UNIVERSITÉ DE SHERBROOKE

1. IDENTIFICATION ET RENSEIGNEMENTS GÉNÉRAUX

Titre officiel du cours :	**INF804 – Sécurité des logiciels**
Nombre de crédits :	3 crédits – 135 heures
Programme :	Microprogramme de 2e cycle en sécurité informatique - volet prévention
Cours préalables ou concomitants :	INF801
Lieu du cours :	Moodle
Session :	hiver 2020
Date de début :	8 janvier 2020
Date de fin :	15 avril 2020
Date limite d'abandon :	21 janvier 2020 (sans frais) 15 mars 2020
Rencontres synchrones :	Tous les mercredis, de 18h00 à 21h00
Personne(s)-ressource(s) :	Michel Hébert *michel.hebert3@usherbrooke.ca* Pierre-Martin Tardif *pierre-martin.tardif@usherbrooke.ca*

2. MISE EN CONTEXTE

DESCRIPTION OFFICIELLE DU COURS

Cible(s) de formation :

Ce cours est composé de deux volets complémentaires. Le premier volet se concentre sur la sécurité des données avec les objectifs de compétence suivants :

D1 : Justifier la sécurité des données
D2 : Expliquer l'interaction entre la gouvernance et la sécurité des données
D3 : Décrire les rôles et les tâches liés à la sécurité des données
D4 : Établir une démarche pour la mise en place de la sécurité de données
D5 : Caractériser les outils et techniques utilisées dans la sécurité des données.

Le second volet vise la sécurité informatique dans les activités de développement de logiciel. Les objectifs de compétence de ce volet sont :

L1 : Comprendre le cycle de vie de développement sécuritaire.
L2 : Comprendre la sécurité applicative et les concepts de base qui s'y rapportent.

Contenu :

Pour le volet sur les données :

Définition du vocabulaire concernant la gestion des données ; motivation d'affaires et exigences légales de la sécurité des données ; arrimage entre la gouvernance et la sécurité des données ; contexte de la sécurité des données ; exigences, principes, politiques et standards de la sécurité des données ; gestion des autorisations aux données et surveillance des accès ; étapes de mise en place de la sécurité des données ; chiffrement et anonymisation des données

Pour le volet sur le développement logiciel :

Programmation sécuritaire. Les tests de pénétration. Le contrôle des accès. La sécurité sur mobile: analyses d'applications iOS et Android.

UNIVERSITÉ DE SHERBROOKE

PLACE DU COURS DANS LE PROGRAMME

INF804 est un cours à option dans le programme. Il présente la sécurité informatique dans la perspective du développement logiciel et des données.

OBJECTIFS DU MICROPROGRAMME[1]

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.

CHARGE DE TRAVAIL

Les 3 crédits équivalent à 135 heures, soit 45 heures de rencontres collectives et 90 heures de travail personnel, réparties de la façon suivante :

Enseignement magistral	37 heures
Laboratoires en classe	6 heures
Conférences	2 heures
Lecture personnelle	45 heures
Activités de consolidation	45 heures
TOTAL	**135 heures**

3. DÉROULEMENT DU COURS

Séance	Description	Enseignant
Séance 1 : *8 janvier 2020* (D1, D2)	• Présentation du plan de cours • Les impacts du manque de sécurité dans les données • Le vocabulaire de la sécurité des données • La définition de la gouvernance des données	MH

[1] Extrait de la fiche signalétique

Séance	Description	Enseignant
Séance 2 : *15 janvier 2020* (D2)	• Le lien entre la gouvernance des données et leur sécurité • Les dimensions de la gestion des données • L'importance des métadonnées • Principes en information généralement reconnus (GAIP)	MH
Séance 3 : *22 janvier 2020* (D2, D3)	• Triangle C-I-D • Principes de sécurité • Sécurité des données dans leur cycle • Les fuites de données	MH
Séance 4 : *29 janvier 2020* (D4, D5)	• Définition d'un programme de sécurité des données • Politiques et directives	MH
Séance 5 : *5 février 2020* (D4, D5)	• Mise en place d'un programme de sécurité • Gestion du risque sur les données	MH
Séance 6 : *12 février 2020* (D5)	• Contrôles de sécurité des données proposés par ISO 27002	MH
Séance 7: *19 février 2020* (D1, D2, D3, D4 et D5)	• Chiffrement des données au repos, en mouvement et à l'utilisation • Anonymisation des données • Synthèse sur la sécurité des données	MH
Examen intra *Du 20 février 2020 au 25 février 2020*	• Portant sur le volet Données • Fait sur Moodle	
Séance 8 : *26 février 2020* (L1)	• Concepts : données, code, objet, module, librairie, composant, service, programme • Notions de système d'information, de fabrique de logiciels, de compilateur, d'interpréteur, de complexité, de qualité et de sécurité • Retour sur le cycle de développement de système : étapes, efforts	PMT

UNIVERSITÉ DE SHERBROOKE

Séance	Description	Enseignant
Séance 9 : *4 mars 2020* (L1)	• La gouvernance du développement logiciel ○ Les structures décisionnelles ○ La surveillance et les indicateurs clés de performance ○ L'équilibre entre la confiance et le contrôle ○ L'importance de la gestion des risques ○ L'orientation client • Retour sur les cadres sécuritaires • Présentation du laboratoire sur Juice Shop d'OWASP	PMT
Séance 10 : *22 mars 2020* (L1)	• Les besoins et exigences en sécurité • Traçabilité • Critères de priorisation • Équilibrage des besoins et contraintes • Gestion des environnements • ISO 25001 et ISO 27034	PMT
Séance 11 : *18 mars 2020* (L2)	• Environnement de développement sous Windows ○ Langages disponibles ○ Appels systèmes ○ Cryptologie ○ Durée de vie ○ Authentification	PMT
Séance 12 : *25 mars 2020* (L2)	• Environnement de développement sous Linux / Android / MacOS / iOS ○ Langages disponibles ○ Appels systèmes ○ Cryptologie ○ Durée de vie • Journalisation	PMT
Séance 13 : *1er avril 2020* (L2)	• Conférence sur la sécurité liée à l'utilisation des conteneurs de déploiement	PMT + conférencier

Séance	Description	Enseignant
Séance 14 : *8 avril 2020* (L1 et L2)	• Environnement de développement Web • Présentation des étudiants sur Juice Shop	PMT
Séance 15 : examen final *Du 15 avril 2020 au 21 avril 2020*	• Portant sur le volet Développement • Fait sur Moodle	

4. CONSIDÉRATIONS MÉTHODOLOGIQUES

APPROCHES MÉTHODOLOGIQUE ET PÉDAGOGIQUE

Le cours INF804 privilégie une diversité de méthodes pédagogiques, dont la pratique réflexive, les groupes de discussion, l'apprentissage par problèmes, la méthode des cas et l'apprentissage par projet. Il est attendu que chaque individu participant au cours s'engage de manière active et régulière en intervenant dans les séances AdobeConnect et les forums de discussion.

Puisqu'il s'agit d'un cours en ligne, toutes les ressources et les consignes sont disponibles sur Moodle 2: http://www.usherbrooke.ca/moodle2-cours/.

5. ÉVALUATION DES APPRENTISSAGES

ÉVALUATION N^{O} 1: **QUIZ**

- ***Compétence mobilisée:*** Ensemble de toutes les compétences.
- ***Description:*** Sous la forme d'un quiz sur Moodle, contenant de 2 à 4 questions à choix multiples. Chaque quiz sera disponible dans les 24 heures suivant la séance de cours.
- ***Critères d'évaluation*** Choix de la bonne réponse donne les points, 0 autrement.
- ***Notation:*** Maximum de 13 quiz, chacun évalué sur 100%, dont la somme sera rapportée sur 20% de la note finale.
- ***Date de remise:*** Doivent être complétées avant le début de la séance suivante.

ÉVALUATION N^{O} 2: **ÉTUDE DE CAS SUR LA SÉCURITÉ DES DONNÉES.**

- ***Compétence mobilisée:***
  D3 : Décrire les rôles et les tâches liés à la sécurité des données
  D4 : Établir une démarche pour la mise en place de la sécurité de données
  D5 : Caractériser les outils et techniques utilisées dans la sécurité des données.
- ***Description:*** À partir d'un cas fictif fourni par le chargé de cours, décrire un plan de mise en place d'amélioration de la sécurité des données.
- ***Critères d'évaluation*** *Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle 2.*
- ***Notation:*** 25%
- ***Date de remise:*** Au plus tard le 25 février 2020, 23h59

ÉVALUATION N^{O} 3: **EXAMEN INTRA**

- ***Compétence mobilisée:*** L'ensemble des compétences du volet données
- ***Description:*** Sous la forme d'un quiz contenant de questions à choix multiples et à développement, démontrer la compréhension de la matière vue dans le cours. Il s'agit d'un examen de deux heures à faire sur la plateforme Moodle.
- ***Critères d'évaluation*** *Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle 2.*

  Parmi les critères :

  - Justesse et complétude de la réponse
  - Richesse des éléments fournis
- ***Notation:*** 15%
- ***Date de remise:*** *À faire sur Moodle individuellement, entre le 20 février et le 25 février 2020*

ÉVALUATION N^{O} 4: **Laboratoire d'exploration sur Juice Shop d'OWASP**

- ***Compétence mobilisée:*** L2 - Comprendre la sécurité applicative et les concepts de base qui s'y rapportent
- ***Description:*** Ce laboratoire est réalisé par l'étudiant d'une façon autonome. Il comporte une présentation finale en classe lors de la séance 14.
- ***Critères d'évaluation*** *Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle 2.*
- ***Notation:*** Rapport écrit – 20%, présentation – 5% pour un total de 25% de la note finale
- ***Date de remise:*** Rapport écrit – 1er avril 2020, présentation – 8 avril 2020

ÉVALUATION N^{O} 4: **EXAMEN FINAL**

- ***Compétence mobilisée:*** L'ensemble des compétences du volet développement logiciel
- ***Description:*** Sous la forme d'un quiz contenant de questions à choix multiples et à développement, démontrer la compréhension de la matière vue dans le cours. Il s'agit d'un examen de trois heures à faire sur la plateforme Moodle.
- ***Critères d'évaluation*** *Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle 2.*

  Parmi les critères :

  - Justesse et complétude de la réponse
  - Richesse des éléments fournis
- ***Notation:*** 15%
- ***Date de remise:*** *Du 16 avril 2020 au 21 avril 2020*

6. RÈGLEMENTS ET AUTRES

PROMOTION DE LA QUALITÉ DE LA LANGUE

Pour promouvoir la qualité du français, les fautes d'orthographe, de lexique et de syntaxe sont prises en considération. Dans tous les travaux, elles seront comptabilisées comme suit : 0,25 pour chaque faute jusqu'à concurrence de 10% de la note maximale pour chaque objet d'évaluation.

Vous êtes fortement encouragés à effectuer une relecture attentive des travaux avant leur remise officielle et à utiliser les outils de correction disponibles.

PRÉSENTATION DES TRAVAUX

Les travaux doivent obligatoirement être soumis sur le site Moodle 2 du cours à la date d'échéance prévue.

Les fichiers électroniques doivent obligatoirement être soumis en format PDF pour faciliter l'insertion de commentaires.

L'intitulé du fichier doit comprendre le numéro du travail, votre nom et votre prénom (exemple pour le travail 1 : *Travail1_Nom_Prénom.docx*).

UNIVERSITÉ DE SHERBROOKE

DÉLITS RELATIFS AUX ÉTUDES[2]

Le terme « délit » désigne toute infraction ou toute tentative de commettre une infraction, ainsi que toute participation à une infraction ou à une tentative de commettre une infraction, par une personne assujettie à une règle qui lui est applicable en raison de son statut.

Outre la contravention à toute règle applicable à la personne assujettie en vertu d'une source autre que le Règlement des études (Règlement 2575-009), l'Université considère trois (3) types de délits : les délits relatifs aux études, les délits relatifs à l'Université ou aux membres de la communauté universitaire et les délits relatifs aux activités de stage. Ces délits sont présentés aux articles suivants :

Un délit relatif aux études désigne tout acte trompeur ou toute tentative de commettre un tel acte, quant au rendement scolaire ou une exigence relative à une activité pédagogique, à un programme d'études ou à un parcours libre. 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 ou des passages ou idées tirés de l'œuvre d'autrui (ce qui inclut notamment le fait de ne pas indiquer la source d'une production, d'un passage ou d'une idée tirés de l'œuvre d'autrui);
b) commettre un auto-plagiat, 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 aide non autorisée, qu'elle soit collective ou individuelle, pour une production faisant l'objet d'une évaluation;
e) copier, contrefaire ou falsifier un document pour l'évaluation d'une activité pédagogique.

RESPECT DES DÉLAIS[3]

Tout défaut de remplir les exigences d'évaluation prévues au plan de l'activité pédagogique, par exemple pour une production attendue ou un examen, entraîne la **valeur zéro (0)**, à moins que les raisons et les preuves fournies par l'étudiante ou l'étudiant n'aient été acceptées par la faculté ou le centre universitaire de formation.

[2] Extrait du Règlement des études 2017-2018

[3] Extrait du Règlement des études 2017-2018

L'étudiante ou l'étudiant doit **justifier par écrit** son défaut de se soumettre à une évaluation auprès de la faculté ou du centre universitaire de formation. Cette justification doit être **déposée dans le respect du délai** déterminé au règlement complémentaire de la faculté ou du centre universitaire de formation.

Le cas échéant, la faculté ou le centre universitaire de formation peut accorder un délai pour la présentation d'une production, soumettre l'étudiante ou l'étudiant à un examen supplémentaire, apporter des modifications aux exigences de stage ou ne pas tenir compte de cet élément d'évaluation dans l'attribution de la note finale.

7. NOTATION

L'attribution d'une cote au CeFTI n'a rien du hasard. Les enseignants doivent identifier les frontières de cote en fonction d'un modèle basé sur la loi de probabilité de Laplace-Gauss. Voici les règles d'attribution en vigueur au CeFTI.

1. Identification d'une moyenne cible pour l'activité par la direction

- Début de programme : [2,6..3,0]
- Milieu de programme : [2,9..3,3]
- Fin de programme : [3.2..3,7]

2. L'enseignant propose des coupures en conformité avec le règlement des études de l'Université, https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

- A+, A, A- : Excellent
- B+, B, B- : Très bien
- C+, C, C- : Bien
- D+, D : Passable
- E : Échec

3. Les cotes sont transmises à la direction du CeFTI avant d'être officialisées.

L'avantage d'un tel système est la transposition du rendement de l'étudiant en fonction du groupe dans lequel il évolue. L'évaluation reste équitable entre les cohortes. L'enseignant a la liberté de proposer une répartition qui déroge de la règle, lorsqu'il juge avoir un groupe particulier.

Ce processus a été discuté et approuvé par le comité de programme au CeFTI le 25 mai 2017.

RÉVISION D'UNE NOTE[4]

L'Université reconnaît à toute étudiante ou étudiant le droit à une révision de la note finale sous forme de lettre qui lui est attribuée pour une activité pédagogique ou le test institutionnel de français (TIF), à la condition qu'elle ou qu'il en fasse la demande au moyen du formulaire institutionnel **au plus tard vingt (20) jours ouvrables** après que la note confirmée par la faculté ou le centre universitaire de formation apparaît à son dossier.

8. RÉFÉRENCES BIBLIOGRAPHIQUES

Obligatoire

Shon Harris et Fernando Maymim, All in one CISSP exam guide, 8th edition, McGraw Hill Education, 2018, 1408 pages.

CSA Group, ISO 27001 14e éd., 2015; disponible sur IHS Markit : https://global.ihs.com/doc_detail.cfm?&rid=IHS&item_s_key=00487261&item_key_date=830230&input_doc_number=ISO27001&input_doc_title=

CSA Group, ISO 27002 8e éd., 2015; disponible sur IHS Markit : https://global.ihs.com/doc_detail.cfm?&rid=IHS&item_s_key=00508550&item_key_date=830230&input_doc_number=ISO27002&input_doc_title=

Autres

A. Calder et S. Watkins, IT Governance – An international guide to data security and ISO27001/ISO27002, 6e éd., London, Koganpage, 2015

J. Hintsbergen, K. Hintzbergen, A. Smulders et H. Baars, Foundation of Information Security – Based on ISO 27001 and ISO 27002, 3e éd., Zaltbommel, Van Haren Publishing, 2015

DAMA, Data Management Body of Knowledge (DAMA DM BoK), 2e éd. Basking Ridge, NJ, Technics Publications, 2017.

J. Ladley, Data governance How to design, deploy and sustain an effective data governance program, 1re éd. Waltham, MA: Elsevier B.V., 2012.

[4] Extrait du Règlement des études 2017-2018

R. S. Seiner, Non-Invasive Data Governance – The Path of Least Resistance and Greater Success, 1re éd. Basking Ridge, NJ, Technics Publications, 2014.

D. Plotkin, Data stewardship: an actionable guide to effective data management and data governance, 1re éd. Waltham, MA, Elsevier B.V., 2014.

T. C. Redman, Data Driven Profiting from your most Important Business Asset, 1re éd. Boston, MA, Harvard Business Press, 2008.

P. Aiken et T. Harbour, Data strategy and the enterprise data executive: ensuring that business and IT are in synch in the post-big data era, 1re éd. Basking Ridge, NJ, Technics Publications, 2017.

M. W. Harkins, Managing Risk and Information Security - Protect to Enable, 2e éd. Folsom, California, Apress Open, 2016.

Des références additionnelles seront identifiées durant le cours.