INSTITUT
GRASSET

Sécurité de l'information

Plan de cours

Programme d'études : Techniques de l'informatique, profil programmation nouveaux médias (420.B0)

Code du cours : 420-SY4-AG

Titre du cours : Sécurité de l'information

Énoncé de la (ou des) compétence(s) :
Effectuer des opérations de prévention en matière de sécurité de l'information (00Q8)

Pondération : 2-2-2 **Nombre d'unités** : 2

Nombre d'heures de cours : 60

Session : Hiver 2022

Professeur : FRÉDÉRIC LAZURE

Disponibilités : Sur rendez-vous ou par messagerie Omnivox (MIO)

1. Présentation générale du cours

But du cours et lien avec le programme de formation ou avec la séquence de cours

Le cours Sécurité de l'information aborde la protection de l'information par le biais du contrôle de risques et son lien particulier avec l'informatique et la communication réseau. Le cours détaille les différents concepts de sécurité informatiques, les équipements, les logiciels, les algorithmes ainsi que les bonnes pratiques permettant de rendre accessible l'information à l'audience désirée exclusivement. La visée du cours couvre l'équipement physique, virtuel, infonuagique et les personnes auxquelles est confiée l'information.

Le cours Sécurité de l'information est situé à la 2e session. Il couvre tous les éléments de la compétence 00Q8-Effectuer des opérations de prévention en matière de sécurité de l'information. Cette compétence n'est pas partagée par les autres cours du programme.

Objectif terminal du cours

À la fin du cours, l'étudiant sera en mesure de comprendre, de mettre en place, de dépanner et d'effectuer des opérations de prévention sur des systèmes de contrôle de l'information.

2. Compétence ministérielle

Compétence : Effectuer des opérations de prévention en matière de sécurité de l'information (00Q8)
Atteinte : Complète
Contexte de réalisation :

- À l'aide de mesures de sécurité reconnues.
- À l'aide de logiciels de sécurité informatique et de bibliothèques de cryptographie.

Éléments de la compétence	Critères de performance
1. Analyser des risques en matière de sécurité de l'information.	1.1 Inventaire précis de l'équipement informatique et des applications installés. 1.2 Inventaire adéquat des menaces potentielles et des vulnérabilités. 1.3 Détermination correcte des conséquences sur la sécurité. 1.4 Choix approprié des mesures de sécurité à appliquer.
2. Appliquer des mesures de sécurité reconnues pour protéger le réseau.	2.1 Utilisation appropriée des stratégies de sauvegarde. 2.2 Utilisation appropriée des stratégies d'attribution des droits d'accès. 2.3 Configuration et personnalisation correctes des logiciels antivirus et coupe-feu. 2.4 Utilisation appropriée des utilitaires de cryptographie.
3. Appliquer des mesures de sécurité reconnues pour protéger une application.	3.1 Utilisation appropriée des stratégies de sécurisation des données entrées par l'utilisatrice et l'utilisateur.

	3.2 Utilisation appropriée des techniques de contrôle des erreurs et des exceptions. 3.3 Utilisation appropriée de mécanismes d'authentification et d'autorisation sécuritaires.

Organisation des activités d'enseignement et d'apprentissages

a) Approches pédagogiques privilégiées

- Cours magistraux accompagnés de supports visuels
- Laboratoires ou ateliers
- Recherches individuelles ou en équipe
- Mises en situation
- Travail pratique dirigé
- Étude de cas
- Exercices

b) Calendrier des activités

À noter : certaines périodes de cours pourraient être données en présentiel, vous serez avisés par votre professeur si c'est le cas.

Numéro de séance	**Contenu**	**Informations (évaluations, activités, ateliers, lectures, etc.)**
1	• Historique de la sécurité de l'information • Historique de la cryptographie • Les différentes définitions de la sécurité • Objectifs de la sécurité de l'information : Confidentialité, Intégrité, Disponibilité, Imputabilité, Non-répudiation et Authenticité.	Installation et utilisation d'une solution cryptographique forte
2	• Introduction à la gestion de risques (analyse, types de risques, danger, probabilité, impact, gravité, contrôles, risque résiduel, acceptabilité) • Le problème de la sécurité comme une pensée après coup (*afterthought*) • Design pour la sécurité • Vérification des entrées de l'utilisateur et validation des données	Exercice de gestion de risque Exercices de vérification des entrées de l'utilisateur et de validation des données
3	• Identification des risques de sécurité reliés au développement d'applications • Mécanismes de contrôle des erreurs et des exceptions • Implémentation d'algorithmes cryptographiques • Exemples de code générant des vulnérabilités	• Exercice de contrôle des erreurs et des exceptions

4	• Notion d'inventaire des équipements, des services informatiques, des rustines (patches) de sécurité et des failles potentielles. • Vulnérabilités *zero-day* Virus, Malware, Worms, Cryptovirology, Ransomware, Trojan, Botnet, etc.	Exercices de création et de maintenance d'inventaire.
5	Logiciels de sécurité informatique	Installation et configuration de logiciels de sécurité informatique Inventaire et mise à jour des risques
6		**Examen intra 1** **Pondération : 25%**
7	• Alice, Bob et les autres : les exemples classiques de la cryptographie • Algorithmes cryptographiques et applications, suite. • Type de chiffrements : faible, symétrique, asymétrique, hachage • Masque jetable et cryptographie quantique • Vulnérabilité et génération de nombres aléatoires. • Présentation du TP	Choix du sujet de TP Exercice d'évaluation de risque et d'implémentation de contrôle Implémentation d'algorithmes cryptographiques
8	• Principales attaques réseaux. • Analyse d'une attaque informatique • Fonctionnement, installation et configuration des différents équipements et logiciels de sécurité réseau.	Installation, configuration et opération de logiciels de sécurité réseau.
9	• Bonnes pratiques : mots de passe, listes d'accès, listes blanches, listes noires, authentification à facteurs multiples, mots de passe à usage unique, etc. • *Air gap* et ses limitations	Exercices de création d'utilisateur et implémentation de mesures de sécurité associées
10	• Mise en place de stratégies de sauvegarde et test des sauvegardes. • Stratégie de sauvegarde 3-2-1	Mise en place d'une stratégie de sauvegarde complète.
11	Introduction aux conteneurs (Docker)	Déploiement de divers conteneurs Prise en main du TP
12	Prise en main du TP	**Remise : Travail pratique 1** **Pondération : 35%**

13	• Lois et régulations de la sécurité informatique. • Audit et conformité • Tests d'infiltration (*Penetration testing*)	Tests d'infiltration Exercice d'audit
14	Période de révision de la matière et de complément d'information	Révision de la matière du cours
15		**Évaluation finale** **Pondération : 40%**

Ce calendrier peut être sujet à modification durant la session.

3. Évaluations

a) Évaluations formatives

- Laboratoires et exercices pratiques permettant de découvrir, de tester et d'évaluer de nouvelles technologies.
- Communication des résultats des recherches.

b) Afin de vérifier l'atteinte de la compétence visée, voici les évaluations sommatives de ce cours :

Évaluation	Date (numéro de séance)	Pondération	Éléments de compétences visés
Examen intra 1 **Forme** : Individuel **Description** : Examen théorique et pratique sur la matière des 6 premiers cours **Critères d'évaluation** : (00Q5) 1.1 à 1.4 2.1 à 2.4 3.1 à 3.3	Séance 6	25%	(00Q8) 1. Analyser des risques en matière de sécurité de l'information. 2. Appliquer des mesures de sécurité reconnues pour protéger le réseau. 3. Appliquer des mesures de sécurité reconnues pour protéger une application.
Titre : Travail pratique **Forme :** En relation avec le TP du cours de *réseaux informatiques*, faire une analyse de risque de l'application et mettre en place des contrôles suffisants pour rendre le risque acceptable.	Séance 12	35%	(00Q8) 1. Analyser des risques en matière de sécurité de l'information. 2. Appliquer des mesures de sécurité reconnues pour protéger le réseau.

La solution devra inclure un minimum de 5 mesures originales. **Critères d'évaluation :** • Respect des consignes • Pertinence des logiciels • Justesse de l'interprétation de l'information technique • Précision de l'analyse de risque • Exactitude des spécifications • Qualité de la sélection des contrôles • Acceptabilité du risque résiduel			3. Appliquer des mesures de sécurité reconnues pour protéger une application.
Évaluation finale **Forme** : Individuel **Description** : Examen théorique et pratique sur la matière de l'ensemble du cours **Critères d'évaluation** : (00Q8) 1.1 à 1.4 2.1 à 2.4 3.1 à 3.3	Séance 15	40%	(00Q8) 1. Analyser des risques en matière de sécurité de l'information. 2. Appliquer des mesures de sécurité reconnues pour protéger le réseau. 3. Appliquer des mesures de sécurité reconnues pour protéger une application.

4. Politiques

a) Politiques issues de la PIEA

- **Absences aux examens**
  L'étudiant doit :

  1.7.1.3 *Informer son professeur en cas d'absence à un examen en cours de session et présenter une preuve justificative. L'étudiant doit également convenir des modalités de reprise avec son professeur ou se conformer aux modalités prévues au plan de cours. L'autorisation de reprise ne sera accordée que pour un cas de force majeure, hors du contrôle de l'étudiant, confirmé par une preuve (maladie grave, citation à comparaître devant un tribunal, décès d'un proche, accident, etc.).*

  1.7.1.4 *Informer la Direction des études ou le directeur adjoint de l'Institut en cas d'absence à un examen final et présenter une preuve justificative. La Direction des études ou le directeur adjoint de l'Institut fixe le moment de la reprise de l'examen dans les meilleurs délais. L'autorisation de reprise ne sera accordée que pour un cas de force majeure hors de votre contrôle confirmé par une preuve (maladie grave, citation à comparaître devant un tribunal, décès d'un proche, etc.).*

- **Retards dans la remise des travaux**

  2.3.3.1 *Pour les travaux dont le délai de production est d'une semaine (7 jours) ou moins, le professeur peut refuser le travail et inscrire la note zéro.*

  2.3.3.2 *Pour les travaux dont le délai de production est de plus d'une semaine (8 jours et plus), le professeur peut enlever jusqu'à 10 % des points par jour de retard, incluant les jours de fin de semaine.*

- **Évaluation de la langue**

  L'évaluation tient compte du français écrit, et ce jusqu'à 10% de la note finale.

  1.6.6.1 *L'étudiant doit présenter ses travaux et ses examens dans un français de qualité.*

- **Le plagiat**

  3.3 Le plagiat (Dionne, 2013, p.199)

  Le plagiat est l'acte de faire passer pour siens des textes, des contenus, des réponses ou des idées d'autrui, sans citer la source.

  3.4 La fraude, la tricherie et la tentative de tricherie

  La fraude est un acte de tromperie qui vise l'obtention d'un avantage personnel, parfois au détriment des autres.

  3.5 Conséquences

  Tout plagiat, toute fraude, toute tentative de plagiat ou de fraude, toute coopération à un plagiat ou à une fraude et toute présence de matériel non autorisé est passible de la note zéro pour l'activité concernée et peut entraîner une réévaluation des résultats antérieurs.

  Les appareils électroniques, comme les téléphones cellulaires et les montres intelligentes, peuvent contenir une foule d'informations (notes de cours, solutionnaires, formules, etc.) en plus de permettre d'entrer en communication avec autrui. À moins d'une autorisation explicite du professeur, leur utilisation est formellement interdite durant toute évaluation, sous peine de sanction pour fraude. De façon préventive, durant les évaluations, les appareils électroniques doivent être laissés à l'extérieur du local d'examens. Si un étudiant conserve sur lui un appareil électronique lors d'une évaluation, il sera automatiquement convoqué par la direction des études qui pourrait appliquer des sanctions. En cas de récidive, la direction des études pourrait recommander des sanctions allant jusqu'au renvoi du collège.

b) Politiques de l'Institut

- **Politique de contenu**

  Sont à proscrire tous les contenus à caractère irrespectueux, diffamatoire ou explicite, qu'ils soient sexuels, racistes, religieux ou autres. Tout contenu devra être validé par le professeur avant d'être diffusé.

- **Politique d'enregistrement des cours**

  Il est strictement interdit d'enregistrer les cours sans l'autorisation écrite du professeur, que ce soit un enregistrement audio et/ou vidéo fait à partir d'un téléphone intelligent ou à l'aide de n'importe quel autre support.

- **Politique de comportement en classe**

  L'étudiant(e) dont le comportement nuit au bon déroulement du cours pourra se voir refuser l'accès au cours et devra rencontrer le coordonnateur à cet effet. Seront considérés comme nuisibles au bon déroulement du cours :
  -Manque de respect à l'égard de l'enseignant(e) ou des étudiants
  -Non-respect des consignes de l'enseignant(e)
  -Ne pas effectuer en classe le travail exigé par l'enseignant(e)
  -Travailler en classe sur le contenu d'un autre cours
  -Tout autre comportement jugé nuisible au bon déroulement du cours par l'enseignant(e)

5. Ouvrage(s) ou matériel suggéré pour ce cours

Médiagraphie

L'étudiant qui reçoit des fichiers numériques dans le cadre de son cours peut en imprimer une copie et conserver ces fichiers numériques jusqu'à 30 jours après l'évaluation finale, mais il ne peut pas les transmettre à quelqu'un d'autre, que ce soit sous forme numérique ou imprimée, ni en faire une exploitation commerciale sous quelque support que ce soit.

Livres suggérés:

GHERNAOUTI, S. *Cybersécurité: Analyser les risques, mettre en oeuvre les solutions*, Dunod, 2019, 391 pages

SCHNEIER, Bruce, *Applied Cryptography: Protocols, Algorithms and Source Code in C* (20th Anniversary Edition), John Wiley & Sons, 2015, 784 pages

AGGARWAL, M. *Network Security with PfSense*, Packt Publishing, 2018, 152 pages