UNIVERSITÉ DE SHERBROOKE

1. IDENTIFICATION ET RENSEIGNEMENTS GÉNÉRAUX

Titre officiel du cours :	**INF809 – Architecture de sécurité**
Nombre de crédits :	3 crédits – 135 heures
Programme :	Microprogramme de 2e cycle en sécurité informatique - volet prévention Microprogramme de 2e cycle en sécurité informatique - volet réaction
Cours préalables ou concomitants :	INF801 – Concept de base en sécurité des TI
Lieu du cours :	Moodle
Session :	Hiver 2020
Date de début :	7 janvier 2020
Date de fin :	14 avril 2020
Date limite d'abandon :	14 mars 2020
Rencontres synchrones :	Tous les mardis à partir du 7 janvier 2020 18h00 à 21h00
Personne(s)-ressource(s) :	Éric Daigneault
Courriel(s) :	eric.daigneault@usherbrooke.ca

2. MISE EN CONTEXTE

DESCRIPTION OFFICIELLE DU COURS

Cible(s) de formation :

Comprendre les modèles (référence) d'architecture. Appliquer les standards d'architecture dans un contexte d'entreprise. Formuler une architecture pour les besoins de sécurité d'une entreprise. Faire l'analyse et l'évaluation d'un document d'architecture de sécurité (AS).

Contenu :

Contexte : besoins, marché et tendances, définitions. Modèle de sécurité : place de l'AS dans l'architecture d'affaires, applicative, matérielle et de données. Principes d'architecture (se traduisent comment dans la pratique) : zero-trust, modèle d'accès, isolation, DICAI. Modèle de référence : standard TOGAF et Archimate, des objets réutilisables. Niveaux d'architecture : AS au

niveau affaires, AS au niveau applicatif, AS au niveau technologique, AS au niveau des données. Vues : mise en pratique; outils. Projet (tel que Archimatetool).

PLACE DU COURS DANS LE PROGRAMME

Cette activité de formation s'inscrit en tant qu'activité optionnelle du microprogramme. Son positionnement permet à l'étudiant d'acquérir les connaissances de base fondamentales à la compréhension de ce qu'est l'architecture de sécurité dans un contexte d'entreprise, à son rôle dans les organisations et des attentes à son égard.

Le cours permet de contextualisé la mise en application et la valeur de la pratique d'architecture de sécurité.

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 trois (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 en classe (étude de cas et/ou simulation)	6 heures
Lecture personnelle	60 heures
Activités à la maison (simulation, cas, labo)	30 heures
TOTAL	135 heures

[1] Extrait de la fiche signalétique

3. DÉROULEMENT DU COURS

	Module	Description	Enseignant
Introduction et notion de base	**Séance 1 :** **Introduction et contexte de l'architecture de sécurité** *7 janvier 2020*	• Présentation du cours INF809 • Signification du concept d'architecture en contexte technologique • Besoins du marché et attentes • Survol des modèles d'architecture d'entreprise et d'architecture de sécurité • Principes DICAI en AS	ED
	Séance 2 : **Positionnement de l'architecture de sécurité** *14 janvier 2020*	• Mise en contexte de l'architecture de sécurité dans l'organisation • Rôle de l'AS dans la traduction des besoins d'affaires • Survol des interactions avec les pratiques technologiques. Place de l'architecture de sécurité dans : 1. Architecture d'affaires 2. Architecture applicative 3. Architecture matérielle 4. Architecture de données • Alignement à la stratégie d'entreprise Lecture : ESA chapitre 1-2 (p.3-33)	ED
	Séance 3 : **L'architecture d'entreprise et les modèles de référence TOGAF et SABSA** *21 janvier 2020*	• Qu'est-ce que l'AE • Les types d'artefacts en AE • Standards TOGAF et Zachman • Les différents cadres de références en AS • SABSA 1. Ses utilisations potentielles 2. La matrice SABSA et sa signification 3. Cycle de vie 4. Son utilisation 5. L'importance d'un cadre de référence 6. Les principes directeurs	

		Note : Remise de l'étude de cas Lecture : ESA chapitre 3 (p.33-44) + Notes supplémentaires http://pubs.opengroup.org/architecture/togaf91-doc/arch/index.html Partie 1 – Introduction Partie 2 – ADM (section 5-6-7-8-9-10-11-12) Les objectifs et approches Partie 3 – ADM Guidelines (section 18-19.1-19.2-19.3) Partie 4 – Content Framework (section 33-35.1 à 35.5-35.7.2) Partie 5 – Continuum (section 38-39-41.1) Partie 6 – TRM (section 43.1-43.2-43.3.1) Partie 7 – Capability Framework (section 45)	
	Séance 4 : **Conférencier** *28 janvier 2020*	• Conférencier – TBD (à confirmer)	ED
	Séance 5 : **L'approche systémique en architecture de sécurité** *4 février 2020*	• Concept théorique de sécurité d'un système et de son abstraction • Alignement avec les objectifs stratégiques de l'organisation et de son environnement • Comment gérer la complexité en architecture • L'importance de la traçabilité des décisions • Définition des objectifs et mesures d'efficacité • Techniques de modélisation 1. Processus d'affaire 2. Arbre de dépendances 3. FSM 4. Modèle de confiance • Langage de modélisation Archimate et Archimate tool Lecture : ESA chapitre 5 (p55-77) + notes supplémentaires	ED

Stratégie de défense	**Séance 6 :** **Architecture contextuelle** *11 février 2020*	• Les objectifs d'affaires • Les contraintes • Modélisation et scénario des menaces • Matrice de risques et priorisation Lecture : ESA chapitre 9 (p167-216)	ED
	Séance 7 : **Architecture conceptuelle – partie 1** *18 février 2020*	• La vue d'ensemble et la vision stratégique • La réflexion conceptuelle • L'approche par couche pour la mise en place de l'architecture de sécurité • Assurance de sécurité (Security Assurance) • Les modèles de confiance et modèle **zero trust** Lecture : ESA chapitre 10 (p.217-268)	ED
	Séance 8 : **Architecture conceptuelle – partie 2** *25 février 2020*	• L'isolation du périmètre 1. Son évolution 2. La nouvelle réalité de l'infonuagique et des entreprises digitales 3. Concept de défense en profondeur • VPN et coupe-feu • Concept de durée de vie dans l'AS Lecture : ESA chapitre 10 (p.269-284) **Examen Intra (25%)**	ED
Le design	**Séance 9 :** **Architecture logique – partie 1** *3 mars 2020*	• Différence entre connaissance, information et données • Différence des besoins de sécurité pour l'information statique et dynamique • Les différents types de politique de sécurité ➔ Réf. ESA chapitre 14 … suite sur les services de sécurité la semaine prochaine. Lecture : EAS chapitre 11 (p.285-330) Lecture : EAS chapitre 14 (p.409-434)	ED

	Séance 10 : **Architecture logique – partie 2** *10 mars 2020*	• Les différents types de service de sécurité : 1. Prévention 2. Isolation 3. Détection et notification 4. Gestion des évènements systèmes 5. Remise en fonction 6. Assurance de sécurité Lecture : ESA chapitre 11 (p.285-330)	ED
	Séance 11 **Architecture logique – fin** **Architecture physique – partie 1** *17 mars 2020*	AS Logique • Les domaines de l'AS logique 1. Réseau 2. Intergiciel 3. Application AS physique • Modèle d'affaire 1. Systèmes de fichiers et gestion de l'accès 2. Systèmes d'encryption … suite sur les modèles d'affaire la semaine prochaine. Lecture : ESA chapitre 12 (p331-376)	ED
	Séance 12 **Architecture physique** *24 mars 2020*	• Modèle d'affaire 3. Sécurité des bases de données 4. Sécurité matériel - HSM - TPM • TCB et anneaux de protection • Topologie réseau • Topologie des répertoires • Revue de la chaine « Stratégie de défense → Service à mettre en place → mécanisme physique de sécurité à installer » Lecture : ESA chapitre 12 (p331-376)	ED

	Séance 13 **Composantes de l'architecture** *31 mars 2020*	• Structures de données • Standards de sécurité • Les différentes solutions de sécurités et les différents outils de sécurité • Transport sécurisé • Service Web • Intégration des composantes et SOA Lecture : ESA chapitre 13 (p.377-406)	ED
Conclusion	**Séance 14 :** **L'architecture et la gestion du risque** *7 avril 2020*	• Le lien entre l'AS et la gestion des risques • Les types de risques à considérer en AS • Les standards reconnus en gestion de risque • Comment construire un programme basé sur les risques Lecture : ESA chapitre 15 (p.435-485) et autres notes de cours **Examen final (25%)**	ED
	Séance 15 **Présentation des résultats de l'étude de cas** *14 avril 2020*	Présentation des résultats de l'étude de cas (40%)	ED

4. CONSIDÉRATIONS MÉTHODOLOGIQUES

APPROCHES MÉTHODOLOGIQUE ET PÉDAGOGIQUE

Le cours INF809 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: **Étude de cas – Intégrer les 5 étapes (le contexte, la conceptualisation, la logique, le physique et les composantes requises) pour construire une AS simple mais complète.**

- ***Compétence mobilisée:*** Travail d'intégration des notions d'architecture, allant du contexte du cas aux composantes requises pour activer la stratégie proposée.
- ***Description:*** Étude de cas représentant une problématique concrète devant laquelle l'étudiant devra, tout au long du semestre, développer les éléments requis pour présenter une architecture de sécurité d'entreprise cohérente.

  Le cas sera déposé sur Moodle

  Travail à compléter individuellement
- ***Critères d'évaluation*** *Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle 2.*
- ***Notation:*** 40 % de la note finale
- ***Date de remise:*** TBD

ÉVALUATION N^{O} 2: **Examen Intra – Notion de base et stratégie de sécurité**

- ***Compétence mobilisée:*** Compréhension de l'architecture de sécurité dans un contexte d'entreprise ainsi que de son rôle stratégique dans la défense de l'organisation
- ***Description:*** Examen de 90 minutes à développement simple.

  Travail à compléter seul

  Voir grille déposée sous moodle.
- ***Critères d'évaluation*** *Pour les consignes précises et la grille d'évaluation, consultez Moodle 2.*
- ***Notation:*** 25 % de la note finale
- ***Date de remise:*** 25 février 2020

ÉVALUATION N^{O} 3: **Examen final – Design, ROI et Gestion de risque**

- ***Compétence mobilisée:*** Compréhension de l'architecture de sécurité dans un contexte d'entreprise, de son design, des impacts monétaire et de sa relation avec la gestion de risque de l'organisation.
- ***Description:*** Examen de 90 minutes à développement simple.

  Travail à compléter seul

  Voir grille déposée sous moodle.
- ***Critères d'évaluation*** *Pour les consignes précises et la grille d'évaluation, consultez Moodle 2.*
- ***Notation:*** 25 % de la note finale
- ***Date de remise:*** 7 avril 2020

ÉVALUATION N^{O} 4: **Participation aux discussions du cours**

- ***Compétence mobilisée:*** L'ensemble de la matière vue durant le cours
- ***Description:*** L'étudiant démontre son intérêt et son évolution par sa participation aux diverses discussions suscitées par la matière lue et/ou vue en cours.
- ***Critères d'évaluation*** *Participation aux discussions*
- ***Notation:*** 10 % de la note finale
- ***Date de remise:*** N/A

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).

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;

[2] Extrait du Règlement des études 2017-2018

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.

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

Comment une cote est évaluée au CeFTI ?

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

[3] Extrait du Règlement des études 2017-2018

- 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

Livre obligatoire pour le cours

John Sherwood, Andrew Clark and David Lynas, Enterprise Security Architecture – A business-Driven approach, CRC Press, 2005, 608 pages.

[4] Extrait du Règlement des études 2017-2018