UQÀM | Département d'informatique

INF8700 - Sécurité des systèmes, données et contrats
Plan de cours - Automne 2019

Sécurité des systèmes, données et contrats

Groupe 020

Mardi, de 17h30 à 20h30 SH-3540 (cours magistral)

RESPONSABLE(S) DU COURS

Nom de l'enseignant : Nsiempba, Jude
Bureau : DS-7325
Téléphone : (514) 987-3000 #3497
Disponibilité : mardi 16h30-17h30
Courriel : nsiempba.jude@uqam.ca
Site Web : https://etudier.uqam.ca/cours?sigle=INF8700&p=1575

DESCRIPTION DE L'ANNUAIRE

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

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.

Au terme du cours, l'étudiant sera à mesure de :

1. définir les objectifs de sécurité, les exprimer en termes de besoins spécifiques (confidentialité, intégrité, disponibilité, etc.);
2. faire un inventaire des éléments du patrimoine informationnel d'une organisation;
3. 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);

4. de préconiser une stratégie de traitement du risque et des mesures de protection des actifs personnels /d'entreprise;
5. maitriser les notions nécessaires à la compréhension des contrats et des propriétés intelligents;
6. comprendre les rudiments/bases sur les développements récents de la loi canadienne sur la cyber-sécurité.

PLAN DE COURS DETAILLE

Séance	Date	Thèmes abordés
1.	10 septembre 2019 **Sujet travail de session (Cas d'entreprise)** **Sujet travail individuel [1]**	Introduction : sécurité informatique/informationnelle, vocabulaire Sensibilisation à la sécurité informationnelle : - concepts[1] de base en sécurité, - objectifs[2] de sécurité, - politique de sécurité. ▪ Titre : Mise en place d'un système de gestion de la sécurité de l'information basé sur la norme ISO 27001. ▪ Plan de travail : (à définir) ▪ Formation des équipes de travail et assignation des entreprises aux équipes Lectures : (à définir)
2.	17 septembre 2019	Sécurité informationnelle et l'organisation : - parties prenantes, - rôles et responsabilités, - équipe de sécurité, - impartition.
3.	24 septembre 2019 **Remise travail individuel [1]**	Gestion des actifs (1) - Inventaire et classification des ressources informationnelles - Interconnexion de systèmes et partage d'information Livrable : (à définir)
4.	1 octobre 2019 **Suivi travail de session**	Gestion des actifs (2) - Interconnexion de systèmes et partage d'information (suite et fin) - Sensibilité des informations
5.	8 octobre 2019	Évaluation, gestion et mitigation des risques (1) - présentation de la norme ISO 27001

[1] Vulnérabilité, menace, risque, contremesures, 3**P** (**P**révention, **P**rotection, **P**unition)
[2] Confidentialité, intégrité, disponibilité, non-répudiation, traçabilité

	Travail de session	**Livrable 1** : Politique de sécurité (contexte et enjeux, objectifs de sécurité)
6.	15 octobre 2019	Évaluation, gestion et mitigation des risques (2) - présentation de la norme ISO 27005 - Méthodologies d'analyse de risque [OCTAVE, MEHARI]
7.	22 octobre 2019 **Sujet travail individuel [2]**	Évaluation, gestion et mitigation des risques (3) - Méthodologies d'analyse de risque o OCTAVE o MEHARI
8.	29 octobre 2019 **Remise travail individuel [2]**	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) o Types : infrastructure, systèmes d'exploitation, applications et données. - Responsabilités des utilisateurs Livrable (à définir)
9.	5 novembre 2019 **Travail de session**	Contrôles cryptographiques (1) - Introduction aux mécanismes sécuritaires modernes : chiffrage symétriques et asymétriques; fonctions de hachage; protocoles sécuritaires; authentification. **Livrable 2:** rapport d'inventaire des actifs informationnels de l'entreprise à l'étude
10.	12 novembre 2019	Contrôles cryptographiques (2) - Installation, configuration des contrôles - Planification et acceptation des systèmes
11.	19 novembre 2019 **Conférencier invités (1)**	Thème: Loi et règlements
12.	26 novembre 2019	Application aux services de commerce électronique - Chaînes de blocs et monnaies électroniques - Mécanismes de paiement - Contrats
13.	3 décembre 2019	Présentation des projets de session
14.	10 décembre 2019 **Travail de session**	Examen final **Livrable : rapport final**

MODALITÉS D'ÉVALUATION

Travail de session (en groupe de 2)	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 2 ou 3 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 rapports seront remis, à chaque fois, la semaine suivante. 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 DE SUJETS DES TRAVAUX INDIVIDUELS (LISTE NON-EXHAUSTIVE)

1. Anonymat, vie privée et confidentialité (Anonymat et identité sur internet versus droit à la vie privée);
2. Sécurité informatique et Internet des objets;
3. Aléa moral et risque en sécurité informatique
4. Géolocalisation et vie privée
5. Audits (externes/ internes) et gestion des risques en sécurité informatique
6. Solutions infonuagiques et sécurité des données.

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.