UPEC
Connaissance - Action
UNIVERSITÉ
PARIS-EST CRÉTEIL
VAL DE MARNE

Diplôme d'Université

Sécurité de l'information

et du système d'information

En partenariat avec

EULEOS

Livret Stagiaire V7 – 10-2019

Présentation de la formation

OBJECTIFS DE LA FORMATION

Comprendre les enjeux de la cybersécurité et connaître les menaces.

Savoir se protéger et protéger son activité qu'elle soit individuelle ou collective.

IMPACT PROFESSIONEL

En fonction de son profil :

- Informaticien : évolution vers des fonctions de cadre ou d'agent en charge de la sécurité du système d'information.
- Libéral, auto-entrepreneur, gérant, artisan/commerçant : sécurisation de son activité contre les cyberattaques.

ORGANISATION DE LA FORMATION

126h (21 jours) réparties sur 6 mois :

- 24h de rappels généraux (option).
- 12h d'introduction au contexte.
- 7 modules thématiques de 12h.
- 1 journée de soutenance finale.

SECTEURS D'ACTIVITÉ

Tous les secteurs d'activité sont concernés par la cybersécurité.

NOS ATOUTS

- Des formateurs professionnels et académiques expérimentés.
- Un cadre de formation de qualité et une équipe à votre écoute.
- Des partenaires professionnels engagés aux côtés de l'IAE : banques et acteurs industriels, etc.
- Obtention d'un diplôme académique.

Informations pratiques

Pour travailler sur les contenus de la formation, vous devez venir avec un ordinateur portable d'une configuration suffisante (modèle récent).

Avec votre inscription à l'Upec, vous bénéficiez de tous les avantages offerts par le statut d'étudiant : accès aux ressources numériques, accès à la bibliothèque, CROUS, etc.

En cas de problème avant ou pendant la formation, contacter la formation :

N° téléphone / adresse mail

IAE Gustave Eiffel

4 route de Choisy, 94000 Créteil

Accès : métro ligne 8 (arrêt Créteil Université) ; bus TVM (arrêt Créteil Université)

Programme de la formation / référentiel d'activités et de certification

Unités d'enseignement et matières	Volume horaire (présentiel)	Coefficient (ECTS)	Modules du référentiel ANSSI SecnumEdu-FC inclus dans les unités d'enseignement
UE 1 : Comprendre le contexte de la cybersécurité • ECUE 1.1 : Éléments de contexte sur l'informatique et les systèmes d'information *(en option)* • ECUE 1.2 : Cybersécurité : les enjeux, les menaces, les risques, les métiers	**36h** 24h 12h	**2**	Module 1 – Cybersécurité : notions de bases, enjeux et droit commun
UE 2 : Identifier et gérer les risques	**12h**	**1**	
UE 3 : Définir et organiser la sécurité du SI • ECUE 3.1 : Politique de sécurité, Principe de SMSI • ECUE 3.2 : Audit de sécurité • ECUE 3.3 : Intégrer la sécurité dans les projets, sensibiliser et former, sécuriser les identités • ECUE 3.4 : Préparer et gérer les crises, assurer la continuité, surveiller l'activité	**48h** 12h 12h 12h 12h	**3**	Module 2 – L'hygiène informatique pour les utilisateurs Module 3 – Gestion et organisation de la cybersécurité Module 5 – Administration sécurisée du SI interne d'une entreprise Module 6 – La cybersécurité des entreprises ayant externalisé tout ou partie de leur SI
UE 4 : Intégrer l'environnement juridique, règlementaire et normatif	**12h**	**1**	Module 4 – Protection de l'innovation et cybersécurité
UE 5 : Mettre en place la sécurité technique du SI	**12h**	**1**	Module 7 – Sécurité des sites internet gérés en interne
UE 6 : Mémoire de fin de formation	**6h**	**1**	

Référentiel d'activités		Référentiel de certification	
Domaines d'activités	**Compétences associées**	**Résultats attendus observables et/ou mesurables**	**Critères, conditions d'évaluation**
1- Comprendre le contexte de la cybersécurité	1.1- Connaître les éléments de définition de la cybersécurité (enjeux, besoin, métiers, composants, risques, etc.) 1.2- Connaître les différents types d'attaque. 1.3- Connaître les activités et métiers de la cybersécurité.	1.1 à 1.3 - Connaissances attestées par les réponses à un QCM sur l'ensemble des éléments abordés.	1.1 à 1.3 - Validation du QCM avec au moins 85% de bonnes réponses.
2- Identifier et gérer les risques	2.1- Connaître les principaux risques. 2.2- Analyser les risques. 2.3- Traiter les risques et construire des plans d'actions.	2.1 - Connaissances attestées par les réponses à un QCM sur l'ensemble des éléments abordés. 2.2 à 2.3 – Rédaction d'un micro-mémoire d'étude de cas sur un cas d'école ou sur l'activité professionnelle.	2.1 - Validation du QCM avec au moins 85% de bonnes réponses. 2.2 à 2.3 – Micro-mémoire conforme aux attentes.
3- Définir et organiser la sécurité du SI	3.1- Définir une politique de sécurité. 3.2- Mener ou commanditer un audit de sécurité. 3.3- Intégrer la sécurité dans la conception et la réalisation du SI. 3.4- Sensibiliser et former les collaborateurs. 3.5- Préparer la gestion des crises, gérer les crises. 3.6- Sécuriser les identités. 3.7- Sécuriser l'infrastructure. 3.8- Surveiller l'activité.	3.1 à 3.8 - Rédaction d'un micro-mémoire d'étude de cas sur un cas d'école ou sur l'activité professionnelle.	3.1 à 3.8 - Micro-mémoire conforme aux attentes.
4- Intégrer l'environnement juridique, réglementaire et normatif	4.1- Connaître l'environnement normatif (COBIT, ITIL, ISO, etc.) 4.2- Connaître l'environnement législatif (LPM, NIS, etc.) 4.3- Connaître l'environnement règlementaire et ses conséquences (CNIL, RGPD).	4.1 à 4.3 - Connaissances attestées par les réponses à un QCM sur l'ensemble des éléments abordés.	4.1 à 4.3 - Validation du QCM avec au moins 85% de bonnes réponses.
5- Mettre en place la sécurité technique du SI	5.1- Sécuriser l'infrastructure réseau. 5.2- Sécuriser l'infrastructure logicielle (OS, données, etc.) 5.3- Sécuriser le site web. 5.4- Utiliser les outils de la sécurité. 5.5- Utiliser la cryptologie.	5.1 à 5.5 - Rédaction d'un micro-mémoire d'étude de cas sur un cas d'école ou sur l'activité professionnelle.	5.1 à 5.5 - Micro-mémoire conforme aux attentes.

Descriptif des modules d'enseignement

ECUE 1.2 : Cybersécurité : les enjeux, les menaces, les risques, les métiers (12h)

Objectifs	**Compétences et connaissances**
Connaître les éléments de contexte de la cybersécurité : enjeux, besoins, métiers, compétences, risques, attaques, etc.	1.1- Connaître les éléments de définition de la cybersécurité (enjeux, besoin, métiers, composants, risques, etc.) 1.2- Connaître les différents types d'attaque. 1.3- Connaître les activités et métiers de la cybersécurité.

Contenu

- Éléments de définition de la cybersécurité :
  - *Notions de vulnérabilité / menaces / attaques.*
  - *Les 5 composantes du SI : réseaux, OS, serveurs et postes de travail, applications et… les utilisateurs.*
  - *Sécurité et sûreté / la sureté de fonctionnement*
  - *Quelques exemples « historiques » d'accidents de SI*
  - *Les grands acteurs de la sécurité des SI : constructeurs, éditeurs, gouvernements*
  - *Les OIV (Opérateurs d'Importance Vitale) et les enjeux gouvernementaux.*
  - *La défense en profondeur*
  - *Le service de l'information stratégique et sécurité économiques (SISSE)*
- Les différents types d'attaque :
  - *La guerre de l'information, intelligence et veille économique*
  - *L'espionnage industriel et la fuite d'information (Quelques grands exemples historiques)*
  - *Les motivations des attaques*
  - *Les différentes attaques : rançongiciels, virus, ver, trojans, rootkits, malwares, backdoor, spyware, keylogger, ….*
  - *Décodage des attaques récentes*
  - *L'ingénierie sociale*
- Les activités et métiers de la cybersécurité :
  - *Les métiers et fonctions sensibles de l'entreprise*
  - *Le RSSI, chef d'orchestre de la sécurité*
  - *Le Risk Manager, l'administrateur de la sécurité,l'auditeur : les fonctions d'inspection / contrôle / audit et conseil*
  - *Le CIL (CNIL), le DPO (RGPD)*
  - *Les « asset owners » ou propriétaires des données.*

Évaluation

- Connaissances attestées par les réponses à un QCM sur l'ensemble des éléments abordés.
- Validation du QCM avec au moins 85% de bonnes réponses.

Supports / outils / bibliographie

- Makhlouf, A., Hennion, R. (2018), Cybersécurité: Un ouvrage unique pour les managers, Eyrolles.
- Boyer, B. (2015), Dictionnaire de la Cybersécurité et des Réseaux, Nuvis.
- Debize, T. (2016), Sécurité informatique: Pour les DSI, RSSI et administrateurs, Eyrolles.
- Arpagian, N. (2015), La cybersécurité, Presses Universitaires de France.
- Foray, B. (2011), La fonction RSSI - Guide des pratiques et retours d'expérience, Dunod.
- Flaus, J.-M. (2019), Cybersécurité des systèmes industriels, ISTE Editions.

UE 2 : Identifier et gérer les risques (12h)

Objectifs	**Compétences et connaissances**
Être capable d'identifier les risques qui pèsent sur une activité ou un organisme et de construire une réponse globale à ces risques.	2.1- Connaître les principaux risques. 2.2- Analyser les risques. 2.3- Traiter les risques et construire des plans d'actions.

Contenu

- Les principaux risques :
  - *Les besoins de sécurité*
  - *D I C : Disponibilité, Intégrité et Confidentialité + preuve et traçabilité*
  - *Risques et menaces : accident, erreur, malveillance*
  - *La continuité d'activité*
- L'analyse des risques :
  - *Les risques opérationnels / physiques / logiques*
  - *Les risques liés aux technologies : cloud, big data, transactions financières, systèmes embarqués*
  - *Les risques liés aux comportements : BYOD, e-paiement, nomadisme, le risque social*
  - *Les risques humains : phishing, hoax, spam, ...*
  - *Les caractéristiques du risque : potentialité / impact / gravité*
  - *Le point de vue des assureurs*
  - *Une base de connaissance des menaces et des vulnérabilités spécifiques*
  - *L'analyse de risque dans le cadre de l'ISO27001 - L'approche PDCA*
- Le traitement des risques et la construction des plans d'actions :
  - *La réponse : prévention / protection / report du risque / externalisation*
  - *Le traitement des risques et les bonnes pratiques*
  - *Les méthodes et référentiels : Marion, FEROS, EBIOS, MEHARI*
  - *L'élaboration d'un plan d'action (travail pratique sur un cas)*
  - *L'assurance ou externalisation du risque résiduel*

Évaluation

- Connaissances attestées par les réponses à un QCM pour l'item 2.1, rédaction d'un micro-mémoire d'étude de cas sur un cas d'école ou sur l'activité professionnelle pour les items 2.2 et 2.3.
- Validation du QCM avec au moins 85% de bonnes réponses et conformité du micro-mémoire aux attentes.

Supports / outils / bibliographie

- Documents des formateurs
- Documents ANSSI (Guide d'hygiène informatique)
- Arduin, P.-E. (2018), La menace intérieure, ISTE Editions.
- Stamboliyska, R. (2017), La face cachée d'internet : hackers, dark net..., Larousse.
- Planche, A. (2018), La sécurité informatique en mode projet - Organisez la sécurité du SI de votre entreprise, Editions ENI.

ECUE 3.1 : Politique de sécurité, Principe de SMSI (12h)	
Objectifs Déployer les processus de maîtrise de la sécurité dans l'Entreprise	**Compétences et connaissances** 3.1- Définir une politique de sécurité.

Contenu

- Politique générale et politique de sécurité des systèmes d'information (PSSI)
- Directives techniques et organisationnelles
- Déclinaisons opérationnelles
- Système de Management de la Sécurité
- Norme ISO27001
- Guide de bonne pratique 27002

Évaluation

- QCM 27001
- Micro-mémoire sur un cas pratique de mise en place d'un SMSI.
- Validation du QCM avec au moins 85% de bonnes réponses et conformité du micro-mémoire aux attentes.

Supports / outils / bibliographie

- Documents des formateurs
- Quizz
- Normes ISO
- Ghrab, M. I. (2018), Audit de la sécurité des systèmes d'information, Univ Européenne.
- Bennasar, M. (2010), Plan de continuité d'activité et système d'information Vers l'entreprise résiliente, Dunod.
- Blokdyk, G. (2017), Computer emergency response team: Everything You Need to Know, CreateSpace Independent Publishing Platform.
- Liorrier, M., Bilet, V. (2018), Survivre à une cyberattaque: Anticiper, prévenir, réagir, VA press.

ECUE 3.2 : Audit de sécurité (12h)	
Objectifs Savoir commanditer ou participer à un audit de sécurité.	**Compétences et connaissances** 3.2- Mener ou commanditer un audit de sécurité.

Contenu

- La démarche de contrôle : plan, référentiels, déroulement, cadrage, investigations, restitution et le plan de remédiation
- Les méthodes d'investigation : objectifs, types et natures d'investigations, entretiens, gestion de la preuve
- Le rapport : quantitatif et qualitatif
- Le plan de recommandations et le suivi des actions
- Le métier d'auditeur et les acteurs du marché

Évaluation

- QCM Certified Information Systems Auditor (CISA)
- Micro-mémoire sur un cas pratique de relevé de constats.
- Validation du QCM avec au moins 85% de bonnes réponses et conformité du micro-mémoire aux attentes.

Supports / outils / bibliographie

- Documents des formateurs
- Quizz
- Normes ISO 19011
- Ghrab, M. I. (2018), Audit de la sécurité des systèmes d'information, Univ Européenne.
- Bennasar, M. (2010), Plan de continuité d'activité et système d'information Vers l'entreprise résiliente, Dunod.
- Blokdyk, G. (2017), Computer emergency response team: Everything You Need to Know, CreateSpace Independent Publishing Platform.
- Liorrier, M., Bilet, V. (2018), Survivre à une cyberattaque: Anticiper, prévenir, réagir, VA press.

ECUE 3.3 : Intégrer la sécurité dans les projets, sensibiliser et former, sécuriser les identités (12h)

Objectifs	**Compétences et connaissances**
Prendre en compte la sécurité informatique tout au long des projets Sensibiliser les utilisateurs et maîtriser leurs accès	3.3- Intégrer la sécurité dans la conception et la réalisation du SI. 3.4- Sensibiliser et former les collaborateurs. 3.6- Sécuriser les identités.

Contenu

- Intégrer la sécurité dans la conception et la réalisation du SI :
  - *La spécification de mesures de sécurité : le « PAS projet »*
  - *Architecture sécurisée*
  - *La sécurité des développements : Standard ISO 27034-1, OWASP, les recommandations de l'ANSSI*
  - *Tests et recette de sécurité*
  - *Sécurisation des prestations externalisées : clauses contractuelles, PAS*
  - Traitement et recyclage des déchets d'équipements électriques et électroniques (DEEE)
- Sensibiliser et former les collaborateurs :
  - *Une composante essentielle de la sécurité des SI : les RH*
  - *Le public : qui, quoi, comment,... et pourquoi*
  - *La stratégie RH dans ce domaine de la sécurité*
  - *Ethique et déontologie professionnelle*
  - *la « e-réputation »*
  - *La charte de sécurité, annexe du RI et du contrat de travail (étude de document)*
  - *Présentation d'une campagne de sensibilisation des utilisateurs, sur une base de série télévisée (dessins animés)*
- Sécuriser les identités et les acces :
  - *Identification, authentification*
  - *Sécurité des mots de passes (Unix / Windows)*
  - *Principe du mot de passe unique (SSO)*
  - *Annuaire (LDAP, ...)*
  - *Biométrie*

Évaluation

- Rédaction d'un micro-mémoire d'étude de cas sur un cas d'école ou sur l'activité professionnelle.
- Conformité du micro-mémoire aux attentes.

Supports / outils / bibliographie

- Documents des formateurs
- Quizz
- Films
- Ghrab, M. I. (2018), Audit de la sécurité des systèmes d'information, Univ Européenne.
- Bennasar, M. (2010), Plan de continuité d'activité et système d'information Vers l'entreprise résiliente, Dunod.
- Blokdyk, G. (2017), Computer emergency response team: Everything You Need to Know, CreateSpace Independent Publishing Platform.
- Liorrier, M., Bilet, V. (2018), Survivre à une cyberattaque: Anticiper, prévenir, réagir, VA press.

ECUE 3.4: Préparer et gérer les crises, assurer la continuité, surveiller l'activité (12h)

Objectifs	**Compétences et connaissances**
Maitriser les mesures permettant d'assurer la surveillance des S.I et leur hébergement Savoir réagir en cas d'incident	3.5- Préparer la gestion des crises, gérer les crises. 3.7- Sécuriser l'infrastructure. 3.8- Surveiller l'activité

Contenu

- Préparer la gestion des crises, gérer les crises :
  - *Le management de crise : quelques exemples récents de crises SI*
  - *Les types de crises et leurs conséquences*
  - *La préparation, donc l'anticipation des crises*
  - *Plans de sauvegarde / secours / repli*
  - *Les plans de reprise d'activité (PRA) et plans de continuité d'activité (PCA)*
  - *Le plan de gestion de crise (élaboration d'un exemple pratique) ?*
- Sécuriser l'infrastructure d'hébergement :
  - *Sécurité et exploitation : l'hébergement sécurisé*
  - *Le Cloud et la localisation des données*
  - *Visite (si possible) d'un grand DataCenter*
- Surveiller l'activité :
  - *Les systèmes de surveillance : Security Operations Center (SOC), Network Operations Center (NOC)*
  - *Le Computer Emergency Response Team (CERT), le Prestataire de Réponse à Incidents de Sécurité (PRIS)*
  - *Les systèmes de surveillance : SOC, NOC*
  - *Le CERT, le PRIS*

Évaluation

- Rédaction d'un micro-mémoire d'étude de cas sur un cas d'école ou sur l'activité professionnelle – préparation d'un PCA simple.
- Conformité du micro-mémoire aux attentes.

Supports / outils / bibliographie

- Documents des formateurs
- Quizz
- Ghrab, M. I. (2018), Audit de la sécurité des systèmes d'information, Univ Européenne.
- Bennasar, M. (2010), Plan de continuité d'activité et système d'information Vers l'entreprise résiliente, Dunod.
- Blokdyk, G. (2017), Computer emergency response team: Everything You Need to Know, CreateSpace Independent Publishing Platform.
- Liorrier, M., Bilet, V. (2018), Survivre à une cyberattaque: Anticiper, prévenir, réagir, VA press.

UE 4 : Intégrer l'environnement juridique, réglementaire et normatif (12h)	
Objectifs Positionner correctement son activité et la sécurité du SI dans l'environnement juridique, règlementaire et normatif en vigueur.	**Compétences et connaissances** 4.1- Connaître l'environnement normatif (COBIT, ITIL, ISO, etc.) 4.2- Connaître l'environnement législatif (LPM, NIS, etc.) 4.3- Connaître l'environnement règlementaire et ses conséquences (CNIL, RGPD).

Contenu

- L'environnement normatif (COBIT, ITIL, ISO, etc.) :
  - *Les normes ISO 27000*
  - *ITIL et les bonnes pratiques*
  - *OWASP (Open Web Application Security Project)*
- L'environnement législatif (LPM, NIS, etc.) :
  - *Les lois françaises sur la propriété intellectuelle*
  - *L'application du code du travail à la sécurité des SI*
  - *Les lois numériques et financières*
  - *Les réglementations internationales : SOX, COSO*
- L'environnement règlementaire et ses conséquences (CNIL, RGPD) :
  - *Un environnement français et européen.*
  - *Les grands principes de la CNIL – Rôle , pouvoir et consultation*
  - *Les obligations liées au RGPD et les sanctions possibles*
- Les modalités de protection du patrimoine immatériel de l'entreprise
  - Protection du potentiel scientifique et technique de la Nation (PPST, Zone à régime restrictif ZRR)
  - Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation

Évaluation

- Connaissances attestées par les réponses à un QCM sur l'ensemble des éléments abordés.
- Validation du QCM avec au moins 85% de bonnes réponses.

Supports / outils / bibliographie

- Banck, A. (2019), RGPD : la protection des données à caractère personnel, Gualino.
- Guillemain, M. (2019), L'application du RGPD par les organisations, EMS Editions.
- Fernandez-Toro, A. (2018), Management de la sécurité de l'information : Présentation générale de l'ISO 27001 et de ses normes associées - Une référence opérationnelle pour le RSSI, Eyrolles.
- Ministère des Armées (2018), Loi de programmation militaire 2019-2025, https://www.defense.gouv.fr/actualites/articles/le-president-de-la-republique-promulgue-la-loi-de-programmation-militaire-2019-2025.

UE 5 : Mettre en place la sécurité technique du SI (12h)	
Objectifs Agir concrètement pour la sécurité technique du SI en utilisant les outils et démarches appropriées.	**Compétences et connaissances** 5.1- Sécuriser l'infrastructure réseau. 5.2- Sécuriser l'infrastructure logicielle (OS, données, etc.) 5.3- Sécuriser le site web. 5.4- Utiliser les outils de la sécurité. 5.5- Utiliser la cryptologie.

Contenu

- Sécuriser l'infrastructure réseau :
  - *La sécurité des réseaux (LAN / WAN) et les protocoles réseaux.*
  - *La sécurité de la voix sur IP.*
  - *Sécurisation des réseaux wi-fi*
  - *Sécurité du RFID et IoT*
  - *Les protocoles sécurisés : VPN, SSL, SSH, IPSEC,*
- Sécuriser l'infrastructure logicielle et matérielle :
  - *Operating System*
  - *Bases de données*
  - *Durcissement des configurations*
- Sécuriser les applications web :
  - *OWASP (Open Web Application Security Project)*
- Utiliser les outils de la sécurité :
  - *Anti virus / Anti spams*
  - *Filtrage internet*
  - *Firewall*
  - *Les outils d'analyse et d'audits techniques.*
  - *Sondes et Détection d'intrusion, analyse de trafic*
  - *- Certains modules pourront être en anglais, présentés par des éditeurs de ces outils.*
- Utiliser la cryptologie :
  - *Introduction et enjeux des deux types de cryptographie.*
  - *Protocoles d'échanges de clés et clés de groupes.*
  - *Signature numérique, Identification et authentifications.*
  - *Infrastructure à clé publique (PKI).*

Évaluation

- Rédaction d'un micro-mémoire d'étude de cas sur un cas d'école ou sur l'activité professionnelle.
- Conformité du micro-mémoire aux attentes.

Supports / outils / bibliographie

- Ghernaouti, S. (2016), Cybersécurité - Sécurité informatique et réseaux, Dunod.
- Engebretson, P. (2017), Les bases du hacking, Pearson France.
- Pérez, A. (2014), La sécurité des réseaux, ISTE Editions.
- ACISSI (2017), Sécurité informatique - Ethical Hacking : Apprendre l'attaque pour mieux se défendre, Editions ENI.

Référentiel de compétences par UE

UE 1 : Comprendre le contexte de la cybersécurité (36h)

- Connaître les éléments de définition de la cybersécurité (enjeux, besoin, métiers, composants, risques, etc.)
- Connaître les différents types d'attaque.
- Connaître les activités et métiers de la cybersécurité.

UE 2 : Identifier et gérer les risques (12h)

- Connaître les principaux risques.
- Analyser les risques.
- Traiter les risques et construire des plans d'actions.

UE 3 : Définir et organiser la sécurité du SI (36h)

- Définir une politique de sécurité, comprendre le principe du SMSI.
- Commanditer ou participer à un audit de sécurité.
- Intégrer la sécurité dans la conception et la réalisation du SI.
- Sensibiliser et former les collaborateurs.
- Préparer la gestion des crises, gérer les crises.
- Sécuriser les identités.
- Sécuriser l'infrastructure.
- Surveiller l'activité.

UE 4 : Intégrer l'environnement juridique, réglementaire et normatif (12h)

- Connaître l'environnement normatif (COBIT, ITIL, ISO, etc.)
- Connaître l'environnement législatif (LPM, NIS, etc.)
- Connaître l'environnement règlementaire et ses conséquences (CNIL, RGPD).

UE 5 : Mettre en place la sécurité technique du SI (12h)

- Sécuriser l'infrastructure réseau.
- Sécuriser l'infrastructure logicielle (OS, données, etc.)
- Sécuriser le site web.
- Utiliser les outils de la sécurité.
- Utiliser la cryptologie.

UE 6 : Mémoire de fin de formation

Les compétences validées par l'UE 6 sont les mêmes que celles des UE 1 à 5 dans le cadre d'une analyse critique d'une mise en situation professionnelle donnant lieu à la rédaction d'un mémoire et à une soutenance.