ne sont pas reconnus comme des auteurs au sens de la Loi et que les contenus générés ne répondent pas aux critères d'une œuvre protégée, notamment aux critères d'originalité.
- L'entreprise qui fournit le service pourrait émettre certaines exigences dans ses conditions d'utilisation. Comme l'algorithme et le code informatique appartiennent à l'entreprise qui les a développés, nous devons tenir compte de ces conditions. Celles-ci pourraient également fournir des précisions relatives à la **réutilisation des données soumises (confidentialité)**.

Comment déclarer l'utilisation d'outils d'intelligence artificielle générative

Dans l'esprit d'une conduite intègre et responsable, vous devez TOUJOURS mentionner de façon explicite toute utilisation de l'intelligence artificielle, conformément au Règlement des études (9.4.1 Délits relatifs aux études). De plus, à des fins pédagogiques, il est recommandé de toujours intégrer à la production les requêtes, de même que les réponses intégrales générées par les outils d'IAG. Celles-ci pourront être intégrées directement dans le corps du texte ou en note de bas de page. Les réponses longues pourraient être insérées en annexe de votre document ou dans des documents supplémentaires, selon les directives de la personne enseignante.

L'utilisation de ces deux documents s'avèrera utile, ils se trouvent sous licence libre, donc vous pouvez utiliser les tableaux et les adapter selon votre besoin:

1. Modèle de citation : Ce formulaire, à remplir par l'enseignant, donne un exemple aux étudiants de citation de l'IAg dans la réalisation d'un travail évalué ou non.
2. Déclaration d'usage : Ce formulaire, à remplir par les étudiants, doit être remis avec une réalisation afin de déclarer l'usage de l'IAg dans la réalisation, qu'elle soit évaluée ou non.

Référence

La Faculté des sciences tient à remercier le SSF pour la production des documents.

- Cabana, M. et Côté, J.-A. (2024). Balises d'utilisation des outils d'intelligence artificielle générative. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.
- Cabana, M. et Beaudet, M. (2024). Directives de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.
- Cabana, M. (2024). Formulaire de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.