# INF8700
# Sécurité des systèmes, données et contrats

Plan de cours

## Responsable(s) du cours

**Coordination :** BÉGIN, Guy
PK-4825
poste 4081
begin.guy@uqam.ca
www.info.uqam.ca/~begin/index.html

**Enseignement :**

NSIEMPBA, Jude Jacob
PK-4115/DS-7325
poste 3497
nsiempba.jude@uqam.ca
http://info.uqam.ca/~nsiempba/

Les étudiants doivent consulter réguliérement le forum dans Moodle, moyen de communication du professeur avec le groupe-cours.

## Description du cours

### Objectifs

Introduire les étudiants à la sécurité des systèmes informatiques et des données. Sensibiliser les étudiants aux risques et menaces. Introduire les techniques permettant d'assurer la sécurité des processus. Introduire les méthodes de mitigation du risque et de gestion de la sécurité.

#### 2.1.1 Sommaire du contenu

Sensibilisation à la sécurité informationnelle : concepts de base en sécurité :informationnelle, Objectifs de sécurité, lois et règlements. La sécurité informationnelle et l'organisation : parties prenantes, rôles et responsabilités, équipe de sécurité, impartition.

Gestion des actifs : inventaire et classification des ressources informationnelles. Interconnexion de systèmes et partage d'information. Sensibilité des informations.

Évaluation, gestion et mitigation des risques.

Gestion des contrôles : besoins d'affaire du contrôle d'accès, gestion des identités et des accès : à l'infrastructure, aux systèmes d'exploitation, aux applications et aux données. Responsabilités des utilisateurs.

Contrôles cryptographiques : introduction aux mécanismes sécuritaires modernes : chiffrage symétriques et asymétriques ; fonctions de hachage ; protocoles sécuritaires ; authentification. Installation, configuration des contrôles. Planification et acceptation des systèmes.

Application aux services de commerce électronique. Chaînes de blocs et monnaies électroniques. Mécanismes de paiement. Contrats.

## Objectifs du cours

Au terme du cours, l'étudiant sera à mesure de : - définir les objectifs de sécurité, les exprimer en termes de besoins spécifiques (confidentialité, intégrité, disponibilité, etc.) ; - faire un inventaire des éléments du patrimoine informationnel d'une organisation ; - évaluer les scénarios de risque (identifier les éléments à risque, les aléas et vulnérabilités susceptibles de causer des dommages, d'en fixer les priorités carte d'exposition) ; - préconiser une stratégie de traitement du risque et des mesures de protection des actifs personnels /d'entreprise ; - maitriser les notions nécessaires à la compréhension des contrats et des propriétés intelligents ; - comprendre les rudiments/bases sur les développements récents de la loi canadienne sur la cyber-sécurité.

## Contenu du cours

Chapitre 1 : Sensibilisation à la sécurité informationnelle Chapitre 2 : Sécurité informationnelle et l'organisation Chapitre 3 : Gestion des risques - Normes ISO 27001 et 27005 - Méthodes : Octave et Méhari Chapitre 4 : Lois,règlements,contrats Chapitre 5 : Gestion des contrôles Chapitre 6 : Contrôles cryptographiques Chapitre 7 : Applications

## Modalités d'évaluation

- Travail de session (en groupe de 3-5) 40%
  - Livrable 1 (5%)
  - Livrable 2 (10%)
  - Présentation PowerPoint en classe du travail de session (5%)
- Rapport final (20%)
- Travaux individuels [1] [2] (10 % chacun) 20%

- Examen final 40%

**Travail de session**

Les étudiants seront formés en classe sur, entre autres sujets, les méthodologies d'analyse de risque MEHARI ET OCTAVE et, en complément à cette formation théorique, ils conduiront sur le terrain, en équipe de 3 ou 5 étudiants, une activité authentique qui se rapproche le plus des pratiques professionnelles. Ils auront à définir concrètement un cadre de gestion des risques en sécurité de l'information d'une PME.

**Travaux individuels [1][2]**

Les sujets des travaux seront disponibles aux séances 2 et 7 et les dates de remise des rapports seront indiquées, à chaque fois, dans l'énoncé. Les travaux à faire individuellement visent à évaluer l'assimilation des concepts et méthodes vus en cours. D'amples explications seront données en classe.

Liste des sujets des travaux individuels (Liste non-exhaustive)

1)Modèle d'aide à la décision en sécurité informatique basé sur des métriques 2)Anonymat, vie privée et confidentialité (Anonymat et identité sur internet versus droit à la vie privée) 3)Sécurité informatique et Internet des objets 4)Aléa moral et risque en sécurité informatique 5)Géolocalisation et vie privée 6)Audits (externes/ internes) et gestion des risques en sécurité informatique 7)Solutions infonuagiques et sécurité des données 8)Crypto-monnaie et cyber-risque 9)«Habituation to Security warnings»

## Manuels et notes de cours

Aucun manuel n'est obligatoire pour ce cours. Toutefois, -les normes ISO 17799, ISO 27001 et ISO 27005, -les guides COBIT 5 for Information Security et CSX Cyber-Security Fundamentals Study Guide, -les acétates du cours ainsi que les lectures complémentaires et certains ouvrages recommandés seront utilisés. Pour plus de détails, consultez la page Web du cours à l'adresse : https ://moodle.uqam.ca.

## Calendrier détaillé du cours

**Semaine 1,2**

Chapitre 1 : Sensibilisation à la sécurité informationnelle

- Présentations du plan de cours
- Introduction : sécurité informatique/informationnelle, vocabulaire
- Concepts de base en sécurité,
- Objectifs de sécurité,
- Politique de sécurité.

**Semaine 3**

Chapitre 2 : Sécurité informationnelle et l'organisation - parties prenantes, - rôles et responsabilités, - équipe de sécurité, - impartition.

**Semaine 4,5**

Chapitre 3 : Gestion des risques - Inventaire et classification des ressources informationnelles - Interconnexion de systèmes et partage d'information - Sensibilité des informations

**Semaine 6,7,8**

Chapitre 3 : Gestion des risques (suite)

Évaluation, gestion et mitigation des risques - présentation de la norme ISO 27001 - présentation de la norme ISO 27005

Méthodologies d'analyse de risque [OCTAVE, MEHARI]

**Semaine 9**

Chapitre 4 : Lois,règlements,contrats

**Semaine 10,11**

Chapitre 5 : Gestion des contrôles - Besoins d'affaire du contrôle d'accès - Gestion des identités et des accès (matrice des profils d'accès) par type de ressources) - Types : infrastructure, systèmes d'exploitation, applications et données. - Responsabilités des utilisateurs

**Semaine 12,13**

Chapitre 6 : Contrôles cryptographiques

- Introduction aux mécanismes sécuritaires modernes : chiffrage symétriques et asymétriques ; fonctions de hachage ; protocoles sécuritaires ; authentification
- Installation, configuration des contrôles
- Planification et acceptation des systèmes

**Semaine 14,15**

Chapitre 7 : Application aux services de commerce électronique - Chaînes de blocs et monnaies électroniques - Mécanismes de paiement - Contrats

**L'autorisation de reprendre un examen en cas d'absence est de caractère exceptionnel. Pour obtenir un tel privilège, l'étudiant-e doit avoir des motifs sérieux et bien justifiés.**
Il est de la responsabilité de l'étudiant-e de ne pas s'inscrire à des cours qui sont en conflit d'horaire, tant en ce qui concerne les séances de cours ou d'exercices que les examens. **De tels conflits d'horaire ne constituent pas un motif justifiant une demande d'examen de reprise.**
Dans le cas d'une absence pour raison médicale, l'étudiant-e doit joindre un certificat médical original et signé par le médecin décrivant la raison de l'absence à l'examen. Les dates d'invalidité doivent être clairement indiquées sur le certificat. Une vérification de la validité du certificat pourrait être faite. Dans le cas d'une absence pour une raison non médicale, l'étudiant-e doit fournir les documents originaux expliquant et justifiant l'absence à l'examen ; par exemple, lettre de la Cour en cas de participation à un jury, copie du certificat de décès en cas de décès d'un proche, etc. Toute demande incomplète sera refusée. Si la direction du programme d'études de l'étudiant-e constate qu'un étudiant a un comportement récurrent d'absence aux examens, l'étudiant-e peut se voir refuser une reprise d'examen.
L'étudiant-e absent-e lors d'un examen doit, dans les cinq (5) jours ouvrables suivant la date de l'examen, présenter une demande de reprise en utilisant le formulaire prévu, disponible sur le site Web du département à l'adresse suivante : info.uqam.ca/politiques/.
L'étudiant-e doit déposer le formulaire dûment complété au secrétariat de la direction de son programme d'études : PK-3150 pour les programmes de premier cycle, PK-4150 pour les programmes de cycles supérieurs. Pour plus de détails sur la politique d'absence aux examens du Département d'informatique, consultez le site web suivant : info.uqam.ca/politiques.

**PLAGIAT Règlement no 18 sur les infractions de nature académique. (extraits)**
**Tout acte de plagiat, fraude, copiage, tricherie ou falsification de document commis par une étudiante, un étudiant, de même que toute participation à ces actes ou tentative de les commettre, à l'occasion d'un examen ou d'un travail faisant l'objet d'une évaluation ou dans toute autre circonstance, constituent une infraction au sens de ce règlement.**

**La liste non limitative des infractions est définie comme suit :**

- **la substitution de personnes ;**
- **l'utilisation totale ou partielle du texte d'autrui en la faisant passer pour sien ou sans indication de référence ;**
- **la transmission d'un travail pour fins d'évaluatiion alors qu'il constitue essentiellement un travail qui a déjà été transmis pour fins d'évaluation académique à l'Université ou dans une autre institution d'enseignement, sauf avec l'accord préalable de l'enseignante, l'enseignant ;**
- **l'obtention par vol, manoeuvre ou corruption de questions ou de réponses d'examen ou de tout autre document ou matériel non autorisés, ou encore d'une évaluation non méritée ;**
- **la possession ou l'utilisation, avant ou pendant un examen, de tout document non autorisé ;**
- **l'utilisation pendant un examen de la copie d'examen d'une autre personne ;**
- **l'obtention de toute aide non autorisée, qu'elle soit collective ou individuelle ;**
- **la falsification d'un document, notamment d'un document transmis par l'Université ou d'un document de l'Université transmis ou non à une tierce persone, quelles que aoient les circonstances ;**
- **la falsification de données de recherche dans un travail, notamment une thèse, un mémoire, un mémoire-création, un rapport de stage ou un rapport de recherche ;**
- **Les sanctions reliées à ces infrations sont précisées à l'article 3 du Règlement no 18.**

Les règlements concernant le plagiat seront strictement appliqués. Pour plus de renseignements, veuillez consulter les sites suivants : www.sciences.uqam.ca/etudiants/integrite-academique.html et www.bibliotheques.uqam.ca/plagiat/le-plagiat-liens-rapides.

**Politique no 16 visant à prévenir et combattre le sexisme et les violences à caractère sexuel**

**Pour consulter la politique no 16 :**

instances.uqam.ca/wp-content/uploads/sites/47/2018/05/Politique_no_16.pdf

**Services offerts :**

Pour obtenir de l'aide, faire une divulgation ou une plainte :
Bureau d'intervention et de prévention en matière de harcèlement
514 987-3000, poste 0886
Pour la liste des services offerts en matière de violence sexuelle à l'UQAM et à l'extérieur de l'UQAM : harcelement.uqam.ca

CALACS Trêve pour Elles – point de services UQAM :
514 987-0348
calacs@uqam.ca
trevepourelles.org

Soutien psychologique (Services à la vie étudiante) :
514 987-3185
Local DS-2110

Service de la prévention et de la sécurité : 514 987-3131

Les étudiants qui ont une lettre signée de leur conseillère ou conseiller de l'Accueil et de soutien aux étudiants en situation de handicap (ASESH), dans laquelle il est fait état de leur inscription au ASESH à titre d'étudiant(e) en situation de handicap, sont invités à remettre ce document à leurs professeur(e)s et chargé(e)s de cours dès le début de la session afin que les aménagements dans le respect des exigences académiques soient déterminées de concert avec chacun des professeur(e)s et chargé(e)s de cours. Les étudiants qui ont une déficience et qui ne seraient pas inscrits au ASESH sont priés de se présenter au AB-2300.
Étudiants avant une déficience de type visuelle, auditive, motrice, trouble d'apprentissage, trouble envahissant du développement et trouble de santé mentale :
Les étudiant(e)s qui ont une lettre d'*Attestation des mesures d'aménagements académiques* obtenue auprès d'une conseillère, d'un conseiller de l'ACCUEIL ET SOUTIEN AUX ÉTUDIANTS EN SITUATION DE HANDICAP (ASESH) doivent rencontrer leurs enseignant(e)s au début de la session afin que des mesures d'aménagement en classe ou lors des évaluations puissent être mises en place. Ceux et celles qui ont une déficience ou une incapacité mais qui n'ont pas cette lettre doivent contacter l'ASESH au (514) 987-3148 ou se présenter au AB-2300 le plus tôt possible.