BTS SIO 2020 - Document d'accompagnement pédagogique

Ce document d'accompagnement pédagogique a été rédigé par les membres de la commission en charge de la rédaction du référentiel. Il a été soumis à la consultation des enseignants, cette version tient compte des avis et remarques issus de cette consultation.

Sommaire

Version du 30 octobre 2020

Table des matières

Introduction

L'évolution du référentiel du BTS Services informatiques aux organisations a été réalisée à la demande de la 16ème commission professionnelle consultative (CPC) du ministère de l'éducation nationale. Le fait que ce diplôme soit préparé en formation professionnelle nécessitait de le réviser pour suivre les préconisations d'organisation des diplômes en blocs de compétences issues de la loi sur la formation professionnelle de 2014 (réaffirmées par la loi pour la liberté de choisir son avenir professionnel de 2018).

L'occasion qui était donnée de revoir le contenu du diplôme a permis de prendre en compte de nouvelles exigences pour exercer le métier de la personne titulaire du diplôme.

Une évolution du référentiel pour une construction en blocs de compétences

La loi de mars 2014 relative à la formation professionnelle[1] institue le compte personnel de formation permettant aux salariés et demandeurs d'emploi de bénéficier de formations lorsque celles-ci sont inscrites au registre national des certifications professionnelles (RNCP).

Les BTS sont inscrits au RNCP mais pour être accessibles via le compte personnel de formation (CPF), il est nécessaire qu'ils soient organisés en blocs de compétences indépendants permettant aux salariés ou demandeurs d'emploi de mobiliser leurs droits acquis dans le cadre du CPF pour la préparation d'un bloc dans une approche progressive de préparation au diplôme ou dans un souci d'acquisition des compétences spécifiques au bloc.

Le Copanef[2] propose la définition suivante « *Les blocs de compétences se définissent comme des éléments identifiés d'une certification professionnelle s'entendant comme un ensemble homogène et cohérent de compétences. Ces compétences doivent être évaluées, validées et tracées. Sous ces conditions, elles constituent une partie identifiée de la certification professionnelle.*
Le « bloc de compétences » s'apparente à une activité ou un domaine d'activité au sein d'une certification professionnelle. »[3]

Ainsi, chaque domaine d'activité défini dans le référentiel des activités professionnelles correspond à un bloc de compétences du référentiel de certification et à une épreuve.
La construction du diplôme en blocs de compétences répond donc à l'aspiration d'offrir une variété de parcours pour obtenir la qualification : préparer le diplôme en formation initiale, compléter une obtention partielle du diplôme par la formation à un ou plusieurs blocs, préparer un bloc du diplôme.

Une évolution du référentiel pour de nouvelles exigences professionnelles

Les organisations de toute taille ont besoin d'être accompagnées pour répondre aux besoins stratégiques, humains, organisationnels et technologiques de leur transformation numérique. Les informaticiens contribuent à cette transformation en mettant en œuvre des solutions numériques adaptées à la stratégie des organisations mais aussi en étant auprès des utilisateurs pour les aider dans l'appropriation des services informatiques.

Les nouvelles technologies (réseaux sociaux, mobilité, analyse de données, Cloud ou encore intelligence artificielle) permettent de développer de nouveaux services qui intègrent les processus des organisations et pour lesquelles les compétences informatiques évoluent. La préoccupation de la sécurité des systèmes informatiques est omniprésente dans la mise en œuvre des services.

Ainsi le référentiel du BTS Services informatiques a évolué pour prendre en compte ces transformations et notamment les fonctions support et cybersécurité ont été renforcées. Les connaissances managériales, juridiques et économiques propres à l'exercice du métier sont intégrées

[1] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028683576&categorieLien=id
[2] Comité paritaire interprofessionnel national pour l'emploi et la formation
[3] Extrait du document www.fpspp.org/portail/.../definition-blocs-de-competences-bureau-9juin2015.docx

dans la définition des blocs professionnels car elles font partie intégrante de la construction des compétences.

La préparation au diplôme en formation initiale et l'approche blocs de compétences

En formation initiale, il s'agit de permettre aux apprenants d'obtenir le diplôme dans sa totalité, qui ne se limite pas à la somme des blocs. Par ailleurs, la définition des compétences fait appel à des connaissances qui peuvent être aussi présentes dans un autre bloc.

Plusieurs dispositifs dans la grille horaire de formation initiale contribuent à installer de la transversalité entre les blocs :

- un horaire spécifique d'ateliers de professionnalisation qui permet de travailler en mode projet et de convoquer des compétences de différents blocs ;
- un horaire spécifique de culture économique, juridique et managériale qui s'articule avec les enseignements de blocs professionnels et d'ateliers de professionnalisation pour mobiliser les connaissances managériales, juridiques et économiques propres à l'exercice du métier ;
- des stages en milieu professionnel.

Organisation du référentiel

Le référentiel est en fait multiple et l'arrêté du 29 avril 2019 présente en fait plusieurs référentiels en annexe.

Référentiel d'activités professionnelles
Le référentiel d'activités professionnelles permet de décrire les activités du métier visé par le diplôme. La modélisation du métier qui en est faite implique de faire des choix. Ces choix ont été guidés d'une part par l'évolution du métier, d'autre part par l'écriture en blocs de compétences.

Référentiel de compétences
Le référentiel de compétences décrit les compétences professionnelles, les indicateurs de performance et les savoirs associés aux activités décrites dans le référentiel des activités professionnelles.

Les règles d'écriture
Plusieurs règles d'écriture ont été utilisées :

- chaque bloc correspond à un domaine d'activités ;
- chaque activité est associée à une compétence ;
- chaque compétence est explicitée par différents éléments comme le montre l'extrait du référentiel ci-dessous.

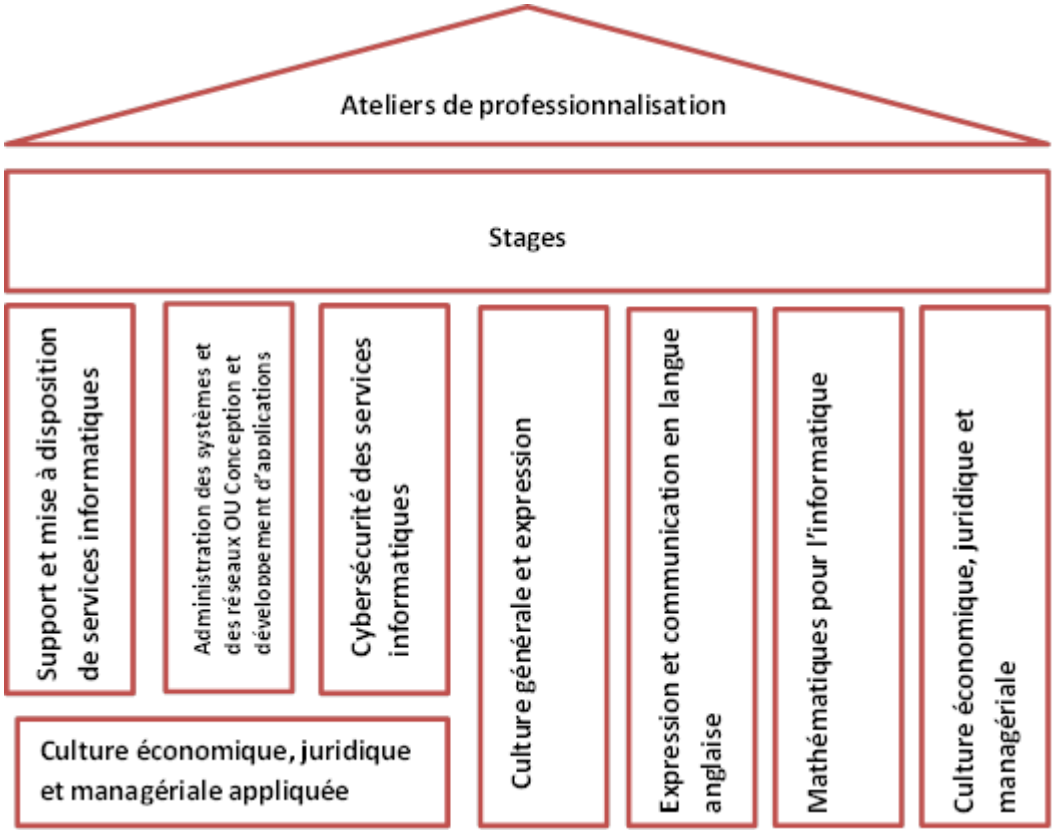
Les éléments décrivant un bloc de compétences
Afin de décrire les compétences propres au métier, plusieurs éléments ont été utiles à préciser :

- le contexte décrit les exigences associées à la conduite de l'activité ;
- les ressources disponibles pour mener l'activité ;
- le degré d'autonomie et les responsabilités exercées ;
- La description de chaque compétence du bloc en trois colonnes comme ci-dessous.

Référentiel d'évaluation
Il décrit les épreuves certificatives du diplôme.
L'annexe II.E décrit l'environnement technologique mobilisé pour la certification des blocs professionnels. Cet environnement est également mobilisé en formation.

Présentation synthétique de la structure de la formation

Le tableau ci-dessous illustre la construction du diplôme en blocs de compétences :



À propos de l'organisation des enseignements

La structuration du diplôme en blocs de compétences implique une nouvelle approche de la formation. Chaque bloc correspondant à une finalité métier bien identifiée, il est important que les étudiants, les apprentis, aient une bonne connaissance des attentes, des missions confiées et des responsabilités associés à chacune de ces finalités. A l'issue de la formation, il s'agit pour chaque étudiant ou apprenti d'être prêt à débuter dans le métier qui correspond aux blocs de compétences pour lesquels la certification a été obtenue.

Pour le BTS SIO ce sont typiquement les métiers suivants : support et mise à disposition de services informatiques (options SISR et SLAM) ; administration systèmes et réseau (option SISR) ; développement d'applications (option SLAM) ; cybersécurité (options SISR et SLAM).

Le précédent référentiel (introduit en 2011) organisait principalement les enseignements autour de modules (SI1, SI2, SISR1, SLAM1,..), chaque module correspondant à une période et à un objet d'enseignement. Le nouveau référentiel n'impose pas une telle organisation, il précise uniquement les compétences à travailler pour se former à différentes finalités métier (les blocs de compétences). Dans un centre de formation, il revient à chaque équipe d'enseignants, de formateurs, de décider de la façon d'organiser les enseignements en répartissant l'horaire disponible et les compétences à travailler.
Ce choix à faire est nouveau, il doit tenir compte de différents facteurs.

Les choix d'organisation des enseignements peuvent être très variables en fonction de la modalité choisie : en formation initiale sous statut scolaire, en formation initiale en apprentissage, en formation continue. Elle est aussi fonction de la complétude recherchée par les apprenants : le diplôme dans son ensemble ou bien un ou plusieurs blocs de compétences seulement.

La distribution des compétences à travailler entre les enseignants / formateurs au cours de chaque semestre est un exercice indispensable qui nécessite une bonne coordination au sein de l'équipe pédagogique en charge de la formation. Cette distribution doit tenir compte au mieux des quotités de service, des compétences et appétences des enseignants et des ressources disponibles.

Au cours de la formation, un ou plusieurs enseignants peuvent prendre en charge tout ou partie des compétences d'un même bloc ou de différents blocs. Cette répartition des compétences entre enseignants peut aussi tenir compte d'un degré d'approfondissement dans l'acquisition des compétences en fonction de l'option du diplôme choisie : une initiation en début de première année, une consolidation progressive, un approfondissement en seconde année.

Même si l'énoncé des compétences dans le référentiel ne traduit pas une progression pédagogique, certaines compétences globales ou détaillées peuvent être en dépendance les unes par rapport aux autres (il est logique de travailler d'abord l'une avant d'autres) ; alors que d'autres compétences peuvent être travaillées en parallèle. Il convient de tenir compte de ces relations de dépendances dans l'attribution entre les enseignants des compétences à travailler avec les étudiants.

Propositions de scénarios d'organisation des enseignements

Dans l'hypothèse d'une formation initiale visant l'acquisition complète du diplôme sur deux années, le présent guide d'accompagnement propose une partition des compétences à travailler sur les différents semestres de la formation (voir l'annexe 1).

Les quelques principes suivants ont été retenus pour élaborer cette proposition :

- L'existence des deux options SISR et SLAM qui s'adressent à un public différent ;
- Le fait que ces options peuvent correspondre à des compétences et/ou à des appétences spécifiques des enseignants ;
- La nécessité probable de scinder le volume horaire d'un bloc sur différents enseignants ;
- La recherche d'ensembles cohérents de compétences à travailler avec un même enseignant ;
- Le fait que certaines compétences peuvent logiquement commencer à être travaillées avant d'autres.

Afin de clarifier ces propositions, les blocs et les compétences ont été numérotés, ainsi la première compétence globale du bloc 1 est numérotée B1.1. Les compétences détaillées n'ont pas été numérotées.

De même, les ensembles de compétences pouvant constituer des unités d'enseignement sont identifiés selon qu'ils s'adressent à tous les étudiants car faisant partie du tronc commun de la formation (TC1, TC2, etc.) ou qu'ils s'adressent uniquement aux étudiants préparant une des deux options (R pour SISR et D pour SLAM). Cette numérotation n'a rien d'officiel ni de contraignant, elle permet seulement de désigner plus aisément dans le présent document les ensembles de compétences.

L'horaire global assigné à un bloc pour un semestre donné est naturellement respecté. Les volumes horaires hebdomadaires associés à ces ensembles sont purement indicatifs même s'ils ont été réfléchis pour être réalistes.

Un même enseignant peut naturellement prendre en charge plusieurs ensembles de compétences.

Dans la majorité des cas, les compétences rassemblées appartiennent à un seul et même bloc. Parfois cependant, certains ensembles rassemblent des compétences issues de différents blocs, ceci est notamment le cas des compétences du bloc 3-Cybersécurité qui peuvent rejoindre celles des autres blocs.

Il est important de noter que **ces propositions d'organisation des enseignements n'ont aucun caractère contraignant**, chaque équipe fera librement ses choix en tenant compte des différents paramètres qui ont été énoncés plus haut.

Bloc 1 - Support et mise à disposition des services informatiques

Rappel du référentiel des activités professionnelles (RAP)

La personne titulaire du diplôme exerce des activités de support et de mise à disposition de services informatiques pour répondre aux besoins d'une organisation cliente. Elle travaille pour le compte de l'entité informatique interne d'une organisation cliente, d'une entreprise de services du numérique, d'une société de conseil en technologies ou encore d'un éditeur de logiciels informatiques.

Les contextes de travail, ouverts et évolutifs, nécessitent de mener une veille informationnelle et technologique et de prendre en compte leurs aspects humains, technologiques, organisationnels, économiques et juridiques.
La personne titulaire du diplôme intervient dans un environnement technologique opérationnel.

Présentation

Le développement des compétences de ce bloc apporte aux étudiants et aux apprentis une première initiation à l'informatique d'entreprise en ayant affaire à ses différentes composantes : les utilisateurs, les équipements, les services réseaux et applicatifs. Plus prosaïquement, il s'agit aussi de leur permettre de choisir leur option (SISR ou SLAM) à l'issue du premier semestre.

Pour être en capacité de prendre en charge les demandes d'assistance de premier niveau, les étudiants doivent connaître les principes de base qui régissent les réseaux et le développement d'applications. Ce bloc doit leur permettre d'acquérir ces principes. Cette préparation gagnera à prendre appui sur un référentiel de bonnes pratiques de gestion des services informatiques tel que ITIL.

La lecture du référentiel indique que, dans ce bloc, on prépare les étudiants à être à même de répondre aux attentes des utilisateurs ou des clients en s'assurant de la disponibilité des services existants et de la mise à disposition de nouveaux services. Ce rôle consiste à apporter un premier niveau de support informatique aux utilisateurs au sein de l'organisation : bon fonctionnement du poste de travail en réseau, disponibilité des logiciels et des applications, réponses aux demandes d'assistance de premier niveau et orientation des autres demandes pour une prise en charge adaptée, déploiement et configuration d'un nouveau service. Il s'agit également de participer au développement de la présence en ligne de l'organisation.

Cette mission s'exerce dans un périmètre donné en respectant les étapes du processus de prise en compte des demandes d'intervention. Ceci nécessite en premier lieu de prendre le temps de bien écouter et d'interpréter les demandes des utilisateurs et des clients. Il s'agit ensuite de réceptionner ces demandes, de les qualifier, les traiter ou de les relayer vers une personne ou une entité habilitée et compétente. La mission comporte également l'information des utilisateurs et des clients concernant le support et la mise à disposition des services informatiques. Elle implique également de rendre compte de ses activités afin de constituer une documentation.

Ainsi, dans ce bloc, on pourra chercher, le plus souvent possible, à placer les étudiants en situation d'interpréter une demande d'assistance, d'identifier les équipements matériels et logiciels concernés, de définir un niveau de gravité, de prendre en charge la demande ou bien de la relayer en tenant compte du niveau de compétence requis pour la traiter.

L'enseignement de CEJMA doit permettre aux étudiants d'appréhender le contexte économique, juridique et managérial dans lequel s'inscrit l'activité informatique.

Positionnement du bloc 1

Ce bloc est très majoritairement enseigné en début de formation, notamment en première année où il a un double rôle : d'une part, apporter les bases indispensables pour devenir informaticien (en développement d'applications, en architecture systèmes et réseau) et, d'autre part, éclairer le choix d'option que les étudiants doivent faire à la fin du premier semestre.

Ce bloc 1 se prolonge toutefois sur les deux années, avec un volume horaire décroissant, de façon à conforter les compétences acquises en matière de support informatique et d'intégration de service à l'aune des nouvelles méthodes, techniques et outils vus au cours de la formation dans les autres blocs.

Ressources générales

Le métier du support informatique :
https://www.optimadsi.fr/support-et-maintenance/
https://www.youtube.com/watch?v=jsMq3OLgKMs
https://www.youtube.com/watch?v=7_TeLk88vpk
https://www.youtube.com/watch?v=v0xWktnZBho

Centre de services informatiques :
https://fr.wikipedia.org/wiki/Service_support_(ITIL)
https://freshservice.com/fr/it-service-desk-software/

B1.1 Gérer le patrimoine informatique

Cette compétence implique d'amener les étudiants à appréhender tout ou partie des équipements qui constituent le patrimoine informatique d'une organisation (matériels, logiciels, applications, contrats, licences, brevets, etc.). Il ne s'agit pas seulement de connaître le patrimoine informatique de l'organisation mais aussi d'en interpréter le rôle vis à vis des utilisateurs et des clients en tenant compte des aspects juridiques et économiques. Ainsi, il faut être à même de faire le lien entre, d'une part, une demande d'assistance ou de mise à disposition d'un service, et, d'autre part, les équipements, matériels et logiciels, concernés mais aussi les utilisateurs et clients potentiellement impactés.

Semestre 1 (4+6) 150h	**Semestre 2 (2+0+2) 60h**	**Semestres 3 et 4 (2+0+0) 24h +24h**
• Recenser et identifier les ressources numériques • Mettre en place et vérifier les niveaux d'habilitation associés à un service	• Exploiter des référentiels, normes et standards adoptés par le prestataire informatique • Gérer des sauvegardes • *Mettre en place et vérifier les niveaux d'habilitation associés à un service (suite)*	• Vérifier les conditions de la continuité d'un service informatique • Vérifier le respect des règles d'utilisation des ressources numériques
Rappel des savoirs Patrimoine informatique : définition, outils de gestion Système informatique Système d'exploitation : gestion des utilisateurs, habilitations et droits d'accès	**Rappel des savoirs** Typologie et techniques de sauvegarde et de restauration Typologie des supports de sauvegarde Système d'exploitation : gestion des utilisateurs, habilitations et droits d'accès	**Rappel des savoirs** Plans de continuité et de reprise d'activité Disponibilité d'un service informatique : enjeux techniques, économiques et juridiques
Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA		
Variété des acteurs de l'industrie informatique Gestion des actifs informatiques (IT Asset Management) Contrats liés à la gestion du patrimoine informatique Typologie des licences logicielles et modalités de tarification Enjeux techniques et économiques des normes et standards Obligations légales en matière de conservation et d'archivage des données Valeur juridique de la charte informatique Responsabilités du salarié utilisateur de ressources informatiques		

Rappels : indicateurs de performance

- *Le recensement du patrimoine informatique est exhaustif et réalisé au moyen d'un outil de gestion des actifs informatiques.*
- *Les référentiels, normes et standards sont mobilisés de façon pertinente.*
- *Les droits mis en place correspondent aux habilitations des acteurs.*
- *Les conditions de continuité et de reprise d'un service sont vérifiées et les manquements sont signalés.*
- *Les sauvegardes sont réalisées dans les conditions prévues conformément au plan de sauvegarde.*
- *Les restaurations sont testées et opérationnelles.*
- *Les écarts par rapport aux règles d'utilisation des ressources numériques sont détectés et signalés.*

Recenser et identifier les ressources numériques

Explorer le patrimoine informatique d'une petite organisation peut être une façon d'entrer dans la fonction support en prenant connaissance des équipements installés : postes de travail et leurs systèmes d'exploitation, logiciels installés, équipements d'interconnexion (commutateurs, bornes wifi, routeurs, solution d'accès à internet, objets connectés), serveurs et services installés localement ou accessibles à distance.
On pourra étudier progressivement des organisations de plus grande taille disposant d'un patrimoine plus important, plus complexe. Conformément au référentiel, on peut cependant limiter autant que nécessaire le périmètre étudié afin d'adapter la formation aux capacités déjà acquises par les étudiants ainsi qu'aux besoins d'apprentissage.

Mettre en place et vérifier les niveaux d'habilitation associés à un service

Les équipements n'ont de rôle que par les usages qui en sont faits par les utilisateurs et les clients. Les notions d'habilitations et de droits d'accès doivent permettre de repérer qui a besoin de quel service informatique, pour quoi faire, avec quel niveau de disponibilité.

Exploiter des référentiels, normes et standards adoptés par le prestataire informatique

La gestion du patrimoine informatique suppose de mobiliser des normes et des standards afin de favoriser l'interopérabilité entre les diverses ressources informatiques, d'harmoniser les pratiques, et d'améliorer la qualité et la performance des services. Au-delà de ces enjeux techniques, les étudiants seront sensibilisés aux impacts économiques des normes et standards sur l'offre, à la concurrence et à la compétitivité des acteurs du secteur informatique (notion abordée dans le thème 4 question 1 du programme de CEJM).

Gérer des sauvegardes

La gestion des sauvegardes participe de la disponibilité et de la reprise des services après un incident. À travers l'étude des techniques de sauvegarde et de restauration, on amènera les étudiants à avoir un regard vigilant sur la gestion de ces processus pour la sûreté et la sécurité des données de l'organisation.

Vérifier les conditions de la continuité d'un service informatique

Il s'agira ici de sensibiliser les étudiants aux notions de disponibilité, de continuité et de reprise d'activité. À partir d'un plan de continuité, on pourra par exemple amener les étudiants à vérifier que les conditions de celui-ci ont bien été testées et validées.

Vérifier le respect des règles d'utilisation des ressources numériques

Il s'agira également ici de sensibiliser les étudiants sur l'importance de la mise en place de règles d'utilisation des ressources numériques et sur la vigilance à avoir quant à leur compréhension et à leur mise en pratique. Cette compétence appelle un important travail en lien avec CEJMA sur la charte informatique et la responsabilité du salarié comme détaillé plus bas.

Ressources

- https://fr.wikipedia.org/wiki/Gestion_des_identit%C3%A9s_et_des_acc%C3%A8s
- https://www.reseaucerta.org/content/inventaire-et-gestion-parc-informatique
- https://fr.wikipedia.org/wiki/Plan_de_reprise_d%27activit%C3%A9
- https://fr.wikipedia.org/wiki/Plan_de_continuit%C3%A9_d%27activit%C3%A9_(informatique)
- https://fr.wikipedia.org/wiki/Sauvegarde_(informatique)

Apports CEJMA

Dans le cadre de l'enseignement de CEJMA, et en prolongement du thème 1 du programme de CEJM "Comment s'établissent les relations entre l'entreprise et son environnement", il conviendra d'identifier les acteurs du secteur informatique avec lesquels l'organisation est en relation dans le cadre de la gestion de son patrimoine informatique (constructeurs, éditeurs, hébergeurs, ESN etc.) mais aussi les enjeux pour une organisation de la gestion de ses actifs informatiques (IT Asset Management) en repérant les avantages obtenus ainsi que les risques encourus en cas d'une gestion insuffisante ou inexistante.

La gestion du patrimoine informatique implique donc de s'intéresser au contenu des contrats conclus par l'organisation avec ses différents partenaires. L'étude d'extraits de contrats informatiques peut permettre de mettre en évidence les clauses importantes en matière de gestion du patrimoine informatique (ex : clause relative à la garantie, à la durée du contrat, à la limitation de la responsabilité du prestataire, les modalités de rupture du contrat en cas de changement de prestataire ou de ré-internalisation de l'activité informatique etc.). Une attention particulière pourra être portée à la gestion des actifs logiciels (Software Asset Management) dont l'utilisation est encadrée par des contrats de licences logicielles. L'étude comparative d'un contrat de licence libre et d'un contrat de licence propriétaire permettra aux étudiants de cerner les droits accordés aux utilisateurs, les divers modèles de tarification, ainsi que les effets de la clause d'audit de plus en plus présente dans les contrats de licences.

Gérer les sauvegardes, activité essentielle dans la gestion du patrimoine informatique, s'inscrit dans un cadre juridique. Les étudiants seront amenés à repérer les obligations des organisations en matière d'archivage de données (respecter les durées minimales de conservation des données, assurer l'intégrité, la disponibilité, la sécurité, la confidentialité et la traçabilité de ces données) afin de produire une preuve recevable en cas de contentieux. Une attention particulière devra être portée à l'archivage des données à caractère personnel qui fait l'objet du RGPD.

Enfin, la gestion du patrimoine informatique suppose que l'ensemble des utilisateurs respectent les règles d'utilisation des ressources numériques fixées généralement dans une charte informatique dont la valeur juridique dépend des conditions de son élaboration (la charte informatique est étudiée dans le thème 4 question 2 du programme de CEJM). À partir d'exemples de chartes informatiques, les étudiants pourront appréhender le rôle de ce document interne à l'organisation, la portée des règles qui y figurent et comprendre que le non-respect de ces règles engage la responsabilité civile et/ou pénale du salarié.

Ressources CEJMA :

- www.village-justice.com/articles/audit-licence-logiciel-par-editeur-nos-recommandations,30128.html
- www.journaldunet.com/solutions/expert/34438/le-software-asset-management---un-enjeu-majeur-pour-les-entreprises
- www.cigref.fr/sam-software-asset-cloud-management
- www.ivision.fr/pme-pourquoi-effectuer-un-audit-informatique/
- https://eduscol.education.fr/numerique/dossier/archives/metadata/normes-et-standards
- Economie du Numérique et de l'internet, Eric Malin et Thierry Pénard, Edition Vuibert, 2010
- Les contrats du numérique - Philippe Le Tourneau - Edition Dalloz
- Droit et expertise des contrats informatiques - Hubert Bitan - Edition Lamy
- Cyberdroit - le droit à l'épreuve de l'internet - Christiane Féral-Schuhl - Edition Dalloz 2018/2019

B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution

Cette compétence implique d'avoir une bonne connaissance du système informatique de l'organisation cliente. On souhaite ici préparer spécifiquement les étudiants à la prise en compte des demandes d'assistances des utilisateurs et des demandes d'évolution des services informatiques. Ceci nécessite tout d'abord d'apprendre à interpréter une demande : de qui émane-t-elle ? à quel niveau d'habilitation ? quels services sont potentiellement concernés, quels équipements ? Quel niveau de service minimal est attendu et quelles obligations du prestataire en découlent ?

Pour répondre aux incidents et demandes d'évolution, les bases de la programmation, des systèmes et du réseau sont abordées ici. En formation initiale, les étudiants sont amenés à choisir leur spécialité à la fin du premier semestre. Il semble donc pertinent de situer ces apprentissages au cours du premier semestre afin que les étudiants soient en capacité de faire leur choix de spécialité en connaissance de cause.

On pourra privilégier une pédagogie active où les étudiants sont placés en situation de réellement dépanner des utilisateurs ou des clients. Ces situations peuvent être vécues ou observées en entreprise (stage, contrat d'apprentissage), dans les ateliers de professionnalisation, ou bien dans le centre de formation.

Semestre 1 (4+0+6) 150h	Semestre 2 (2+0+2) 60h	Semestres 3 et 4 (2+0+0) 24h +24h = 48h
• Traiter des demandes concernant les services réseau et système, applicatifs • Traiter des demandes concernant les applications	• Collecter, suivre et orienter des demandes • *Traiter des demandes concernant les services réseau et système, applicatifs (suite)* • *Traiter des demandes concernant les applications (suite)*	• *Traiter des demandes concernant les services réseau et système, applicatifs* • *Traiter des demandes concernant les applications (suite)*
Rappel des savoirs Méthodes et outils de diagnostic Bases du réseau : modèles de référence, médias d'interconnexion, protocoles de base et services associés, adressage, nommage, routage, principaux composants matériels, notion de périmètres réseau Principaux composants matériels des équipements utilisateur et des serveurs Système d'exploitation : logiciels des équipements utilisateur et des serveurs, fonctionnalités des systèmes d'exploitation des équipements utilisateur	**Rappel des savoirs** Outils et méthodes de gestion des incidents Méthodologie de repérage de la cause d'un incident, d'une panne Base de connaissances d'un centre d'assistance (helpdesk) Prise de contrôle d'un poste de travail Bases du réseau : modèles de référence, médias d'interconnexion, protocoles de base et services associés, adressage, nommage, routage, principaux composants matériels, notion de	Rappel des savoirs Normes et standards concernant la gestion des configurations et la gestion d'incidents Base de connaissances d'un centre d'assistance (helpdesk) (suite)

et serveurs, virtualisation Bases de la programmation : structures de données et de contrôle, procédures, fonctions, utilisation d'objets Langage de commande d'un système d'exploitation : commandes usuelles (et script)	périmètres réseau (suite)) Bases de la programmation : structures de données et de contrôle, procédures, fonctions, utilisation d'objets (suite) Langage de commande d'un système d'exploitation : (commandes usuelles et) script (suite)	
Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA Entente de niveau de service et contrat d'assistance : obligations et responsabilités		

Rappels : indicateurs de performance

- *En utilisant les outils adaptés, les demandes d'assistance ont été prises en compte, correctement diagnostiquées et leur traitement correspond aux attentes.*
- *La réponse à une demande d'assistance est conforme à la procédure et adaptée à l'utilisateur.*
- *La méthode de diagnostic de résolution d'un incident est adéquate et efficiente.*
- *Une solution à l'incident est trouvée et mise en œuvre.*
- *Le cycle de résolution des demandes respecte les normes et standards du prestataire informatique.*
- *L'utilisation d'un logiciel de gestion de parc et d'incidents est maîtrisée.*
- *Le compte rendu d'intervention est clair et explicite.*
- *La communication écrite et orale est adaptée à l'interlocuteur.*

Traiter des demandes concernant les services réseau et système, applicatifs

Il s'agit ici de donner aux étudiants les notions de base de système et de réseau en prenant appui sur des situations concrètes. Des jeux de rôle peuvent être proposés aux étudiants : certains jouent le rôle d'utilisateurs, d'autres sont en charge du support, d'autres encore introduisent un dysfonctionnement du plus simple (par exemple débrancher l'alimentation de l'imprimante) au moins simple (par exemple doublonner une adresse IP, déboguer un script qui démarre ou arrêter des services). Les interventions correctives ou évolutives sont réalisées sur site ou à distance.

S'il s'agit de prendre en charge une demande d'aide, la réponse doit comporter une explication, éventuellement une démonstration sur poste, voire la rédaction d'un mode d'emploi. Ceci peut permettre de tester la compréhension et le niveau de compétence atteint.

S'il s'agit d'un dysfonctionnement, la réponse apportée implique une recherche méthodique de la ou des causes de l'incident puis une décision de traiter soi-

même la demande ou bien de la relayer auprès de la personne habilitée et la mieux à même de la prendre en charge.

S'il s'agit d'une demande d'évolution d'un service, il convient là aussi de repérer les équipements, les logiciels ou les applications concernés puis de prendre en charge ou de confier le traitement de la demande.

La documentation sur les normes et standards qui font référence au sein de l'organisation sera fournie.

Traiter des demandes concernant les applications

Il s'agit ici de donner aux étudiants les notions de base de la programmation en prenant appui sur des situations concrètes. Des jeux de rôle peuvent être proposés : certains jouent le rôle d'utilisateurs des applications (remontée d'erreurs ou demandes d'évolution), d'autres sont en charge du support, d'autres encore introduisent un dysfonctionnement du plus simple (erreur syntaxique) au moins simple (erreurs de compilation, programme qui n'effectue pas la tâche demandée).

On pourra amener les étudiants à repérer le script ou le programme concerné puis à lire et interpréter un script ou un programme en vue d'en comprendre le fonctionnement et de corriger un bogue. L'apport des concepts pourra se faire en utilisant du code progressivement plus complexe ; il sera toujours adapté au niveau de compétence atteint par chaque étudiant pour permettre à chacun de progresser dans son apprentissage.

Cette compétence pourra être travaillée en concertation avec les enseignants de mathématiques en charge de l'algorithmique appliquée.

La documentation sur les normes et standards qui font référence au sein de l'organisation sera fournie.

Collecter, suivre et orienter des demandes

Travailler cette compétence suppose la mise à disposition d'un contexte de travail : une organisation cliente, son métier, ses acteurs, leurs rôles, les ressources informatiques qu'ils utilisent, un système informatique composé de ressources matérielles et logicielles, d'un outil de gestion des configurations et des tickets d'assistance (par exemple GLPI), d'applications et d'une base de données, et un contrat d'entente de niveau de service (SLA).

Ressources

- ITIL et la gestion des incidents : https://fr.wikipedia.org/wiki/Gestion_des_incidents
- L'organisation de la gestion des incidents en BTS SIO (Réseau Certa) : https://www.reseaucerta.org/organisation-gestion-incidents
- La maintenance des accès utilisateurs (Réseau Certa) : https://www.reseaucerta.org/content/le-module-sisr1
- Gérer vos incidents avec le référentiel ITIL sur GLPI : https://openclassrooms.com/fr/courses/1730486-gerez-vos-incidents-avec-le-referentiel-itil-sur-glpi

Apports CEJMA

L'étude d'un accord de niveau de service (en anglais SLA - Service Level Agreement), peut permettre aux étudiants de repérer les obligations relatives aux niveaux de services que doit respecter le prestataire ainsi que les cas dans lesquels sa responsabilité contractuelle peut être limitée voire exonérée.

Ressources CEJMA :

- www.lemagit.fr/conseil/Gartner-9-criteres-pour-etablir-un-contrat-de-SLA-en-interne
- www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203473-sla-service-level-agreement-definition-traduction/
- Les contrats du numérique - Philippe Le Tourneau - Edition Dalloz
- Droit et expertise des contrats informatiques - Hubert Bitan - Edition Lamy

B1.3 Développer la présence en ligne de l'organisation

Travailler cette compétence implique de se soucier du métier de l'organisation cliente, de ses objectifs et de sa communication auprès de ses clients ou usagers, ainsi que de la visibilité de cette communication sur le web. Bien entendu ce sont les objets sous-jacents de cette communication qui sont principalement étudiés : CMS, charte graphique, langages du web, SGBD, langage de requête. Les aspects juridiques inhérents au développement de la présence en ligne de l'organisation pourront être étudiés dans le cadre de l'enseignement de CEJMA.

Semestre 1 (4+0+6) 150h	Semestre 2 (2+0+2) 60h	Semestres 3 et 4 (2+0+0) 24h +24h = 48h
• Participer à l'évolution d'un site Web exploitant les données de l'organisation.	• Référencer les services en ligne de l'organisation et mesurer leur visibilité. • *Participer à l'évolution d'un site Web exploitant les données de l'organisation (suite)*.	• Participer à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques • *Participer à l'évolution d'un site Web exploitant les données de l'organisation (suite)*.
Rappel des savoirs Conventions d'écriture électronique Bases de la programmation Web : langage de présentation et de mise en forme, langage d'accès aux données, langage de contrôle Langage d'interrogation de données Système de gestion de contenus : fonctionnalités et paramétrage	**Rappel des savoirs** Référencement et mesure d'audience d'un service en ligne Charte graphique	
Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA		
E-réputation d'une organisation : modalités de construction, atteintes, protection juridique et enjeux économiques Mentions légales et conditions générales d'utilisation d'un site Web Droit d'utilisation des contenus externes Responsabilité de l'éditeur et de l'hébergeur du site Web Nom de domaine : formalisme, organismes d'attribution et de gestion, conflits et résolution Réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel		

Rappels : indicateurs de performance

- *L'image de l'organisation est conforme aux attentes et valorisée.*
- *Les enjeux économiques liés à l'image de l'organisation sont identifiés et les obligations juridiques sont respectées.*
- *Les mentions légales sont accessibles et conformes à la législation.*
- *La visibilité des services en ligne de l'organisation est satisfaisante.*
- *Le site Web a évolué conformément au besoin exprimé.*

Participer à l'évolution d'un site Web exploitant les données de l'organisation

Cette compétence suppose qu'un site web existe pour l'organisation cliente, dans un premier temps il s'agit de l'étudier pour connaître le système de gestion de contenu (CMS) ou l'architecture utilisé, la base de données associée, la charte graphique mise en place, le code utilisé. C'est là l'occasion d'une initiation à la programmation web avec différents langages : langages à balise (HTML, CSS, XML), langages de contrôle (Javascript, PHP, Python...) et langages d'accès aux données et d'interrogation.

Là encore les sites proposés sont plus ou moins complexes pour tenir compte du niveau de compétence atteint par chaque étudiant. Les fonctionnalités de paramétrage d'un CMS peuvent constituer un point de départ. Une partie de la base de données associée au CMS peut servir de point d'appui. Enfin, du code spécifique exploitant les données de l'organisation cliente peut être étudié puis adapté pour répondre à un nouveau besoin.
Ces travaux seront aussi l'occasion de rappeler aux étudiants que l'exploitation de données à caractère personnel est réglementée (réglementation étudiée en CEJM - thème 4 - question 2 et complétée dans le bloc 3).

Dans le cadre de l'enseignement de CEJMA, il sera pertinent d'attirer l'attention des étudiants sur la réglementation relative au site internet.
Il pourra être proposé aux étudiants d'étudier un site web d'une organisation afin dans un premier temps de repérer le nom de domaine du site, la présence des mentions légales, des CGU, des modalités d'acceptation des CGU par l'utilisateur sur le site web, des mentions relatives aux cookies et de réfléchir à leur utilité, puis dans un second temps de vérifier la conformité du site à la réglementation à partir de sources d'informations officielles (site de la CNIL, site economie.gouv.fr etc.).
La consultation des sites des autorités de régulation des noms de domaine (site de l'AFNIC, site de l'ICANN) permettra aussi de compléter les savoirs relatifs aux noms de domaine en prolongement du thème 4 question 2 du programme CEJM : choix du nom de domaine, formalités d'enregistrement, gestion des noms de domaine par des autorités de régulation, résolution des litiges par voie extrajudiciaire telle la procédure Syreli.

Référencer les services en ligne de l'organisation et mesurer leur visibilité.

Travailler cette compétence nécessite de connaître les méthodes et les principaux outils du référencement sur le web : métadonnées associées à un site, à une page, balises de référencement, mots clés qui seront utilisés pour trouver le site de l'organisation cliente, tests de compatibilité...

Mesurer la visibilité d'un service en ligne peut amener à exploiter un outil d'analyse d'audience.

On pourra également aborder ici l'impact du choix d'un langage ou d'une infrastructure de programmation (*framework)* web sur le référencement d'un site.

Ressources

- Consignes Google aux webmasters : https://support.google.com/webmasters/answer/35769?hl=fr
- Cours OpenClassrooms sur l'optimisation du référencement d'un site web : https://openclassrooms.com/fr/courses/5922626-optimisez-le-referencement-de-votre-site-seo-en-ameliorant-ses-performances-techniques

Participer à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques

L'enseignement de CEJMA sensibilisera les étudiants sur l'obligation pour l'éditeur de respecter le droit d'auteur, le droit à l'image ainsi que la réglementation en matière de liberté d'expression, lors de la publication de contenus sur le site internet de l'organisation et sur tout autre média numérique.

La valorisation de l'image de l'organisation sur les médias numériques contribue à la construction de sa e-réputation. On pourra, d'une part, faire réfléchir les étudiants à la complexité de la construction de l'e-réputation d'une organisation : diversité des parties prenantes (clients, salariés, influenceurs, concurrents, associations, analystes ... et l'organisation elle-même), diversité des supports numériques (sites web, blog, forum, article de presse, réseaux sociaux…) et, d'autre part, leur montrer les enjeux économiques liés à l'e-réputation en termes d'avantages (différenciation, fidélisation de la clientèle etc.) et de risques (détérioration de l'image, perte de parts de marché et dégradation du chiffre d'affaires etc.).

A partir d'exemples réels, les étudiants pourront appréhender les impacts économiques liés à l'e-réputation de l'organisation ainsi que les divers procédés qui permettent de porter atteinte à l'e-réputation (rumeur, dénigrement, diffusion de fausses informations, atteintes à ses noms de domaine : typosquattage, cybersquattage, usurpation de son identité). Des dispositifs juridiques, des actions devant les tribunaux permettent de protéger l'organisation victime d'atteinte à sa e-réputation. Quelques exemples pourront être étudiés (action en dénigrement, droit de réponse etc.).

Ressources CEJMA :

- www.legalis.net
- www.gfii.fr/fr/document/e-reputation-et-identite-numerique-des-organisations
- Cyberdroit - le droit à l'épreuve de l'internet - Christiane Féral-Schuhl - Edition Dalloz 2018/2019
- Le droit de l'internet - Vincent Fauchoux, Pierre Deprez - Edition Lexis Nexis 2017

B1.4 Travailler en mode projet

Cette compétence est éminemment transversale tant elle peut être travaillée et sollicitée dans l'ensemble des blocs de compétences professionnelles de la formation. C'est pourquoi il est recommandé de la travailler dès le début du second semestre.

Semestre 1 (4+0+6) 150h	Semestre 2 (2+0+2) 60h	Semestres 3 et 4 (2+0+0) 24h +24h = 48h
	• Analyser les objectifs et les modalités d'organisation d'un projet • Évaluer les indicateurs de suivi d'un projet et analyser les écarts • Planifier les activités	• *Planifier les activités (suite)*
	Rappel des savoirs Outil de gestion de projet : fonctionnalités et paramétrage	**Rappel des savoirs** Planification de projet : approche prédictive et séquentielle, approche agile.

Rappels : indicateurs de performance

- *Les objectifs et les modalités d'organisation du projet sont explicités.*
- *L'analyse des besoins et de l'existant est pertinente.*
- *Les activités personnelles sont planifiées selon une méthodologie donnée et les ressources humaines, matérielles et logicielles nécessaires sont mobilisées de manière efficace et pertinente.*
- *Le découpage en tâches est réaliste.*
- *Les livrables sont conformes.*
- *Le projet est documenté.*
- *Un compte rendu clair et concis est réalisé et les écarts sont justifiés.*
- *La communication écrite et orale est adaptée à l'interlocuteur*

Analyser les objectifs et les modalités d'organisation d'un projet

Cette compétence suppose qu'un exemple de projet soit présenté aux étudiants et apprentis. Ce projet sera suffisamment significatif pour mettre en évidence les notions d'objectif à atteindre, d'échéance, de planification des activités, de ressources humaines et matérielles, d'indicateurs de suivi de projet notamment l'analyse des écarts. Différentes modalités de planification peuvent être présentées pour un même projet : approche prédictive et séquentielle, approche itérative et agile.

Par la suite, les étudiants sont fréquemment invités à travailler en mode projet pour leurs travaux en entreprise comme en centre de formation, en séance de cours en classe comme durant les ateliers de professionnalisation.

Évaluer les indicateurs de suivi d'un projet et analyser les écarts
Parmi les méthodes de gestion de projet, on pourra faire référence à la méthode agile, en s'appuyant sur les graphiques d'avancement (*burndown chart*) de *sprint* et de *release* générés automatiquement par la plupart des outils de gestion de projets agiles (Tuleap, GitLab,..).

Planifier les activités
Cette compétence est travaillée naturellement au cours de la formation au fur et à mesure de la participation des étudiants à différents projets en centre de formation comme en entreprise.
Un apport méthodologique est toutefois nécessaire pour planifier les activités de façon rationnelle : diagramme de Gantt, réseau PERT, méthode Kanban...

Ressources :

Quels outils pour travailler en mode projet ?
https://www.chefdentreprise.com/Thematique/digital-innovation-1074/Breves/Les-raisons-adopter-logiciel-securite-informatique-341768.htm
Le travail collaboratif : https://fr.wikipedia.org/wiki/Travail_collaboratif
Gestion de projet : https://fr.wikipedia.org/wiki/Gestion_de_projet

B1.5 Mettre à disposition des utilisateurs un service informatique

Cette compétence sollicite et conforte les compétences précédemment citées dans ce bloc. Connaissant le contexte et les objectifs d'une organisation cliente et les attentes des parties prenantes, il s'agit de rendre disponible un nouveau service numérique aux utilisateurs. Bien entendu, le choix du service à mettre en place ainsi que l'ampleur du déploiement déterminent la complexité du projet.

Semestre 1 (4+0+6) 150h	Semestre 2 (2+0+2) 60h	Semestres 3 et 4 (2+0+0) 24h +24h = 48h
• Déployer un service	• *Déployer un service (suite)* • Réaliser les tests d'intégration et d'acceptation d'un service • Accompagner les utilisateurs dans la mise en place d'un service	• *Réaliser les tests d'intégration et d'acceptation d'un service (suite)*
Rappel des savoirs Services et protocoles réseaux standard et de base	**Rappel des savoirs** Principes d'architecture d'un service Techniques et outils de déploiement des services informatiques Techniques et outils de test des services informatiques	Rappel des savoirs Service informatique : prestations, moyens techniques, rôles des parties prenantes

Rappels : indicateurs de performance

- *Des tests pertinents d'intégration et d'acceptation sont rédigés et effectués.*
- *Les outils de test sont utilisés de manière appropriée.*
- *Un rapport de test du service est produit.*
- *Un support d'information est disponible.*
- *Les modalités d'accompagnement sont définies.*
- *Le service déployé est opérationnel et donne satisfaction à l'utilisateur.*

Déployer un service

On pourra débuter par la mise à disposition d'un service relativement simple mais qui peut amener à se poser les bonnes questions : comment mettre à disposition une nouvelle imprimante ? Pour quels types d'utilisateurs ? Avec quelles habilitations ? Existe-t-il un serveur d'impression ? Comment l'imprimante est-elle reliée au réseau ? Où placer l'imprimante physiquement ?

Le déploiement et les mises à jour de logiciels bureautiques peuvent aussi constituer un objectif pour travailler cette compétence. La mise à disposition d'une application web doit aussi être considérée comme un projet significatif pour travailler la compétence.

Réaliser les tests d'intégration et d'acceptation d'un service
On cherche ici à sensibiliser les étudiants à vérifier le bon aboutissement du processus de mise à disposition d'un service informatique. Ceci comporte une partie technique (les tests d'intégration) mais aussi une dimension humaine (les tests d'acceptation).

Accompagner les utilisateurs dans la mise en place d'un service
Sachant que tout changement dans les modalités de déroulement d'un processus provoque des inquiétudes, il s'agit de donner aux étudiants les principes de base de l'accompagnement : écouter les utilisateurs / les clients, les informer, les faire participer tout au long du processus, les impliquer dans les tests.

Ressources :

- Dossier Manager Go sur la conduite du changement
- https://www.manager-go.com/gestion-de-projet/conduite-du-changement.htm

B1.6 Organiser son développement professionnel

Nous avons, là encore, une compétence fortement transversale qui sera sollicitée tout au long de la formation. Cette compétence participe directement à l'acquisition de la professionnalité des étudiants et apprentis. On cherche à permettre à chacun de prendre conscience des opportunités offertes par sa formation, par ses rencontres avec des représentants de la profession, par les projets auxquels elle ou il a pu participer. Au fond, il s'agit de développer, progressivement, régulièrement, son projet professionnel.

Le portfolio retrace le parcours de professionnalisation et décrit les réalisations professionnelles élaborées au cours de la formation et l'acquisition des compétences décrites dans le bloc de compétences « Support et mise à disposition de services informatiques ». Les stages permettent également d'alimenter le portfolio à partir des situations réelles vécues ou observées et de conserver ainsi des traces pertinentes des observations, analyses et travaux réalisés dans ce cadre.

Semestre 1 (4+0+6) 150h	Semestre 2 (2+0+2) 60h	Semestres 3 et 4 (2+0+0) 24h +24h = 48h
• Gérer son identité professionnelle • Développer son projet professionnel • Mettre en place son environnement d'apprentissage personnel	• Mettre en œuvre des outils et stratégies de veille informationnelle • *Mettre en place son environnement d'apprentissage personnel (suite)* • *Développer son projet professionnel (suite)*	• *Mettre en œuvre des outils et stratégies de veille informationnelle (suite)* • *Développer son projet professionnel (suite)*
Rappel des savoirs Gestion des relations professionnelles : identité numérique professionnelle, techniques de rédaction de curriculum vitae et de lettre de motivation, présence sur les réseaux sociaux professionnels (outils, atouts et risques) Panorama des métiers de l'informatique	Rappel des savoirs Veille informationnelle et curation : sources d'information, stratégies et outils.	

Rappels : indicateurs de performance

- *Les besoins de formation sont identifiés pour assurer le support ou mettre à disposition un service.*
- *L'identité professionnelle est pertinente et visible sur un réseau social professionnel.*
- *L'environnement d'apprentissage personnel est délimité et expliqué.*
- *La veille est régulière et vise à :*
    - *repérer les techniques et technologies émergentes du secteur informatique ;*

- *utiliser de manière approfondie des moyens de recherche d'information ;*
- *renforcer ses compétences.*

Gérer son identité professionnelle
Cette compétence invite à réfléchir à son avenir professionnel, à ce que l'on souhaite faire, à ce que l'on souhaite devenir en tant que professionnel, et à considérer qu'il s'agit là d'un processus réflexif qu'il convient de gérer le mieux possible.

Développer son projet professionnel
Développer son projet professionnel est un processus permanent qui nécessite de faire un diagnostic de ses compétences et appétences, lesquelles évoluent au gré des réalisations et des rencontres. C'est aussi faire des choix et s'y tenir. C'est également se faire connaître (relations professionnelles, réseaux sociaux, CV...) et se faire reconnaître (références, lettre de motivation, certifications professionnelles…).

La construction du portfolio numérique peut être initiée et son suivi effectué.

Mettre en place son environnement d'apprentissage personnel
La variété de métiers de l'informatique ainsi que l'évolution rapide des technologies et des méthodes, nécessitent d'inscrire très tôt les étudiants dans un processus continu de formation, et, souvent dans les métiers de l'informatique, d'auto-formation. La capacité à se former est consubstantielle du métier d'informaticien.

Mettre en œuvre des outils et stratégies de veille informationnelle
Là encore, l'évolution rapide des technologies, des méthodes, des outils, des acteurs du marché de l'informatique nécessitent d'inscrire très tôt les étudiants dans un processus continu de veille informationnelle. Ceci peut naturellement être travaillé en apprenant à exploiter de façon efficiente les ressources du web et en mettant en place des outils pour mieux organiser sa veille et gagner en efficacité (outils de curation, de partage…).

Ressources :

La formation en faveur du développement professionnel
https://travail-emploi.gouv.fr/formation-professionnelle/article/la-formation-professionnelle-principes-generaux

Quelques principes et outils
https://lemag.digitools.io/MagDigital/marketing-ameliorer-votre-veille-informationnelle/

Bloc 2 SISR - Administration des systèmes et des réseaux

Rappel du référentiel des activités professionnelles (RAP)

En prenant en compte les besoins métiers de l'organisation, la personne titulaire du diplôme participe à l'administration des systèmes et du réseau de l'organisation. Elle répond aux attentes des utilisateurs ou des clients en réalisant ou en modifiant des solutions d'infrastructure pour assurer le niveau de disponibilité adapté de ces solutions ainsi que la qualité de service des équipements réseaux.

Les interventions concernent à la fois les équipements réseaux et les services qui s'appuient sur des systèmes, eux-mêmes installés sur des serveurs physiques ou virtuels ; certains de ces éléments pouvant être accessibles dans le réseau local ou à travers une solution en nuage (cloud).

Présentation

Ce bloc permet de construire les savoirs et savoir-faire liés à la conception, à l'installation et à l'administration d'une infrastructure réseau qui est vue comme l'ensemble des éléments matériels et logiciels nécessaires à une organisation pour mettre à disposition des services. Il permet également de consolider les techniques de résolution d'incidents liés aux composants réseaux, systèmes et services et de perfectionner les techniques de rédaction d'un compte rendu, d'une documentation, d'une procédure d'installation et de configuration.

L'objectif final à atteindre est la mise en œuvre d'une architecture raisonnablement complexe documentée et administrée offrant un ou plusieurs services à l'utilisateur en respectant une qualité de service définie et en supportant les pannes grâce aux dispositifs et procédures de continuité de service.

Les compétences ne sont pas construites indépendamment les unes des autres. La démarche préconisée n'est pas de traiter les notions relatives aux trois compétences principales (conception, installation et administration) de manière chronologique, académique et indépendante mais de les associer autour d'objets métiers concrets (infrastructure, serveurs et systèmes, services) et de préoccupations de niveau de service (haute disponibilité, qualité de service).

Ainsi, la construction des compétences peut être conçue autour des objets d'étude suivants :

- infrastructures : conception, priorisation des flux, qualité de service, disponibilité, supervision et métrologie des éléments d'interconnexion ;
- systèmes (serveurs ou équipements utilisateurs) et serveurs : mise en production, déploiement, administration, supervision et métrologie, disponibilité, automatisation, sauvegarde et restauration ;
- services perçus par les utilisateurs : qualité, disponibilité, contrat de service, supervision et métrologie, plans de continuité et de reprise d'activité.

Un découpage selon les préoccupations métiers est également envisageable :

- disponibilité des services : conception, installation, administration et supervision des éléments d'infrastructure, des systèmes et des services pour assurer la disponibilité des services ;
- qualité de service : conception, installation, administration et supervision des éléments d'infrastructure, des systèmes et des services pour assurer la qualité de service attendue.

Mais quelle que soit la démarche adoptée, on n'enseigne pas des savoirs généraux (la haute disponibilité en général, la sauvegarde en général, etc.) mais on s'appuie toujours sur des objets métiers (la sûreté d'un système serveur, la disponibilité mise en œuvre sur un élément d'interconnexion réseau, la qualité d'un service en particulier, la continuité de service d'un serveur, la haute disponibilité d'un service, etc.) :

- qualité, sûreté et continuité doivent être vus comme des objectifs à atteindre sur chaque objet d'étude (serveurs, services et infrastructures réseaux) à partir d'actions précises (exploitation, administration, supervision) ;
- les compétences techniques construites sont mobilisées dans les ateliers de professionnalisation dans des situations complexes afin d'aboutir aux compétences professionnelles attendues.

L'étudiant doit être confronté dès que cela est possible à un environnement de production opérationnel conforme à l'environnement technologique décrit dans l'annexe II.E du référentiel. Cet environnement s'inscrit dans un contexte organisationnel réaliste dans lequel s'expriment les besoins, les contraintes techniques, juridiques, …

Le travail en mode projet peut aussi être mobilisé dans ce bloc à la fois comme approche pédagogique rendant actif les étudiants, et pour rendre la contextualisation plus réaliste.

L'enseignement de CEJMA permettra aux étudiants de bien cerner le contexte juridique dans lequel s'inscrivent la conception puis la mise en œuvre de la solution d'infrastructure réseau.

Positionnement du bloc 2 SISR

Le semestre 2 propose une première approche dans une vision administrateur (par rapport à la vision plutôt utilisateur du premier semestre du bloc 1) où les notions de base relatives aux systèmes et aux réseaux abordées dans le bloc 1 au cours du premier semestre sont consolidées et enrichies.

Le semestre 2 permet :

- de fortement consolider les outils et techniques relatifs à la gestion des incidents et des problèmes systèmes et réseau des équipements utilisateurs étudiés dans le bloc 1 en étendant le périmètre aux incidents de la couche d'accès des éléments d'interconnexion et au premier niveau de la couche de distribution : diagnostic et résolution d'incidents, restauration d'environnement ;
- d'approfondir la conception et l'adaptation des infrastructures réseau : installation et configuration des éléments d'interconnexion et des services techniques réseau ; principes des architectures réseau, outils de conception et de simulation, séparation des flux (Vlan, DMZ, autres périmètres de sécurité, etc.), adressage IP, routage et translation d'adresses réseau, accès distant. Le filtrage est abordé, il sera approfondi en seconde année notamment dans le bloc 3.

Durant ce semestre, on ne traite pas les questions liées à la disponibilité, à la répartition de charges, à la qualité de service et à la performance qui seront abordées en deuxième année. La sécurité est traitée dans le bloc 3 mais bien évidemment déjà mobilisée dans le bloc 2 (par exemple, l'accès distant est bien sécurisé).

La deuxième année approfondit les principes des architectures réseaux et aborde la sûreté, c'est à dire les notions de disponibilité/permanence, de répartition de charges, de qualité de service, de performance et traite la supervision.

Là encore, on n'étudie pas les aspects liés à la sécurité qui sont traités dans le bloc 3 mais les compétences techniques construites dans ce dernier bloc peuvent être mobilisées dans celui-ci (et vice versa).

Ressources générales

Les ressources du réseau Certa : http://www.reseaucerta.org/ (faire une recherche sur le mot 'réseau' , 'disponibilité' ou 'sécurité' par exemple)
Cours système et réseaux d'OpenClassRoom : https://openclassrooms.com/fr/search?page=1&categories=Syst%C3%A8mes%20%26%20R%C3%A9seaux
La bibliothèque numérique ENI : https://www.editions-eni.fr/livres-numeriques
L'internet rapide et permanent : http://irp.nain-t.net/doku.php
L'afnic : https://www.afnic.fr/fr/
Itil France : http://www.itilfrance.com/
Mooc Fun : https://www.fun-mooc.fr/

B2.1 SISR - Concevoir une solution d'infrastructure réseau

À partir de l'analyse d'un besoin, l'étudiant est amené à proposer et à justifier plusieurs solutions permettant de produire le service attendu et à estimer leurs coûts pour la partie qui le concerne. La solution choisie tiendra compte également des aspects éthiques et environnementaux.

Le service attendu s'intègre dans un existant et représente principalement l'évolution d'un processus déjà informatisé (ajout de fonctionnalités ou prise en charge d'une nouvelle réglementation par exemple) ou d'une architecture technique (changement de technologie, ajout d'un service technique, etc.).

À partir de la description de l'architecture applicative, de l'architecture technique et de l'architecture réseau de l'organisation concernée par la demande d'un nouveau service, l'étudiant doit analyser comment ce service va interagir avec les services existants et recenser les composants qui vont être impactés par sa mise en place : composants à remplacer ou à modifier.

L'étudiant doit savoir situer son action par rapport à l'organisation cliente à l'origine de la demande et par rapport au prestataire informatique dans le respect des liens contractuels qui les lient sur la qualité de service attendu (contrat de niveau de service).

L'activité de conception intervient à un degré variable quand l'étudiant est confronté à un nouveau besoin qui se complexifie au fil du temps.
Si le besoin est exprimé à travers un cahier des charges (notamment en seconde année), c'est l'occasion d'en définir les principaux composants et d'aborder notamment les notions de besoins, d'exigences, de qualité, de contraintes. L'étudiant peut, par exemple, à partir de situations concrètes, repérer les exigences liées à la qualité (conformité, performance et respect des normes et de la réglementation).
Cette compétence se consolidera efficacement dans les ateliers de professionnalisation où les étudiants pourront être confrontés à un cahier des charges plus complexe.

L'enseignement de CEJMA aura pour objectif d'éclairer les étudiants et apprentis sur les enjeux juridiques liés à la rédaction du cahier des charges et à la conclusion des contrats entre le prestataire et l'organisation cliente.

Semestre 2 - 90h (2+4)	Semestres 3 et 4 - 216h (3+6)
• Analyser un besoin exprimé et son contexte juridique • Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique • Maquetter et prototyper une solution d'infrastructure.	• *Analyser un besoin exprimé et son contexte juridique (suite)* • *Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique (suite)* • Choisir les éléments nécessaires pour assurer la qualité et la disponibilité d'un service. • Élaborer un dossier de choix d'une solution d'infrastructure et rédiger les spécifications techniques • *Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue (suite)* • Déterminer et préparer les tests nécessaires à la validation de la solution d'infrastructure retenue

Rappel des savoirs Principes des architectures réseau : modèles de référence, normes et technologies, périmètres de réseau, routage, plans d'adressage Outil de conception et de simulation d'architecture réseau : techniques, fonctionnalités et paramétrage	 Cahier des charges techniques et formalismes usuels de représentation d'une architecture technique Principes avancés d'architecture des infrastructures réseaux : services à l'utilisateur, services système et services réseau, priorisation des flux, qualité de service, disponibilité, virtualisation, ... Disponibilité des services, des systèmes, des serveurs et des infrastructures réseaux : méthodes, technologies, techniques, normes et standards associés Qualité de service : méthodes, technologies, techniques, normes et standards associés
Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA Cahier des charges et ses enjeux juridiques Contraintes éthiques et environnementales dans le choix d'une infrastructure réseau Contrat de prestation de services informatiques et ses clauses spécifiques Contrat d'entente de niveau de service (ou SLA) déjà étudié dans le bloc 1	

Rappel : Indicateurs de performance (surlignés, les indicateurs qui relèvent plutôt de la seconde année)

Les fonctionnalités et les exigences liées à la qualité attendue de la solution d'infrastructure sont identifiées.
Les contextes d'utilisation, les processus et les acteurs sur lesquels la solution d'infrastructure à produire aura un impact sont décrits.
Les composants de l'architecture technique sur lesquels la solution d'infrastructure à produire aura un impact sont recensés.
Les risques liés à une mauvaise utilisation ou à un dysfonctionnement de la solution d'infrastructure sont identifiés.
Les choix de solutions répondant au besoin exprimé (adaptation d'une solution existante ou réalisation d'une nouvelle) sont décrits et justifiés en termes de coût, de délai et de qualité.
La solution proposée tient compte des limites de responsabilité du prestataire informatique vis-à-vis de son métier et de son environnement.
Le dossier de choix et l'argumentaire technique sont rédigés et prennent en compte des préoccupations éthiques et environnementales.
Les éléments permettant d'assurer la qualité et la continuité des services sont justifiés et caractérisés :

- *les éléments à sauvegarder et à journaliser pour assurer la continuité du service et la traçabilité des transactions sont identifiés ;*
- *les procédures d'alerte associées au service sont spécifiées ;*
- *les solutions de fonctionnement en mode dégradé et les procédures de reprise du service sont décrites.*

La maquette et le prototype sont conformes au besoin exprimé.
Les tests d'acceptation nécessaires à la validation de la solution d'infrastructure sont recensés.
Les jeux d'essai pertinents et les procédures pour la réalisation des tests sont préparés.

Analyser un besoin exprimé et son contexte juridique

C'est le point de départ de toute construction de compétence : le besoin est exprimé dans un contexte professionnel précis. Selon l'objectif, le semestre et le moment dans le semestre, l'analyse de besoin sera plus ou moins complexe. Le besoin exprimé peut être un "prétexte" permettant d'introduire une nouvelle notion comme être un besoin plus global et plus complexe exprimé dans un cahier des charges que les étudiants doivent prendre en charge en autonomie et parfois en groupe (mode projet) et en justifier les solutions sur tous les aspects.

Les principes avancés des architectures réseaux sous-jacentes doivent être abordés en fonction du besoin exprimé. On peut imaginer également ici que les étudiants les découvrent en autonomie. Ce sera également l'occasion de donner à l'étudiant les éléments de compréhension de l'architecture technique et d'en étudier les formalismes usuels de représentation.

L'enseignement de CEJMA pourra compléter la lecture technique du cahier des charges par une approche juridique, et notamment amener les étudiants et apprentis à réfléchir sur l'intérêt et la valeur juridique de ce document pré-contractuel. Il pourra faire le lien entre la rédaction du cahier des charges et les obligations respectives de l'organisation cliente (obligation de collaboration) et du prestataire (obligation de conseil) dans les contrats de prestations de service ainsi que la mise en œuvre de la responsabilité civile contractuelle des parties en cas de non-respect.
Une attention particulière pourra être portée sur le niveau de service minimal que le prestataire s'engage à délivrer à l'organisation cliente dans le cadre du contrat d'entente de niveau de service (SLA), ainsi que les cas dans lesquels sa responsabilité contractuelle peut être limitée voire exonérée (notion déjà abordée dans le bloc 1).

Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique

Dans un environnement professionnel, toute modification d'une infrastructure doit faire l'objet d'une étude préalable.
L'étudiant doit mesurer l'impact d'une modification d'un élément d'une solution d'infrastructure sur le système informatique et sur l'activité de l'organisation.
Les étudiants doivent être sensibilisés à la notion de régression dès le second semestre.

Choisir les éléments nécessaires pour assurer la qualité et la disponibilité d'un service.

La qualité de service est principalement abordée à travers les critères d'évaluation de l'efficacité de l'infrastructure liée à la performance et à la disponibilité et pourront être abordées en liaison avec les problématiques de répartition de charges. Ces notions sont traitées en deuxième année même si une première approche a pu être faite en première année, dans le bloc 1.

Élaborer un dossier de choix d'une solution d'infrastructure et rédiger les spécifications techniques

L'étudiant doit être capable de décrire l'infrastructure générale du réseau proposée intégrant *a minima* son plan d'adressage, son plan de nommage, les liaisons filaires ou non, les matériels d'interconnexion ainsi que les zones logiques créées par le paramétrage des matériels d'interconnexion et le niveau de sécurité associé à ces zones. La segmentation du réseau en zones logiques est abordée dans le bloc 2. Ces zones logiques peuvent être associés aux

performances ou à la sécurité. La sécurité s'entend dans le bloc 2 en termes d'habilitation à accéder à une zone ou non pour un utilisateur travaillant dans l'infrastructure sans intention malveillante. Le bloc 3 s'intéresse à la segmentation comme élément nécessaire mais non suffisant pour lutter contre les malveillances. Dans le cadre de ces activités, un outil de modélisation des infrastructures réseau sera avantageusement mis en œuvre.
L'étudiant doit parvenir à une compréhension globale des architectures décrites pour pouvoir situer son travail dans un environnement professionnel. Si tous les protocoles utilisés dans la description d'une solution d'infrastructure doivent être cités, seuls les protocoles standards, leur rôle dans les échanges et leur interdépendance seront étudiés de manière approfondie.

L'enseignement de CEJMA aura pour objectif de sensibiliser les étudiants et apprentis aux problématiques éthiques et environnementales soulevées par l'activité informatique, et ce, à partir d'exemples choisis dans l'actualité. L'environnement économique et légal oblige de plus en plus les organisations à adopter des démarches éthiques et éco responsables dans la conception d'une solution d'infrastructure réseau. Les étudiants et apprentis tiendront compte de ces préoccupations dans l'élaboration du dossier de choix d'une solution d'infrastructure (la notion d'externalités négatives générées par l'activité des organisations ainsi que l'étude de la responsabilité éthique, sociale, sociétale et environnementale des entreprises sont abordées respectivement dans le thème 1 question 1 et le thème 3 question 4 du programme de CEJM).

Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue

Maquette et prototype permettent de disposer d'une projection réaliste de ce que sera le service attendu, de le tester et de repérer les problèmes de mise en production avant la phase de déploiement. La maquette consiste à illustrer le plus fidèlement possible le service attendu à partir d'un outil de simulation. Le prototype est une version réalisée dans un environnement de test proche de l'environnement de production.

Les outils et techniques de simulation sont étudiés à l'occasion de la réalisation des maquettes et prototypes.

Les outils de virtualisations peuvent aussi être mis en œuvre pour simuler la solution et faciliter l'apprentissage dans différents environnements tout comme ils doivent être abordés comme solution d'infrastructure opérationnelle dans les organisations.

Déterminer et préparer les tests nécessaires à la validation de la solution d'infrastructure retenue

L'étudiant doit comprendre l'importance des tests dans la production d'un service et être capable d'en caractériser les critères d'acceptation (fiabilité, performance, conformité) et les jeux d'essai correspondants (données, conditions de fonctionnement, scénarios).

Les étudiants doivent être sensibilisés dès la première année à la nécessité des tests et à leur mise en œuvre. Mais leur élaboration proprement dite peut être différée en seconde année.

Ressources CEJMA :
Rapports Cigref « Ethique et numérique » 2014 et 2018 www.cigref.fr/wp/wp-content/uploads/2018/10/Cigref-Syntec-Numerique-Referentiel-pratique-Ethique-et-Numerique-2018.pdf
www.greenit.fr
www.lemagit.fr/conseil/Gartner-9-criteres-pour-etablir-un-contrat-de-SLA-en-interne
www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203473-sla-service-level-agreement-definition-traduction/
Les contrats du numérique - Philippe Le Tourneau - Edition Dalloz
Droit et expertise des contrats informatiques - Hubert Bitan - Edition Lamy

B2.2 SISR - Installer, tester et déployer une solution d'infrastructure réseau

On se préoccupe ici de la mise en production d'une solution d'infrastructure.

Cette compétence, à travailler dès le début du deuxième semestre, nécessite de disposer de l'équipement nécessaire. En effet, la configuration d'une maquette permet souvent de valider une solution mais il faut impérativement que l'étudiant pratique la configuration des éléments d'interconnexion et qu'il soit confronté le plus souvent possible, physiquement ou dans le *cloud*, à un environnement de production (ou à un environnement très proche) tel que décrit dans l'annexe II.E du référentiel.

Semestre 2 - 90h (2+4)	Semestres 3 et 4 - 216h (3+6)
• Installer et configurer des éléments d'infrastructure • Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure • Tester l'intégration et l'acceptation d'une solution d'infrastructure • Déployer une solution d'infrastructure	• *Installer et configurer des éléments d'infrastructure (suite)* • Installer et configurer des éléments nécessaires pour assurer la continuité des services • Installer et configurer des éléments nécessaires pour assurer la qualité de service • *Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure (suite)* • *Tester l'intégration et l'acceptation d'une solution d'infrastructure (suite)* • *Déployer une solution d'infrastructure (suite)*
Rappel des savoirs Installation et configuration des éléments d'interconnexion et des services techniques réseau Techniques, outils et protocoles d'administration à distance Déploiement d'éléments d'infrastructure : méthodes, technologies, techniques, normes et standards associés Techniques et outils de test des services informatiques Langage de commande d'un système d'exploitation : commandes et script d'administration d'une solution d'infrastructure	Mise en œuvre des solutions permettant d'atteindre les niveaux de disponibilité et de qualité de service à plusieurs niveaux : • infrastructures : performance, disponibilité, administration • systèmes (serveurs ou équipements utilisateurs) • serveurs : mise en production, déploiement, administration, disponibilité, automatisation • services perçus par les utilisateurs : qualité, disponibilité

Rappels : Indicateurs de performance (surlignés, les indicateurs qui relèvent plutôt de la seconde année)

Des éléments d'infrastructure (élément d'interconnexion, service, serveur, équipement utilisateur) sont installés et configurés.
Les éléments d'infrastructure permettant d'assurer la continuité de service sont installés et configurés.
Le service fonctionne avec la disponibilité attendue.
Une procédure de remplacement ou de migration d'un élément d'infrastructure est élaborée et mise en œuvre en respectant la continuité d'un service.
Les éléments d'infrastructure permettant d'assurer la qualité de service sont installés et configurés.
Le service fonctionne avec la qualité attendue.
La solution d'infrastructure est installée et configurée dans les règles de l'art :

- *l'environnement de test est mis en place,*
- *les tests pertinents d'intégration et d'acceptation sont effectués,*
- *le rapport de tests est rédigé,*
- *la documentation est à jour et disponible,*
- *la solution d'infrastructure tient compte des préoccupations de développement durable.*

L'intégration de la solution ne génère pas de dysfonctionnement du réseau ou dans le réseau.
Une procédure claire de déploiement de la solution est rédigée.
La solution d'infrastructure est déployée selon la procédure et la planification définies.

Installer et configurer des éléments d'infrastructure

Les éléments d'infrastructure dont il s'agit ici constituent principalement, en première année, la couche d'accès et le premier niveau de la couche de distribution (tels que définis dans le modèle hiérarchique en trois couches popularisé par Cisco). Une première approche concernant les serveurs réalisée dans le bloc 1, complétée dans ce bloc sera approfondie en deuxième année.

Les solutions d'infrastructure installées et configurées deviennent au fil du temps progressivement plus complexes.

Les services informatiques recourent à la virtualisation des machines serveurs voire des machines clientes, afin de réduire les coûts de possession d'infrastructures. Cela permet également l'exploitation optimisée des machines et des systèmes, ainsi que le déploiement et la reconfiguration rapide de nouvelles plateformes. L'étudiant doit être familiarisé avec la mise en œuvre d'au moins un environnement de virtualisation et en avoir compris les concepts.

Installer et configurer des éléments nécessaires pour assurer la continuité de services

La continuité de service au sens d'ITIL est avant tout un mode de gestion qui demande des actions ininterrompues dans le temps. Ce mode de fonctionnement, appliqué à une unité, impose très souvent que les unités en relation doivent également fonctionner en continu, c'est ainsi toute la chaîne qui est impliquée.
La continuité de service sous-entend donc le maintien des services, éventuellement en mode dégradé, et la reprise de l'activité normale du service suite à la panne de l'un de ses éléments.

La reprise de service doit permettre après une interruption de service de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données.

La continuité de service et la reprise de service doivent être abordées en relation avec un référentiel de bonnes pratiques comme ITIL et les normes et standards associés, sans que ceux-ci fassent l'objet d'une étude détaillée.

L'étudiant doit pouvoir situer son action dans le cadre d'un plan de secours informatique et d'un plan de continuité d'activité et être sensibilisé à l'importance d'anticiper les réponses techniques aux dysfonctionnements les plus prévisibles.

Il est également sensibilisé aux principes généraux de la tolérance de pannes, de la sauvegarde, de la restauration des données, de la répartition de charges et de la gestion de la priorité des flux.

Cette compétence se travaille à partir de la deuxième année, même si une sensibilisation a déjà été réalisée dans le bloc 1 et au cours du second semestre dans le bloc 2.

Installer et configurer des éléments nécessaires pour assurer la qualité de service

Au sens large, la notion de qualité de service découle directement de l'organisation tayloriste du travail et se rapporte à tout ce qui est mesurable dans l'ensemble des propriétés et caractéristiques d'un produit ou d'un service qui lui confèrent l'aptitude à satisfaire des besoins de consommateurs exprimés ou implicites.

Dans une acception plus étroite, assurer la qualité de service (QoS) correspond à la volonté d'optimiser les ressources d'un réseau et de garantir de bonnes performances aux applications critiques pour l'organisation (source Wikipédia).

Dans son acception la plus large, la qualité de service peut être abordée à travers l'étude de contrats de service. Cette étude peut mettre en évidence les critères de qualités les plus fréquemment rencontrés : bande passante, latence, gigue, taux de perte des paquets … On peut alors étudier ce qui peut être mis concrètement en place pour atteindre ces objectifs, dans les différents composants de l'infrastructure.

La QoS peut être abordée à travers un service qui est particulièrement concerné : par exemple la Voix sur IP. Il s'agira de découvrir l'intérêt des mécanismes de QoS et leur mise en œuvre concrète dans l'infrastructure réseau.

Cette compétence peut se travailler essentiellement en seconde année.

Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure

L'étudiant sera amené à rédiger ou mettre à jour une procédure d'installation et une documentation à destination des utilisateurs finaux. La distinction entre les deux est clairement définie et la documentation doit être adaptée à la cible. Les documents doivent être élaborés selon les bonnes pratiques en vigueur et en utilisant les fonctionnalités avancées des traitements de texte.

Les outils internes de communication sont systématiquement pratiqués pour les besoins de la gestion partagée d'une documentation. Il est préférable que l'étudiant soit placé, dès la première année, dans un environnement collaboratif proche de celui disponible chez un prestataire informatique.

Lorsqu'il s'agit de la mise à disposition d'un nouveau service à l'utilisateur, l'étudiant doit être capable de situer son action dans le processus d'accompagnement du changement lié à la mise en place de ce nouveau service. Il mobilise ici les compétences développées dans le bloc 1 (notamment celle concernant l'accompagnement des utilisateurs dans la mise en place d'un service) et consolidées en atelier de professionnalisation. Il peut également être amené à construire un scénario de formation adapté à la cliente visée.

Tester l'intégration et l'acceptation d'une solution d'infrastructure

L'étudiant doit être capable de tester l'installation et la configuration des composants de base d'un réseau permettant de maîtriser les aléas de l'environnement de production.

Cette compétence se construit dès le semestre 2 même si les environnements de tests sont plus étoffés et professionnels la seconde année.

Dans une logique d'apprentissage (notamment au semestre 2), les tests à mettre en œuvre peuvent être fournis directement par le formateur et non forcément élaborés par l'étudiant.

L'apprentissage peut s'appuyer sur les acquis du bloc 1 (compétence "Réaliser les tests d'intégration et d'acceptation d'un service") et sur les activités réalisées en atelier de professionnalisation.

Déployer une solution d'infrastructure

Pour déployer une solution d'infrastructure, on pourra avoir recours à un langage de script, à un environnement de déploiement intégré à l'infrastructure de réseau ou à un outil spécifique de déploiement.

Les différentes techniques de déploiement sont abordées à partir de situations concrètes. Il ne s'agit pas d'en faire une liste exhaustive mais de dégager les principales techniques en analysant leurs avantages et inconvénients, en s'appuyant notamment sur un référentiel de bonnes pratiques. Dans la mesure du possible, ces techniques doivent être mises en œuvre pratiquement.

L'apprentissage peut s'appuyer sur les acquis du bloc 1 (compétence "Déployer un service").

B2.3 SISR - Exploiter, dépanner et superviser une solution d'infrastructure réseau

Une solution d'infrastructure étant installée, son exploitation implique d'être capable de l'administrer efficacement, de la superviser, de gérer sa qualité et d'en assurer la continuité. On se préoccupe en priorité ici de performance, de disponibilité au niveau des éléments d'interconnexion du réseau, du système et des services. L'exploitation d'une solution d'infrastructure participe également à la détection des problèmes et peut être à l'origine d'une demande de changement.

L'enseignement de CEJMA complétera les aspects techniques liés à cette compétence par l'étude de contrats de prestations de services spécifiques tels que le contrat de maintenance informatique ou de supervision par exemple. On étudiera aussi la responsabilité de l'administrateur système et réseau qui pourrait être engagée à l'occasion des opérations d'exploitation, de dépannage et de supervision.

Semestre 2 - 90h (2+4)	Semestres 3 et 4 - 216h (3+6)
• Administrer sur site et à distance des éléments d'une infrastructure • Automatiser des tâches d'administration • Gérer des indicateurs et des fichiers d'activité des éléments d'une infrastructure • Identifier, qualifier, évaluer et réagir face à un incident ou à un problème	• *Administrer sur site et à distance des éléments d'une infrastructure (suite)* • *Automatiser des tâches d'administration (suite)* • *Gérer des indicateurs et des fichiers d'activité des éléments d'une infrastructure (suite)* • *Identifier, qualifier, évaluer et réagir face à un incident ou à un problème (suite)* • Évaluer, maintenir et améliorer la qualité d'un service
Rappel des savoirs Technologie, techniques, normes et standards, outils et méthodes associés au diagnostic et à la gestion des incidents et des problèmes. Techniques, outils et protocoles d'administration à distance Langage de commande d'un système d'exploitation : commandes et script d'administration d'une solution d'infrastructure	Sauvegarde et restauration : stratégies, techniques, typologie des supports de sauvegarde et technologies associées Plans de continuité et de reprise d'activité Supervision et métrologie des infrastructures réseaux : méthodes, technologies, techniques, normes et standards associés

Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA

Contrat de prestation de services informatiques et ses clauses spécifiques
Responsabilité civile et pénale de l'administrateur système et réseau

Rappels : Indicateurs de performance (surlignés, les indicateurs qui relèvent plutôt de la seconde année)

Un dispositif d'administration sur site et à distance est configuré et exploité.
Les conditions d'administration des éléments d'infrastructure sont maîtrisées.
L'automatisation des tâches d'administration répond au besoin exprimé.
Les outils nécessaires à la production d'indicateurs d'activité et à l'exploitation de fichiers d'activité sont installés et configurés.
Les dysfonctionnements récurrents dans une solution d'infrastructure sont repérés et leurs causes identifiées.
Le degré d'urgence et le niveau d'intervention sont définis.
Les conséquences techniques du problème sont évaluées.
L'incident est résolu ou escaladé de manière efficiente, en tenant compte des délais et procédures en vigueur.
Le problème est résolu ou escaladé de manière efficiente, en tenant compte des délais et procédures en vigueur.
Les rapports d'incidents et les comptes rendus de problèmes sont rédigés et adaptés à chaque destinataire tant par leur contenu que par leur présentation.
Des mesures correctives sont proposées ou mises en œuvre pour maintenir ou améliorer la qualité d'un service.
Les éléments d'une solution d'infrastructure et leur utilisation sont supervisés.
Les indicateurs et les fichiers d'audit sont analysés et exploités.
Des alertes adaptées à la criticité du service sont générées.
Les procédures d'alerte destinées à rétablir la qualité du service sont appliquées.
Le fonctionnement du service en mode dégradé et la disponibilité des éléments d'infrastructure permettant une reprise du service sont périodiquement vérifiés.
Le rétablissement de la qualité du service est assuré dans les délais prévus.

Administrer sur site et à distance des éléments d'une infrastructure

Après éventuellement une première configuration, les éléments d'infrastructure doivent être installés dans un local technique comme c'est généralement le cas dans un environnement professionnel. L'accès à distance est donc obligatoire. On privilégiera des protocoles de prise en main à distance sécurisés.

Automatiser des tâches d'administration

Les langages de commande ou de script sont utilisés pour automatiser des tâches d'administration de gestion et d'administration système courantes. On étudiera un ou plusieurs langages de script associés aux systèmes d'exploitation choisis.

L'exploitation des fichiers d'activité, la personnalisation de l'environnement de travail de l'utilisateur, le déploiement d'un service peuvent constituer un terrain d'application privilégié.

Cette compétence peut commencer à être travaillée dès le début du deuxième semestre puisque les étudiants connaissent les bases relatives aux systèmes d'exploitation et à la programmation.

Gérer des indicateurs et des fichiers d'activité des éléments d'une infrastructure

Il peut s'agir dans un premier temps d'identifier les fichiers d'activités puis de les exploiter pour résoudre un problème spécifique, lors de l'installation d'un service par exemple.

Une démarche plus systématique peut être adoptée dans un second temps : elle peut par exemple consister à mettre en place puis à exploiter un serveur de centralisation des journaux d'évènements.

Identifier, qualifier, évaluer et réagir face à un incident ou à un problème

Sur des situations professionnelles de plus en plus complexes, l'étudiant doit être capable de :

- prendre en charge une demande d'assistance et participer à sa résolution en s'appuyant sur les compétences techniques acquises ;
- participer à la construction d'une réponse à une interruption de service dans le respect des procédures mises en place.

À travers ces situations, l'étudiant doit comprendre l'intérêt d'anticiper les principaux cas d'interruption de services à travers la mise en place de plans de secours informatiques s'appuyant sur différentes solutions techniques.

L'étudiant doit également être en mesure de situer son action dans le cadre d'une gestion des problèmes et des changements. Il doit notamment faire la distinction entre les notions d'incident et de problème.

Évaluer, maintenir et améliorer la qualité d'un service

L'étudiant doit pouvoir mesurer l'incidence d'un dysfonctionnement sur la continuité de service et l'importance de surveiller l'état des services et d'anticiper les actions à mettre en place en cas de dégradation d'un service.

L'étudiant doit pouvoir rendre compte d'une surveillance effective de ces éléments.

Les activités liées à la supervision doivent pouvoir être réalisées sur une infrastructure en état de fonctionnement et s'appuyer sur des outils de découverte automatique des composants de l'infrastructure.

On mettra en œuvre une solution de supervision en étudiant les protocoles associés (SNMP par exemple). On mettra en place des solutions de métrologie au niveau des matériels d'interconnexion et des solutions permettant de contrôler les flux.

Les opérations d'installation, de déploiement, de dépannage, de supervision d'une solution d'infrastructure réseau donnent lieu lorsqu'elles sont réalisées par un prestataire à la conclusion d'un contrat de prestations de services.

L'enseignement de CEJMA proposera, en cohérence avec le thème 1 question 2 et du thème 4 question 2 du programme de CEJM, l'étude de certains de ces contrats (inhérents à la spécialité SISR du BTS SIO) afin d'y repérer les clauses spécifiques notamment celles relatives aux obligations respectives des parties (informations, conseils, collaboration, délivrance etc.), les cas dans lesquels les parties engagent leur responsabilité, les causes d'exonération ou de limitation de responsabilité respectives ainsi que les clauses de résiliation du contrat.

Les étudiants seront également sensibilisés au cadre juridique spécifique de l'administrateur système et réseau en s'appuyant notamment sur l'analyse de décisions de justice.
Au travers de ses missions (informer/former/conseiller/sécuriser, contrôler l'activité sur le réseau etc.), l'administrateur système et réseau est titulaire de droits mais également soumis à un certain nombre d'obligations légales et contractuelles (obligation de loyauté, de transparence, de confidentialité, obligation en cas d'atteinte à la sécurité du réseau, ou encore de diffusion de contenus illicites etc.), et peut engager sa responsabilité civile et/ou pénale en cas de non-respect de ses obligations.
Les cas dans lesquels l'administrateur système réseau pourra s'exonérer de sa responsabilité pourront également être abordés.
Les fondements de la responsabilité civile et pénale sont étudiés dans le thème 3 question 3 CEJM.

Ressources CEJMA :
www.legalis.net
www.droit-technologie.org/contentieux/contentieux-lies-aux-contrats-informatiques/#_ftn15
Revues Lexisnexis communication commerce électronique - Panorama de jurisprudence relative aux contrats informatiques -numéro 7-8 juillet/août 2019
www.jurisexpert.net/cadre-juridique-des-administrateurs-reseaux/
Bonnes pratiques juridiques Administrateur systèmes et réseaux - Alain Bensoussan
Les contrats du numérique - Philippe Le Tourneau - Édition Dalloz
Droit et expertise des contrats informatiques - Hubert Bitan - Edition Lamy

Bloc 2 SLAM - Conception et développement d'applications

Rappel du référentiel des activités professionnelles (RAP)

Pour répondre aux besoins croissants de digitalisation au sein des organisations, les étudiants et apprentis conçoivent, développent et participent au déploiement ainsi qu'à la maintenance des composants logiciels d'une solution applicative. Pour ce faire, elles et ils s'appuient sur des méthodes permettant d'accélérer les phases de développement d'applications informatiques grâce à leur approche modulaire et à la réutilisation de composants logiciels.

Il s'agit également de mettre en œuvre les méthodes et outils de conception, de modélisation, d'administration et de maintenance des bases de données, structurées ou non, à l'heure où les données numériques deviennent un enjeu majeur pour les organisations.

Présentation
Ce bloc prépare les étudiants à devenir des concepteurs-développeurs d'applications. L'acquisition des compétences de ce bloc apporte donc aux étudiants des bases solides dans le domaine de la programmation procédurale, orientée objet et événementielle, de la conception d'architectures logicielles, de l'exploitation et de la manipulation des données ainsi que dans la gestion de projet.

Afin d'acquérir ces compétences, les étudiants peuvent être mis en situation à travers des études de cas et des scénarii qui leur permettront d'appréhender toutes les étapes d'un développement applicatif. L'approche préconisée est de les amener à réaliser des analyses techniques des expressions de besoins et à proposer des solutions en termes d'architectures logicielles et de technologies. Ils apprendront à développer des applications variées : applications mobiles, applications client-lourd, applications client-léger, services web. Ils vont acquérir les techniques de déploiement de ces applications et à en assurer la maintenance en apportant des améliorations correctives et/ou évolutives. Par ailleurs, les étudiants vont également acquérir les compétences liées à la programmation à travers des infrastructures de programmation (*frameworks)*.

Ce bloc apporte également des compétences liées aux différents formats de données exploitées dans les applications et aux architectures des bases de données relationnelles et NoSQL. L'accès aux données depuis les applications peut être réalisé à travers des requêtes du langage de la base de données utilisée, des API ou via des ORM (Object-Relational Mapping).

Le cycle de développement des applications sera abordé en appliquant les méthodes de gestion de projets traditionnelles et agiles.

Une veille technologique sur les langages, les architectures logicielles et les technologies permettra à l'enseignant d'orienter ses choix pédagogiques pour être en adéquation avec les besoins du marché du travail.

L'enseignement de CEJMA permettra aux étudiants de bien cerner le contexte juridique dans lequel s'inscrivent le développement et la maintenance des solutions applicatives, ainsi que la conception et l'exploitation des bases de données.

Positionnement du bloc 2 SLAM
Ce bloc de spécialité commence au **2ème semestre** de la formation initiale pour les étudiants qui ont fait le choix de l'option SLAM. Ce bloc se poursuit en 2ème année.

Durant le semestre 1, les étudiants ont été initiés, dans le bloc 1, aux concepts de base de la programmation à travers une approche, majoritairement, procédurale.

Le **semestre 2** a pour objectif de consolider ces concepts et d'introduire :
- la programmation orientée objet ;
- la modélisation et le maquettage d'une solution applicative ;
- l'adaptation d'une base de données en réponse à de nouveaux besoins ;
- l'accès aux données à travers des requêtes du langage de la base depuis une application.

Les semestres 3 et 4 ont pour objectifs :
- de consolider et approfondir les concepts introduits au semestre 2 ;
- de développer des applications variées (client mobile, léger, lourd) en s'appuyant sur des frameworks et des patterns éprouvés ;
- de programmer et exploiter des services web ;
- d'accéder aux données en privilégiant des ORM ;
- de concevoir et d'adapter des bases de données relationnelles et NoSQL ;
- d'intégrer en continu les versions d'une solution applicative, que ce soit en local ou dans le *cloud*.

Durant les trois semestres, ce bloc apporte les compétences liées à la gestion de projets (agile ou conventionnelle), à la sûreté et à l'estimation du coût d'usage d'une solution applicative.

Dans le cadre du développement d'applications manipulant des données à caractère personnel, les étudiants devront mettre en pratique les compétences du bloc 3 liées au RGPD en matière de traitement, de stockage et d'archivage des données.

Ressources générales
Les ressources du réseau Certa : http://www.reseaucerta.org/
La bibliothèque numérique ENI : https://www.editions-eni.fr/livres-numeriques
Gestion de projet : https://openclassrooms.com/fr/courses/4192086-gerez-votre-projet-informatique-facilement
Modélisation UML : https://openclassrooms.com/fr/courses/2035826-debutez-lanalyse-logicielle-avec-uml/2048781-les-differents-types-de-diagrammes

B2.1 SLAM Concevoir et développer une solution applicative

Cette compétence implique d'amener les étudiants à analyser l'expression de nouveaux besoins. Les étudiants participent à la conception de l'architecture logicielle et sont capables de proposer et d'argumenter leurs choix techniques en termes d'architectures, de langages, de types de bases de données. Lors de cette phase d'analyse, les étudiants interagissent avec différents acteurs en s'appuyant sur des outils collaboratifs de gestion et de suivi de projets.

A l'issue de cette phase, les étudiants mettent en œuvre la solution choisie en respectant les contraintes logicielles, matérielles et réglementaires rencontrées lors de la phase d'analyse. Ils planifient et exécutent des plans de tests (unitaires, fonctionnels, de non-régression, d'acceptation) pour valider leur développement applicatif. Les savoirs et savoir-faire nécessaires à chaque étape du cycle de vie d'une solution applicative sont apportés progressivement, sont consolidés et approfondis tout au long de la formation.

Les méthodes de développement agile et l'utilisation de contextes dans le *cloud* sont recommandées pour permettre aux étudiants de s'initier au développement dans le *cloud* et aux techniques de développement/opérations (DevOps) d'intégration continue et de déploiement continu (CI/CD) en local et dans le *cloud*.

Semestre 2 (1+3) 60h	**Semestres 3 et 4 (2+4) 72h + 72h**
• Analyser un besoin exprimé et son contexte juridique • Modéliser une solution applicative	• *Analyser un besoin exprimé et son contexte juridique (suite)* • *Modéliser une solution applicative (suite)* • Participer à la conception de l'architecture d'une solution applicative • Exploiter les technologies *Web* et mobile pour mettre en œuvre les échanges entre applications, y compris de mobilité
Rappel des savoirs Méthodes, normes et standards associés au processus de conception et de développement d'une solution applicative Architectures applicatives : concepts de base et typologies Techniques et outils d'analyse et de rétro-conception Typologie et techniques des cycles de production d'un service et acteurs associés	**Rappel des savoirs** *Méthodes, normes et standards associés au processus de conception et de développement d'une solution applicative (suite)* *Architectures applicatives : concepts de base et typologies (suite)* Architectures et techniques d'interopérabilité entre applications. *Techniques et outils d'analyse et de rétro-conception (suite)* *Typologie et techniques des cycles de production d'un service et acteurs associés (suite)* Fonctionnalités d'un outil de gestion de projets Composition du coût d'une solution applicative Concepts et techniques de développement agile
• Identifier, développer, utiliser ou adapter des composants logiciels	• *Identifier, développer, utiliser ou adapter des composants logiciels (suite)* • Exploiter les ressources du cadre applicatif (*framework*)

Rappel des savoirs Concepts de la programmation objet : classe, objet, abstraction, interface, héritage, polymorphisme. Interfaces homme-machine : principes ergonomiques, techniques de conception, d'évaluation et de validation Concepts de la programmation événementielle : techniques de gestion des événements et exploitation de bibliothèques de composants graphiques	**Rappel des savoirs** *Concepts de la programmation objet (suite)* : annotations, patrons de conception, interface de programmation d'applications *Interfaces homme-machine : principes ergonomiques, techniques de conception, d'évaluation et de validation (suite)* *Concepts de la programmation événementielle : techniques de gestion des événements et exploitation de bibliothèques de composants graphiques (suite)* Programmation au sein d'un cadre applicatif (framework) : structure, outil d'aide au développement et de gestion des dépendances, techniques d'injection des dépendances
● Utiliser des composants d'accès aux données	● *Utiliser des composants d'accès aux données (suite)*
Rappel des savoirs Caractéristiques des formats de données : **structurées** ou non Persistance et couche d'accès aux données	**Rappel des savoirs** *Caractéristiques des formats de données : **structurées ou non** (suite)* *Persistance et couche d'accès aux données (suite)*
● Exploiter les fonctionnalités d'un environnement de développement et de tests	● *Exploiter les fonctionnalités d'un environnement de développement et de tests (suite)* ● Réaliser des tests nécessaires à la validation ou à la mise en production d'éléments adaptés ou développés ● Intégrer en continu des versions d'une solution applicative ● Évaluer la qualité d'une solution applicative
Rappel des savoirs Fonctionnalités avancées d'un environnement de développement	**Rappel des savoirs** *Fonctionnalités **avancées** d'un environnement de développement (suite)* Techniques de gestion des versions Techniques et outils de tests et d'intégration de composants logiciels
● Rédiger des documentations techniques et **d'utilisation** d'une solution applicative	● *Rédiger des documentations **techniques** et d'utilisation d'une solution applicative (suite)*
Rappel des savoirs Techniques et outils de documentation	**Rappel des savoirs** *Techniques et outils de documentation (suite)*
Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA	
Cahier des charges et ses enjeux juridiques Contraintes éthiques et environnementales dans la conception d'une solution applicative Contrat de développement (formation, exécution, inexécution) et ses clauses spécifiques Typologie de licences logicielles et droits des utilisateurs Protection juridique des productions de solutions applicatives : droit d'auteur, modes de protection indirects et conditions de brevetabilité	

Responsabilité civile et pénale du concepteur de solutions applicatives
Réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel

Rappel : Indicateurs de performance

- *La modélisation de l'application est conforme aux besoins.*
- *La maquette des éléments applicatifs de la solution respecte les fonctionnalités exprimées*
- *Les spécifications de l'interface utilisateur répondent aux contraintes ergonomiques*
- *Le choix des composants logiciels à utiliser et/ou à développer est pertinent*
- *Les composants logiciels sont validés par les procédures de tests unitaires et fonctionnels*
- *Un service Web est exploité pour échanger des données entre applications*
- *Les données persistantes liées à la solution applicative sont exploitées à travers :*
  - *un langage de requête lié à la base de données qui peut être le langage de requête proposé par les échanges applicatifs des technologies Web,*
  - *un langage de requête présent dans l'outil de correspondance objet-relationnel*
  - *toute autre solution de persistance*
- *Le développement répond à l'expression des besoins fonctionnels et respecte les contraintes techniques figurant dans le cahier des charges*
- *Les tests d'intégration sont réalisés*
- *Un outil collaboratif de gestion des itérations de développement et de versions est utilisé*
- *Une documentation des versions vient appuyer l'intégration continue*
- *Les composants logiciels sont documentés de manière à être réutilisés*
- *Un document est rédigé pour chaque contexte d'utilisation de l'application et est adapté à chaque destinataire tant par son contenu que par sa présentation*
- *Le développement tient compte des préoccupations de développement durable.*
- *L'application développée est opérationnelle conformément au cahier des charges et stable dans l'environnement de production*
- *Les tests de non régression sont réalisés.*

Analyser un besoin exprimé et son contexte juridique

Cette compétence place les étudiants en situation d'analyser un besoin applicatif exprimé par un client. Les étudiants pourront, à partir d'un cahier des charges fourni par l'enseignant, apprendre à délimiter le domaine d'étude, à identifier les acteurs, les finalités et les fonctionnalités de l'application, et à appréhender une architecture applicative et ses composants. Ils se forment ainsi à la première étape du processus de développement d'une solution applicative.

Cette compétence, initiée au semestre 2, met l'accent, en 2ème année, sur une approche plus agile du cycle de conception de la solution applicative. C'est

donc une consolidation de la compétence “Travailler en mode projet” du bloc 1 dans le domaine du développement avec une mise en pratique qui privilégie les méthodes agiles. Le calcul de coût du développement sera également étudié.

Le besoin fourni par l’enseignant peut être exprimé sous différentes formes : scénarii, descriptions de cas d’utilisation (*use case*), récits d’utilisateur (*user stories*). Cette compétence peut être travaillée en fournissant un dossier de spécifications et en demandant aux étudiants de décrire une fonctionnalité de leur choix à travers un récit d’utilisateur pour apporter plus de précisions au développeur. A travers cette compétence, les étudiants consolident les concepts de l’agilité dans le développement : vocabulaire (itération, incrémentation, *backlog*...), acteurs (*scrum master, product owner*...), outils de suivi de projet et logiciels de gestion de projets.

Des jeux de rôle peuvent être organisés pour permettre à chaque étudiant d’endosser un rôle particulier (*scrum master, product owner*, MOA, MOE) afin de comprendre les responsabilités et la fonction de chaque rôle dans les projets de développement d’application ainsi que les interactions entre les différents acteurs d’un projet en mode agile.

L’enseignement de CEJMA pourra compléter la lecture technique du cahier des charges par une approche juridique, et notamment amener les étudiants à réfléchir sur l’intérêt et la valeur juridique de ce document précontractuel. Il pourra faire le lien entre la rédaction du cahier des charges et les obligations respectives de l’organisation cliente (obligation de collaboration) et du prestataire (obligation de conseil) dans le contrat de développement ainsi que la mise en œuvre de la responsabilité civile contractuelle des parties en cas de non-respect.

Ressources suggérées :

- Langage UML ou tout outil de modélisation équivalent pour créer tout diagramme utile pour la maîtrise d’ouvrage (diagramme de cas d’utilisation, d’activités, d’états-transition…).
- L’agilité dans l’entreprise - modèle de maturité - rapport cigref 2015
- Méthode agile : Scrum
- Plateformes collaboratives de communication avec le client : Balsamiq[4], Trello, Slack
- Logiciels de gestion de projet : Jira, Kanboard, Redmine….

Ressources CEJMA :

- www.alain-bensoussan.com/avocats/methodes-agiles-responsabilites-imprevision
- Les contrats du numérique - Philippe Le Tourneau - Edition Dalloz
- Droit et expertise des contrats informatiques - Hubert Bitan - Edition Lamy

Modéliser une solution applicative

Après analyse du cahier des charges, les étudiants apprennent à modéliser l’architecture applicative retenue. Ils se familiarisent avec les diagrammes de modélisation courants (diagramme de cas d’utilisation, diagramme d’activités, diagramme de classes) et commencent à pratiquer le maquettage d’interface.

[4] *Shareware* mais à ce jour il y a la possibilité d’une offre gratuite pour une utilisation en classe (https://balsamiq.com/givingback/free/classroom/)

En seconde année les étudiants consolident l'utilisation des diagrammes vus au 2ème semestre et sont capables d'interpréter et de concevoir tout autre diagramme nécessaire à la modélisation de l'architecture applicative telle que les diagrammes de séquence, diagrammes de classes et interactions entre classes, diagramme d'objets, diagrammes de déploiement....

Ressources suggérées :

- Langage UML : diagramme de cas d'utilisation, d'activités, de classes, de séquence, description de cas d'utilisation
- Outils de maquettage fonctionnel : Mockflow, Mockups, Pencil Evolus...

Identifier, développer, utiliser ou adapter des composants logiciels

L'acquisition de cette compétence s'appuie sur la réalisation d'applications graphiques (client lourd/léger), d'applications mobiles et d'applications Web avec ou sans *framework*.

Il s'agit ici de consolider la maîtrise des concepts de base de la programmation traités dans le bloc 1 et d'introduire les concepts fondamentaux de la programmation orientée objet (POO) à travers des exemples d'applications fournis par l'enseignant. La mise en pratique de ces concepts sera réalisée de manière progressive à travers des modifications de situations professionnelles existantes et l'expression de nouveaux besoins. Les étudiants seront amenés à utiliser des classes prédéfinies du langage, à en définir de nouvelles, à instancier des objets et à mettre en œuvre le concept d'héritage entre classes et ses mécanismes (encapsulation, instanciation, redéfinition de méthodes, surcharge de méthodes, casting, classes abstraites, interfaces, polymorphisme, programmation générique). Ils sont capables d'implémenter des cas d'utilisation dans le langage POO choisi, de traduire un diagramme de classes et les différents liens entre classes dans le langage POO. Les différentes techniques pour organiser un nombre fixe ou indéterminé d'objets seront également étudiées dans cette compétence (tableaux, collections, dictionnaires…).

Enfin, une introduction aux outils graphiques proposés par le langage et l'environnement de développement utilisé permettra d'initier les étudiants aux IHM, aux composants graphiques des bibliothèques logicielles et aux concepts de la programmation événementielle. Cela leur permettra de consolider davantage les concepts liés aux interfaces et à l'héritage.

Les étudiants programment dans un environnement de développement intégré et sont amenés à exploiter progressivement ses fonctionnalités.

Tout au long de leur apprentissage, les étudiants respectent les bonnes pratiques du développement logiciel.

En seconde année cette compétence approfondit les concepts fondamentaux de la POO et les enrichit à travers la métaprogrammation par annotations et la programmation par les *frameworks*.

Le concept de réutilisation de composants amène les étudiants à mettre en œuvre des patrons de conception (*design pattern*) éprouvés et à exploiter davantage la programmation par les composants à travers l'utilisation de *frameworks* populaires chez les développeurs. Les caractéristiques du *framework* et les techniques pour programmer au sein de ce dernier doivent être maîtrisées pour développer des applications répondant à de nouveaux besoins ou de nouvelles améliorations.

Les concepts de la métaprogrammation par les annotations pour séparer les traitements métier des services annexes sont étudiés. Ces concepts seront approfondis et mis en pratique dans d'autres cadres tels que la documentation d'une application, la journalisation ou encore lors de la mise en œuvre d'un ORM (*Object-Relational Mapping*).

La programmation par configuration est exploitée à travers les techniques d'injection des dépendances afin de faciliter la configuration de l'application logicielle.

Ressources suggérées :

- Langages de programmation objet : Java, Python, C#, C++, etc. La liste présentée n'est pas exhaustive et le choix du langage pour l'apprentissage de la POO devrait tenir compte, autant que possible, de la popularité du langage dans la profession.
- Environnement de développement : NetBeans, Eclipse, IntelliJ, VisualStudio…
- Patrons de conception : les 23 patrons du GoF (Gang Of four)
- Frameworks PHP : Symfony, Laravel, CodeIgniter, Zend etc.
- Frameworks JavaScript : React, Angular....
- Framework Python : Django, Flask etc.
- *Framework Java : J2EE, Spring, Apache Struts etc.*

Utiliser des composants d'accès aux données

Cette compétence étudie les différentes API (*Application Programming Interface*) qui implémentent la couche de persistance des données et permettent à la couche métier d'accéder à ces données à travers des objets.

Pour ne pas perdre de vue l'objectif de cette compétence au second semestre et ne pas complexifier son apprentissage, on s'appuie sur le langage d'accès et d'interrogation de données que les étudiants ont manipulé dans le bloc 1 (1er semestre) ou qu'ils manipulent dans l'activité B2.3 du bloc 2.

Les étudiants vont apprendre, depuis leur application, à dialoguer avec le SGBD et à programmer les opérations CRUD *(Create, Read, Update, Delete)* sur les enregistrements des bases de données à travers les requêtes (SQL ou non) exécutées grâce aux méthodes de l'API choisie. Les données récupérées depuis la base de données peuvent être encodées dans le format souhaité : JSON, XML, HTML...

Les situations professionnelles proposées s'appuient sur des bases de données fournies et implémentées par l'équipe pédagogique sur un serveur distant.

En seconde année cette compétence approfondit les concepts de la couche de persistance de données étudiés au semestre 2 et l'enrichit à travers l'exploitation d'outils de mapping objet-relationnel (*ORM*) dans le cas des bases de données relationnelles.

Les applications développées par les étudiants interagissent également avec des bases de données NoSQL hébergées sur des serveurs locaux ou dans le cloud.

L'apprentissage de la compétence s'appuie sur des bases de données fournies par l'enseignant ou construites par les étudiants dans la compétence B2.3.

Les situations professionnelles présentant de nouveaux besoins sollicitent des compétences associées aux deux activités B2.1 et B2.2. Une collaboration entre les enseignants en charge de ces activités B2.1 et B2.3 est vivement recommandée. Elle mettra les étudiants dans un contexte pluridisciplinaire nécessitant de leur part à la fois une réflexion sur les données à manipuler, le choix de la technologie appropriée (SQL vs NoSQL) et l'impact de ce choix sur le développement de l'application et l'accès aux données.

Il conviendra de rappeler aux étudiants que l'exploitation de données à caractère personnel est réglementée (réglementation étudiée en CEJM - thème 4 - question 2 et complétée dans le bloc 3).

Ressources suggérées :

- Bases de données SQL : Mysql, Oracle, PostgreSQL…
- Bases de données NoSQL : MongoDB, Neo4j, Elasticsearch, Cassandra,...
- API d'accès aux données : PDO (PHP Data Objects), JDBC (Java DataBase Connectivity), ODBC, Mongo DB, JNoSQL, GraphQL ...
- ORM : Hibernate, JPA, Doctrine 2, EJB, Django ORM, Entity framework …
- Solutions cloud : services Amazon AWS (DynamoDB), Google (Cloud datastore), Microsoft Azure…
- Architectures Docker et conteneurisation

Exploiter les fonctionnalités d'un environnement de développement et de tests

Cette compétence est naturellement indispensable pour les deux compétences précédentes. Les étudiants doivent acquérir les connaissances sur les fonctionnalités de base d'un environnement de développement intégré (IDE) afin d'en exploiter les différents outils de base : éditeur de code avec les possibilités d'auto-complétions, de coloration syntaxique, de mise en forme. Ils peuvent également compiler et exécuter leur application. Il s'agit ici de leur permettre de manipuler un environnement convivial et intuitif pour faciliter le développement de leurs applications.

Au fur et à mesure de leur apprentissage, les étudiants explorent d'autres possibilités de l'IDE telles que les fonctionnalités de débogage ou de génération automatique de code (constructeurs, getters/setters, redéfinition de méthodes).

La mise en place de tests de validation d'une application est une compétence qui doit être introduite dans ce bloc le plus tôt possible. On s'intéressera aux tests unitaires. Dans un premier temps, des plans de tests peuvent être fournis par l'enseignant et analysés, voire modifiés par les étudiants. Les étudiants peuvent, dans un second temps, s'inspirer de ces tests et se servir des modèles générés par l'IDE pour développer leurs propres tests unitaires des fonctionnalités ajoutées.

Dans cette compétence, initiée au semestre 2, les étudiants exploitent en seconde année les fonctionnalités avancées de l'IDE telles que : la liste des tâches, la comparaison d'éléments, l'utilisation de l'aide en ligne ou d'une page documentée d'un élément, la génération de la documentation, l'utilisation de l'historique local, le nettoyage de code, la mise en œuvre du débogueur, le ré-usinage de code (*refactoring)*, la gestion de versions ou encore l'installation de modules d'extensions (*plugins*) pour réaliser des interfaces graphiques.

Les étudiants sont capables de naviguer dans le code de leur application en exploitant les fonctionnalités citées ci-dessus et en personnalisant davantage la configuration de leur IDE en fonction des besoins du développement logiciel.

Ils exploiteront également les menus de tests et les modèles générés par l'IDE permettant d'exécuter et d'analyser le résultat des tests unitaires ou de couverture.

Ressources suggérées :

- Environnement de développement intégré : NetBeans, Eclipse, IntelliJ, VisualStudio, Visual Studio Code ...

Rédiger des documentations techniques et d'utilisation d'une solution applicative

L'accent sera mis, au semestre 2, sur les techniques de rédaction de la documentation d'utilisation d'une solution applicative et de son cycle de vie (planification, production, test, livraison). Les étudiants identifient qui est l'utilisateur final et choisissent le type de document adéquat à exploiter selon le contexte pour accompagner l'utilisateur dans la prise en main de l'application. L'interface de l'application ainsi que l'intégralité de ses fonctionnalités sont décrites de manière claire et synthétique avec des captures d'écrans illustrant l'enchaînement des étapes. Les formats sont variés : document HTML, PDF, bulles d'aide qui renvoient à des fichiers d'aide ou encore la mise en œuvre d'un Wiki ou d'une FAQ.

Des exemples de documentation d'utilisation d'applications et/ou logiciels peuvent être fournis et les étudiants seront invités à jouer le rôle de l'utilisateur final afin de les amener à repérer les points positifs, les défauts et manques de ces documentations, et à s'interroger sur le contenu pertinent de ce type de documentation.

Quant à la documentation technique, elle sera découverte par les étudiants à travers la consultation de documentation technique des composants qu'ils utilisent dans leur développement.

Étape importante du développement d'une application, la documentation technique est souvent négligée par les étudiants. Il est donc important de les sensibiliser sur son intérêt pour maintenir et faire évoluer une application. La documentation technique d'une application englobe :

- les prérequis techniques (hardware, os, composants externes mais nécessaires à l'application…),
- la description technique des différentes classes, interfaces et méthodes du projet. Cette documentation doit être générée automatiquement par le Framework de documentation spécifique au langage utilisé,
- un document d'installation et de déploiement de l'application,
- une description des fonctionnalités et de l'architecture de l'application.

Le framework peut être intégré à l'IDE pour exploiter efficacement ses fonctionnalités. Il est également important que les étudiants soient capables de faire la différence entre commenter un code et le documenter (commentaire de fond).

Ressources suggérées :

- Techniques de rédaction : https://www.techscribe.co.uk/ta/how-to-write-user-documentation.htm
- phpDocumentor : https://www.phpdoc.org/
- JavaDoc : https://docs.oracle.com/javase/8/docs/technotes/tools/windows/javadoc.html
- pydoc : https://docs.python.org/fr/2.7/library/pydoc.html
- outil polyvalent de documentation disponible pour plusieurs OS et langages : doxygen : http://doxygen.nl

Participer à la conception de l'architecture d'une solution applicative
En seconde année les étudiants approfondissent les différentes couches techniques et logicielles d'une architecture N-tiers (présentation, applicative, objets métiers, serveur de données) et participent à sa conception et à sa mise en œuvre. Ils doivent être capables de justifier le choix de l'architecture logicielle de l'application et de documenter ses composants et ses connecteurs. Les concepts liés aux architectures orientées services (SOA), micro services (REST), FAAS (*Function As A Service* ou encore *ServerLess computing)* seront également étudiés dans cette compétence, de même que les outils de leur mise en œuvre tels que l'exploitation du *cloud* ou les techniques de conteneurisation. Avec l'arrivée de nouvelles technologies, il est important de suivre l'évolution des architectures logicielles pour aborder, autant que possible, les nouvelles tendances d'architectures.

L'enseignement de CEJMA aura pour objectif de sensibiliser les étudiants aux problématiques éthiques et environnementales soulevées par l'activité informatique, et ce, à partir d'exemples choisis dans l'actualité. L'environnement économique et légal oblige de plus en plus les organisations à adopter des démarches éthiques et éco responsables dans la conception d'une solution applicative (logiciel éco-conçus, conception responsable de services numériques etc.). Les étudiants tiendront compte de ces préoccupations dans le développement de leur solution (*la notion d'externalités négatives générées par l'activité des organisations ainsi que l'étude de la responsabilité éthique, sociale, sociétale et environnementale des entreprises sont abordées respectivement dans le thème 1 question 1 et le thème 3 question 4 du programme de CEJM).*

Ressources CEJMA :
- Rapports Cigref « Ethique et numérique » 2014 et 2018
- www.cigref.fr/wp/wp-content/uploads/2018/10/Cigref-Syntec-Numerique-Referentiel-pratique-Ethique-et-Numerique-2018.pdf
- www.greenit.fr

Exploiter les technologies *Web* pour mettre en œuvre les échanges entre applications, y compris de mobilité
En seconde année, les étudiants mobilisent les concepts d'architectures orientés services/microservices (compétence : *participer à la conception de l'architecture d'une solution applicative*) afin d'identifier et de mettre en place les interfaces nécessaires pour échanger des données entre applications hétérogènes dans un contexte technologique distribué. Ils choisissent parmi différents formats d'échange (XML, JSON, HTML, CSV) la représentation des données de retour. Dans ce cadre, le fonctionnement d'un *web service* ainsi que les règles de son implémentation seront étudiés : identification de la ressource (URL), identification des opérations (requêtes/réponses HTTP), accès aux ressources, jeton d'authentification...

Cette compétence peut être acquise, par exemple, à travers un contexte d'une application mobile ou non qui nécessite des données issues d'une base de données (relationnelle ou non) située sur un serveur distant ou dans le *cloud*.

Ressources

- Utilisation de web services, etc.
- Architectures REST, N-tiers, MSA, architectures à base de conteneurs : docker...

Exploiter les ressources du cadre applicatif (*framework*)

Cette compétence est liée à la programmation par les *frameworks*. Dans ce cadre, les étudiants développent des applications logicielles à partir d'un *framework*. Ils sont capables d'investir les principales fonctionnalités du *framework* et être capables de justifier leur choix de cadre applicatif. Ils exploitent les outils et les commandes propres au *framework* pour construire la structure de leur application, optimiser son développement et gérer ses dépendances.

Ressources :

- Langages de programmation orientés objet
- Frameworks PHP : Symfony, Laravel, CodeIgniter, Zend…
- Frameworks JavaScript : React, Angular, JQuery…
- Framework Python : Django, Flask…
- Framework Java : J2EE, Spring, Apache Struts...

Réaliser des tests nécessaires à la validation ou à la mise en production d'éléments adaptés ou développés

Cette compétence concerne tous les tests nécessaires pour valider les fonctionnalités d'une application. A partir des cas d'utilisations, les étudiants seront capables de concevoir un plan de tests et de planifier des jeux d'essais. On abordera ici le cycle de vie d'un test (schéma *Arrange-Act-Assert*), les assertions, les tests fonctionnels, les tests d'intégration et on consolidera la pratique de tests unitaires abordés au 2ème semestre. On privilégiera l'utilisation de *frameworks* de tests quand cela est possible.

Dans une démarche de projet agile, cette compétence peut être abordée en même temps que la compétence concernant l'intégration continue.

Ressources :

- Environnement de développement intégré : NetBeans, Eclipse, IntelliJ, VisualStudio…
- Frameworks de tests : JUnit, PHPUnit, Visual Studio Unit

Intégrer en continu des versions d'une solution applicative

Cette compétence permet aux étudiants l'acquisition de nouvelles pratiques en matière de développement, d'intégration et de déploiement des applications. Elle amène les étudiants à mettre en œuvre des outils d'automatisation et à adopter une démarche DevOps pour intégrer, livrer et déployer en continu une application. En effet, l'approche DevOps s'appuie sur les cycles itératifs et le CI/CD. La pratique de l'intégration continue (*Continuous Integration - CI*) consiste à vérifier que toute modification apportée par un développeur ne produit pas de régression dans l'application. Les étudiants s'initient aux outils qui

permettent de construire un *build* qui compile et exécute, de manière automatisée, les tests unitaires. Cette automatisation permet de détecter rapidement les problèmes liés à l'intégration de nouveaux composants/modules pour les équipes de développement et d'exploitation. Chaque changement qui passe les tests automatisés est ensuite déployé automatiquement en production (*Continuous Deployment - CD*). A travers ce cycle itératif, les étudiants prennent conscience des problématiques liées au déploiement et sont capables d'identifier clairement les étapes qui sont en échec. Ils comprennent également l'intérêt de l'automatisation des tâches du cycle CI/CD pour mener à la mise à disposition de l'application aux utilisateurs, notamment une réduction des délais de déploiement de l'application ou d'une nouvelle fonctionnalité et l'amélioration de la fiabilité du produit par réalisation des tests.

Afin d'acquérir cette compétence, les étudiants travaillent dans un contexte de projet agile. Des équipes seront constituées. Chaque développeur aura des composants à développer et/ou adapter et chaque étudiant jouera le rôle d'intégrateur agile à un moment donné du développement. L'idée étant de permettre à chacun de manipuler les outils spécifiques d'automatisation du processus d'intégration et de déploiement continu. A tour de rôle, un développeur de l'équipe endossera le rôle de client.

On peut faire travailler les différentes équipes avec des outils différents et un comparatif de ces outils pourra être réalisé afin de permettre aux étudiants de faire un choix judicieux d'outils d'intégration continue dans d'autres projets. Chaque équipe peut présenter les caractéristiques et fonctionnalités des outils CI/CD à travers une démonstration aux autres étudiants.

A travers l'utilisation d'outils CI/CD, les étudiants assimilent les différentes étapes du cycle de vie des applications : développement, intégration et test, distribution et déploiement. Ces étapes désignées par "pipeline CI/CD" reposent sur la collaboration agile entre les développeurs et les équipes d'exploitation.

Cette compétence peut être également exploitée dans les ateliers de professionnalisation afin d'illustrer le métier DevOps en constituant des équipes composées d'étudiants de l'option SISR et de l'option SLAM. Elle nécessite comme prérequis la compétence de gestion de projet et le cycle de développement d'une application en mode agile.

Ressources :

- Approche CI/CD : https://www.redhat.com/fr/topics/devops/what-is-ci-cd
- Outils CI/CD : Jenkins, GitLab CI/CD, TeamCity, Visual Studio Team Services (VSTS) …
- CI/CD, DevOps, et cloud : https://www.lemagit.fr/conseil/CI-CD-DevOps-et-Cloud-les-elements-cle-de-la-modernisation-des-applications
- CI/CD et Kubernetes => https://docs.microsoft.com/fr-fr/azure/architecture/microservices/ci-cd-kubernetes
- Article : Professionnaliser et fiabiliser ses déploiements avec VSTS et Azure - Programmez - mai 2017

Apports CEJMA :

La compétence "Concevoir et développer une solution applicative" pourra être complétée avec l'enseignement de CEJMA qui abordera les aspects juridiques suivants :

- Le développement d'une solution applicative donne lieu lorsqu'elle est réalisée par un prestataire, à la conclusion d'un contrat de prestation de service informatique. L'enseignant proposera *en prolongement du thème 1 question 2 et du thème 4 question 2 du programme de CEJM,* l'étude d'un contrat de développement de solution applicative afin d'y repérer les clauses spécifiques notamment celles relatives aux obligations respectives des parties (informations, conseils, collaboration, recette, etc.), la clause relative aux droits de propriété intellectuelle, les cas dans lesquels les parties engagent leur responsabilité, les causes d'exonération ou de limitation de responsabilité respectives ainsi que les clauses de résiliation du contrat.
  Une attention spécifique pourra être portée à l'adaptation en amont du cahier des charges ("Agilité du cahier des charges") et du contrat ("Agilité du

contrat"), en cas de mise en œuvre de méthodes agiles dans le cycle de conception de la solution applicative, et ses conséquences sur la responsabilité de l'organisation cliente et du prestataire.

- L'utilisation d'une solution applicative ou d'un composant logiciel doit s'effectuer dans le respect de la licence souscrite. *En prolongement du thème 4 question 2 du programme de CEJM*, une typologie des licences sera proposée aux étudiants afin qu'ils distinguent les droits attachés aux différentes catégories (licence propriétaire/libre, licence libre restrictive (ou licence copyleft) / permissive (ou licence non copyleft) sans attendre l'exhaustivité.
- La solution applicative bénéficie de la protection juridique par le droit d'auteur. *En prolongement du thème 4 question 2 du programme de CEJM*, il conviendra de montrer que la condition d'originalité qui permet au concepteur d'une solution applicative de bénéficier du droit d'auteur a subi des évolutions jurisprudentielles, et d'évoquer les autres dispositifs de protection (protection indirecte par les dépôts pour faire la preuve de l'antériorité, par le droit des marques, des dessins et modèles et sous certaines conditions par le brevet).
- La responsabilité du concepteur d'une solution applicative peut être engagée : responsabilité civile du concepteur de solutions applicatives en cas de non-respect de ses obligations et de préjudices causés au client (insuffisance d'informations fournies au client, délivrance non conforme, dépassement des délais et du budget etc.), et responsabilité pénale en cas de commission d'une infraction (copie illicite du code source d'un logiciel ou de composants logiciels, reproduction illicite de créations graphiques etc.). Les cas dans lesquels le concepteur de solutions applicatives pourra s'exonérer de sa responsabilité pourront également être abordés notamment en cas de défaut de collaboration du client. Cette étude s'appuiera *sur les savoirs acquis dans le thème 3 question 3 du programme de CEJM* et sur l'analyse de la jurisprudence.

Ressources CEJMA :

- www.legalis.net
- www.droit-technologie.org/contentieux/contentieux-lies-aux-contrats-informatiques/#_ftn15
- Revues Lexisnexis communication commerce électronique - Panorama de jurisprudence relative aux contrats informatiques -numéro 7-8 ; juillet/août 2019
- Les contrats du numérique - Philippe Le Tourneau - Edition Dalloz
- Droit et expertise des contrats informatiques - Hubert Bitan - Edition Lamy
- Cyberdroit - le droit à l'épreuve de l'internet - Christiane Féral-Schuhl - Edition Dalloz 2018/2019
- Droit des créations immatérielles - Hubert Bitan- Edition Lamy

B2.2 SLAM Assurer la maintenance corrective ou évolutive d'une solution applicative

Cette compétence s'inscrit naturellement dans le cycle de développement d'une application. Elle apporte les savoirs et les techniques nécessaires à la maintenance préventive, corrective et évolutive d'une application.

Semestre 2	**Semestres 3 et 4**
Les heures d'enseignement de ce bloc sont intégrées dans la compétence 2.1	
• Évaluer la qualité d'une solution applicative • **Recueillir**, analyser et **mettre à jour** les informations sur une version d'une solution applicative • Analyser et **corriger** un dysfonctionnement • Elaborer et réaliser des tests des éléments mis à jour • Mettre à jour la documentation technique et **d'utilisation** d'une solution applicative	• *Évaluer la qualité d'une solution applicative (suite)* • *Recueillir, **analyser** et mettre à jour les informations sur une version d'une solution applicative (suite)* • ***Analyser** et corriger un dysfonctionnement (suite)* • *Elaborer et réaliser des tests des éléments mis à jour (suite)* • *Mettre à jour la documentation **technique** et d'utilisation d'une solution applicative (suite)*
Rappel des savoirs Techniques de gestion des erreurs et des exceptions	**Rappel des savoirs** *Techniques de gestion des erreurs et des exceptions (suite)*
Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA	
Contrat de maintenance applicative (formation, exécution, inexécution) et ses clauses spécifiques	

Indicateurs de performance

- *La modélisation de l'application existante est mise à jour par les nouvelles fonctionnalités et/ou les nouveaux correctifs apportés.*
- *L'interface utilisateur est mise à jour en respectant les contraintes ergonomiques.*
- *Des composants logiciels sont adaptés pour améliorer la qualité de la solution applicative.*
- *Les composants logiciels adaptés et/ou corrigés sont validés par les procédures de tests unitaires et fonctionnels.*
- *Le dysfonctionnement de la solution existante est corrigé selon les procédures en vigueur et dans les délais.*
- *La documentation technique et d'utilisateurs de la solution applicative sont mises à jour.*
- *L'application améliorée et/ou corrigée est opérationnelle et stable dans l'environnement de production.*

- *L'évolution de la solution applicative répond aux besoins exprimés dans le cahier des charges*
- *Les accès aux données persistantes à travers le langage de requête du système de gestion de base de données relationnel, le langage de requête proposé par les échanges applicatifs des technologies Web, le langage de requête de l'outil de correspondance objet-relationnel ou toute autre solution de persistance sont mis à jour.*

Évaluer la qualité d'une solution applicative

L'enseignant peut s'appuyer sur la norme ISO 9126 (remplacée par l'ISO 25010) pour initier les étudiants à la qualité logicielle : capacité fonctionnelle, facilité d'utilisation, fiabilité, performance, maintenabilité et portabilité. Il s'agit ici de sensibiliser les étudiants à chacun des six groupes d'indicateurs de la norme. Des applications mal conçues, peu lisibles ou peu évolutives mettant l'accent sur un ou plusieurs indicateurs de qualité défaillants seront fournies par l'enseignant. Les étudiants s'exercent à repérer les défauts de l'application et à y remédier.
L'accent est mis sur le respect des standards de codage et de documentation de l'équipe au travers d'outils d'analyse statique de code.

Les étudiants approfondissent, en seconde année, les bonnes pratiques de développement et exploitent des outils d'audit de code. Les concepts de gestion des exceptions et de journalisation sont également étudiés pour fiabiliser les applications développées.

L'audit des applications peut être l'occasion de sensibiliser les étudiants à la maintenance préventive qui peut être nécessaire suite à des évolutions technologiques (composants ou méthodes obsolètes), réglementaires (applications existantes ne prenant pas en compte le RGPD alors qu'elles manipulent des données à caractère personnel) ou de sécurité (découverte de faille de sécurité étudiée dans le bloc 3).

La revue de code est également un moyen de former les étudiants à l'amélioration de la qualité d'un développement en détectant les défauts au plus tôt, que ce soit sur le fond (fonctionnement) ou sur la forme (respect des standards, lisibilité…). On peut pratiquer une revue de code par un pair dans le cadre d'un projet en binôme (à chaque développement d'une fonctionnalité par un étudiant, l'autre étudiant est chargé de s'occuper de la revue) ou une revue de code collective organisée par l'enseignant. Le système de gestion de versions peut être configuré pour notifier toute modification d'un développement aux relecteurs désignés.

Ressources :

- Norme ISO 9126 : https://fr.wikipedia.org/wiki/ISO/CEI_9126
- Les 5 règles pour maintenir un code maintenable - Principes SOLID (Single responsability - Open closed - Segregation - Dependency inversion) : Linux Magazine Sept-Oct 2019
- Coder proprement, Robert C. Martin, Pearson, 2019
- Php CodeSniffer, Standard (JavaScript), CheckStyle (Java), pycodestyle (Python)...
- https://promyze.com/wp-content/uploads/cartographie-de_23365438-5.png
- Frameworks de journalisation
- Sonarqube....

Recueillir, analyser et mettre à jour les informations sur une version d'une solution applicative
Les outils de gestion de versions et de collaboration sont devenus incontournables dans le milieu du développement. Les étudiants vont être amenés à travailler à plusieurs sur des projets informatiques, que ce soit en ateliers de professionnalisation ou dans les cours de développement. Il s'agit donc de leur faire découvrir les fonctionnalités basiques d'un gestionnaire de versions de code source pour qu'ils puissent collaborer efficacement et être sûrs de toujours travailler sur la bonne version du projet.

Dans un premier temps, les étudiants manipulent les commandes de base de l'outil en local pour bien comprendre le fonctionnement et le principe d'historisation de code. La deuxième étape consistera à les faire travailler sur un serveur de gestion de versions distant.
Afin d'encourager cette pratique, les applications pédagogiques devront être fournies par l'enseignant à travers un serveur de gestion de versions.

Cette compétence, initiée au semestre 2, est exploitée en seconde année de manière plus approfondie et plus soutenue. Les possibilités et les commandes avancées des outils de gestion de versions et de collaboration sont étudiées telles que la gestion des branches, exclusion de suivi de version, historique, nettoyage… La gestion de tickets d'incidents fournis par l'outil de versionnage est intégrée dans la compétence.

Ressources :

- Git, GitLab, Subversion, Enalean Tuleap (FR)…

Analyser et corriger un dysfonctionnement

L'enseignant fournit des applications présentant des dysfonctionnements en adéquation avec les compétences acquises dans le bloc 2.1 et 2.3. Les étudiants s'appuient sur leurs connaissances, en cours de formation, pour analyser le code, identifier la source de l'anomalie et la corriger.

Elaborer et réaliser des tests des éléments mis à jour

Cette compétence est liée au test d'une application lors d'une mise à jour évolutive et/ou corrective. Elle englobe la réalisation de tests unitaires, fonctionnels des éléments modifiés et/ou mis à jour et de non-régression. Elle s'appuie sur les savoirs et savoir-faire de la même compétence du bloc 2.1.

Il serait pertinent de s'appuyer sur les techniques CI/CD pour automatiser ces tests.

Mettre à jour la documentation technique et d'utilisation d'une solution applicative

L'accent est mis sur la documentation d'utilisation d'une application que les étudiants sont capables de maintenir et de versionner. Cette compétence met en pratique et consolide les techniques de la compétence "Rédiger une documentation d'utilisation" du bloc 2.1.

En seconde année les étudiants sont capables de maintenir et de versionner une documentation technique d'une solution applicative. Cette compétence met en pratique et consolide les techniques de la compétence "Rédiger une documentation technique" du bloc 2.1.

Dans le cadre de **l'enseignement de CEJMA**, un contrat de maintenance d'une solution applicative pourra être proposé aux étudiants afin qu'ils y repèrent les obligations respectives des deux parties (possibilité de compléter avec l'étude de quelques décisions de justice).

B2.3 SLAM Gérer les données

Cette compétence travaille davantage sur l'analyse, la conception, l'exploitation sécurisée des données d'une organisation et l'administration des bases de données. Avec l'arrivée des données massives (big data) et des nouvelles architectures pour leur stockage et leur traitement, les étudiants sont amenés à gérer les données dans un contexte de bases de données relationnelles et NoSQL. Cette compétence s'appuiera sur les compétences du bloc 3 en matière de traitement des données à caractère personnel.

Semestre 2 (1+1) - 30h	**Semestres 3 et 4 (1+2) - 36h + 36h**
• Exploiter des données à l'aide d'un langage de requêtes • Concevoir ou **adapter** une base de données	• *Exploiter des données à l'aide d'un langage de requêtes (suite)* • ***Concevoir** ou adapter une base de données (suite)* • Développer des fonctionnalités applicatives au sein d'un système de gestion de bases de données (relationnel ou non) • Administrer et déployer une base de données
Rappel des savoirs Méthodes et outils de modélisation des données Typologie des bases de données Caractéristiques des formats de données structurées ou non Langage et outils de manipulation d'une base de données. Langage de contrôle des données Langage de définition des données. Modèles de référence de représentation des données. Outil de génération et de rétro-conception	**Rappel des savoirs** Techniques et outils avancés intégrés au système de gestion de base de données : transactions, gestion des erreurs, mesure de performances, méthodes et techniques d'optimisation des données et de leur accès, méthodes et techniques de disponibilité et d'intégrité des données. Principaux concepts des systèmes de gestion de bases de données : structure et implémentation des données, architecture et infrastructure de stockage, contrainte d'intégrité, de confidentialité et de sécurité des données, propriétés de cohérence, de disponibilité et de distribution des données. Langage d'automatisation des actions dans une base de données. *Langage de définition des données, des contraintes et de contrôle des données (suite).* *Outil de génération et de rétro-conception (suite).*
Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA	
Réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel Protection juridique des bases de données par le droit d'auteur et le droit du producteur Responsabilité civile et pénale du concepteur de bases de données	

Indicateurs de performance

- *L'exploitation des données permet de construire l'information attendue*
- *Les accès aux données sont contrôlés conformément aux habilitations définies par le cahier des charges.*
- *Les traitements pris en charge par les composants développés dans la base de données sont conformes aux demandes du cahier des charges.*

- *Les données sont modélisées conformément au besoin de la solution applicative.*
- *Le choix du type de base de données est pertinent.*
- *L'accessibilité des données est conforme à la qualité de service attendue.*
- *La base de données est sauvegardée selon la planification retenue.*
- *Des tests de restauration sont effectués.*
- *La base de données est opérationnelle et stable dans l'environnement de production.*

Exploiter des données à l'aide d'un langage de requêtes
L'apprentissage de cette compétence s'appuie sur des bases de données relationnelles et non relationnelles. Les étudiants apprennent à interpréter les modèles de référence de représentation des données, à distinguer les différents modèles de base de données, à stocker et à exploiter des données structurées ou non (JSON, XML, données clé/valeur, graphe…) dans un système de gestion de base de données.

Il s'agit d'approfondir, en seconde année, les connaissances sur les techniques et outils avancés intégrés au système de gestion de base de données.
Les étudiants utilisent le langage de requêtes pour créer, modifier, implémenter les tables virtuelles et à améliorer les performances d'accès aux données.

Ressources :
- Systèmes de gestion de bases de données : mySQL, PostgreSQL, SQL Server, MongoDB, Redis, Neo4j, Cassandra …
- Langages de requêtes : SQL, fonctions MongoDB, GraphQL, Cassandra Query language, Cypher...

Concevoir ou adapter une base de données
Cette compétence est un premier apprentissage des méthodes et outils de modélisation des données, mais également du langage de requête dans le but **d'adapter** une base de données pour qu'elle soit stable dans son environnement de production.

Les étudiants doivent savoir faire évoluer une base de données en utilisant un formalisme de représentation des données (UML, entité-association). Ils sont capables de décrire le modèle de données sur différents niveaux (conceptuel, relationnel, objet...) et de valider le schéma de données. Les requêtes de lecture, de création et de modification du modèle de données sont étudiées. Dans le cadre de SGBDR, le langage de définition de données (LDD), de manipulation (LMD) et de contrôle de données (LCD) sont exploités pour construire et/ou adapter le schéma de la base de données.

Les étudiants exploitent des requêtes avancées pour la gestion et le stockage des données dans la base.

Les bases de données existantes, le schéma ou le diagramme de la base de données ainsi que le descriptif des modifications et des nouvelles règles de gestion du système d'information sont fournis par l'enseignant.

Les outils de modélisation permettent de générer le script nécessaire pour créer la base de données.

En seconde année, en respectant le formalisme de représentation des données et à partir d'une expression de nouveaux besoins, les étudiants doivent être capables de concevoir une base de données et de la valider. Avec l'arrivée des données massives (*big data)* et des données de moins en moins structurées, la conception des bases de données ne peut se limiter aux SGBDR. Les concepts des bases de données non relationnelles sont également abordés dans cette compétence. Cela permet aux étudiants de choisir le type adéquat de SGBD à concevoir et à mettre en place en fonction de l'analyse des données à manipuler et du contexte technologique du système d'information. Cette conception peut être réalisée depuis le langage de la base de données ou via une API.

L'implémentation de différents types de bases de données peut être facilitée par l'utilisation de solutions *cloud* ou de conteneurisation.

Ressources :

- Systèmes de gestion de bases de données : mySQL, PostgreSQL, SQL Server, MongoDB, Redis, Neo4j, Cassandra …
- Langages de requêtes : SQL, fonctions MongoDB, GraphQL, Cassandra Query language, Cypher…
- Docker / Kubernets, AWS, ...

Développer des fonctionnalités applicatives au sein d'un système de gestion de base de données (relationnel ou non)

Cette compétence est initiée en 2ème année. Elle apporte les savoirs et savoir-faire permettant aux étudiants de développer dans le langage d'une base de données. Les contraintes d'héritage sont mises en œuvre grâce aux déclencheurs dans un contexte de SGBDR et via les ORM pour les SGBD NoSQL. D'autres composants propres au SGBDR sont également étudiés tels que des procédures stockées, curseurs… Lors du développement de ces composants, les étudiants sont amenés à identifier et à gérer les erreurs éventuelles.

Administrer et déployer une base de données

Cette compétence est également initiée en 2ème année. Elle apporte aux étudiants les principaux concepts et procédures nécessaires à la sauvegarde et à la restauration d'une base de données relationnelle ou non relationnelle. Les étudiants installent et configurent des outils de sauvegarde et de restauration. Ils définissent les plans de sauvegarde, planifient les sauvegardes et automatisent les procédures de sauvegarde. Ils mettent en place des tests de restauration d'une base de données relationnelle ou non relationnelle afin de valider la disponibilité des données.

Les étudiants peuvent utiliser des solutions *cloud*, de virtualisation ou de conteneurisation pour mettre en place les serveurs de bases de données.

L'enseignement de CEJMA mettra l'accent sur le cadre juridique relatif à la conception et à l'exploitation des bases de données :

- *En prolongement du thème 4 question 2 du programme de CEJM*, il conviendra par l'analyse de décisions de justice d'attirer l'attention des étudiants sur la complexité de la protection juridique de cet actif immatériel (protection du concepteur de la base de données par le droit d'auteur, protection du producteur par le droit sui generis (droit du producteur)
- La responsabilité civile et pénale du concepteur d'une base de données peut être engagée en cas de non-respect des obligations contractuelles, de dommages causés ou de commission d'une infraction.
- Il conviendra également de rappeler aux étudiants que l'exploitation de données à caractère personnel est réglementée (réglementation étudiée en CEJM - thème 4 - question 2 mais aussi dans le bloc 3).

Ressources

- Outils de conteneurisation et de virtualisation : Docker / Kubernetes, VMWare, VirtualBox...
- Cloud computing : AWS, Microsoft Azure.
- Environnement de modélisation des SI. Exemples : Win'design, PowerAMC, JMerise…
- Outil de gestion des performances
- Langages de requête
- SGBDR : mySQL, SQL Server, Oracle, db2, Postgresql
- SGBD NoSQL : mongoDB, couchDB, Cassandra, DynamoDB...

Ressources CEJMA :

- Legalis.net
- Cyberdroit - le droit à l'épreuve de l'internet - Christiane Féral-Schuhl - Edition Dalloz 2018/2019
- Droit des créations immatérielles - Hubert Bitan - Edition Lamy

Bloc 3 - Cybersécurité des services informatiques

Rappels RAP :

La personne titulaire du diplôme participe à la mise en œuvre de la politique de sécurité de l'organisation en prenant en compte les enjeux éthiques et déontologiques.
Elle contribue à la protection des données de l'organisation, à la sensibilisation des utilisateurs aux usages et à la sécurisation de leurs accès aux services numériques.
Elle applique les procédures d'exploitation de sécurité, apportant ainsi son soutien aux opérations d'audit et de contrôle.
En fonction de sa spécialité, elle est en mesure :

- *de déployer et d'administrer des solutions de gestion de la sécurité, ainsi que de paramétrer les éléments de sécurité des équipements des serveurs, des services et des terminaux traitants*
- *d'appliquer les recommandations de sécurité dans le développement d'une application informatique.*

Elle participe à la détection, à l'investigation et à la réponse aux incidents de sécurité dans son domaine d'expertise.

Préambule

Il est très important de lever l'ambiguïté entre les deux termes : **sécurité et sûreté**. En anglais, *security* désigne la sécurité et *safety* désigne la sûreté. En français les 2 mots sont souvent confondus. Le bloc 3 s'appuie sur la distinction opérée entre autres par CyberEdu. La sécurité traite les problèmes liés aux actes malveillants. La sûreté se préoccupe de la continuité et de qualité de service et donc des conditions nécessaires à la résilience (capacité à résister à un incident) des architectures réseaux ou applicatives. La cybersécurité n'a de sens que si elle intervient dans un environnement où la sûreté est assurée. Le bloc 3 traite de la sécurité, la sûreté est traitée par le bloc 2 pour chaque option. Le bloc 3 au 3ème et 4ème semestre synthétisera ces 2 approches.

La sécurité utilise un vocabulaire précis. La norme ISO CEI_27000 donne une vue globale des normes de sécurité informatique. La norme ISO 7498-2 définit 59 termes. On ne prétendra pas à cette exhaustivité, par contre on veillera à la justesse des termes utilisés. À l'issue de la première année, l'étudiant doit, à l'aide de ce vocabulaire, pouvoir conceptualiser les enjeux principaux de la sécurité et apporter des réponses opérationnelles aux risques connus concernant, entre autres, le poste de travail et les services en ligne dans le respect de la réglementation. La deuxième année mobilisera ce vocabulaire dans le cadre de la spécialité choisie.

Les normes, mais aussi la réglementation, fixent le contenu de l'enseignement du bloc 3, notamment le RGPD (Règlement général sur la protection des données directive européenne). Mais ce bloc ne se résume pas au seul respect du RGPD, il se préoccupe de la malveillance visant l'ensemble du patrimoine informatique des organisations. Cependant le RGPD est un cadre structurant les problématiques de sécurité car il fixe des obligations de résultats aux organisations. Si la plupart des dispositions du RGPD traitent de la sécurité des données personnelles, d'autres concernent plutôt le droit des individus sur leurs données personnelles recueillies. Le bloc 3 ne découpe pas le RGPD et traite donc les 2 aspects, ce qui offre la possibilité de travaux pertinents notamment pour la spécialité SLAM (d'ailleurs, si la sécurité informatique se définit par rapport à la malveillance, on peut légitimement considérer comme malveillance par rapport à un individu le non-respect de ses droits).

Enfin le RGPD montre que le vocabulaire technique, les concepts associés et les réponses opérationnelles ne sont pas les seuls aspects de la sécurité dont les organisations se soucient. La sécurité ne peut se réduire simplement à cela. La réglementation fixe des obligations. Les enjeux économiques associés sont importants. Elle devient une préoccupation majeure du management. C'est pourquoi le bloc 3 s'appuiera en permanence sur les apports CEJM (voir le

guide d'accompagnement CEJM), enrichis par l'enseignement spécifique de CEJMA.

Positionnement du Bloc 3
L'ambition est importante mais doit rester adaptée au niveau et à l'horaire fixés par le référentiel.
Il s'agit de former aux compétences permettant d'appréhender les problématiques de sécurité pour intervenir efficacement dans un contexte fortement encadré réglementairement, notamment par le RGPD.

Le bloc 3 démarre dès le premier semestre. Les 2 premiers semestres sont communs, les 2 derniers semestres sont spécifiques à l'option.
Le tronc commun est neutre par rapport au choix de l'option. L'étudiant/apprenti ne doit pas associer les compétences enseignées à l'une ou l'autre option. Il doit percevoir ces compétences comme nécessaires à une technicienne ou à un technicien informatique dans l'exercice de son métier en répondant aux exigences de sécurité.

Au premier semestre sont enseignés le Bloc 1 et le Bloc 3.
Bloc 1 et bloc 3 sont indépendants même s'il y a des recouvrements. Cependant les compétences de base en programmation et réseau sont prises en charge par le Bloc 1 au premier semestre nécessitant éventuellement de reporter des enseignements du Bloc 3 au second semestre.
Le premier semestre doit prendre appui sur les usages des étudiants pour introduire la protection des données personnelles, objet du RGPD et commencer à construire des compétences opérationnelles autour de la sécurité du poste de travail. L'identité numérique et la preuve introduiront les éléments de base de la sécurité (mesures de sécurité nécessaires aux services de sécurité) qui seront approfondis dans les 2 années.

Au deuxième semestre, les étudiants ont fait leur choix d'option et le bloc 2 commence. Mais le bloc 3 reste commun. En prenant appui sur les acquis réseaux et programmation, on poursuit l'apprentissage de la sécurité du poste mais on l'étend aux accès serveurs via le réseau (locaux ou à distance). Les protocoles de sécurité de la chaîne de liaison réseau sont étudiés (objectifs et mise en œuvre pour certains sans approfondissement). Les vulnérabilités des applications notamment Web sont vues aussi. Ces éléments doivent être perçus par les étudiants des 2 options comme nécessaires à la mise en œuvre des protections réseaux et système pour SISR, à la mise en place d'environnements de développement sécurisés et de transactions sécurisées pour les SLAM. Une approche différenciée par option au niveau des travaux pratiques peut s'envisager.

Les troisième et quatrième semestres sont spécifiques à chaque option. Ils vont permettre d'approfondir pour chacune d'elles les bonnes pratiques de sécurité dans un contexte opérationnel respectant lui-même les bonnes pratiques de sûreté (qu'il faut donc vérifier au préalable).

Les connaissances théoriques, si elles sont nécessaires, ne suffisent pas, les techniques doivent être appliquées de manière répétée pour contribuer à la compréhension des problèmes.
La démarche suivante peut être appliquée : pour chaque domaine d'activité, on présente ou on fait découvrir le problème, on expose ou on fait rechercher des solutions et on met en situation de projet les étudiants pour mettre en œuvre les solutions qu'ils auront choisies par rapport à un problème qui leur aura été posé. Les jeux de rôle ou les jeu sérieux mettant en situation des exercices de sécurité informatique est une piste intéressante pour l'apprentissage. Les jeux existants ne sont pas forcément du niveau de nos étudiants mais on peut s'en inspirer et les adapter.

Ressources générales
Le site incontournable de l'Anssi.
https://www.ssi.gouv.fr/

Un Mooc de l'Anssi pour s'initier à la cybersécurité. https://secnumacademie.gouv.fr
Un guide RGPD pour les développeurs de la CNIL
https://www.cnil.fr/fr/la-cnil-publie-un-guide-rgpd-pour-les-developpeurs
Cybermalveillance.gouv.fr est le programme gouvernemental assumant un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès des entreprises et de la population française en général.
https://www.cybermalveillance.gouv.fr/
https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles (ces fiches CNIL résument assez bien les objectifs du bloc 3 RGPD).
https://www.ssi.gouv.fr/particulier/formations/cyberedu/ (cyberEdu est une référence importante pour le bloc3).
https://www.ssi.gouv.fr/guide/maitrise-du-risque-numerique-latout-confiance/
https://www.iso.org/fr/standard/73906.html (cette norme est une introduction à l'ensemble des normes de sécurité).
https://www.iso.org/obp/ui/#iso:std:iso:7498:-2:ed-1:v1:fr (Cette norme définit entre autres le vocabulaire de la sécurité).
https://tools.ietf.org/html/rfc4949#page-9 (Glossaire sécurité IETF 2007)
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwjWqtDC-6_kAhWa8uAKHX4oCEcQFjABegQIARAC&url=https%3A%2F%2Fconf-ng.jres.org%2F2017%2Fdocument_revision_2442.html%3Fdownload&usg=AOvVaw34VsMfa8h8FHefaQ999BB- (une présentation des différents exercices de sécurité pour un niveau universitaire, à adapter bien sûr).
https://referentiels-metiers.opiiec.fr/fiche-metier/84-responsable-securite-de-l-information (métiers de la sécurité)

B3.1 - Protéger les données à caractère personnel

Cette compétence implique d'identifier les données à caractère personnel, les données sensibles et les risques associés pour les recenser et vérifier ou mettre en place leur protection. L'étudiant doit, dans le respect de la réglementation, définir ses droits en tant qu'usager et ses responsabilités en tant qu'informaticien. Les mesures de protection sont listées (ce qui doit être fait et non comment le faire) et des préconisations sont élaborées et diffusées. Cette compétence prendra appui sur les enseignements de CEJM et de CEJMA.

Semestre 1 (2 + 2) 60h	Semestre 2 (2 + 2) 60h	Semestres 3 et 4 (2+2) 48h + 48h
• Recenser les traitements sur les données à caractère personnel au sein de l'organisation • Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel • Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel • Sensibiliser les utilisateurs à la protection des données à caractère personnel		
Rappel des savoirs Typologie des risques et leurs impacts. Sécurité et sûreté : périmètre respectif. Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve.		
Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA Les données à caractère personnel : définition, réglementation, rôle de la CNIL		

Rappels : indicateurs de performance
La collecte, le traitement et la conservation des données à caractère personnel sont effectués conformément à la réglementation en vigueur.
La charte informatique contient des dispositions destinées à protéger les données à caractère personnel.
Des supports de communication pertinents sont accessibles et adaptés aux utilisateurs.
Le recensement des traitements des données à caractère personnel est exhaustif.
Des moyens de protection sont mis en place pour garantir la confidentialité et l'intégrité des données personnelles en tenant compte des risques identifiés.

Recenser les traitements sur les données à caractère personnel au sein de l'organisation

Cette compétence implique d'identifier les données à caractère personnel, les traitements sur ces données mais aussi les supports et les équipements sur lesquels sont stockées ou traitées ces données. Cela a le mérite de donner très rapidement la mesure des tâches à accomplir pour respecter la réglementation.

Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel

Identifier les enjeux de la sécurité du SI (protection des données personnelles, des données de l'organisation, des applications et des équipements) et ses objectifs (réduction des risques et limitation des impacts). Cela peut constituer un point de départ intéressant permettant de définir les notions de base et le vocabulaire, en répondant aux questions suivantes : que protège-t-on ? Quels sont les risques et les menaces ? Quels sont les grands principes de la sécurité ? L'étude de contextes simples, proches du quotidien ou issus de l'expérience des étudiants est à privilégier.

Les étudiants peuvent être amenés progressivement à découvrir les notions suivantes :

- Le système d'information à protéger (données à caractère personnel, données sensibles, applications, identités numériques, équipements : les OS et les machines) : inventorier les biens, identifier les composants.
- Typologie des risques et leurs impacts : données à caractère personnel (analyse d'impact relative à la protection de données à caractère personnel), données sensibles, ressources numériques, environnement en ligne (réseau social, espace collaboratif, ...), nomadisme numérique, équipement personnel de communication, identité et réputation numérique (sources de la présence digitale et risques associés), traces numériques (nature, typologie, pistage).
- Réalité du risque : vulnérabilité, menace, exploit, attaque (vocabulaire, exemples)
- Principes de la sécurité : Disponibilité Intégrité Confidentialité Preuve (DICP).
- Sécurité et sûreté : périmètres respectifs.

Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel

Cette compétence implique la connaissance de la réglementation (RGPD). Une collaboration avec le professeur de CEJM et l'enseignant de CEJMA est recommandée afin de s'assurer que l'acquisition des savoirs soit menée en parallèle au semestre 1.

En prolongement du thème 4 question 2 du programme de CEJM, l'enseignement de CEJMA abordera les points suivants :

- les obligations du responsable de traitement : tenue du registre des activités de traitement, désignation d'un DPO, réalisation d'une étude d'impact comprenant *privacy by design privacy by default* et la mise en œuvre de sa responsabilité en cas de non-conformité à la réglementation ;
- les obligations spécifiques du sous-traitant (société de sécurité informatique, intégrateur de logiciels, entreprises de services du numérique, etc.) qui traite des données à caractère personnel pour le compte d'une autre organisation, et, dont la responsabilité sera susceptible elle aussi d'être engagée en cas de manquement.

Sensibiliser les utilisateurs à la protection des données à caractère personnel

Cette compétence peut être un point d'entrée intéressant car directement en lien avec les usages du numérique faits par les étudiants. On peut leur faire constater à partir des documents notamment de la CNIL, les données personnelles qu'ils fournissent en ligne et, à partir de ce constat, élaborer avec eux un premier document de préconisation de protection de la vie privée.

Recommandations pédagogiques

On pourra s'appuyer sur l'expérience de l'étudiant en tant qu'utilisateur ou utilisatrice final pour l'amener à sa responsabilité en tant que qu'utilisateur/informaticien dans l'organisation et ce que cela implique comme compétences à acquérir.
Cette introduction à la sécurité (dès le premier semestre de la première année) ne nécessite donc pas de compétences techniques préalables autres que celles d'un usager des outils informatiques. Cependant elle sera déterminante pour la suite car elle pose les bases de la réglementation et du RGPD notamment.
Un vocabulaire commence à être mis en place ici, on veillera à sa définition en s'appuyant sur les normes en vigueur.
L'exploitation des ressources institutionnelles (CNIL) sera une aide précieuse (voir notamment l'étude de cas Captoo).
Il y a un lien fort avec le deuxième domaine d'activité. On peut d'ailleurs très bien envisager d'inverser la progression et de partir de l'identité numérique et des traces numériques pour aborder la protection nécessaire (et règlementaire) des données personnelles.

La CNIL (voir ressources) fournit des contenus utilisables ici, entre autres, les 9 domaines structurants qu'elle a définis forment une base directement exploitable :

1. Appréhender les données personnelles et leurs enjeux.
2. Vie privée, libertés fondamentales et protection des données personnelles.
3. Comprendre l'environnement numérique au plan technique pour protéger sa vie privée.
4. Comprendre l'environnement numérique au plan économique et le rôle des données dans l'écosystème.
5. Appréhender la régulation des données personnelles, connaître la loi.
6. Appréhender la régulation des données personnelles : maîtriser leur usage.
7. Maîtriser mes données : apprendre à exercer mes droits.
8. Maîtriser mes données : apprendre à me protéger en ligne.
9. Agir dans le monde numérique : devenir un citoyen numérique.

Ressources

Les ressources mentionnées ci-dessous fournissent des pistes didactiques intéressantes à mettre en œuvre. Elles ont l'avantage pour certaines d'avoir été élaborées par un des acteurs principaux en France : la CNIL.

http://eduscol.education.fr/pid25852-cid129745/le-referentiel-cnil-de-formation-des-eleves-a-la-protection-des-donnees-personnelles.html
Référentiel de formation CNIL (PIA - Privacy impact assessment ; AIPD - Analyse d'impact relative à la protection des données) : https://www.cnil.fr/fr/PIA-privacy-impact-assessment
Etude de cas CNIL : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-captoo-fr.pdf
https://www.cnil.fr/fr/respecter-les-droits-des-personnes

Autres ressources :

https://www.cigref.fr/wp/wp-content/uploads/2017/11/CIGREF-GT-AFAI-CIGREF-TIF-Donnees-Personnelles-et-Systemes-d-Informations-GDPR-2017.pdf
https://www.digitemis.com/2017/07/18/qu-est-ce-que-l-analyse-d-impact-version-rgpd-pia-dpia-eivp/
https://www.cnil.fr/fr/PIA-privacy-impact-assessment (tout niveau)
http://www.cil.cnrs.fr/CIL/IMG/pdf/cahier_28_V2.pdf (niveau 2)

https://www.ifaci.com/wp-content/uploads/RISPOLI-Nadege.pdf (audit)

Cours en ligne « protégez les données personnelles » :
https://openclassrooms.com/fr/courses/5280946-protegez-les-donnees-personnelles
Mooc d'initiation au RGPD proposé par la CNIL (https://atelier-rgpd.cnil.fr/)
Publication de guides sur le site de la CNIL (guide du sous-traitant, guide de la sécurité des données personnelles…)
Cyberdroit - le droit à l'épreuve de l'internet - Christiane Féral-Schuhl - Edition Dalloz 2018/2019

B3.2 Préserver l'identité numérique de l’organisation

Cette compétence implique de définir ce qu’est une identité numérique et la façon dont elle se construit. Des documents de la CNIL cités précédemment sont recommandables ici. Mais il s’agit bien de l’identité numérique de l'organisation et non de l’individu. L’identité numérique diffère de l’e-réputation.

La protection de cette identité passe entre autres par la sécurisation des transactions établies par elle, ce qui implique l’utilisation de la preuve numérique (ou preuve électronique).

Cette compétence permet de porter une attention spécifique à la protection juridique de l’identité numérique et à la réglementation relative à la preuve électronique (notions étudiées en CEJMA).

Semestre 1 (2 + 2) 60h	Semestre 2 (2 + 2) 60h	Semestres 3 et 4 (2+2) 48h + 48h
• Protéger l’identité numérique d’une organisation • Déployer les moyens appropriés de preuve électronique	• *Déployer les moyens appropriés de preuve électronique (suite)*	
Rappel des savoirs Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve. Protection et archivage des données : principes et techniques. Chiffrement, authentification et preuve : principes et techniques.		

Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA

L'identité numérique de l'organisation : risques et protection juridique.
Droit de la preuve électronique

Rappels : indicateurs de performance

L'identité numérique de l'organisation est protégée en s'appuyant sur des moyens techniques et juridiques.
La preuve électronique est déployée de manière sécurisée et dans le respect de la législation.

Protéger l'identité numérique d'une organisation

Cette compétence doit amener l'étudiant à :

- caractériser ce qu'est l'identité numérique d'une organisation (identités multiples et données associées à une identité) ;
- recenser les sources de la présence digitale (emails, messagerie instantanée, sites web institutionnels et applications web, les applications mobiles, les réseaux sociaux et traces associées) ;
- lister les menaces associées (hameçonnage, fausses applications mobiles, défacement, ingénierie sociale, etc.) ;
- lister les mesures de protection (veille sur l'utilisation de l'identité numérique de l'entreprise et des comptes à, authentification forte sur les comptes mails et réseaux sociaux, activation de protection des comptes mails telles que SPF DKIM DMARC, protection des noms de domaine DNSSEC, DANE, etc.).

Les notions d'identité numérique d'une personne physique et de délit d'usurpation d'identité numérique ainsi que la protection des noms de domaine sont étudiées dans le thème 4 question 2 du programme de CEJM.

L'enseignement de CEJMA permettra de compléter l'analyse technique relative à la protection de l'identité numérique d'une organisation par une analyse juridique.
En s'appuyant sur des décisions de justice, les étudiants pourront étudier des situations dans lesquelles l'identité numérique d'une organisation a été menacée afin d'y repérer notamment les modalités utilisées, les conséquences pour l'organisation victime, les sanctions prononcées, mais surtout le fondement juridique de la décision rendue (délit d'usurpation d'identité numérique, délit d'escroquerie, délit d'accès frauduleux à un système de traitement automatisé de données, etc.).

Déployer les moyens appropriés de preuve électronique

Cette compétence implique de traiter les bases de l'authentification, de la confidentialité et de la preuve afin d'en comprendre les principes et mettre en œuvre des outils simples. Des éléments incontournables, comme ceux qui suivent, permettent d'appuyer les compétences :

- principes du chiffrement symétrique et asymétrique ;
- principes de l'authentification : hachage, signature ;
- principes de la preuve numérique : horodatage, certificats, chaîne de blocs (Blockchain) ;
- conservation de la preuve numérique ;
- l'identité numérique sécurisée : authentification numérique, principes et outils prouvant une identité numérique, schéma d'authentification numérique, OpenId, identité institutionnelle.

Recommandations pédagogiques

Le lien avec le domaine d'activité précédent est très fort. Les traces numériques qu'on peut associer à une identité numérique constituent des données personnelles pour les individus et des informations parfois confidentielles pour les organisations. Ces deux domaines d'activité peuvent être abordés conjointement ou dans n'importe quel ordre.

On peut partir des usages de l'étudiant en tant qu'utilisateur final et des traces qu'il laisse sur les réseaux sociaux en particulier ainsi que de nombreux exemples récents d'usurpation d'identité. Il faut qu'il en déduise la conséquence d'une mauvaise maîtrise de son identité et la nécessité de la protéger. La compréhension des éléments de base de la preuve électronique est une priorité.

Les moyens de protection formant la preuve électronique ne sont pas vus en détails mais on en décrit les grands principes (hachage d'un fichier, signature d'un mail…). On illustre avec des outils simples : un logiciel de hachage, un logiciel de cryptographie, un logiciel utilisant des clés asymétriques pouvant produire une preuve électronique. L'étudiant doit comprendre le rôle d'un certificat comme la façon de l'utiliser.

Si la notion de BlockChain est abordée, sa pratique n'est pas nécessaire et peut être approfondie plus tard en fonction de choix didactiques et du développement de cette technologie.

La preuve numérique permet d'aborder les mécanismes de sécurité (hachage, chiffrement, signature …) permettant de mettre en place les services de sécurité (authentification, confidentialité, intégrité, non répudiation) à tous les niveaux (applicatifs, systèmes, réseaux). L'authentification permet aussi d'identifier l'entité accédant aux ressources et donc de gérer les contrôles d'accès (autorisations, habilitations, privilèges). Tout cela est à la base des objectifs principaux de la sécurité : empêcher l'accès non autorisé à des données, interdire leur modification non autorisée et bannir l'accès non autorisé à des ressources.

On ne peut pas atteindre la maîtrise de ces mécanismes dès le premier semestre, ce sera un travail permanent sur les 2 années ; il est préférable d'aborder ces éléments au plus tôt pour fixer le vocabulaire et commencer des travaux simples qui s'enrichiront et se complexifieront au fur et à mesure de l'apprentissage.

La définition juridique de la preuve, la valeur probante de l'écrit sur support électronique et les conditions de recevabilité de la preuve électronique sont

étudiées dans le thème 4 question 2 du programme de CEJM.

Ressources

https://www.cnil.fr/fr/maitriser-mes-donnees
https://eduscol.education.fr/internet-responsable/communication-et-vie-privee/maitriser-son-identite-numerique.html
https://www.confiance-numerique.fr/wp-content/uploads/2014/05/feuille_de_route_nationale_identite_numerique_acn_v1.0.pdf

Autres ressources

https://blogrecherche.wp.imt.fr/files/2016/03/Cahier-Identites-numeriques_web.pdf
https://www.akaoma.com/conseil-expertise-securite-informatique/ereputation-reputation-numerique
http://www.lerti.fr/
https://books.openedition.org/pupvd/3972
https://www.docusign.fr/sites/default/files/Protect-and-Sign_Personal-Signature_PSGP-v-1-4s.pdf
https://www.cegid.com/fr/blog/archivage-a-valeur-probante/
https://www.solutions-numeriques.com/dossiers/larchivage-a-vocation-probatoire/
https://www.legalis.net/legaltech/dematerialisation-raphael-dassignies/
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf (par exemple fiche n° 24, pages 32 et 33 à propos de la messagerie professionnelle), autre lien vers la ressource : https://www.ssi.ens.fr/guide_hygiene_informatique_anssi.pdf

Ressources CEJMA

Cyberdroit - le droit à l'épreuve de l'internet - Christiane Féral-Schuhl - Edition Dalloz 2018/2019
https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/7444/show/securiser-les-communications-sur-internet-de-bout-en-bout-avec-le-protocole-dane.html
www.gfii.fr/uploads/docs/e-reputation-et-identite-numerique-des-organisations.pdf
www.legalis.net

B3.3 Sécuriser les équipements et les usages des utilisateurs

Les équipements des utilisateurs et leurs usages constituent sans doute un des maillons les plus vulnérables de la sécurité des systèmes d'informations. Il s'agit donc ici d'informer sur les risques et les menaces et de construire les savoirs opérationnels pour mettre en œuvre les bonnes pratiques permettant de sécuriser les équipements et les usages de l'utilisateur.

Cette compétence pourra être complétée avec l'enseignement de CEJMA pour mettre en évidence les principaux enjeux des nouvelles modalités de travail qui se développent dans les entreprises.

Cette compétence doit amener l'étudiant à :

- recenser les risques et les menaces ;
- repérer les comportements à risque ;
- préconiser les bons usages ;
- sécuriser l'accès physique au poste fixe, nomade ou mobile (protection physique, séquence de démarrage, chiffrement disque, supports amovibles, verrouillage, contrôle des canaux de connexion réseau, wifi, bluetooth…) ;
- sécuriser l'accès logique au poste fixe ,nomade ou mobile (ouverture de session, mot de passe, pare-feu, antivirus, automatisation des mises à jour…) ;
- durcir le système en limitant les logiciels installés et les utilisateurs configurés ;
- restreindre les privilèges et gérer les habilitations ;
- établir des connexions nomades sécurisées ;
- auditer la sécurité d'un poste de travail.

Semestre 1 (2 + 2) 60h	Semestre 2 (2 + 2) 60h	Semestres 3 et 4 (2+2) 48h + 48h
• Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter • Identifier les menaces et mettre en œuvre les défenses appropriées • Gérer les accès et les privilèges appropriés • Vérifier l'efficacité de la protection	• *Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter (suite)* • *Identifier les menaces et mettre en œuvre les défenses appropriées (suite)* • *Gérer les accès et les privilèges appropriés (suite)* • *Vérifier l'efficacité de la protection (suite)*	.

Rappel des savoirs Typologie des risques et leurs impacts. Sécurité des terminaux utilisateurs et de leurs données : principes et outils. Authentification, privilèges et habilitations des utilisateurs : principes et techniques. Gestion des droits d'accès aux données : principes et techniques.	**Rappel des savoirs** Sécurité des communications numériques : rôle des protocoles, segmentation, administration, restriction physique et logique. Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique.	
Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA La sécurité des équipements personnels des utilisateurs et de leurs usages : prise en compte des nouvelles modalités de travail, rôle de la charte informatique		

Rappels : indicateurs de performance

Des supports de communication interne sont accessibles aux utilisateurs.

Les outils de défense mis en œuvre permettent de prévenir les menaces identifiées

- *l'accès physique au terminal et à ses données est sécurisé ;*
- *les applications installées sont vérifiées par des procédures automatisées et des logiciels de sécurité ;*
- *les flux réseaux sont identifiés et sécurisés.*

Les accès et privilèges respectent les règles organisationnelles :

- *les utilisateurs sont authentifiés ;*
- *les habilitations sont configurées ;*
- *l'accès aux données est contrôlé ;*
- *les privilèges sont restreints.*

L'efficacité de la protection mise en œuvre est évaluée.

Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter

Les problématiques du nomadisme et de l'utilisation d'équipements personnels doivent être particulièrement traitées.

En prolongement du thème 5 du programme de CEJM, l'enseignement de CEJMA amènera les étudiants à réfléchir aux enjeux des nouvelles modalités de travail tels le télétravail, le nomadisme, le PAP pour « prenez vos appareils personnels » (BYOD en anglais) en identifiant les avantages qu'elles procurent pour les salariés et l'employeur mais aussi les risques notamment en termes de sécurisation des données, et de violation de la vie privée.

Une attention spécifique sera portée ici au rôle et à la valeur juridique de la charte informatique destinée à encadrer les usages des ressources numériques. Des exemples de chartes informatiques pourront être proposés aux étudiants et apprentis afin de cerner la pertinence des règles qui y figurent.

Identifier les menaces et mettre en œuvre les défenses appropriées

On travaille ici sur la sécurité des terminaux utilisateurs et de leurs données avec pour objectif le paramétrage de la protection d'un terminal utilisateur fixe ou

nomade et la sécurisation de sa connexion au réseau interne ou distant. On étudiera aussi les solutions virtualisées. Les étudiants peuvent être amenés progressivement à découvrir les éléments suivants :

- Panorama des risques et des menaces associés à l'utilisation des terminaux utilisateurs fixes, nomades et mobiles
- Sécurité de l'accès physique au terminal et à ses données : protection physique, séquence de démarrage, chiffrement du disque, supports amovibles
- Sécurité de l'accès logique : ouverture de session, authentification des utilisateurs, mot de passe, authentification forte (ou à facteurs multiples), durcissement du système, verrouillage de la session, gestion des privilèges et des habilitations
- Sécurité des applications et des données : vérification des applications installées, mises à jour logicielles et systèmes, des anti-virus, de l'antimalware, des antispyware, détection des rootkits, sauvegarde du système et des données
- Contrôle des flux réseaux sur le poste de travail : chaîne de connexion au réseau (protocoles et équipements standards) fixe et nomade, interne ou distante, pare-feu, utilisation de connexions nomades sécurisées (VPN ou Zero Trust), navigation privée, contrôle du pistage, contrôles des accès distants au poste
- Virtualisation des postes de travail et des applications : accès sécurisé à un poste de travail virtualisé et à des applications publiées.

Gérer les accès et les privilèges appropriés

La sécurité mise en œuvre sur les terminaux implique de gérer les utilisateurs, c'est à dire contrôler leurs droits d'accès et leur authentification, faire respecter les bons usages, et déterminer les impacts d'une perte de DCP (Données à caractère Personnel) ou de données professionnelles. Les notions suivantes peuvent être abordées :

- Restrictions des privilèges et des habilitations.
- Méthodes d'authentification : gestion du mot de passe, utilisation de gestionnaire de mot de passes, autres outils d'authentification, authentification forte sur les réseaux sociaux, activation de protection des comptes mails telles que SPF DKIM DMARC, SMTP authentifié…
- Charte informatique, comportements à risques, bons usages.
- Identification des impacts potentiels sur la vie privée de la perte de données à caractère personnel (*PIA Privacy Impact Assessment*).
- Identification des impacts d'une perte de données professionnelles.

La gestion des droits d'accès aux données doit être abordée aussi dans ses principes et étendue à des environnements répartis sur un réseau (comment les accès d'un utilisateur authentifié sur un terminal sont-ils vérifiés par une ressource disponible sur le réseau ?). La compréhension de ces mécanismes implique un détour théorique (léger) par les processus. Les notions suivantes peuvent être abordées :

- Gestion des processus et de leurs droits : principes locaux et distants (UID, PID …).
- Gestion des fichiers et de leurs contrôles d'accès (Access Control List).
- Gestion des droits d'accès sur une architecture répartie : principes.
- Gestion des droits d'accès à une base de données : principes.

Vérifier l'efficacité de la protection

La sécurité d'un terminal utilisateur doit être vérifiée et les principes de l'audit de sécurité introduits. Les notions suivantes peuvent être abordées :

- Gestion des contrats de service (présentation).
- Gestion des incidents de sécurité (présentation).
- Plans de secours : présentation sans approfondissement du PRA et du PCA.
- Traçabilité des actions menées (le RGPD impose la journalisation), authentification des utilisateurs, imputabilité du responsable de l'action effectuée, journalisation des événements (observation des fichiers journaux (logs), mise en œuvre d'un outil de journalisation, stratégie d'audit d'accès sur un

dossier ou un fichier).
- Typologie des audits techniques : principes (boite noire, boite grise, boite blanche).
- Audit technique du terminal utilisateur préventive et réactive.

Recommandations pédagogiques

Encore une fois, on partira du comportement des étudiants face aux ressources informatiques pour illustrer les bons et les mauvais usages.

Le nombre d'éléments abordés peut sembler important mais on est ici sur 2 semestres, ce qui permet de commencer rapidement par des activités simples de sécurité du poste de travail jusqu'à des travaux plus complexes sur les flux réseaux. En outre de nombreuses notions sont communes avec le domaine d'activité suivant qui démarre au 2ème semestre.

On se limite ici au poste de travail et à la chaîne de connexion physique qui le relie au commutateur d'accès et à la ressource accédée, ainsi qu'aux objectifs de sa configuration logique (VLAN, adressage IP, DNS , PROXY, VPN...). La compréhension de cette chaîne de connexion est requise pour les 2 options. L'établissement d'une liaison sécurisée peut être étudiée à ce stade, c'est à dire qu'on peut mettre en œuvre une liaison VPN pour un utilisateur nomade (et ce pour les 2 options). Il sera aussi possible d'étudier une solution basée sur un modèle de sécurité *zero trust*. Le bloc 3 spécifique SISR approfondira ces éléments.
Il y a des points de recouvrement avec le bloc 1 au premier semestre notamment sur les parties système et réseau. Les objectifs diffèrent cependant. Le bloc 1 se préoccupe d'une utilisation sûre (sauvegarde, tolérance aux pannes, dépannage, prise de contrôle à distance …). Le bloc 3 se préoccupe de sécurité. La reprise des éléments réseaux vus au premier semestre par le bloc 1 constitue d'ailleurs un approfondissement.
Il y a aussi un point de recouvrement avec le bloc 2 notamment SISR. Mais le degré d'approfondissement n'est pas le même. Le Bloc 3 se préoccupe ici du poste de travail (et non de l'architecture réseau) du rôle de quelques éléments de la chaîne de liaison (VLAN, adresse IP du poste, adresse serveur DNS, adresse routeur, commutateur d'accès, borne wifi, accès distant) et non du contenu des échanges protocolaires en tant que ces éléments participent à des vulnérabilités courantes et pour mieux appréhender les techniques de sécurisation de la chaîne de liaison.

L'étude du modèle OSI ou TCP/IP paraît indispensable pour la compréhension de la chaîne de liaison.

Il est difficile, compte tenu du temps imparti, d'être exhaustif et approfondi. On privilégie donc les principes et la méthode en veillant cependant à ce que des compétences opérationnelles soient acquises. On peut imaginer pour cela différents scénarii pédagogiques qui font confiance à l'étudiant pour trouver et mettre en œuvre les mesures de sécurité plutôt qu'à un TP détaillé du professeur. On peut par exemple prévoir une séquence pédagogique où des groupes d'étudiants sont chargés de sécuriser un poste en fonction d'objectifs professionnels suivie d'une séquence pédagogique où les groupes d'étudiants sont chargés d'auditer (et rendre compte) les postes sécurisés par leurs pairs (ce scénario pouvant être décliné avec différents types de postes et de systèmes).

Ressources

https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf (en annexe de ce document de nombreux liens à exploiter).
https://www.ssi.gouv.fr/administration/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf (déjà cité)
https://www.cnil.fr/fr/securite-gerer-les-habilitations (niveau 1)

https://www.globalsecuritymag.fr/Guide-pratique-la-revue-des,20180524,78780.html
https://www.globalsign.fr/fr/blog/gestion-des-identites-vs-gestion-des-acces/ (quelques définitions intéressantes)
https://haveibeenpwned.com/ (les étudiants pourront vérifier si leur adresse mail a déjà été compromise)
https://www.globalsecuritymag.fr/Pourquoi-le-modele-Zero-Trust-va,20190517,87152.html (zero trust vs vpn)
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail
https://www.stormshield.com/fr/actus/teletravail-et-cybersecurite-comment-allier-mobilite-et-securite-informatique
https://www.cybermalveillance.gouv.fr/blog
https://www.ssi.gouv.fr/administration/bonnes-pratiques/
https://www.ssi.gouv.fr/uploads/2016/05/cyberedu_module_3_reseau_et_applicatifs_02_2017.pdf
https://www.purevpn.fr/quest-ce-quun-vpn/protocoles/ipsec
https://www.cybermalveillance.gouv.fr/cybermenaces

Ressources CEJMA

www.journaldunet.fr/management/guide-du-management/1201309-charte-informatique-rgpd-cnil/
www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques
Cyberdroit - le droit à l'épreuve de l'internet - Christiane Féral-Schuhl - Edition Dalloz 2018/2019

B3.4 Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

Cette compétence doit apporter les savoirs et savoir-faire permettant de mettre en place la sécurité au niveau d'une organisation tant au niveau de ses équipements que de ses applicatifs. En termes de savoirs, on ne rentre pas dans le détail de tous les composants nécessaires à la sécurité, on s'intéresse plutôt à leur rôle (on vérifie qu'ils sont en place et qu'ils fonctionnent) qui seront approfondis en 2ème année. En termes de savoir-faire on peut se fixer pour objectif de vérifier la sécurité d'un serveur hébergeant un applicatif web accessible en ligne, vérifier la sécurité d'un réseau d'accès et de vérifier la sécurité de l'application web (très simple) et de mettre en œuvre quelques dispositifs simples.

L'enseignement de CEJMA complétera l'approche technique de cette compétence en mettant en exergue les risques économiques et juridiques des cyberattaques pour l'organisation ainsi que la réglementation en matière de lutte contre la fraude informatique.
Un panorama des organisations de lutte contre la cybercriminalité sera proposé aux étudiants et apprentis.

Semestre 1 (2 + 2) 60h	Semestre 2 (2 + 2) 60h	Semestres 3 et 4 (2+2) 48h + 48h
	• Caractériser les risques liés à l'utilisation malveillante d'un service informatique • Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité • Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation • Organiser la collecte et la conservation des preuves numériques • Appliquer les procédures garantissant le respect des obligations légales	
	Rappel des savoirs Typologie des risques et leurs impacts. Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve. Authentification, privilèges et habilitations des utilisateurs : principes et techniques. Gestion des droits d'accès aux données : principes et techniques.	

	Sécurité des communications numériques : rôle des protocoles, segmentation, administration, restriction physique et logique. Protection et archivage des données : principes et techniques. Chiffrement, authentification et preuve : principes et techniques. Sécurité des applications Web : risques, menaces et protocoles. Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique.	
Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA Les risques des cyberattaques pour l'organisation : économique, juridique, atteinte à l'identité de l'entreprise Réglementation en matière de lutte contre la fraude informatique : infractions, sanctions Les organisations de lutte contre la cybercriminalité Obligations légales de notification en cas de faille de sécurité		

Rappels : indicateurs de performance
Les risques associés à l'utilisation malveillante d'un service informatique sont caractérisés.
Les conséquences des actes malveillants sur un service informatique sont identifiées.
Les obligations légales en matière d'archivage et de protection des données sont identifiées et respectées.
Les preuves numériques sont conservées de manière sécurisée et dans le respect de la législation.
Des procédures garantissant le respect des obligations légales sont opérationnelles et appliquées :

- *un schéma présentant la segmentation du réseau est disponible ;*
- *les principes de mise en œuvre des contrôles des connexions aux réseaux sont validés ;*
- *l'authentification et la confidentialité des échanges sont vérifiées ;*
- *la sécurité de l'administration est prise en compte ;*
- *les accès physiques et logiques à un serveur ou à un service sont vérifiés en fonction des habilitations et des privilèges définis ;*
- *les accès aux données sont contrôlés à chaque étape d'une transaction ;*
- *les systèmes et les applications sont actualisés en fonction des alertes de sécurité ;*
- *les vulnérabilités connues sont contrôlées.*

Caractériser les risques liés à l'utilisation malveillante d'un service informatique
Cette compétence doit amener l'étudiant à recenser les menaces et les risques associés à des services en ligne. Par rapport au poste de travail on change de dimension puisque l'application et les données sont celles de l'organisation.

Les attaques subies par les organisations sont nombreuses (DDOS, logiciel rançonneur, Keylogger, vulnérabilité des réseaux sans fils, Hameçonnage, etc…). Par rapport à cela différentes organisations font des préconisations ou proposent des services (CNIL, ANSSI, HEXATRUST, ENISA, ENCRYPTION EUROPE, DG DEVCO, DG CNECT, EUROPEAN COMMISSION – FPI, etc.)

On peut s'intéresser à la cartographie et à la gestion des risques.

L'enseignement de CEJMA permettra de compléter les conséquences techniques des risques liés à l'utilisation malveillante d'un service informatique en abordant les conséquences économiques (pertes financières, détérioration de l'image de l'organisation, etc.) et juridiques (atteintes au patrimoine informationnel et notamment aux données à caractère personnel, violation des droits de propriété intellectuelle, atteinte à l'identité de l'organisation etc.) qui peuvent en découler.

Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité
Cette compétence complète la première et doit amener progressivement l'étudiant à :

- décrire les principes permettant de garantir la DIC des services et données en ligne (hors mise en œuvre) ;
- interpréter un schéma réseau détaillant la DIC ;
- interpréter une cartographie simple d'un système d'information (principes).

Les conséquences vont amener à s'interroger sur les moyens et technique à mettre en œuvre (sauvegarde décentralisée sur support amovible ou distante, stockage en lieu sécurisé, duplication de certaines informations sensibles, accès aux données sensibles et droit d'utilisation-consultation-modification, etc…) et débouche sur l'application de procédures.

Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation
A travers cette compétence on sensibilise l'étudiant à l'obligation de sécurité et de confidentialité imposée par la loi et à ce que cela implique en termes des procédures à mettre en œuvre.

Les étudiants seront amenés à repérer les obligations des organisations en matière d'archivage de données afin de produire une preuve recevable en cas de contentieux (respecter les durées minimales de conservation des données, assurer l'intégrité, la disponibilité, la sécurité, la confidentialité et la traçabilité de ces données). Une attention particulière devra être portée à l'archivage et là a sécurisation des données à caractère personnel qui font l'objet d'une réglementation spécifique (RGPD).

Organiser la collecte et la conservation des preuves numériques
Les outils numériques utilisés par l'organisation (courriel, signature numérique, documents numériques …) peuvent être demandés par une autorité judiciaire et/ou utilisables devant les tribunaux. Sans rentrer dans les détails, il s'agit ici de sensibiliser l'étudiant à la nécessité d'archivage protégée de ces éléments mais aussi à la façon de les collecter au niveau des applications ou des systèmes.

Appliquer les procédures garantissant le respect des obligations légales
Il s'agit d'une part d'explorer la sécurité des accès aux ressources numériques de l'organisation dans ses dimensions système et réseau. L'étudiant doit savoir interpréter un schéma réseau, identifier les problématiques de sécurité associées aux serveurs et aux services en ligne La configuration des éléments

sera soit fournie soit effectuée par les étudiants en fonction de leur option. Les solutions virtualisées sont étudiées aussi. Les notions suivantes peuvent être abordées :

- Risques associés aux protocoles standards du réseau : exemples.
- Segmentation du réseau en zones de sécurité : principes et équipements.
- Restriction des connexions réseaux (couches basses) internes distantes et nomades : principes et outils (802.1X, Wifi .etc.).
- Rôle des différentes authentifications (authentification système, applicative, base de données, habilitations des processus, cookies, tickets, OTP etc.).
- Authentification et confidentialité des échanges : rôle des protocoles standards.
- Protection de l'administration du SI : présentation générale des bonnes pratiques (habilitations, privilèges, réseau dédié à l'administration, etc.).
- Restriction physique et logiques des accès à un serveur et à un service en ligne : sécurité physique des serveurs, principes de la gestion centralisée des utilisateurs et de leurs habilitations, gestion de sessions distantes et de leurs droits, gestion centralisée des ressources et de leurs contrôles d'accès, virtualisation (principes et outils).
- Protection et archivage des données : système d'archivage électronique, sauvegarde, destruction de données.
- Mise à disposition d'un service sur un serveur et gestion de ses habilitations.
- Contrôle des listes d'accès aux données en ligne.
- Contrôle des vulnérabilités connues des applications en ligne.
- Vérification des accès aux données par chaque transaction applicative.
- Utilisation des protocoles de chiffrement.
- Mise en place d'une veille sur les alertes de sécurité.
- Actualisation de la version des systèmes, des applications et de leurs composants en fonction des alertes de sécurité.
- Vérification de la sécurité des éléments d'administration.
- Vérification des procédures d'archivage et de protection des données et particulièrement l'archivage de la preuve numérique.

D'autre part, et c'est un élément important, les bases de la sécurité des applications web sont aussi étudiées. Les vulnérabilités connues et leurs contre-mesures sont traitées à partir d'exemples simples. La prise en compte du RGPD au niveau applicatif doit aussi être traitée. Les notions suivantes peuvent être abordées :

- Panorama des risques et des menaces associés à l'architecture Web
- Protocoles de base et contre-mesures permettant de sécuriser des échanges Web : principes.
- Procédures applicatives associées au RGPD (droit à l'oubli, à la portabilité, etc.).
- Revue de code (tests de pénétration).
- Bonnes pratiques de sécurité dans l'utilisation de CMS.

L'enseignement de CEJMA permettra de rappeler l'obligation pour toute organisation de notifier à la CNIL les violations de données à caractère personnel présentant un risque pour les droits et libertés des personnes et, dans certains cas, de les notifier également aux personnes concernées lorsque le risque est élevé (nouvelle obligation introduite dans le RGPD).

Recommandations pédagogiques

Certaines parties de ce domaine d'activité ont des relations fortes avec le domaine d'activité précédent, c'est une extension des concepts liés au poste de travail aux serveurs, l'étudiant devant appréhender le changement de dimension en termes de sécurité.

La mise en œuvre des éléments de disponibilité intégrité et confidentialité sera détaillée en deuxième année. Il s'agit donc ici essentiellement d'en donner les principes, d'en exposer les objectifs et les contraintes légales. La notion de serveur (données et traitements) est forte ici avec tout ce que cela implique comme protection des accès en ligne.
Les problématiques d'une authentification distante avec leurs conséquences sur la gestion des droits d'accès à une ressource en ligne doivent être particulièrement soulignées.

Quelle que soit l'option choisie, la lecture d'un schéma réseau avec la compréhension des zones de sécurité et du rôle des matériels d'interconnexion est requise (la configuration et l'administration de ces matériels sont bien sûr détaillées dans l'option SISR, lire un schéma réseau ne signifie pas le concevoir ou le paramétrer !). On peut imaginer un exercice de sécurité papier montrant un schéma réseau avec des zones réseaux non sécurisées et demander à le sécuriser.

Il paraît opportun ici de présenter les vulnérabilités *Web* (OWASP, pour les deux options) au niveau des principes. On peut illustrer avec un ou deux exemples simples comme l'injection SQL ou des failles JavaScript. Une approche plus détaillée pourra être vue en option SLAM.

Difficile d'être totalement exhaustif encore une fois, il est surtout essentiel de fixer les concepts et de les illustrer pratiquement en choisissant ce qu'on souhaite approfondir.

L'objectif est la vérification des éléments de sécurité. On peut imaginer deux types d'exercices, soit on donne un contexte configuré et on demande son audit voire sa mise en conformité soit on demande aux étudiants de créer un contexte simple qu'ils sécurisent.

On doit essayer de gérer des activités compatibles avec les deux options sans privilégier l'une par rapport à l'autre (ne faire que du système ou du réseau serait contre-productif pour les étudiants SLAM). Il paraît donc souhaitable de s'appuyer sur les compétences des deux options pour enrichir mutuellement les étudiants.
Ainsi on peut imaginer que les étudiants SLAM développent une ou plusieurs petites applications (*Web* ou autres, avec un CMS ou pas) en s'attachant à sécuriser l'écriture (dans la limite des connaissances à ce stade) et en prenant en compte le RGPD dans ses dimensions applicatives. Cela peut donner lieu à des développements réalisables à ce niveau comme par exemple la prise en charge du droit à l'oubli ou l'exportation des données personnelles dans un format lisible. En effet cela reste somme toute de la programmation.
Les étudiants de l'option SISR s'attacheront plus particulièrement quant à eux à sécuriser les serveurs d'applications, de données et les échanges, chaque groupe validant (ou pas) ensuite les travaux de l'autre groupe.

La mise en œuvre d'échanges HTTP sécurisés est vivement recommandée à ce stade.

Aux semestres 3 et 4, en prolongement des savoirs techniques et professionnels associés à la compétence **Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaque**s, les étudiants découvriront dans le cadre de l'enseignement CEJMA :

- Les divers dispositifs juridiques nationaux et européens : convention européenne sur la cybercriminalité, loi relative à la fraude informatique, Loppsi 2, loi pour la confiance dans l'économie numérique, réglementation relative à la protection des données à caractère personnel qui permettent de

lutter contre la cybercriminalité et de sanctionner les auteurs de cyberattaques, mais, aussi les responsables de traitement, les sous-traitants qui manquent à leur obligation de sécuriser les données à caractère personnel.

- L'existence d'organismes de lutte contre la cybercriminalité à l'échelle nationale, mais aussi à l'échelle européenne et internationale : CNIL, ANSSI, C3N, ENISA, office central de lutte contre la cybercriminalité (police nationale), BEFTI, centre européen de lutte contre la cybercriminalité etc. Une énumération et une étude exhaustives de ces organismes ne sont pas attendues.

Ressources

https://clusif.fr/publications/gestion-gouvernance-identites-acces-guide-pratique-mise-oeuvre/
https://www.ssi.gouv.fr/uploads/2012/01/anssi-guide-passerelle_internet_securisee-v2.pdf
https://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf
https://www.ssi.gouv.fr/uploads/2018/11/guide-cartographie-systeme-information-anssi-pa-046.pdf
https://www.reseaucerta.org/securisation-des-applications-web-owasp-activite1
https://www.reseaucerta.org/securisation-des-applications-web-owasp-activite-2
https://bohzo.developpez.com/rgpd-guide-pratique-developpeurs/
www.village-justice.com/articles/les-reponses-judiciaires-face-cybercriminalite,28927.html
https://www.mag-securs.com/dossiers/id/29345/forensics-une-plongee-au-coeur-du-crime-numerique.aspx (droits d'accès des comptes à privilèges) voir aussi PAM PSM IAM PIM (Privileges access… Privilege session…Identity Privilege Identity)
https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Virtualisation_NoteTech_v1-1.pdf
https://resinfo.org/IMG/pdf/virtu-pour-quoi.pdf (virtualisation et sécurité)
https://www.ossir.org/jssi/jssi2009/3A.pdf (virtualisation et sécurité)
https://www.ifaci.com/wp-content/uploads/RISPOLI-Nadege.pdf (audit)
http://www.crcc-paris.fr/sites/default/files/ressources/upload/guide_audit_def_11h46.pdf

Ressources CEJMA :
Les Cyberisques : la gestion juridique des risques à l'ère immatérielle – Edition Lexinexis
Cyberdroit - le droit à l'épreuve de l'internet - Christiane Féral-Schuhl - Edition Dalloz 2018/2019

B3.5 A - Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service (option A)

Cette compétence est spécifique à l'option SISR. Elle permet à l'étudiant de participer à la validation de la sûreté d'une infrastructure et à la mise en œuvre de solutions de sécurité dans le respect des normes et des bonnes pratiques.
L'enseignement de CEJMA pourra compléter les aspects techniques de cette compétence par un éclairage juridique sur la responsabilité de l'administrateur systèmes et réseaux qui ne prendrait pas les mesures nécessaires pour assurer la sécurité de l'infrastructure réseau.

Cette compétence doit amener l'étudiant à :

- vérifier la sûreté d'une infrastructure ;
- respecter la réglementation en matière de données personnelles ;
- intégrer la sécurité dans toute la démarche projet ;
- mettre en œuvre des dispositifs d'authentification et de confidentialité ;
- mettre en œuvre des dispositifs de préventions ;
- mettre en œuvre des dispositifs de détection ;
- mettre en œuvre les protections de base sur les vulnérabilités connues ;
- journaliser les accès (principes) ;
- sécuriser l'environnement d'administration ;
- gérer les incidents de sécurité.

Semestre 1 (2 + 2) 60h	Semestre 2 (2 + 2) 60h	Semestres 3 et 4 (2+2) 48h + 48h
		• Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique • Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure • Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité • Prévenir les attaques • Détecter les actions malveillantes • Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures

		Rappel des savoirs Sûreté des infrastructures réseaux : bonnes pratiques, normes et standards. Cybersécurité : bonnes pratiques, normes et standards. Technologies et équipements de la sécurité informatique des infrastructures réseau, systèmes et services. Outils de sécurité : prévention et détection des attaques, gestion d'incidents.
Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA Responsabilité civile et pénale de l'administrateur systèmes et réseaux		

Rappels : indicateurs de performance
Les dispositifs participant à la disponibilité sont validés (les éléments critiques sont résilients, la charge est répartie efficacement, la qualité des services sensibles est assurée).
Les failles potentielles sont identifiées grâce à une activité de veille sur les vulnérabilités.
Les bonnes pratiques de sécurité sont prises en compte.
Les éléments de sécurité de l'architecture sont conformes et documentés.
Les exigences de sécurité sont prises en compte dans le projet de mise en œuvre d'une solution d'infrastructure.
Les dispositifs de détection et de protection des attaques sont opérationnels.
Les processus de résolution d'un incident ou d'un problème sont respectés.
Le compte rendu d'intervention est clair et explicite.
Les contre-mesures mises en place corrigent et préviennent les incidents de sécurité
Les contre-mesures sont documentées de manière à en assurer le suivi.
La communication écrite et orale est adaptée à l'interlocuteur.

Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique
Pour bien sécuriser un réseau, un administrateur se doit de maîtriser son infrastructure. C'est pourquoi une partie de l'apprentissage doit être consacrée à l'étude détaillée d'infrastructures réseaux tant au niveau des interactions des composants que de leur configuration. La sûreté (bonnes pratiques résilience et qualité de service) doit être vérifiée avant de se préoccuper de la sécurité (malveillance). L'étudiant doit identifier les composants d'une architecture résiliente, repérer un dysfonctionnement et proposer une solution. Les notions suivantes peuvent être abordées :

- Sûreté des infrastructures réseaux : bonnes pratiques, segmentation du réseau, adressage, disponibilité, répartition de charges, qualité de service.

Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure
Cette compétence doit amener l'étudiant à appréhender la sécurité comme une préoccupation essentielle intégrée à toute la démarche projet et non comme une étape particulière.

Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité
La sécurité doit être mise en œuvre sur une infrastructure sûre. On rappellera les concepts (qui pour la plupart ont été traités en première année et on procédera à la configuration et à l'administration d'éléments de sécurité. Les notions suivantes peuvent être abordées :

- Normes et standards de la sécurité informatique des infrastructures réseau, systèmes et services.
- Sécurité des infrastructures systèmes et réseaux (bonnes pratiques, avis et alerte de sécurité, équipements de sécurité matériels et logiciels, filtrage des accès entrants et sortants, réseau privé virtuel, surcouche sécuritaire de protocole non sécurisé, sous-service spécialisé, infrastructure de gestion de clés publiques, toile de confiance, blockchain, durcissement, zone démilitarisée, séparation des privilèges).
- Protocoles et procédures de la preuve numérique (mise en œuvre PKI ou Blockchain).
- Vulnérabilités et attaques (exemples et mécanismes ⇒ excellente révision sur les protocoles standards).
- Outils : prévention et détection des attaques, gestion d'incidents, reconnaissance par signature, reconnaissance heuristique.
- Systèmes d'authentification et protection des accès aux service (sur différentes couches, 802.1X, VPN, zero trust, etc.).
- Système d'exploitation : gestion des utilisateurs, habilitations et droits d'accès, gestion des processus et de leurs droits., AAA (Authentication Authorization Accountability ⇒ Authentification Autorisation Traçabilité⇒ Qui ? Quoi ? Qui a fait quoi ?).

Prévenir les attaques
Cette compétence s'intéresse particulièrement aux dispositifs de protection (authentification dès l'accès au réseau, contrôle des flux entre les zones de sécurité, tunnelisation des flux externes, contrôle des ports ouverts, IPS, etc.).

Détecter les actions malveillantes
Cette compétence s'intéresse particulièrement aux dispositifs de détection (IDS, pot de miel, journalisation des accès, étude des logs, etc.).

Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures
L'apprentissage SISR de la sécurité peut s'appuyer sur la scénarisation d'incidents de sécurité simples (création délibérée d'une faille), la prise en charge de l'incident, et son traitement dans le respect des bonnes pratiques (notamment la documentation).

Recommandations pédagogiques
La vérification de la sûreté peut donner lieu à différentes modalités d'exercices. On peut travailler sur papier (schéma réseau, scripts de configuration, etc.), sur des simulateurs ou sur une infrastructure réelle. L'étudiant doit être en capacité à partir des documents fournis, de détecter des anomalies et proposer des solutions. Les anomalies peuvent concerner la conception d'une architecture réseau ou la configuration des éléments.

Des exercices (jeux) basés sur des attaques standards (usurpation d'adresses, DDOS, empoisonnement DNS, connexions TCP…) sont envisageables et

permettraient de consolider les connaissances sur les protocoles de base.

Encore une fois, on doit mettre l'étudiant en responsabilité afin qu'il dégage une méthode. Il faut privilégier les situations où l'étudiant propose et met en œuvre. On pourrait ainsi aborder de façon simultanée des technologies différentes avec différents groupes d'étudiants. On peut demander à un premier groupe de sécuriser les accès au réseau, à un deuxième groupe de paramétrer un pare-feu, à un troisième de configurer un IDS, etc. et que chaque groupe présente ses travaux à l'ensemble des groupes. On peut aussi par exemple scénariser un incident de sécurité et demander au groupe disposant de la solution de la mettre en place.

Dans le cadre de l'enseignement de CEJMA, il conviendra de porter une attention spécifique à la responsabilité de l'administrateur systèmes et réseaux dont l'une des missions est d'assurer la sécurisation du système d'information de l'organisation. Lorsqu'il ne prend pas les mesures nécessaires, il risque de manquer à ses obligations contractuelles et d'engager sa responsabilité civile et/ou pénale (à noter que les fondements de la responsabilité civile et pénale sont étudiés dans le thème 3 question 3 CEJM).
De plus dès lors que les contrôles effectués par l'administrateur font ressortir un risque pour le fonctionnement ou la sécurité du système d'information, l'administrateur systèmes et réseaux a l'obligation d'avertir le salarié à l'origine de ce risque mais aussi l'employeur.
L'étude de décisions de justice peut illustrer les cas dans lesquels l'administrateur systèmes et réseaux est mis en cause pour manquement à son obligation de sécurisation.

Ressources
https://www.ssi.gouv.fr/guide/gissip-guide-dintegration-de-la-securite-des-systemes-dinformation-dans-les-projets/ (ancien mais toujours pertinent).
https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/index-fr.aspx (Renforcer la résilience des infrastructures essentielles, avril 2019)
https://www.ssi.gouv.fr/uploads/2012/01/anssi-guide-passerelle_internet_securisee-v2.pdf
https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Politique_pare_feu_NoteTech.pdf
https://www.ssi.gouv.fr/guide/recommandations-de-securisation-dun-pare-feu-stormshield-network-security-sns/
https://www.ssi.gouv.fr/uploads/2019_1435_np.pdf (exemple de qualification d'une sonde, Cybels sensor de Thalès)
https://www.ssi.gouv.fr/guide/recommandations-de-deploiement-du-protocole-802-1x-pour-le-controle-dacces-a-des-reseaux-locaux/
https://www.ssi.gouv.fr/uploads/2015/07/catalogue-cfssi-anssi_2019-2020.pdf (catalogue des stages ANSSI pour 2020).
http://www.aud-it.ch/normes.html
http://securid.novaclic.com/securite-internet/referentiels-securite-si.html
https://www.ssi.gouv.fr/administration/bonnes-pratiques/ Bonnes pratiques de la sécurité des infrastructures systèmes et réseaux
https://security.infoteam.ch/blog/posts/votre-infrastructure-respecte-t-elle-les-normes-de-securite-actuelles.html Bonnes pratiques de la sécurité des infrastructures systèmes et réseaux
https://www.industrie-techno.com/rgpd-comment-dejouer-les-7-cyberattaques-les-plus-frequentes.52618 Exemples d'outils de détection des attaques
https://fr.wikibooks.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_informatiques/S%C3%A9curit%C3%A9_informatique/D%C3%A9tection_d%27intrusion Exemples outils de détection des attaques

Ressources CEJMA :
www.jurisexpert.net/cadre-juridique-des-administrateurs-reseaux/
www.legalis.net
Bonnes pratiques juridiques Administrateur systèmes et réseaux - Alain Bensoussan

B3.5 B - Assurer la cybersécurité d'une solution applicative et de son développement (option B)

Cette compétence est spécifique à l'option SLAM. Elle permet à l'étudiant de participer à la validation de la sûreté d'une solution applicative et de son développement et à la mise en œuvre de solutions de sécurité dans le respect des normes et des bonnes pratiques.
L'enseignement de CEJMA complétera les aspects techniques de cette compétence par un éclairage juridique sur la responsabilité du concepteur d'une solution applicative en cas de faille de sécurité dans la solution applicative développée.
Cette compétence doit amener l'étudiant à :

- vérifier la qualité d'un développement
- respecter la réglementation en matière de données personnelles
- intégrer la sécurité dans toute la démarche projet
- utiliser des flux sécurisés lors de l'échange de données
- mettre en œuvre des authentifications fortes (*framework* d'authentification conseillé)
- signer un code et vérifier la signature d'un code
- mettre en œuvre les protections de base sur les vulnérabilités connues des architectures web (OWASP)
- journaliser les accès
- sécuriser son environnement de développement
- sécuriser son environnement de production
- gérer les incidents de sécurité
- sécuriser la maintenance

Semestre 1 (2 + 2) 60h	Semestre 2 (2 + 2) 60h	Semestres 3 et 4 (2+2) 48h + 48h
		• Participer à la vérification des éléments contribuant à la qualité d'un développement informatique • Prendre en compte la sécurité dans un projet de développement d'une solution applicative • Mettre en œuvre et vérifier la conformité d'une solution applicative et de son développement à un référentiel, une norme ou un standard de sécurité • Prévenir les attaques • Analyser les connexions (logs) • Analyser des incidents de sécurité, proposer et mettre en œuvre des

		contre-mesures
		Rappels des savoirs Développement informatique : méthodes, normes, standards et bonnes pratiques. Aspects réglementaires du développement applicatif : protection de la vie privée dès la conception, protection des données par défaut, sécurité par défaut, droit des individus. Sécurité du développement d'application : gestion de projet, architectures logicielles, rôle des protocoles, authentification, habilitations et privilèges des utilisateurs, confidentialité des échanges, tests de sécurité, audit de code. Vulnérabilités et contre-mesures sur les problèmes courants de développement. Environnements de production et de développement : fonctionnalités de sécurité, techniques d'isolation des applicatifs.
Contribution des savoirs économiques, juridiques et managériaux étudiés en CEJMA Responsabilité du concepteur de solutions applicatives		

Rappels : indicateurs de performance

Le respect des bonnes pratiques de développement informatique est vérifié (les structures de données sont normalisées, les accès aux données sont optimisés, le code est modulaire et robuste, les tests sont effectués).
Les préoccupations de sécurité sont prises en compte à toutes les étapes d'un développement informatique.
Les bonnes pratiques de sécurité sont mises en œuvre à toutes les étapes d'un développement informatique.

Des tests de sécurité sont prévus et mis en œuvre.
Les traitements sur les données à caractère personnel sont déclarés et respectent la réglementation.
Le système d'authentification est conforme aux règles de sécurité.
L'accès aux données respecte les règles de sécurité.
Les échanges de données entre applications sont protégés.
Les composants utilisés sont certifiés, sécurisés et actualisés.
Les contre-mesures mises en place corrigent et préviennent les incidents de sécurité.
Les contre-mesures sont documentées de manière à en assurer le suivi.
La communication écrite et orale est adaptée à l'interlocuteur.

Participer à la vérification des éléments contribuant à la qualité d'un développement informatique
Pour bien sécuriser son application, un développeur doit maîtriser son développement. C'est pourquoi une partie de l'apprentissage doit être consacrée à l'étude détaillée d'applications informatiques tant au niveau des traitements que des données. La sûreté (qualité du développement informatique : et respect des bonnes pratiques) doit être validée. L'étudiant doit vérifier le respect des bonnes pratiques d'un développement informatique, repérer les anomalies et proposer des correctifs. Les notions suivantes peuvent être abordées :

- méthodes, normes et standards associés au processus de conception et de développement d'une solution applicative ;
- architecture applicatives et techniques : concepts de base et typologies ;
- modélisation des données et des traitements (modèles et standards de conception) ;
- SGBD : principaux concepts (structure et implémentation des données, architecture et infrastructure de stockage, contrainte d'intégrité, de confidentialité et de sécurité des données, propriétés de cohérence, de disponibilité et de distribution des données (CAP)), définition des données, contraintes et contrôle de données, outils de manipulation et d'interrogation d'une base de données, automatisation des actions ;
- technologie de programmation : concepts objet (classe, objet, abstraction, interface, héritage, polymorphisme, gestion des exceptions, patron de conception, interface de programmation d'applications (API), utilisation de Framework), persistance et couche d'accès aux données, tests, intégration de composants.

Prendre en compte la sécurité dans un projet de développement d'une solution applicative
Cette compétence doit amener l'étudiant à appréhender la sécurité comme une préoccupation essentielle intégrée à toute la démarche projet et non comme une étape particulière. L'utilisation de méthodes de gestion de projet intégrant la sécurité est recommandée.

On peut aussi s'intéresser à la modélisation des menaces et aux méthodes associées (https://fr.wikipedia.org/wiki/Mod%C3%A8le_de_menace) dès la phase de conception.

Les phases de développement et de déploiement sont aussi bien sûr à prendre en compte.

La phase de maintenance doit s'assurer de la sécurité établie. Il faut procéder à des vérifications périodiques de la sécurité et intégrer en intégrant les menaces apparues après la livraison.

Mettre en œuvre et vérifier la conformité d'une solution applicative et de son développement à un référentiel, une norme ou un standard de sécurité

L'étudiant doit connaître et participer au respect de la réglementation et doit donc prendre en compte la législation dans le développement applicatif :

- Protection de la vie privée dès la conception.
- Protection des données par défaut.
- Sécurité par défaut.
- Respect du droit des individus : droit à l'oubli / droit au déréférencement, droit à la portabilité, droit au consentement renforcé.

Prévenir les attaques

L'étudiant doit pouvoir implémenter des fonctions de sécurité (connaître les principes généraux et savoir implémenter des éléments de base) :

- Sécurité des architectures logicielles (on doit amener l'étudiant à s'interroger sur les problèmes de sécurité en fonction d'une architecture et d'une technologie choisie ⇒ exemple problème de sécurité d'un développement angular utilisant une API REST écrite en PHP).
- Authentification, gestion des méthodes d'authentification (l'utilisation d'un framework d'authentification est recommandée), gestion des sessions, gestion des habilitations et des privilèges, traçabilité, AAA (Authentication Authorization Accountability ⇒ Authentification Autorisation Traçabilité⇒ Qui ? Quoi ? Qui a fait quoi ?).
- Cryptographie, confidentialité des échanges, signature des composants, intégrité des données, preuve numérique, stockage sécurisée des données sensibles.
- Audit de code (exercice croisé entre étudiants pour vérifier le respect de règles données par l'enseignant faisant office de chef de projet).

L'étudiant doit pouvoir sécuriser des environnements de production et de développement (connaître les outils contribuant à la sécurité des applications, participer à la gestion de la sécurité du cycle de développement) :

- Protections offertes par les systèmes d'exploitation.
- Protections offertes par les protocoles.
- Sécurité des environnements de développement et de production.
- Gestion sécurisée des versions.
- Configuration des livrables.
- Tests de sécurité.

Analyser les connexions (logs)

Des environnements intégrant la traçabilité des accès doivent être mis en œuvre et exploités. La journalisation peut être prise en charge par le système ou programmée dans l'application (cet exercice pouvant s'avérer intéressant). Les fichiers de Logs ne doivent pas comporter de données personnelles sauf exception.

Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures

Les notions suivantes peuvent être abordées :

- Vulnérabilités et contre-mesures sur les problèmes courants ;
- Gestion des incidents de sécurité.

Recommandations pédagogiques

La vérification de la sûreté peut donner lieu à différentes modalités d'exercices. On peut travailler sur papier (modèle de données, codes, etc.), ou sur une application réelle. L'étudiant doit être en capacité à partir des documents fournis, de détecter des anomalies de conception ou de réalisation et proposer des solutions.

La vérification des préconisations du RGPD peut donner lieu à des développements complémentaires, par exemple la prise en charge de la restriction de traitement ou la journalisation des accès.

Il faut s'appuyer sur les ressources existantes concernant la sécurité des architectures Web (l'ANSSI propose dans son catalogue 2020 un stage gratuit de 5 jours sur le sujet https://www.ssi.gouv.fr/uploads/2015/07/catalogue-cfssi-anssi_2019-2020.pdf). Pour la mise en œuvre de la sécurité, il est préférable de mettre l'étudiant en responsabilité afin qu'il dégage une méthode. Ainsi on peut demander sur une application existante de développer une authentification forte (il est recommandé d'utiliser une infrastructure de programmation - *framework*), de faire une démonstration de vulnérabilité connue et de ses contre-mesures, ou bien encore de sécuriser un environnement de production. Il faut privilégier le fait que l'étudiant propose et mette en œuvre plutôt que des TP dirigés dès que cela est possible, dans le processus d'apprentissage.

Dans le cadre de l'enseignement de CEJMA, il conviendra de porter une attention spécifique à la responsabilité du concepteur de solution applicative en cas de faille de sécurité dans la solution applicative développée. Sa responsabilité civile peut ainsi être engagée si une vulnérabilité de la solution applicative cause un préjudice au client voire sa responsabilité pénale notamment en cas d'atteinte aux données à caractère personnel (à noter que les fondements de la responsabilité civile et pénale sont étudiés dans le thème 3 question 3 CEJM).

Ressources

https://www.ssi.gouv.fr/uploads/2018/11/guide-securite-numerique-agile-anssi-pa-v1.pdf
https://www.globalsecuritymag.fr/Conference-du-CLUSIF-Developpement,20190606,87838.html
https://www.cnil.fr/fr/securite-encadrer-les-developpements-informatiques
https://www.cnil.fr/fr/kit-developpeur (Kit CNIL pour la qualité et la sécurité du développement)
https://fr.howtodou.com/what-is-security-threat-modeling (modélisation des menaces)
https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards (Bonnes pratiques langages)
https://www.owasp.org/index.php/Maiin_Page
https://bohzo.developpez.com/rgpd-guide-pratique-developpeurs/
https://www.cnil.fr/fr/securite-tracer-les-acces-et-gerer-les-incidents
https://www.reseaucerta.org/securisation-des-applications-web-owasp
https://www.reseaucerta.org/exploitation-docker-linux
https://www.reseaucerta.org/sites/default/files/gsbAngular2_Presentation.pdf La dernière partie (à actualiser) est intéressante du point de vue des concepts de sécurité associé à des Web Services REST.
https://secnum.fr/ Article assez pointu sur les problématiques d'authentification (juillet 2019)
https://blog.octo.com/securiser-une-api-rest-tout-ce-quil-faut-savoir/ Présentation intéressante sur les *framework* d'authentification
https://www.ssi.gouv.fr/uploads/2015/07/catalogue-cfssi-anssi_2019-2020.pdf (catalogue des stages ANSSI 2020)
Normes et standard de la sécurité du développement informatique OWASP SAAM SDLC, .etc.
https://tymate.com/articles/rgpd-et-developpement

https://blog.frelonbleu.com/comment-appliquer-rgpd
Intégration de la sécurité dans la conduite de projet
https://www.cnil.fr/fr/securite-encadrer-les-developpements-informatiques
https://www.ssi.gouv.fr/uploads/2017/07/guide-securite-agile_v0.42_anssi_dinsic.pdf
Constitution et gestion de la preuve numérique (Voir avec docs précédentes et +)

Sécurité des environnements de développement, par exemple :

- https://labelisation.cartes-bancaires.com/sites/default/files/cb-2016-fr-referentiel_labellisation_v1.2.1.pdf
- https://www.cnil.fr/fr/gerer-le-code-source (Gestion de versions bonnes pratiques)

Bonnes pratiques du développement sécurisé, par exemple :

- https://www.has-sante.fr/portail/upload/docs/application/pdf/2016-11/has_ref_apps_oc.pdf
- https://chstudio.fr/2018/01/guide-pour-des-logiciels-php-securises-en-2018/

Framework d'authentification : Oauth jwt, etc.Protection applicative de l'accès aux données
Sécuriser les API REST exemple https://www.codeheroes.fr/index.php/2018/03/23/securiser-une-api-rest/
Sécuriser un ORM : exemple https://docs.microsoft.com/fr-fr/dotnet/framework/data/adonet/ef/security-considerations

Quelques outils permettant de tester, de mettre en oeuvre des techniques de piratage et d'auditer le code d'une application :

- DVWA : http://www.dvwa.co.uk/ application web permettant de tester tout type d'intrusion, et de choisir le niveau de vulnérabilité.
- BEEF : https://beefproject.com/ Outil permettant de tester la vulnérabilité d'un site.
- BURP : https://portswigger.net/burp détecter les éventuelles failles d'un site ou d'une application. Permet également d'intercepter les requêtes envoyées par le navigateur et les modifier à la volée.
- Portail OWASP : https://www.owasp.org/index.php/Main_Page Permet de trouver des exemples de vulnérabilité.
- Liste de vulnérabilité par système. https://www.google.com/url?q=https://www.exploit-db.com&sa=D&ust=1578992809631000&usg=AFQjCNHGXwzXH1kCjO4BAi0mb9QoZFQpcQ
- Wpscan : https://wpscan.org/ Test les vulnérabilités pour Wordpress

Ressources CEJMA
www.journaldunet.com/solutions/expert/52611/les-editeurs-de-logiciels-doivent-ils-etre-tenus-responsables-des-vulnerabilites-des-produits-qu-ils-commercialisent.shtml
www.zdnet.fr/actualites/les-editeurs-doivent-ils-etre-responsables-des-failles-de-securite-2103069.htm
www.journaldunet.com/juridique/juridique051108.shtml
www.alain-bensoussan.com/avocats/habilitations-rgpd-compliant/2017/04/20/
home.cern/fr/news/news/computing/computer-security-do-we-need-more-software-liability
avocatspi.com/2017/02/17/les-nouvelles-obligations-des-editeurs-de-logiciels-saas-au-regard-du-reglement-ue-2016679-relatif-a-la-protection-des-donnees-a-caractere-personnel/
www.lemagit.fr/conseil/Prendre-sa-part-de-responsabilite-dans-la-securite-des-applications-SaaS
www.usinenouvelle.com/article/fourniture-de-logiciels-vers-une-obligation-de-securite.N61606
Legalis.net
Cyberdroit - le droit à l'épreuve de l'internet - Christiane Féral-Schuhl - Edition Dalloz 2018/2019

Les ateliers de professionnalisation

Le rôle de ces temps de formation réguliers de 4h hebdomadaires est clairement défini dans le référentiel : « *Les ateliers de professionnalisation permettent aux étudiants de travailler en mode projet sur des situations professionnelles qui mobilisent des compétences des trois blocs professionnels et renforcent les acquis des enseignements généraux.* »

On peut légitimement penser que ces temps de formation correspondent aux Projets personnalisés encadrés du précédent référentiel.

Ce qui est premier ici c'est la modalité pédagogique : en projet. C'est à dire un travail, significatif d'une activité professionnelle réelle, confié à une équipe composée de plusieurs étudiants ou apprentis, lesquels travaillent le plus possible en autonomie avec les conseils et le soutien attentif et régulier des professeurs de l'équipe pédagogique.

Au fond, on cherche à reproduire au mieux, dans le centre de formation, le contexte et les modalités de travail que pourront rencontrer les jeunes en entreprise, en stage, en apprentissage ou en emploi.

Le rôle essentiel de l'équipe pédagogique est bien de concevoir des situations d'apprentissage professionnellement réalistes permettant aux étudiants / apprentis d'apprendre en faisant, en échangeant avec les pairs et les professeurs, en recherchant l'information utile, en rendant compte des progrès et des difficultés, en présentant le travail réalisé par l'équipe tout en sachant identifier les contributions personnelles.

On veille à ne pas reproduire une situation de travaux dirigés dans laquelle les étudiants suivent des étapes de réalisation préméditées et guidées par le professeur. Le travail en équipe avec le soutien d'un ou plusieurs professeurs de toutes disciplines et enseignements, la nécessité de s'organiser, de communiquer au sein de l'équipe et en dehors, constituent le socle permettant à chacun de construire sa professionnalité. Le manque d'autonomie, naturellement souvent constaté chez les jeunes, nécessite de leur en donner progressivement davantage.

Dans les sections à public mixé où étudiants et apprentis cohabitent dans la même formation les situations professionnelles rencontrées par les apprentis peuvent profiter aux étudiants.

Les projets confiés et les réalisations qui en découlent peuvent assurément permettre d'alimenter ce qui sera présenté par les candidats durant les épreuves professionnelles orales et en particulier d'alimenter le portfolio retraçant le parcours de professionnalisation.

Au cours de la formation, on pourra adopter de préférence une approche progressive tant sur le niveau d'exigence des projets à réaliser (du plus facile au moins facile) que sur le degré d'autonomie laissé dans la recherche des solutions ou des outils adaptés. De même, on pourra avantageusement moduler sur ces deux aspects en tenant compte des capacités et des projets professionnels de chaque étudiant / apprenti.

Dans une certaine mesure, le centre de formation lui-même peut être un contexte professionnel crédible pour les ateliers de professionnalisation. Ceci sous réserve d'une bonne information auprès de la direction et d'un cadrage attentif de l'équipe pédagogique. On sait toutefois qu'il est toujours préférable de mobiliser un contexte qui permette aux apprenants de s'ouvrir à la diversité et à la richesse des situations rencontrées dans les entreprises.

Exemples d'approches pédagogiques en atelier

Exemple 1 : la veille

La capacité à assurer une veille documentaire et technologique est déterminante pour se sentir à l'aise dans le métier d'informaticien. Développer chez les étudiants et les apprentis cette capacité à appréhender, seul ou collectivement, une documentation, un nouvel outil, une nouvelle technologie, prépare un parcours professionnel serein.

Les premiers projets prévoient d'emblée la nécessité de lire des éléments de contexte du projet, de rechercher une information pertinente sur internet, de rechercher des éléments de réponse avant de simplement poser une question.

Exemple 2 : travailler sa professionnalité

Se percevoir comme un professionnel junior ou comme un professionnel en devenir passe par des activités concrètes à réaliser : se présenter dans un CV, une vidéo, un *pitch* ; s'inscrire et participer à des réseaux sociaux professionnels orientés recrutement et valorisation des compétences ; simuler des entretiens d'embauche ; identifier et participer à des dispositifs de formation, etc. L'ensemble de ces activités peut constituer un projet au long cours.

Exemple 3 : support des services informatiques

Le contexte de l'établissement ou du centre de formation, peut constituer une base pertinente pour expérimenter la réalité du contact avec les utilisateurs comme les contraintes d'une intervention pertinente, ceci à la fois pour évaluer le besoin, pour circonscrire le problème, identifier progressivement son origine en éliminant des hypothèses, puis en proposant une solution.

Exemple 4 : développer la présence en ligne de l'organisation

Analyser un site web, l'évaluer, proposer des améliorations en tenant compte des objectifs de l'organisation qui le publie ; les mettre en œuvre en choisissant les moyens les plus adaptés.

Annexe 1 - Scénarios d'organisation des enseignements

Ce document propose différents scénarios d'organisation des enseignements en BTS SIO à partir de la rentrée 2020. Pour chaque semestre de la première année, puis pour les deux semestres de la seconde année, des ensembles de compétences, jugés cohérents aux plans pédagogique et didactique, sont proposés.

Les compétences et les horaires proposés ici le sont à titre purement indicatif, chaque équipe choisira librement la répartition qui conviendra le mieux en tenant compte des appétences et des compétences de chacune et chacun au sein de l'équipe pédagogique.

Voici quelques informations pour faciliter la lecture du tableau :

- Les compétences du référentiel ont été numérotées afin de faciliter leur repérage. Ainsi, la compétence numéro **B1.1** est la première compétence globale citée dans le référentiel pour le bloc 1 : "Gérer le patrimoine informatique".
- Chaque ligne du tableau correspond à un ensemble de compétences qui peuvent être enseignées par un même enseignant. Un même enseignant pouvant naturellement prendre en charge plusieurs de ces ensembles.
- La somme des horaires proposés correspond au volume horaire officiel fixé pour chaque bloc et chaque semestre dans le référentiel du diplôme.
- Les ensembles de compétences sont numérotés :
    - TC (tronc commun), ils s'adressent aux étudiants des deux options.
    - R (réseau), ils s'adressent uniquement aux étudiants ayant choisi l'option SISR.
    - D (développement), ils s'adressent uniquement aux étudiants ayant choisi l'option SLAM.
- Pour les enseignements de tronc commun, les mentions « *orientation réseau* » et « *orientation développement* » sont précisées pour exprimer un équilibre entre des fondamentaux réseau et développement. Le respect de cet équilibre permet un choix éclairé d'option en fin de premier semestre, il permet également l'acquisition des prérequis du bloc 2. Dans le cas où l'enseignement serait réparti entre 2 enseignants seulement, chacun dans une spécialité il est tout à fait possible de répartir l'horaire équitablement.

Ensemble de compétences	Semestre 1 – Proposition 1	Horaires (classe + groupe)
TC1 *Orientation réseau*	**B1.1 Gérer le patrimoine informatique** ● Recenser et identifier les ressources numériques ● Mettre en place et vérifier les niveaux d'habilitation associés à un service **B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution** ● Traiter des demandes concernant les services réseau et système, applicatifs **B1.5 Mettre à disposition des utilisateurs un service informatique (orienté utilisateurs)** ● Déployer un service **B1.6 Organiser son développement professionnel** ● Gérer son identité professionnelle ● Développer son projet professionnel ● Mettre en place son environnement d'apprentissage personnel	2+2
TC2 *Orientation développement*	**B1.1 Gérer le patrimoine informatique** ● Recenser et identifier les ressources numériques ● Mettre en place et vérifier les niveaux d'habilitation associés à un service **B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution** ● Traiter des demandes concernant les applications **B1.3 Développer la présence en ligne de l'organisation** ● Participer à l'évolution d'un site Web exploitant les données de l'organisation. **B1.6 Organiser son développement professionnel** ● Gérer son identité professionnelle ● Développer son projet professionnel ● Mettre en place son environnement d'apprentissage personnel	2+4
TC3	**B3.1 Protéger les données à caractère personnel** ● Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel ● Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel ● Sensibiliser les utilisateurs à la protection des données à caractère personnel **B3.2 Préserver l'identité numérique de l'organisation** ● Protéger l'identité numérique d'une organisation ● Déployer les moyens appropriés de preuve électronique **B3.3 Sécuriser les équipements et les usages des utilisateurs** ● Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter ● Identifier les menaces et mettre en œuvre les défenses appropriées ● Gérer les accès et les privilèges appropriés ● Vérifier l'efficacité de la protection	2+2

Ensemble de compétences	Semestre 1 – Proposition 2 avec intégration du module de sécurité (si par ex. enseignement partagé entre 2 enseignants)	Horaires (classe + groupe)
TC1 *Orientation réseau*	**B1.1 Gérer le patrimoine informatique** ● Recenser et identifier les ressources numériques ● Mettre en place et vérifier les niveaux d'habilitation associés à un service **B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution** ● Traiter des demandes concernant les services réseau et système, applicatifs **B1.5 Mettre à disposition des utilisateurs un service informatique (orienté utilisateurs)** ● Déployer un service **B1.6 Organiser son développement professionnel** ● Gérer son identité professionnelle ● Développer son projet professionnel ● Mettre en place son environnement d'apprentissage personnel **B3.3 Sécuriser les équipements et les usages des utilisateurs** ● Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter ● Identifier les menaces et mettre en œuvre les défenses appropriées ● Gérer les accès et les privilèges appropriés ● Vérifier l'efficacité de la protection	3+4
TC2 *Orientation développement*	**B1.1 Gérer le patrimoine informatique** ● Recenser et identifier les ressources numériques ● Mettre en place et vérifier les niveaux d'habilitation associés à un service **B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution** ● Traiter des demandes concernant les applications **B1.3 Développer la présence en ligne de l'organisation** ● Participer à l'évolution d'un site Web exploitant les données de l'organisation. **B1.6 Organiser son développement professionnel** ● Gérer son identité professionnelle ● Développer son projet professionnel ● Mettre en place son environnement d'apprentissage personnel **B3.1 Protéger les données à caractère personnel** ● Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel ● Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel ● Sensibiliser les utilisateurs à la protection des données à caractère personnel **B3.2 Préserver l'identité numérique de l'organisation** ● Protéger l'identité numérique d'une organisation ● Déployer les moyens appropriés de preuve électronique	3+4

	Semestre 2 - proposition 1	Horaires
TC4 *Orientation réseau*	**B1.1 Gérer le patrimoine informatique - suite** • Exploiter des référentiels, normes et standards adoptés par le prestataire informatique • Gérer des sauvegardes **B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution - suite** • Collecter, suivre et orienter des demandes • Traiter des demandes concernant les services réseau et système, applicatifs **B1.4 Travailler en mode projet** • Analyser les objectifs et les modalités d'organisation d'un projet • Évaluer les indicateurs de suivi d'un projet et analyser les écarts • Planifier les activités **B1.5 Mettre à disposition des utilisateurs un service informatique (orienté utilisateurs) - suite** • Déployer un service - suite • Réaliser les tests d'intégration et d'acceptation d'un service • Accompagner les utilisateurs dans la mise en place d'un service **B1.6 Organiser son développement professionnel - suite** • Mettre en œuvre des outils et stratégies de veille informationnelle • Mettre en place son environnement d'apprentissage personnel - suite • Développer son projet professionnel - suite	1+1
TC5 *Orientation développement*	**B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution - suite** • Collecter, suivre et orienter des demandes • Traiter des demandes concernant les applications **B1.3 Développer la présence en ligne de l'organisation - suite** • Référencer les services en ligne de l'organisation et mesurer leur visibilité. • Participer à l'évolution d'un site Web exploitant les données de l'organisation. **B1.4 Travailler en mode projet** • Analyser les objectifs et les modalités d'organisation d'un projet • Évaluer les indicateurs de suivi d'un projet et analyser les écarts • Planifier les activités **B1.6 Organiser son développement professionnel - suite** • Mettre en œuvre des outils et stratégies de veille informationnelle • Mettre en place son environnement d'apprentissage personnel - suite • Développer son projet professionnel - suite	1+1
TC6	**B3.3 Sécuriser les équipements et les usages des utilisateurs - suite** • Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter - suite • Identifier les menaces et mettre en œuvre les défenses appropriées - suite • Gérer les accès et les privilèges appropriés - suite	2+2

	• Vérifier l'efficacité de la protection - suite **B3.4 Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face aux cyberattaques** • Caractériser les risques liés à l'utilisation malveillante d'un service informatique • Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité • Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation • Organiser la collecte et la conservation des preuves numériques • Appliquer les procédures garantissant le respect des obligations légales	
R1 *Orientation administration des infrastructures*	B2.1 Concevoir une solution d'infrastructure réseau B2.2 Installer, tester et déployer une solution d'infrastructure réseau B2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau	1+3
R2 *Orientation administration des systèmes et des services*	B2.1 Concevoir une solution d'infrastructure réseau B2.2 Installer, tester et déployer une solution d'infrastructure réseau B2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau	1+1
D1	B2.1 Concevoir et développer une solution applicative B2.2 Assurer la maintenance corrective ou évolutive d'une solution applicative	1+3
D2	B2.3 Gérer les données	1+1

	Semestre 2 - proposition 2 : autre logique de découpage SISR	Horaires
TC4 *Orientation réseau*	**B1.1 Gérer le patrimoine informatique - suite** ● Exploiter des référentiels, normes et standards adoptés par le prestataire informatique ● Gérer des sauvegardes **B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution - suite** ● Collecter, suivre et orienter des demandes ● Traiter des demandes concernant les services réseau et système, applicatifs **B1.4 Travailler en mode projet** ● Analyser les objectifs et les modalités d'organisation d'un projet ● Évaluer les indicateurs de suivi d'un projet et analyser les écarts ● Planifier les activités **B1.5 Mettre à disposition des utilisateurs un service informatique (orienté utilisateurs) - suite** ● Déployer un service - suite ● Réaliser les tests d'intégration et d'acceptation d'un service ● Accompagner les utilisateurs dans la mise en place d'un service **B1.6 Organiser son développement professionnel - suite** ● Mettre en œuvre des outils et stratégies de veille informationnelle ● Mettre en place son environnement d'apprentissage personnel - suite ● Développer son projet professionnel - suite	1+1
TC5 *Orientation développement*	**B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution - suite** ● Collecter, suivre et orienter des demandes ● Traiter des demandes concernant les applications **B1.3 Développer la présence en ligne de l'organisation - suite** ● Référencer les services en ligne de l'organisation et mesurer leur visibilité. ● Participer à l'évolution d'un site Web exploitant les données de l'organisation. **B1.4 Travailler en mode projet** ● Analyser les objectifs et les modalités d'organisation d'un projet ● Évaluer les indicateurs de suivi d'un projet et analyser les écarts ● Planifier les activités **B1.6 Organiser son développement professionnel - suite** ● Mettre en œuvre des outils et stratégies de veille informationnelle ● Mettre en place son environnement d'apprentissage personnel - suite ● Développer son projet professionnel - suite	1+1
TC6	**B3.3 Sécuriser les équipements et les usages des utilisateurs - suite** ● Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter - suite	2+2

	• Identifier les menaces et mettre en œuvre les défenses appropriées - suite • Gérer les accès et les privilèges appropriés - suite • Vérifier l'efficacité de la protection - suite **B3.4 Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face aux cyberattaques** • Caractériser les risques liés à l'utilisation malveillante d'un service informatique • Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité • Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation • Organiser la collecte et la conservation des preuves numériques • Appliquer les procédures garantissant le respect des obligations légales	
R1 *Orientation conception et adaptation des infrastructures réseau*	B2.1 Concevoir une solution d'infrastructure réseau B2.2 Installer, tester et déployer une solution d'infrastructure réseau	1+3
R2 *Orientation gestion des incidents et des problèmes systèmes et réseau*	B2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau	1+1
D1	B2.1 Concevoir et développer une solution applicative B2.2 Assurer la maintenance corrective ou évolutive d'une solution applicative	1+3
D2	B2.3 Gérer les données	1+1

	Semestres 3&4 - proposition 1 : blocs 2 et 3 enseignés ensemble	Horaires
TC7	**B1.1 Gérer le patrimoine informatique - suite** ● Vérifier les conditions de la continuité d'un service informatique **B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution - suite** ● Traiter des demandes concernant les services réseau et système, applicatifs ● Traiter des demandes concernant les applications **B1.3 Développer la présence en ligne de l'organisation - suite** ● Participer à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques ● Participer à l'évolution d'un site Web exploitant les données de l'organisation. **B1.4 Travailler en mode projet - suite** ● Planifier les activités **B1.5 Mettre à disposition des utilisateurs un service informatique** ● Réaliser les tests d'intégration et d'acceptation d'un service **B1.6 Organiser son développement professionnel - suite** ● Mettre en œuvre des outils et stratégies de veille informationnelle ● Développer son projet professionnel	2+0
R3 *Orientation administration des infrastructures*	B2.1 Concevoir une solution d'infrastructure réseau B2.2 Installer, tester et déployer une solution d'infrastructure réseau B2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau B3.5 A Assurer la cybersécurité d'une infrastructure réseau	2+3
R4 *Orientation administration des systèmes*	B2.1 Concevoir une solution d'infrastructure réseau B2.2 Installer, tester et déployer une solution d'infrastructure réseau B2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau B3.5 A Assurer la cybersécurité d'un système	1,5+2,5
R5	B2.1 Concevoir une solution d'infrastructure réseau	1,5+2,5

Orientation administration des services	B2.2 Installer, tester et déployer une solution d'infrastructure réseau B2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau B3.5 A Assurer la cybersécurité d'un service	
D3	B2.1 Concevoir et développer une solution applicative B2.2 Assurer la maintenance corrective ou évolutive d'une solution applicative B3.5 B Assurer la cybersécurité d'une solution applicative et de son développement	3+6
D4	B2.3 Gérer les données B3.5 B Assurer la cybersécurité d'une solution applicative et de son développement	2+2

	Semestres 3&4 - proposition 2 : blocs 2 et 3 enseignés séparément	Horaires
TC7	B1.1 Gérer le patrimoine informatique - suite B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution - suite B1.3 Développer la présence en ligne de l'organisation - suite B1.4 Travailler en mode projet - suite B1.5 Mettre à disposition des utilisateurs un service informatique B1.6 Organiser son développement professionnel - suite	2+0
R3 *Orientation administration des infrastructures*	B2.1 Concevoir une solution d'infrastructure réseau B2.2 Installer, tester et déployer une solution d'infrastructure réseau B2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau	1+2
R4 *Orientation administration des systèmes*	B2.1 Concevoir une solution d'infrastructure réseau B2.2 Installer, tester et déployer une solution d'infrastructure réseau B2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau	1+2
R5 *Orientation administration des services*	B2.1 Concevoir une solution d'infrastructure réseau B2.2 Installer, tester et déployer une solution d'infrastructure réseau B2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau	1+2
R6	B3.5 A Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service	2+2
D3	B2.1 Concevoir et développer une solution applicative B2.2 Assurer la maintenance corrective ou évolutive d'une solution applicative	2+4
D4	B2.3 Gérer les données	1+2
D5	B3.5 B Assurer la cybersécurité d'une solution applicative et de son développement	2+2

	Semestres 3&4 - proposition 3 : autre logique de découpage SISR	Horaires
TC7	B1.1 Gérer le patrimoine informatique - suite B1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution - suite B1.3 Développer la présence en ligne de l'organisation - suite B1.4 Travailler en mode projet - suite B1.5 Mettre à disposition des utilisateurs un service informatique B1.6 Organiser son développement professionnel - suite	2+0
R3 *Orientation disponibilité des infrastructures, des systèmes et des services*	B2.1 Concevoir une solution d'infrastructure réseau B2.2 Installer, tester et déployer une solution d'infrastructure réseau B2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau	2+4
R4 *Orientation qualité des infrastructures, des systèmes et des services*	B2.1 Concevoir une solution d'infrastructure réseau B2.2 Installer, tester et déployer une solution d'infrastructure réseau B2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau	1+2
R5	B3.5 A Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service	2+2
D3	B2.1 Concevoir et développer une solution applicative B2.2 Assurer la maintenance corrective ou évolutive d'une solution applicative	2+4
D4	B2.3 Gérer les données	1+2
D5	B3.5 B Assurer la cybersécurité d'une solution applicative et de son développement	2+2

Annexe 2 – Proposition pour une progression pédagogique en CEJMA - semestres 1 et 2

SEMESTRE 1				SEMESTRE 2			
Contributions CEJMA	**Bloc de compétences**	**Prolongements CEJM**	**Nouveaux savoirs à apporter**	**Contributions CEJMA**	**Bloc de compétences**	**Prolongements CEJM**	**Nouveaux savoirs à apporter**
Gestion du patrimoine informatique				**Contraintes éthiques et environnementales dans le choix d'une infrastructure réseau ou dans la conception d'une solution applicative**	**bloc 2**	**Question 3.4**	
- Les acteurs de l'industrie informatique	**bloc 1**	**Question 1.1**					
- Les enjeux liés à la gestion des actifs informatiques	**bloc 1**		**X**	**Le droit de la preuve électronique et Obligations légales en matière de conservation et d'archivage des données**	**blocs 1 et 3**	**Question 4.1**	**X**
- Les clauses des contrats liés à la gestion du patrimoine informatique	**bloc 1**	**Question 1.2 Question 4.2**					
- Le contrat de niveau de service et contrat d'assistance (SLA)	**blocs 1 et 2**		**X**	**L'utilisation des ressources numériques par les salariés** :			
- Licences logicielles (distinction libre/propriétaire) et modalités de tarification	**bloc 1**	**Question 4.1 Question 4.2**		- Le rôle et valeur juridique de la charte informatique,	**blocs 1 et 3**	**Question 4.2**	
- Les enjeux techniques et économiques des normes et standards	**bloc 1**	**Question 4.1**		- Les responsabilités du salarié utilisateur de ressources informatiques,		**Question 5.2**	
				- Les enjeux des		**Question 5.3**	

				nouvelles modalités de travail			
La réglementation relative à la protection des données à caractère personnel	**blocs 1, 2, 3**	**Question 4.2**	**X**	**La réglementation relative au site internet d'une organisation :**	**bloc 1**		
				- Les mentions légales et CGU			**X**
				- Le droit d'utilisation des contenus externes,			**X**
				- Le nom de domaine,		**Question 4.2**	
				- La responsabilité de l'éditeur et de l'hébergeur du site Web			**X**

La colonne "**Contributions CEJMA**" énonce les savoirs à aborder dans le cadre de l'enseignement de CEJMA, les colonnes "**Bloc de compétences"** et **"Prolongements CEJM"** établissent les liens entre les savoirs CEJMA et les blocs professionnels, entre les savoirs CEJMA et le programme de CEJM, enfin la colonne "**Nouveaux savoirs à apporter"** indique les notions qui n'ont pas été traitées en CEJM et qui devront être étudiées en CEJMA.

Proposition pour une progression pédagogique en CEJMA - semestres 3 et 4

SEMESTRES 3 ET 4							
Contributions CEJMA OPTION SLAM	**Bloc de compétences**	**Prolongements CEJM**	**Nouveaux savoirs à apporter**	**Contributions CEJMA OPTION SISR**	**Bloc de compétences**	**Prolongements CEJM**	**Nouveaux savoirs à apporter**
La présence en ligne de l'organisation				**La présence en ligne de l'organisation**			
- L'identité numérique de l'organisation	**bloc 3**	**Question 4.2**		- L'identité numérique de l'organisation	**bloc 3**	**Question 4.2**	
- L'e-réputation de l'organisation	**bloc 1**		**X**	- L'e-réputation de l'organisation	**bloc 1**		**X**
Les relations pré-contractuelles et contractuelles entre le prestataire informatique et son client :				**Les relations pré-contractuelles et contractuelles entre le prestataire informatique et son client :**			
- Le cahier des charges, ses enjeux juridiques et son agilité	**bloc 2**		**X**	- Le cahier des charges, ses enjeux juridiques et son agilité	**bloc 2**		**X**
- Les contrats de prestation de services informatiques liés aux solutions applicatives	**bloc 2**	**Question 1.2** **Question 4.2**		- Les contrats de prestation de services informatiques liés aux infrastructures réseaux	**bloc 2**	**Question 1.2** **Question 4.2**	
La protection juridique des outils et des productions numériques : protection des productions de solutions applicatives, des bases de	**bloc 2**	**Question 2.2** (brevet) **Question 4.2**	**X**				

données, typologie des licences logicielles							
La responsabilité du concepteur de solutions applicatives et de bases de données	**blocs 2 et 3**	**Question 3.3**	**X**	**La responsabilité de l'administrateur système et réseau**	**blocs 2 et 3**	**Question 3.3**	**X**
La cybercriminalité :				**La cybercriminalité :**			
- Les risques des cyberattaques pour l'organisation	**bloc 3**		**X**	- Les risques des cyberattaques pour l'organisation	**bloc 3**		**X**
- Réglementation en matière de lutte contre la fraude informatique	**bloc 3**		**X**	- Réglementation en matière de lutte contre la fraude informatique	**bloc 3**		**X**
- Les organisations de lutte contre la cybercriminalité	**bloc 3**		**X**	- Les organisations de lutte contre la cybercriminalité	**bloc 3**		**X**

La colonne "**Contributions CEJMA**" énonce les savoirs à aborder dans le cadre de l'enseignement de CEJMA, les colonnes "**Bloc de compétences"** et **"Prolongements CEJM"** établissent les liens entre les savoirs CEJMA et les blocs professionnels, entre les savoirs CEJMA et le programme de CEJM, enfin la colonne "**Nouveaux savoirs à apporter"** indique les notions qui n'ont pas été traitées en CEJM et qui devront être étudiées en CEJMA.

Annexe 3 - Guide d'équipement

Le présent document précise les principales caractéristiques des équipements matériels et logiciels à utiliser pour une section de BTS SIO proposant les deux options SISR et SLAM, soit 64 étudiants. Il doit être décliné par les équipes en fonction de ses besoins et des équipements déjà disponibles.

L'environnement technologique qui doit être mis à la disposition des apprenants en BTS SIO est décrit dans le référentiel du diplôme, plus précisément dans l'***Annexe II.E - Environnement technologique pour la certification*** rappelée plus bas.

Avertissements

- Les marques, noms de constructeurs, d'éditeurs ou d'équipements cités dans le présent document ne sont donnés qu'à titre indicatif.

- Le large éventail des systèmes à étudier, la nécessité de pouvoir les faire évoluer dans le temps sans pour autant réinvestir constamment, la puissance requise par les environnements de développement ainsi que la souplesse requise pour l'apprentissage de technologies en constante évolution, rend particulièrement pertinent le recours à des infrastructures disponibles dynamiquement à la demande via un service de *cloud computing* public de type OVH, Microsoft Azure, IBM cloud, Amazon Web Services, Google Cloud Platform, etc.

- Le recours à des logiciels libres qui ont un modèle de propriété intellectuelle conçu pour donner à l'utilisateur une grande liberté d'utilisation, de modification et de diffusion, est recommandé.

- Pour des raisons évidentes de sécurité, il est nécessaire que le réseau informatique utilisé par les apprenants de BTS SIO soit séparé du réseau pédagogique du reste de l'établissement qui accueille la formation. En effet, à défaut d'un cloisonnement strict, la mise en œuvre nécessairement expérimentale des applications, des services et protocoles réseau par les apprenants peut fortement perturber le fonctionnement du réseau pédagogique de l'établissement.

Rappel des exigences du référentiel (annexe II.E)

<u>Équipements communs aux options SISR et SLAM</u>

L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

- *un service d'authentification pour les utilisateurs internes et externes à l'organisation ;*
- *un SGBD ;*
- *un accès sécurisé à internet ;*
- *un environnement de travail collaboratif ;*
- *deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel open source ;*
- *une solution de sauvegarde ;*
- *des ressources dont l'accès est sécurisé et soumis à habilitation ;*
- *deux types de terminaux dont un mobile (type smartphone ou encore tablette).*

Les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

Des outils sont mobilisés pour la gestion de la sécurité :

- *gestion des incidents ;*

- *détection et prévention des intrusions ;*
- *chiffrement ;*
- *analyse de trafic.*

Équipements pour l'option SISR

L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

- *un réseau comportant plusieurs périmètres de sécurité ;*
- *un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité ;*
- *un logiciel d'analyse de trames ;*
- *un logiciel de gestion des configurations ;*
- *une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès ;*
- *une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes ;*
- *une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet) ;*
- *une solution garantissant la continuité d'un service ;*
- *une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion ;*
- *une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion.*

La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

- *une solution permettant la connexion sécurisée entre deux sites distants ;*
- *une solution permettant le déploiement des solutions techniques d'accès ;*
- *une solution gérée à l'aide de procédures automatisées écrites avec un langage de scripting ;*
- *une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau.*

Équipements pour l'option SLAM

L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

- *un ou deux environnements de développement disposant d'outils de gestion de tests et supportant un cadre applicatif (framework) et au moins deux langages ;*
- *une bibliothèque de composants logiciels ;*
- *un SGBD avec langage de programmation associé ;*
- *un logiciel de gestion de versions et de suivi de problèmes d'ordre logiciel ;*
- *une solution permettant de tester les comportements anormaux d'une application.*

Les activités de l'organisation cliente s'appuient sur aux moins deux solutions applicatives opérationnelles permettant d'offrir un accès sécurisé à des données hébergées sur un site distant. Au sein des architectures de ces solutions applicatives doivent figurer l'exploitation de mécanismes d'appel à des services applicatifs distants et au moins trois des situations ci-dessous :

- *du code exécuté sur le système d'exploitation d'une solution technique d'accès fixe (type client lourd) ;*
- *du code exécuté dans un navigateur Web (type client léger ou riche) ;*
- *du code exécuté sur le système d'exploitation d'une solution technique d'accès mobile ;*
- *du code exécuté sur le système d'exploitation d'un serveur.*

Une solution applicative peut être issue d'un développement spécifique ou de la modification du code d'un logiciel notamment open source.

Les solutions applicatives présentes dans le contexte sont opérationnelles et leur code source est accessible dans un environnement de développement opérationnel au moment de l'épreuve.

Accès à internet

Les étudiants en STS SIO devront bénéficier d'un accès internet sans filtrage sur les protocoles ni sur les ports. Cet accès internet devra permettre à la fois, depuis les postes informatiques de la section (et au moins depuis les laboratoires), de bénéficier de l'ensemble de la gamme des services qu'on peut trouver sur internet (téléchargements, mises à jour de systèmes, accès sécurisé à des réseaux distants...) et également de pouvoir, dans le cadre d'activités de mise en place de services, se connecter au réseau de la section de BTS SIO depuis l'extérieur de l'établissement.

Les établissements qui disposent d'un accès restreint à internet, du fait de la présence de plateformes de filtrage dans les académies, devront être équipés d'une ligne numérique indépendante à usage restreint aux activités ne pouvant pas être mises en place avec un accès filtré.

Il est recommandé de disposer d'un deuxième accès internet, éventuellement de moindre débit, pour la mise en œuvre de prototypes d'architectures réseau mettant en œuvre par exemple des connexions VPN ou d'autres liaisons inter-sites.

Pour rappel, l'épreuve pratique nécessite la mise en place d'un contexte d'examen complexe.

Équipements matériels

1. Ferme de serveurs

a) Caractéristiques pédagogiques de la ferme de serveurs

La ferme de serveurs peut être en partie virtualisée dans le cloud, les caractéristiques techniques indiquées dans ce guide peuvent servir au chiffrage de cette solution.
La ferme de serveurs peut héberger différentes sortes de machines virtuelles :

- Des machines virtuelles installées par les enseignants pour répondre à différents scénarios de formation et simuler des contextes : serveurs de base de données, serveurs de déploiement, serveurs FTP, etc.
- Des machines virtuelles mises à disposition des étudiants, mais sur lesquelles ils peuvent intervenir, en administration ou en utilisation, individuellement ou par binôme/groupe
- Des machines virtuelles installées par les étudiants pour un apprentissage précis (par exemple : mise en place d'un serveur de *ticketing*, mise en place d'un *cluster* de serveurs avec répartition de charges, etc.)
- Des machines virtuelles installées par les étudiants pour construire leur contexte d'examen, généralement en binôme ou en groupe.
- Les machines virtuelles nécessaires à la gestion de la ferme de serveurs : *machine hébergeant l'outil d'administration centralisé*, serveur d'annuaire, machine de sauvegarde, etc.

Les étudiants doivent pouvoir administrer les machines virtuelles qui les concernent sans perturber le fonctionnement des autres machines et le travail des autres utilisateurs de la ferme.

La ferme de serveurs a un cycle d'utilisation annuel : mise en place des autorisations, préparation des contextes, passage des épreuves, suppression des éléments obsolètes.

Les enseignants doivent pouvoir exploiter et administrer la ferme de serveurs en ayant la possibilité de :

- créer des dossiers individuels par étudiant ou par groupe de travail afin de séparer leurs machines virtuelles ;
- créer des réseaux virtuels pour isoler les flux des étudiants ou des groupes de travail ;
- mettre à disposition des étudiants des machines virtuelles ou des modèles à déployer.

b) Caractéristiques techniques de la ferme de serveurs

La base commune peut s'articuler autour de 3 serveurs partageant une baie de disques en système RAID, rackés dans une armoire 42U.

Une solution présentant le meilleur rapport performances/prix serait élaborée à partir de serveurs en double attachement direct sur une baie SAN. Les éléments techniques attendus pour une solution de ce type sont indiqués ci-dessous. D'autres solutions peuvent répondre aux besoins mais seront probablement plus onéreuses.

Caractéristiques techniques des serveurs

- Type HP DL380 G10 ou DELL PowerEdge R630 ou R740 (ou au moins équivalent)
- Serveur rackable, 2 sockets minimum, au total 16 cœurs minimum
- Processeur Intel Xeon 2.Ghz minimum (supportant VTX et VTD et l'hyperthreading)
- Taille RAM : 192 Go de mémoire / serveur, extensible jusqu'à 512 Go
- Stockage interne pour installation de l'hyperviseur, éventuellement module pour carte mémoire flash
- Carte contrôleur E/S compatible avec la baie de disques en double attachement
- 8 ports Gigabits
- Double alimentation hot plug

En fonction de la structure du BTS SIO dans l'établissement (nombre de sections, effectifs de 24 ou 32 étudiants), des options supérieures peuvent être envisagées :

- Passage à 256 Go, passage à 512 Go par serveur
- Passage à des processeurs 10 cœurs minimum
- Disques pour stockage interne sur les serveurs - 2 To par serveur
- Modules cartes réseaux Gigabits supplémentaires : 4 ports Gigabits ou 2 ports 10 Gigabits

Caractéristiques techniques de la baie de stockage

- Baie de stockage SAS double contrôleur RAID
- Capacité : 20 To minimum, extensible jusqu'à 40 To
- Disques 10 000 t/min minimum
- Double carte réseau GigabitsEthernet
- Double alimentation
- Option possible : cache SSD ou Auto-tiering pour de meilleures performances.

Équipements connexes à la ferme

- 2 commutateurs de niveau 3 - 48 ports Gbits redondants avec agrégat inter-équipements (stackés)
- NAS rackable pour sauvegardes et ISO - Capacité utile (RAID 5) : 12 To minimum, 2 cartes réseaux GigabitsEthernet minimum (agrégation)
- Onduleurs permettant un fonctionnement de 15 minutes minimum - Nombre nécessaire pour supporter l'ensemble des équipements, 2 pour la redondance des alimentations si l'environnement le permet.
    - Avec carte de management et logiciel de management si nécessaire.
- Câbles nécessaires à l'installation : câbles réseau, câbles SAS, connectique diverse.
- Armoire 42 U
- Console KVM 4 serveurs minimum
- Commutateur 10 gigabits 24 ports (niveau 2).

2. Équipements des salles

a) Salle de cours

Lors des séances en classe entière d'enseignement professionnel, les étudiants doivent pouvoir accéder en tant que de besoin à un environnement informatique, éventuellement par la mise en place d'un accès wifi.

Les séances en division entière nécessitent de disposer d'une salle de cours dotée d'un poste "professeur" équipé d'un accès à internet, d'un dispositif de visualisation collective. Ce poste est équipé de l'ensemble des logiciels requis par la (ou les) parcours proposé(s) par l'établissement et d'un accès Internet et au réseau de la section.

Les séances en demi-division dans le cadre des enseignements généraux nécessitent de disposer d'un espace de travail sur table favorisant le travail de groupe. Les étudiants doivent pouvoir accéder en tant que de besoin à un environnement informatique adapté.

b) Laboratoires informatiques

Les activités menées par les étudiants dans le cadre des blocs, nécessitent une composition de salle spécifique :

- L'option SISR et les blocs orientés systèmes et réseau, nécessitent la mise en place de configurations réseaux expérimentales potentiellement complexes au travers d'éléments d'interconnexion paramétrés par les étudiants. Ces activités nécessitent de disposer d'un laboratoire à la configuration adaptée, doté d'équipements dont les caractéristiques sont données ci-dessous.

- L'option SLAM et les blocs orientés développement d'applications, nécessitent la mise en place d'un laboratoire de services applicatifs, dont les postes sont dotés des applications requises et d'écrans de taille adaptée aux activités de développement d'application sur des environnements professionnels comme indiqué ci-dessous.

La présence d'équipements actifs redondants en réserve (en mode "*spare*") est une façon de garantir l'accès pour tous les étudiants à des matériels en état de fonctionnement, en apprentissage comme à l'examen.

Poste de travail :

Il est nécessaire de disposer de stations de travail suffisamment puissantes, capables de supporter plusieurs environnements virtualisés et donc dotées de capacités importantes.
Tous les appareils, notamment les appareils mobiles, doivent pouvoir se connecter à des ressources en ligne via une liaison filaire ou sans fil, telle qu'une liaison Wifi ou encore une liaison via un réseau de téléphonie sans fil type "4G".

- **Unité centrale**
  - Processeur quad-core ou équivalent (type Intel I7) avec instructions de virtualisation (type Intel-VT ou équivalent)
  - Carte graphique compatible DirectX11 (permettant de travailler avec le framework Unity3D par exemple) avec soit :
    - deux sorties vidéo permettant de faire du bureau étendu
    - une sortie vidéo connectée à un écran ultra large de 29" minimum
  - 16 Go RAM (2 x 8 Go) avec deux emplacements libres de manière à pouvoir accroitre la mémoire vive en cas de besoin à 32 Go minimum.
  - 4 connecteurs USB minimum, prise casque et micro en façade
  - Disque dur 3 pouces 1/2 en SATA 3 d'une taille de 1 To minimum en SSD de préférence
  - Carte réseau Gbits avec PXE gérant le 802.1Q et la création de sous-interfaces
  - Châssis type moyen tour
  - Port série RS 232 pour l'administration d'actifs réseau (à défaut un câble adaptateur USB/Série si non-inclus dans l'unité centrale)
- **Écran(s)**
  - Format selon le nombre de sorties vidéo choisi
  - Résolution FULL HD (1920x1080) ou UWHD (2560x1080)
- **Périphériques**
  - Souris
  - Clavier

Salle “labo” pour une section SISR :

- Un poste de travail, fixe ou portable, par étudiant et un pour l’enseignant
- Armoire(s) de brassage 15U (1 armoire pour 4 étudiants)
- Un commutateur de niveau 2 administrable (type CISCO 2960 Series plus, équivalents HP, DELL...) par étudiant
- Un routeur (type Cisco 1941 avec carte série) pour 2 étudiants.
- Un téléphone IP (avec le protocole SIP) pour 2 étudiants.
- Une borne WIFI (type Cisco Aironet) pour 2 étudiants.
- Un commutateur de niveau 3 (éventuellement avec PoE pour des matériels compatibles) pour 2 étudiants.
- Un casque avec micro par étudiant.
- Une carte réseau supplémentaire par poste.
- Câbles de différentes couleurs pour matérialiser les vlan/flux/groupe, de 1, 2 et 5 m de catégorie 6 avec protection ergot (20 câbles par armoire).
- Un testeur de câble.
- Un câble console par étudiant.
- 5 prises RJ45 pour 2 étudiants (reliées aux armoires de brassage, elles-mêmes reliées au réseau pédagogique du BTS SIO).
- Une solution de pare-feu pour 2 étudiants, matérielle de préférence (type Stormshield SN210, Cisco ASA...).
- Une imprimante.

Salle “labo” pour la section SLAM :

- Un poste de travail par étudiant et un pour l’enseignant
- Une tablette type Android pour deux étudiants, pour le développement mobile. Cette tablette peut également servir aux SISR dans le cadre de l’administration d’un parc de tablettes.
- Une imprimante.

Abonnement à un service de *Cloud computing* public

L’exploitation d’une infrastructure réseau et de développement accessible dans un *cloud* public est recommandée en section de BTS SIO pour deux raisons principales :

- D’une part, dans le but de former les étudiants à cette technologie de plus en plus fréquemment présente dans les entreprises aujourd’hui : fourniture à la demande et paiement à l’usage de ressources de type puissance de calcul, réseau, stockage, bases de données, etc. À la date de production de ce document, le coût estimé par professeur et étudiant est de 100 euros.

- D’autre part, pouvoir disposer rapidement, dynamiquement en fonction des besoins, de ressources matérielles et logicielles nouvelles sans avoir à disposer localement de serveurs physiques ou virtualisés supplémentaires. À la date de production de ce document, le coût estimé par professeur et étudiant est de 200 euros.

Dans tous les cas, l’établissement de formation, doit disposer d’un abonnement à un service de *cloud computing* public de façon à être en capacité de former les apprenants à l'exploitation de cette technologie. Cet abonnement doit permettre un usage dans un contexte pédagogique de classe en fédérant les comptes des étudiants dans une vue professeur.

Les offres de plateformes d’infrastructures en *cloud computing* publiques étant proposées par abonnement, il est nécessaire que cet abonnement permette de compléter autant que nécessaire, et en fonction des besoins, les équipements requis dans ce guide d'équipement qui ne seraient pas physiquement disponibles localement dans l’établissement de formation.

Maintenance des équipements

Les équipements dédiés à la section de BTS SIO doivent faire l'objet d'une maintenance spécifique de façon à s'assurer de la disponibilité et de la qualité des moyens mis à la disposition des apprenants. Cette maintenance peut être assurée dans le cadre d'un contrat global d'établissement, d'un contrat spécifique ou / et par une mission particulière confiée à tout ou partie des enseignants de la section.

Équipements logiciels, abonnements et licences

1. Logiciels communs

Enseignement commun :

- OS station : Microsoft Windows, Linux, Android (versions courantes)
- Suite logicielle de bureautique : LibreOffice (avec extension Grammalecte), Microsoft Office, Google docs...
- Suite de sécurité pour poste de travail : Windows Defender
- Solution de sauvegarde pour poste de travail : backupPC, ComodoBackup
- Outil de représentation graphique de schémas techniques : Microsoft Visio, Dia, LibreOffice Draw mais aussi UML (UMLet, etc.)
- Logiciel d'analyse des échanges de données de protocole : Wireshark
- Simulateur réseau : Cisco Packet Tracer, NetEmul, GNS3, SopiremInfo,
- Environnement(s) de développement d'applications : Visual Studio (version courante) et/ou autres (Netbeans, IntelliJ IDEA …)
- Environnement de programmation spécifique aux mathématiques pour l'informatique : Environnement de développement Python (edupython https://edupython.tuxfamily.org)
- Ensemble de logiciels de gestion de contenus Web : Xampp (windows), Lamp (Linux), uWamp, EasyPHP, laragon
- Socle ou cadre d'application (*framework*) : BootStrap (version courante)
- Système de gestion de base de données : PostgreSQL, Mysql (MariaDB)
- Système de gestion de contenu : Drupal, Wordpress
- Une solution de virtualisation locale de systèmes : Vmware WorkStation, virtualBox
- Logiciel de gestion d'incidents : GLPI
- Logiciel de gestion des configurations : OCS Inventory, Fusion Inventory
- Logiciel permettant le déploiement des solutions techniques d'accès : FOG, CloneZilla
- Logiciel de gestion de projet/planning : GanttProject, Project Libre, Microsoft Project, Tuleap
- Outil de lecture de documents sonores et vidéo : VLC
- Éditeur de texte : Notepad++, sublime text

Ferme de serveurs :

- Serveurs de virtualisation : Proxmox, Vmware, HyperV, …
- Serveurs de stockage : NAS, SAN
- Service d'authentification : OpenLdap, Active Directory
- SGBD : PostgreSQL, MySql, Oracle
- Accès sécurisé à Internet : Proxy + Pare-feu
- Environnement de travail collaboratif : ENT région + Partages Windows et Samba sur Linux
- Solution de sauvegarde : backupPC, ComodoBackup, Bacula, Veam pour les machines virtuelles...
- Solution permettant l'administration à distance sécurisée de serveurs : SSH, Bureau à distance, Putty
- Logiciel de gestion d'incidents : GLPI
- Logiciel de gestion des configurations : OCS Inventory, Fusion Inventory
- Machines virtuelles dédiées aux étudiants

2. Logiciels spécifiques SLAM

- Logiciel de représentation de schémas de données : PowerAMC, WinDesign
- Environnement(s) de développement d'applications : suite JetBrains (IntelliJ, PHPStorm, ... accessibles gratuitement dans le cadre de l'offre éducation de JetBrains), Visual Studio, Netbeans, Visual Studio Code, Android Studio, Eclipse ...
- Socle ou cadre d'application (framework) : Symfony, Laravel, Angular, JQuery, BootStrap (versions courantes) ...
- Système de gestion de base de données : Mysql (MariaDB), PostgreSQL (incluant pgAdmin), Oracle (partie cliente et serveur) (versions courantes), MongoDB, Redis, Neo4j, Cassandra ...
- Logiciel de mapping objet relationnel (ORM) : Entity Framework Microsoft, Hibernate, Doctrine 2 ….
- Logiciel de gestion de version et de suivi de développement :
    - accessibles en ligne ("SAAS") : Tuleap-Campus, Framagit, github, gitlab, trello, bitbucket…
    - à installer (*on premise*) : Redmine, Tuleap, gitlab
- Outils de gestion de projet en mode agile : Jira, Slack
- Un outil de génération et de rétro-conception de bases de données : Power Designer, WinDesign

3. Logiciels spécifiques SISR

- Logiciels d'administration à distance sécurisée de serveurs
- Logiciel de supervision système et réseau : Shinken + Nagvis, Nagios, Zabbix, PRTG, (protocole SNMP), Cacti
- Logiciel rendant un service à l'utilisateur final respectant un contrat de service: Téléphonie IP (Xivo) avec QoS
- Solution d'accès sécurisé au réseau : support de 802.1X, WPA2 (Wifi)
- Logiciel de tolérance de pannes serveur : VMware vSphere vMotion, cluster Proxmox
- Logiciel de répartition de charges : HaProxy, Traefik

- Licences/abonnements :
    - Vmware,
    - Microsoft Azure Dev Tools for teaching,
    - PowerDesigner, WinDesign.