CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Guide pédagogique pour l'intégration de la cybersécurité dans les formations en informatique

Ce document a été rédigé par un consortium regroupant des enseignants-chercheurs et des professionnels du secteur de la cybersécurité.

Table des matières

Introduction

Le Livre blanc sur la défense et la sécurité nationale publié en 2013 indique que « *la sécurité informatique doit être intégrée à l'ensemble des formations supérieures en informatique* », afin de sensibiliser l'ensemble des acteurs aux enjeux de la cybersécurité. Cette démarche CyberEdu, dans laquelle s'inscrit ce guide pédagogique, s'adresse à l'ensemble des métiers de l'informatique, et pas uniquement aux experts de la cybersécurité.

Ce guide pédagogique a pour principal objet l'accompagnement des responsables de formations en informatique non spécialisées en cybersécurité, dans la définition des enjeux, l'identification des thématiques pertinentes et l'élaboration d'une stratégie de prise en compte de ces thématiques dans les formations dont ils ont la charge. Il peut également être utilisé par les enseignants en informatique qui souhaitent intégrer des éléments de cybersécurite dans leurs cours.

Il est structuré en quatre parties auxquelles s'ajoutent quelques références. La première partie présente les enjeux de la cybersécurité. La deuxième est consacrée à la présentation des thématiques retenues pour l'enseignement de la cybersécurité. La troisième partie fournit des orientations pour l'enseignement de la cybersécurité. La quatrième partie traite de dispositifs visant à assurer la qualité des enseignements mis en œuvre à partir des éléments pédagogiques fournis dans le cadre de CyberEdu.

1. Enjeux de la cybersécurité

1.1. Un enjeu économique national

La cybersécurité a été élevée au rang de priorité nationale par le Livre blanc de la défense et la sécurité nationale de 2008, puis dans le Livre blanc de la défense et la sécurité nationale de 2013. Elle constitue un enjeu économique important, notamment au niveau de l'industrie. Conscient de ce fait, le ministère du redressement productif a intégré un plan pour la cybersécurité, dans ses 34 plans pour établir la Nouvelle France Industrielle réunis dans la Solution pour la Confiance Numérique en mai 2015. Pour les entreprises, l'enjeu se traduit par les coûts des différentes attaques informatiques qu'elles subissent. Ponemon Institute, dans une étude sur un panel de 27 entreprises représentatives, a ainsi estimé que ce coût était de 3,89 millions d'euros en moyenne par an, avec 26 attaques réussies par semaine sur l'ensemble des 27 entreprises. En novembre 2013, le cabinet EY mentionnait que la cybersécurité restait la préoccupation première des DSI dans les grandes entreprises. En parallèle, une étude de Kaspersky estime que, en moyenne, renforcer le recrutement dans le domaine de la sécurité coûterait 9 000 € pour une PME et 57 000 € pour une grande entreprise. Le patrimoine informationnel d'une entreprise est un bien essentiel qui se doit d'être protégé efficacement.

1.2. Un enjeu stratégique international

Certaines cyberattaques visent des organisations ou des manifestations internationales. Par exemple, durant la cérémonie d'ouverture des Jeux Olympiques de Londres en 2012, pas moins de 22 types d'attaques différentes ont été dénombrées. Seule une stratégie internationale de cybersécurité peut permettre de lutter efficacement contre la cybercriminalité.

1.3. Un enjeu géopolitique

La cybersécurité est un enjeu crucial pour les états. L'espace numérique est devenu un lieu d'affrontement géopolitique : espionnage du patrimoine scientifique, économique et commercial par des concurrents ou des puissances étrangères, compromission d'informations de souveraineté, etc.

2. Présentation des thématiques

Cette section propose des éléments de programme de formation sous la forme de thématiques cybersécurité pouvant être intégrées à des formations supérieures en informatique.

Elle préconise tout d'abord une sensibilisation et une initiation à la cybersécurité sous la forme d'un module dédié de niveau licence 3 ou équivalent (3è année après le baccalauréat, par exemple 1re année en école d'ingénieur), reposant sur quelques prérequis fondamentaux en informatique : architecture matérielle, système d'exploitation, réseaux, développement.

Ce module se veut générique et n'aborde que les notions intéressant tous les professionnels de l'informatique, notamment celles relevant de l'hygiène informatique.

Pour différents grands métiers de l'informatique, cette section propose également des thématiques plus spécifiques pouvant être intégrées à des modules préexistants de spécialisation, le plus souvent de niveau master (4è et 5è années après le baccalauréat).

Les thématiques de cybersécurité mentionnées dans cette section sont énumérées en annexe B.

Chaque thématique sera abordée à travers différentes unités d'enseignements ayant chacune une granularité suffisamment fine pour faciliter l'intégration dans un (ou des) enseignement(s) informatique(s) existant(s), tout en constituant un ensemble cohérent. À chaque UE sera associée une fiche d'enseignements de cybersécurité en lien avec la thématique abordée. Un numéro sera attribué à chaque fiche pour faciliter la structuration de la présentation.

Pour chaque thématique de cybersécurité, seront précisés :

- Le volume horaire global et éventuellement les possibilités de modulations horaires permettant d'aborder par exemple uniquement les aspects fondamentaux, puis un sous-ensemble un peu plus riche, jusqu'à la totalité de la thématique. Il est souhaitable que cette modulation permette de décliner les 3 niveaux (sensibilisé, formé et expert) du tableau de thématiques par métier disponible en annexe A.
- Les prérequis. Il s'agit de préciser les notions supposées acquises qui sont utilisées dans la formation proposée.
- Les objectifs pédagogiques.
- La description des UE qui la constituent, par exemple sous forme de liste comme suit :
    - » UE 1 : Intitulé de l'UE.

» UE 2 : Intitulé de l'UE.

Le tableau de synthèse précisant pour chaque UE, une synthèse des objectifs pédagogiques, le volume horaire global et les modulations horaires possibles permettant d'aborder par exemple uniquement les notions fondamentales, ou un sous-ensemble cohérent un peu plus riche.

Les fiches de présentation des unités d'enseignements (UE) comportent les éléments constitutifs suivants :

- Intitulé
- Thématique(s) informatique(s) à laquelle est associée l'unité d'enseignement (par exemple les réseaux).
- Numéro de la fiche
- Volume horaire
- Prérequis
- Corequis
- Objectifs pédagogiques
- Plan détaillé
- Conseils pratiques
- Références bibliographiques

Le tableau ci-après donne le modèle suivant lequel sont bâties les fiches pédagogiques.

CyberEdu

Guide pédagogique CyberEdu

Intitulé de l'UE

Thématique	*Numéro de fiche*	*Dernière mise à jour* JJ/MM/AAAA

Volume horaire	Préciser le volume horaire global et éventuellement la nature des enseignements (cours, travaux dirigés, travaux pratiques, projets). Dans la mesure du possible, et si cela se justifie, indiquer une organisation en volumes horaires incrémentaux permettant à l'enseignant, en fonction de ses objectifs, de n'aborder qu'un sous ensemble minimal de la formation (uniquement les notions fondamentales correspondant au niveau « sensibilisé »), puis s'il le souhaite un sous-ensemble cohérent un peu plus riche (niveau « formé »), jusqu'à la totalité de la formation (niveau « expert »).
Prérequis	Préciser les notions supposées acquises qui sont utilisées dans l'UE proposée
Corequis	Préciser succinctement les notions qu'il est nécessaire d'aborder parallèlement, si ces dernières ne sont pas intégrées dans l'UE décrite dans la fiche.
Objectifs	Il s'agit ici de préciser l'objectif pédagogique de l'UE
Plan	Préciser les notions abordées sous forme de plan ; si possible, préciser la durée associée à chaque partie
Conseils pratiques	Fournir les conseils pédagogiques et les détails permettant la bonne mise en œuvre de l'UE.
Matériel didactique et références bibliographiques	Préciser les matériels didactiques s'il y en a. Indiquer les références bibliographiques jugées utiles.

Les conseils pratiques mentionnés dans la fiche UE ont pour but d'aider à la mise en œuvre de la formation par des enseignants non spécialistes de la cybersécurité. Ils pourront, suivant leur taille, faire l'objet d'une fiche d'accompagnement pédagogique séparée, référencée dans la fiche UE.

2.1. Sensibilisation et initiation à la cybersécurité (niveau Licence 3)

Il est important de faire un panorama sur plusieurs facettes de la cybersécurité afin d'informer et éventuellement susciter des vocations. Ce module doit :

- Introduire les notions de base de la cybersécurité : sécurité des systèmes d'informations (SSI), cybersécurité, cyberdéfense, cyberespace, notions de vulnérabilité, de menace, d'attaque, de risque ;
- Présenter les enjeux liés à la cybersécurité pour l'État, les entreprises, les particuliers, ainsi que les enjeux sur le plan international ;

- Aborder, d'un point de vue pratique, les aspects légaux de la cybersécurité : textes de loi relatifs à la SSI, informatique et vie privée, valeur juridique du courrier électronique, notion de charte de sécurité, droits d'auteur et propriété intellectuelle, opérateurs d'importance vitale ;
- Présenter les règles d'hygiène informatique : connaître le système d'information et ses utilisateurs, mettre à jour des logiciels, authentifier les utilisateurs, sécurisation du réseau et des équipements terminaux, surveillance des systèmes, sécurité physique, organisation de la réaction en cas d'incident, audit de sécurité ;
- Donner des informations et des pointeurs sur les organismes de sécurité des systèmes d'information tels que l'ANSSI ;
- Préciser les principaux freins à la cybersécurité ;
- Aborder succinctement les normes de sécurité.

2.2. Thématiques cybersécurité pour les spécialisations (niveau Master)

Les différents métiers de l'informatique reposent sur un ensemble de thèmes fondamentaux : systèmes d'exploitation, réseaux, développement logiciel… Cette sous-section propose les aménagements pour la cybersécurité relatifs à ces volets d'enseignements, étant donné qu'une formation d'informaticien consistera, pour le volet informatique, en un ensemble de modules parmi ces derniers. Le tableau disponible en annexe A donne les thématiques à aborder pour chacun des métiers identifié comme métier de référence du domaine de l'informatique. Des informations sur les métiers de référence et sur la démarche adoptée pour leur élaboration sont disponibles en annexe C.

2.2.1. Systèmes d'exploitation

Le guide « sécurité des systèmes d'exploitation » contient des fiches pédagogiques à destination des enseignants du supérieur qui donnent des cours « systèmes d'exploitation ». Ces fiches pédagogiques ont pour objectif de permettre aux enseignants de tisser les notions de sécurité qu'elles abordent dans des cours déjà construits, et de prévoir leur intégration dans ceux qui vont l'être. L'enseignant pourra par exemple consacrer une quinzaine de minutes à la sécurité à la fin de chaque chapitre de son cours. Les fiches pédagogiques apporteront des repères pédagogiques aux enseignants. Elles présentent de manière structurée et concise les principaux sujets qui ont trait à la sécurité des systèmes d'exploitation. Les fiches comprennent différents points qui, selon la structure du cours préexistant et selon l'intérêt que leur porteront les enseignants, pourront être présentés dans leur totalité ou en partie, dans l'ordre approprié à l'enseignement et au public visés.

Des annexes, certaines conseillées, d'autres optionnelles, viendront prolonger les réflexions techniques qui sont illustrées par les fiches. Certaines d'entre-elles apporteront aux enseignants des illustrations techniques concernant certaines failles de sécurité des systèmes d'exploitation.

Les fiches incluent également des références à des livres, des fiches techniques proposées par l'ANSSI ou à des présentations de référence qui ont été faites lors de conférences.

Ces fiches et leurs annexes ne constituent cependant pas un cours complet sur la sécurité des systèmes d'exploitation. Elles ne sont qu'un support d'apprentissage pour l'enseignant. Leur ambition n'est pas que le professeur ou ses élèves maîtrisent ces différents domaines de la sécurité, mais que ceux-ci soient sensibilisés et aient envie d'approfondir un domaine devenu essentiel à l'utilisation des technologies informatiques liées au domaine des systèmes d'exploitation. Un approfondissement individuel des sujets abordés permettra à chacun d'exploiter pleinement les différentes techniques décrites dans ces fiches pédagogiques. Pour ce faire, un site Internet doit voir le jour (www.cyberedu.fr). Il permettra aux enseignants d'accéder, tant à une base documentaire régulièrement mise à jour, qu'à de nombreuses illustrations des problèmes de sécurité liés à l'actualité, d'échanger avec d'autres collègues sur la mise en place de ces notions de sécurité au sein de leurs cours.

2.2.2. Réseau

Le guide pédagogique sur la sécurité des réseaux contient des fiches pédagogiques à destination des enseignants en réseaux informatiques dans l'enseignement supérieur. Les fiches ont pour objectif de permettre aux enseignants d'illustrer leur cours de réseaux avec des notions de sécurité. Typiquement, l'enseignant consacrera une quinzaine de minutes à la sécurité à la fin de chacun de ses chapitres. Les fiches pédagogiques apportent des repères pédagogiques aux enseignants, en présentant de manière structurée et concise les sujets importants de la sécurité des réseaux qui peuvent être présentés à des étudiants durant un cours de base en réseaux informatiques. Les fiches peuvent être présentées en tout ou partie, dans l'ordre approprié à l'enseignement et aux étudiants visés.

Les fiches ne constituent toutefois pas un cours complet sur la sécurité des réseaux et ne peuvent constituer à elles seules un support d'apprentissage pour l'enseignant. Il n'est pas demandé à l'enseignant de parfaitement maîtriser le domaine de la sécurité, mais il devra se renseigner sur les sujets présentés pour pleinement exploiter les fiches pédagogiques. Pour cela, des liens vers des documents en français ou en anglais sont fournis. Les fiches incluent également des références vers des livres, articles et sites web permettant d'approfondir les sujets abordés.

2.2.3. Développement logiciel

Le guide pédagogique « Sécurité du logiciel » sera constitué d'un ensemble de fiches pédagogiques destinées aux enseignants en compilation et en programmation. Il abordera les aspects relatifs aux vulnérabilités logicielles basiques, en faisant notamment un tour d'horizon des attaques les

plus usuelles et en mettant en évidence le contexte, en termes de langage de programmation ou d'environnement d'exécution, qui les rend possible.

La sécurité intrinsèque des différents langages de programmation sera également abordée. En effet les protections et vulnérabilités des logiciels sont fortement liées au langage de programmation utilisé. Ce guide traitera également des pratiques et méthodologies pour le développement sécurisé (protection de l'environnement de développement, prise en compte de la sécurité dans la gestion de projet, outils de conception ou de génération de code avec possibilité de paramétrages liés à la sécurité). La sécurité se doit en effet d'être prise en compte dès les phases de conception des logiciels. Les techniques et outils d'analyse de vulnérabilité seront également abordés (bases de l'analyse statique de programmes, techniques de test en boîte noire…).

3. Enseigner la cybersécurité

Cette section propose quelques orientations pour l'enseignement de la cybersécurité, sous forme de principes et d'objectifs applicables.

3.1. Sensibiliser aux risques

Cette sensibilisation peut consister à rappeler à l'étudiant les risques auxquels sont exposés les systèmes d'information, leur réalité (une simple revue de presse peut suffire, mais d'autres approches, par exemple au travers de démonstrations, sont également possibles), et les enjeux associés pour lui, son entreprise ou la société.

Il est important d'attirer l'attention de l'étudiant sur le fait qu'en tant que futur professionnel, voire en tant que simple utilisateur, il aura une influence sur le niveau de sécurité des systèmes d'information.

3.2. Inciter à une culture générale et à la veille dans le domaine

L'attaquant malveillant cherchera très souvent le maillon faible du système et adaptera ses techniques d'attaques en conséquence. Il est donc nécessaire, d'une part, d'avoir une culture permettant de comprendre cette démarche, et, d'autre part, de se tenir informé des nouveautés fussent-elles des attaques, des moyens d'attaques (virus, logiciels malveillants…) ou des solutions visant à s'en prémunir (par exemple les logiciels anti-virus).

Les étudiants doivent également être sensibilisés à l'aspect multidisciplinaire de la cybersécurité, dont la mise en œuvre complète fait appel tant à des formalismes informatiques, que mathématiques, électroniques et juridiques.

3.3. Intégrer la cybersécurité dans les modules d'enseignements existants

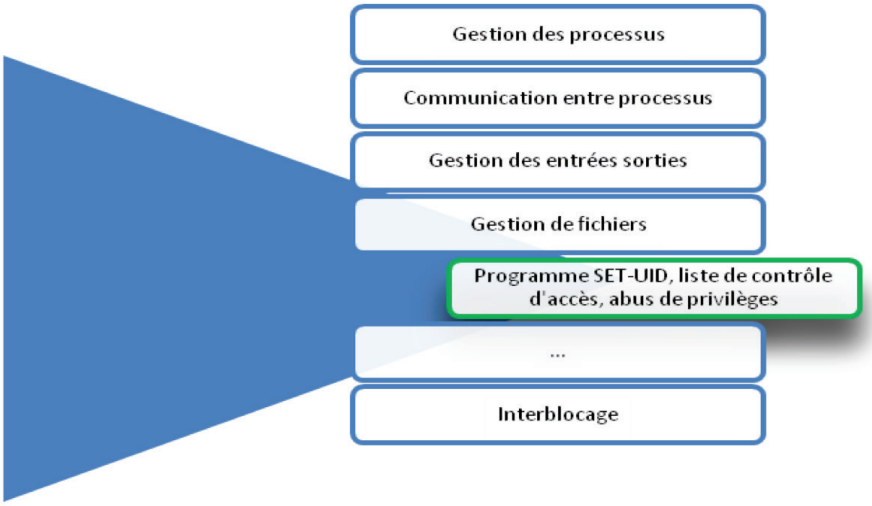
L'intégration de la cybersécurité pourra se faire par tissage de mini modules autonomes, par ajout d'un module de cybersécurité autonome et complet à un cours d'informatique, ou bien encore un apprentissage par la pratique (« learning by doing »). L'idée est de ne pas perturber l'existant dans les cursus classiques ne traitant pas ou peu de la sécurité. L'exemple suivant illustre cette démarche dans le cas d'un enseignement « Cybersécurité et systèmes d'exploitation » :

3.3.1. Un tissage de mini-modules autonomes

Il s'agira ici d'insérer les mini-modules dans le cours classique, à la fin de chaque partie bien identifiée du cours présentant des risques de sécurité connus et/ou nécessitant une protection contre les malveillances. Il est nécessaire pour ce type de cours, non destinés forcément à une

spécialisation dans le domaine de la sécurité, de présenter des risques pour lesquels l'enseignant peut également présenter les moyens de les gérer.

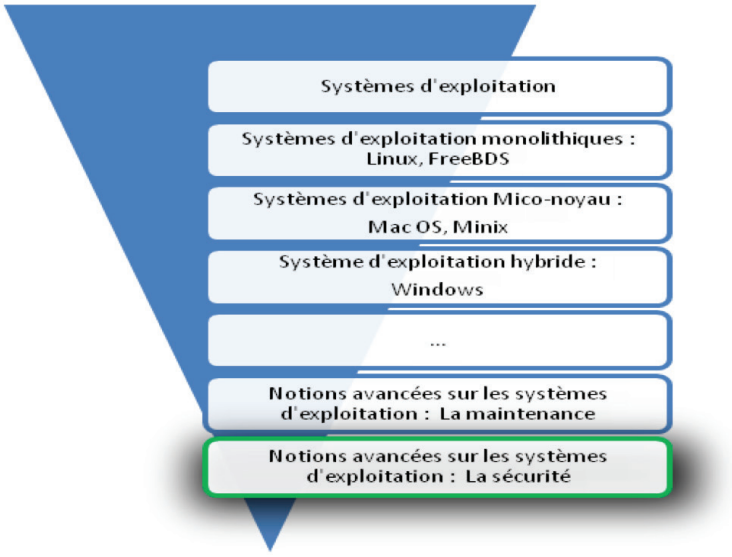
L'avantage c'est que cette approche ne perturbe pas le cursus classique et n'entraîne pas de modification de la partie du cours concernée, mais permet de sensibiliser, d'intéresser, et de susciter des vocations voire de mieux assimiler la partie concernée du cours. En prenant par exemple un module sur les fichiers dans un cours « système d'exploitation », le format pourrait être le suivant :



3.3.2. Ajout d'un module autonome complet

Il s'agit d'ajouter un module autonome complet en fin d'un cours classique sur les systèmes d'exploitation, une fois que tous les éléments importants ont été présentés et assimilés au travers de cours et/ou de travaux pratiques ou dirigés. Il pourrait être classé parmi les cours « Notions avancées sur les systèmes d'exploitation ».

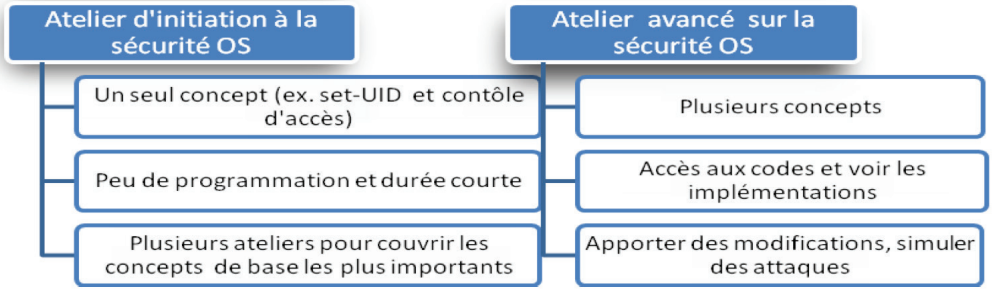
Selon le volume horaire prévu dans le cursus classique pour le cours systèmes d'exploitation, ce module peut prendre la forme d'un cours magistral intégrant des exercices d'application, un travail dirigé ou un didacticiel. L'organisation d'un cours système pourrait être modifiée de la manière suivante :



3.3.3. Apprendre par la pratique « Learning by doing »

Il s'agit d'ici d'appliquer une forme de pédagogie active et reprendre une des deux approches précédents sous un format atelier.

Les étudiants reçoivent des pointeurs sur la sécurité dans les systèmes d'exploitation (pas de cours en classe), avec une indication sur le volume horaire qu'ils doivent y consacrer. Ils assistent ensuite aux ateliers sécurité des systèmes d'exploitation pour la partie pratique et peuvent avoir des réponses sur des aspects non compris ou nécessitant des précisions. Par exemple, un atelier Set-UID pourrait permettre de manipuler ce mécanisme de sécurité et de comprendre pourquoi il est nécessaire et comprendre comment il est mis en œuvre.



De ces 3 approches, l'approche par tissage de mini-modules autonomes est celle à privilégier, compte tenu de la souplesse qu'elle offre pour une intégration progressive, ciblée et optimisée des concepts de cybersécurité dans les enseignements existants.

3.4. Combiner théorie et pratique

Autant que possible, les enseignements de cybersécurité doivent associer une partie pratique aux enseignements théoriques. Ce couplage est indispensable pour permettre aux étudiants de mieux assimiler les concepts abordés et d'être opérationnels. Un appui sur des exemples concrets permettant d'illustrer les problèmes de sécurité et la manière de s'en prémunir est souhaitable pour les différents aspects abordés dans les cours.

3.5. Initier aux principes d'attaques pour mieux défendre

Il est important d'aborder les principes d'attaques. En effet, la compréhension des modes d'attaques permet de mieux préparer la défense contre ces dernières, qu'il s'agisse d'une démarche de défense préventive (intégration de mécanismes a priori pour empêcher les attaques d'atteindre le système) ou réactive (réaction à une attaque ayant atteint le système). Il est toutefois nécessaire d'adapter les types d'attaques considérés aux objectifs de la formation, en prenant en compte les spécificités liées au contexte (Défense ou environnement civil, aspects juridiques...) et en expliquant les contre-mesures existantes.

3.6. L'évaluation des connaissances/compétences acquises

Dans le cas d'un ajout de module indépendant de cybersécurité, l'évaluation du savoir peut être effectuée selon le schéma classique des contrôles oraux ou écrits sur table. L'évaluation du savoir-faire peut être effectuée en intégrant des problèmes de sécurité dans les projets ou les stages que les étudiants auront à mener.

Pour les enseignements de cybersécurité intégrés sous forme de tissage, il n'est pas nécessaire d'avoir des évaluations spécifiques dédiées à ces modules tissés. Des QCMs peuvent cependant permettre de contrôler le savoir acquis.

3.7. Avertissements / Limitations

- Insister sur le caractère évolutif et adaptatif de la menace. En sûreté de fonctionnement, on s'intéresse à éviter ou à tolérer des défaillances dont la cause est non intentionnelle, alors qu'en sécurité, il faut faire face à un attaquant qui analysera les protections déployées et en cherchera le point faible.
- Enseigner surtout la protection (SSI) dans un périmètre donné. Il convient en effet de tenir compte des objectifs de la formation (notamment le métier visé) pour aborder les aspects SSI les plus appropriés.
- Programmation / développement logiciel : comprendre les conséquences de certains *bugs* tolérables a priori mais ayant des conséquences néfastes du point de vue de la sécurité. Par exemple, une application qui génère des fichiers bien formés, mais qui ne met en œuvre aucune mesure de vérification permettant de s'assurer que les fichiers qu'elle lit sont bien formés. Une telle application pourrait être mise à mal si un attaquant forge un fichier dont le contenu ne respecte pas la logique de l'application.
- L'attaquant identifie le maillon faible. Le défenseur doit être capable d'identifier ce maillon faible, du moins dans le périmètre le concernant. Cela demande une culture générale allant au-delà des stricts prérequis permettant d'apporter une réponse fonctionnelle.
- La défense et la lutte contre la cybercriminalité restent l'affaire de spécialistes. L'informaticien ne doit pas faire obstruction, et doit autant que possible en savoir assez pour assister les missions de ces spécialistes.

4. Processus qualité

S'il est vrai que la mise à disposition de matériels et guides pédagogiques permet aux enseignants de disposer d'une bonne base pour l'intégration de la cybersécurité dans leurs enseignements, il n'en demeure pas moins qu'un accompagnement pédagogique allant au-delà de ces éléments soit nécessaire pour assurer une bonne qualité des formations. Nous présentons dans la section ci-après quelques propositions faites dans cette optique.

4.1. Suivi des formations en cybersécurité

Dans l'état actuel, une forme de « tutorat » pédagogique, visant à apporter un soutien aux enseignants non spécialistes pour l'intégration des éléments de cybersécurité dans leurs enseignements est nécessaire pour réussir la transition souhaitée. Dans cette perspective, une association, également nommée CyberEdu, a été fondée en mai 2016.

La mise en place de formations en cybersécurité à destination d'enseignants en informatique non spécialistes de la cybersécurité est une solution complémentaire à la précédente, permettant d'avoir en plus un relais au sein des équipes pédagogiques au sein des établissements. Il est à noter que l'ANSSI a déjà initié des colloques dans ce sens avec des retours très positifs. Ces formations ont par ailleurs permis d'identifier des adaptations nécessaires pour mieux prendre en compte les spécificités des enseignants en comparaison aux personnels issus de l'industrie, afin de mieux répondre à leurs attentes et besoins.

L'organisation d'événements (conférences, tables rondes…) partiellement ou entièrement dédiés à l'enseignement de la cybersécurité, tels que les rendez-vous de l'enseignement sur la sécurité des système d'informations (RESSI) sont également un bon moyen de sensibilisation à l'intégration de cette dernière dans les formations.

4.2. Labellisation des formations par l'association CyberEdu

Les formations qui assurent la mise en place des dispositifs CyberEdu pourront demander le label « CyberEdu » à l'association. Ce label permettra aux étudiants et aux employeurs de repérer facilement et rapidement les formations en informatique qui dispensent le minimum nécessaire de cybersécurité.

L'objectif, pour les responsables de formation est donc de mettre en adéquation les unités d'enseignement dispensées au sein de la formation avec les recommandations CyberEdu (cf. annexe A). Par exemple, il s'agit de dispenser le cours de sensibilisation pour les formations de niveau licence (ou équivalent) en informatique et/ou d'intégrer les éléments de cybersécurité dans

les formations de niveau master (ou équivalent) en réseaux, développement logiciel et systèmes d'exploitation.

Ce label se base sur de l'auto-déclaration de la part des responsables de formations du domaine du numérique et sur la signature d'une charte de l'engagement. Le processus est décrit sur le site de l'association : https://www.cyberedu.fr/.

Annexe A : Thématiques SSI par métiers

	Assistance et support technique client (H1101)	Rédaction technique (H1207)	Défense et conseil juridique (CIL) (K1903)	Maintenance informatique et bureautique (D1407)	Ingénieur technico-commercial en informatique (D1407)	Formation professionnelle (K2111)	Administration de systèmes d'information (M1801)	Conseil et maîtrise d'ouvrage en systèmes d'information (M1802)	Direction des systèmes d'information (M1803)	Etudes et développement informatique (M1805)	Expertise et support technique en systèmes d'information (M1806)	Production et exploitation de systèmes d'information (M1810)
1. Fondamentaux	2	2	2	2	2	2	3	3	3	3	3	3
2. Electronique et architectures matérielles	2			2	1	1		2				
3. Systèmes d'exploitation	2			2	2	2	3	3	3	2	3	3
4. Réseaux et protocoles	2				2	2	3	3	3	2	3	3
5. Cryptologie					1	1	2	2	2	2	2	2
6. Stéganographie et tatouage						1		1				
7. Base de données	2			2	1	2	2	2	2	2	2	2
8. Aspects systèmes et systèmes de systèmes	2					2	3	3	3	3	3	3
9. Normes, certifications et guides			2			1	2	3	2	2	2	2
10. Certifications et évaluations						1		3				
11. Politique cybersécurité et SMSI						2	2	3	3			
12. Droit et réglementation			3			2	2	2	2		2	2
13. Développement logiciel et ingénierie logicielles						2		2	2	3	2	2
14. Gestion de projet						2		3	2	2	2	2
15. Cyberdéfense						1		3				
16. Forensics						1		3				
17. Systèmes spécifiques, informatique industrielle						1		2				
18. Aspects sociaux et sociétaux						2	3	3	3	2	3	3
19. Tests d'intrusion						1	2	3	2		2	2
20. Sécurité physique						2	2	3	2		2	2
21. Problématique SSI en contexte spécifique						1	2	2	2	1	2	2

Niveaux indiqués dans les cases du tableau : 1 : sensibilisé ; 2 : formé ; 3 : expert.

Annexe B : Description des thèmes de la cybersécurité

Thèmes principaux	Détail
1. FONDAMENTAUX	Historique de la cybersécurité
	Vocabulaire et principes fondamentaux de la cybersécurité
	Objectifs et propriétés de la sécurité
	Objectifs et profils des attaquants, typologie des attaques
	Vulnérabilité, menaces et contre-mesures
	Malware : types et évolution, principes de fonctionnement, protection contre les malwares
	Analyse et gestion de risques
	Les acteurs de la cybersécurité France/Monde
	Sûreté de fonctionnement
2. ELECTRONIQUE ET ARCHITECTURES MATERIELLES	Attaques physiques
	Conception de composants sécurisés / électronique
	Architecture des ordinateurs
	Systèmes embarqués
	Carte à puce
3. SYSTEMES D'EXPLOITATION	Principes génériques
	Unix / Linux / MacOS X
	Windows
	OS embarqués, OS mobiles (Android)
	Hyperviseurs et virtualisation
	Malwares : rétro-ingénierie
	Equipements et produits de sécurité système (Antivirus, FW, HIDS)
4. RESEAUX ET PROTOCOLES	Modèles (OSI) et types de réseaux (PAN, LAN, WLAN...)
	Protocoles et services
	Équipements et produits de sécurité réseaux (Firewall, sondes IDS/IPS, passerelles VPN, concentrateurs SSL, switches)
	Outils d'analyse et d'inspection

Thèmes principaux	Détail
5. CRYPTOLOGIE	Fondamentaux des principes (symétrique, asymétrique, hachage)
	Fondamentaux des services (chiffrement, signature…)
	Application, et services (TLS/SSL, chiffrement de disque, dans le Cloud…)
	Ingénierie de la cryptologie
	IGC, gestion des clés / certificats
	Implantations matérielle et logicielles de la cryptographie
	Algorithmes, modes (spécialisation)
6. STEGANOGRAPHIE ET TATOUAGE	Définitions, principes, applications
7. BASES DE DONNEES	Sécurité des bases de données SQL/NoSQL
	Problématiques Big Data, Open Data…
	Vulnérabilité des applications
8. ASPECTS SYSTEMES ET SYSTEMES DE SYSTEMES	Architecture produits
	Architecture systèmes
	Architecture applicatives (sécurisation des applications web…)
	Intégration de la ToIP/VoIP
9. NORMES, CERTIFICATIONS ET GUIDES	ISO 2700X ISO 22301 PCA/PRA
	Standards émanant de l'industrie, normes métiers : trusted computing, UEFI, UIT, IETF, IEEE, W3C, PCI-DSS
	PDCA Management de la qualité: projets (processus / apprentissage) CMMI, SCRUM; Services: ITIL, Lean software
	Guides (ANSSI, ENISA, NIST, SANS, NSA/CSS...)
10. CERTIFICATIONS ET EVALUATION	Schéma de certifications « critères communs »
	Autres schémas : CSPN…
11. POLITIQUE CYBERSECURITE ET SMSI	Organisation de la cybersécurité en France et à l'étranger
	Démarche d'analyse de risque
	Conception et mise en place d'une PSSI
	Supervision
	Contrôle, audit
	CERT
	SOC
	Traitement des incidents de sécurité : CISRT / CALID / DGA-MI
12. DROIT ET REGLEMENTATION	Droit et réglementation génériques en France
	Droit et réglementation spécifiques (O.I.V., métiers)
	Droit et réglementation au niveau international

Thèmes principaux	Détail
13. DEVELOPPEMENT LOGICIEL ET INGENIERIE LOGICIELLE	Compilation / interprétation et exécution
	Développement sécurisé, durcissement de code, analyse formelle
	Architecture logicielle
	Relecture, analyse statique de code, tests
	Environnement de développement
14. GESTION DE PROJET	Gestion de la SSI dans les projets
	Démarche « homologation »
15. CYBERDEFENSE	Doctrine d'emploi (en France et à l'étranger)
	Détection, agrégation, normalisation, corrélation, reporting, stockage
	Réaction, traitement, CISRT, coordination, PCA/PRA, cyberrésilience
	Gestion de crise, communication
	Préservation de la preuve, Réponse juridique
16. FORENSICS	Forensics, analyse post mortem, sûreté des logs
17. SYSTEMES SPECIFIQUES, INFORMATIQUE INDUSTRIELLE	SCADAs
	Objets connectés
18. ASPECTS SOCIAUX ET SOCIETAUX	Ingénierie sociale
	Phishing
	Contournement de la politique de sécurité Ergonomie de la sécurité
	Hygiène informatique : guides ANSSI / ENISA / NIST
	Géopolitique et Intelligence économique
19. TESTS D'INTRUSION	Principes
	Droit
	Outils
20. SECURITE PHYSIQUE	Sécurité physique des SI : de conception, de fonctionnement
	Contrôle d'accès: authentification, autorisation, traçabilité
21. PROBLEMATIQUE SSI EN CONTEXTES SPECIFIQUES	Informatique nébuleuse (cloud computing)
	Infogérance, externalisation, dépérimétrisation
	Mobilité
	Multi-niveaux

Annexe C : Description des métiers

Cette annexe décrit les différents métiers retenus pour structurer les propositions relatives aux thématiques cybersécurité pouvant être intégrées dans les programmes de formation.

Différents référentiels métiers sont disponibles dont certains principalement tournés vers les compétences métiers au sein des entreprises et d'autres établissant le lien avec les compétences aux sortir des écoles.

Parmi les référentiels de la 1re catégorie, nous pouvons mentionner :

- Le rapport du C.I.G.R.E.F. disponible à l'adresse *http://www.cigref.fr/cigref_publications/RapportsContainer/Parus2011/2011_Metiers_des_SI_dans_Grandes_entreprises_Nomenclature_RH_CIGREF_FR.pdf*. Les pages 172-173 de ce rapport décrivent les compétences métiers.
- Les référentiels de l'A.P.E.C. :
  - » Référentiel Apec des métiers IT disponible à l'adresse *http://munci.org/Referentiels-Apec-des-metiers-IT* ;
  - » Référentiel des métiers des systèmes d'information (mai 2014), dont la version la plus récente est disponible à l'adresse *http://cadres.apec.fr/Emploi/Observatoire-de-l-emploi/Les-etudes-Apec-par-thematique/Metiers-et-competences/Les-metiers-cadres-de-la-DSI-en-pleine-mutation/* ;
  - » Référentiel des «métiers en émergence» disponible à l'adresse *http://presse.apec.fr/Presse/Communiques-de-l-Apec/Les-Referentiels/le-referentiel-metiers-en-emergence-vient-de-paraitre* ;
  - » Référentiel des métiers de l'internet (juin 2012) disponible à l'adresse *http://recruteurs.apec.fr/Recrutement/Observatoire-de-l-emploi/Les-etudes-Apec-par-thematique/Metiers-et-competences/Referentiel-des-metiers-de-l-Internet* ;
  - » Référentiel des métiers des télécoms (juin 2008) disponible à l'adresse *http://recruteurs.apec.fr/Recrutement/Observatoire-de-l-emploi/Les-etudes-Apec-par-thematique/Metiers-et-competences/Referentiel-des-metiers-cadres-du-secteur-des-telecoms* ;
- Les référentiels de Syntec-ingénierie disponibles à l'adresse *http://www.syntec-ingenierie.fr/social-et-formation/etudes-referentiels/etudes-metiers-ingenierie/* .

En ce qui concerne les référentiels établissant le lien entre les métiers et les formations, nous pouvons citer :

- Le Registre National des Certifications Professionnelles, registre qui sert aussi de référence au Pôle Emploi quant à produire les fiches du Rome (*http://www.rncp.cncp.gouv.fr/*);
- Les Codes Rome Pole-emploi des métiers du numérique (Informatique-Télécoms & Web-Multimédia) (Pôle Emploi, 2009), disponibles à l'adresse *http://munci.org/De-nouveaux-codes-Rome-pour-les-metiers-du-numerique-informatique-telecoms-web-multimedia* ;

- Le portail « famille des métiers de l'internet » de l'éducation Nationale accessible à l'adresse *http://www.metiers.internet.gouv.fr/* .

Étant donné que le guide pédagogique vise principalement les formations, un adossement sur les référentiels permettant d'établir un lien entre métiers et formations nous a semblé être la solution la plus adaptée. Nous nous sommes par conséquent basés sur le Registre National des Certifications Professionnelles (RNCP). La plupart des Grandes écoles et Universités y qualifient déjà, depuis quelques années, les formations qu'elles dispensent. C'est aussi le R.N.C.P. qui motive aujourd'hui les centres de formations continues, les O.P.C.A. et le Pôle Emploi à engager des financements tout au long de la vie.

Pour information, bien que ce guide ait vocation à fournir des orientations pour l'intégration de la cybersécurité dans les formations supérieures en informatique non spécialisées en cybersécurité, cette liste est complétée par quelques métiers de spécialistes de la cybersécurité.

Dans tous les cas, les métiers présentés doivent être considérés comme représentatifs d'un ensemble de connaissances et compétences, i.e. d'objectifs de formation, et non d'un ensemble d'activités menées par un professionnel de l'informatique. C'est pour cette raison que des métiers tels que consultant ne sont pas repris ici.

Le tableau ci-après donne la liste des métiers retenus, avec précision du domaine d'appartenance dans la nomenclature ROME

	Domaine	Métier
1	Affaires et support technique client	Assistance et support technique client
2	Conception, recherche, études et développement	Rédaction technique
3	Droit	Défense et conseil juridique (CIL)
4	Equipements domestiques et informatique	Maintenance informatique et bureautique
5	Force de vente	Ingénieur technico-commercial en informatique
6	Formation initiales et continue	Formation professionnelle
7	Systèmes d'information et de la télécommunication	Administration de systèmes d'information
8	Systèmes d'information et de la télécommunication	Conseil et maîtrise d'ouvrage en systèmes d'information
9	Systèmes d'information et de la télécommunication	Direction des systèmes d'information
10	Systèmes d'information et de la télécommunication	Etudes et développement informatique
11	Systèmes d'information et de la télécommunication	Expertise et support technique en systèmes d'information
12	Systèmes d'information et de la télécommunication	Production et exploitation de systèmes d'information

Au sein des sous-sections suivantes, les différents métiers sont décrit :

Assistance et support technique client

Définition métier
Réalise et assure l'assistance et le support technique auprès des clients (internes, externes) de l'entreprise en vue de prévenir et de résoudre des problèmes techniques d'exploitation et d'entretien par le traitement de questions et l'apport de solutions techniques selon des impératifs de qualité et de délais.
Niveau
Bac+2 à Bac+5
Code ROME
H1101
Formations
Bac+2 (BTS, DUT, ...) à Bac+5 (Master professionnel, diplôme d'ingénieur, ...) en maintenance industrielle, études et développement ou dans le secteur technique de l'entreprise (mécanique, chimie, ...)
Appellations métier
Directeur / Directrice assistance technique, Expert / Experte support technique, Ingénieur / Ingénieure assistance technique, Ingénieur / Ingénieure service client, Ingénieur / Ingénieure support technique, Représentant technique / Représentante technique utilisateur, Responsable centre de support client, Responsable support technique clients, Spécialiste support technique, Technicien / Technicienne support client, Technicien / Technicienne support technique

Fiche métier disponible à l'adresse :

http://recrutement.pole-emploi.fr/fichesrome/ficherome?codeRome=H1101&domaine=Candidat

Rédaction technique

Définition métier

Conçoit et finalise la documentation technique (notices, plaquettes, manuels, catalogues, bordereaux, ...), associée à des produits, des appareils, des équipements ou des procédés techniques, dans un objectif de déclinaison et d'utilisation.

Effectue le suivi de cohérence (vocabulaire spécifique, ...) de l'ensemble de la documentation technique. Peut intervenir dans un domaine ou sur un type de produit particulier en fonction du niveau de technicité requis par l'objet de sa rédaction. Peut encadrer une équipe de rédacteurs.

Niveau

Bac+2

Code ROME

H1207

Formations

Bac+2 (BTS, DUT) dans un secteur technique (mécanique, électronique, ...) ou scientifique (chimie, biologie, ...)

Appellations métier

Chargé / Chargée d'affaires en rédaction technique, Nomenclaturiste en rédaction technique, Responsable service rédaction technique, Rédacteur / Rédactrice de notices techniques, Rédacteur / Rédactrice technique, Rédacteur / Rédactrice technique en informatique, Technicien rédacteur / Technicienne rédactrice en industrie

Fiche métier disponible à l'adresse :

http://recrutement.pole-emploi.fr/fichesrome/ficherome?codeRome=H1207&domaine=Candidat

Défense et conseil juridique (CIL)

Définition métier

Conseille et informe des personnes physiques ou morales en matière juridique et judiciaire, établit des actes juridiques et effectue la gestion de contentieux. Peut présenter oralement la défense de clients au cours de plaidoiries, peut veiller à la sécurité juridique d'entreprises. Peut former des personnes dans sa spécialité qu'elle actualise par une veille informative.

Niveau

Bac+4 à Bac+5

Code ROME

K1903

Formations

Bac+4 (M1, IUP, ...) à Master (Master professionnel, Master recherche, ...) en droit complété par une spécialisation (avocat, assurance, finance, fiscalité, …)

Fiche métier disponible à l'adresse :

http://recrutement.pole-emploi.fr/fichesrome/ficherome?codeRome=K1903&domaine=Candidat

Maintenance informatique et bureautique

Définition métier

Effectue le dépannage, l'entretien et l'installation d'équipements ou de parcs d'équipements informatiques ou bureautiques (matériels, logiciels, réseaux, ...), selon les règles de sécurité et la réglementation. Peut conseiller, former et assister les utilisateurs (sur site, par télémaintenance, téléassistance, ...). Peut assembler ou intégrer un équipement (configurations standards ou spécifiques, ...). Peut coordonner une équipe.

Niveau

CAP/BEP, BAC, BAC+2

Code ROME

I1401

Formations

Bac (Bac Professionnel, Brevet professionnel, ...) à Bac+2 (BTS, DUT) en informatique, électronique, électrotechnique, … ; Autres possibilités : CAP/BEP en bureautique, reprographie,... ou avec une expérience professionnelle dans le secteur de l'informatique.

Appellations métier

Agent / Agente de maintenance de machines de bureau, Agent / Agente de maintenance de matériels de reprographie, Agent / Agente de maintenance en bureautique, Agent / Agente de maintenance en informatique, Agent(e) maintenance systèmes impression et reprographie, Agent / Agente de maintenance sur télécopieurs, Assistant / Assistante aux utilisateurs en informatique, Assistant / Assistante micro-informatique, Assistant / Assistante sur site informatique, Chef d'équipe de help desk en informatique, Correspondant / Correspondante micro-informatique, Dépanneur / Dépanneuse en micro-informatique grand public, Installateur / Installatrice de matériels de reprographie, Responsable centre d'appels en maintenance informatique, Responsable micro-informatique, Superviseur / Superviseuse help desk en informatique, Superviseur / Superviseuse hot line en informatique, Support aux utilisateurs en informatique, Support technique hot line en informatique, Technicien(ne) assistance à la clientèle en informatique, Technicien/ Technicienne Service Après-Vente en informatique, Technicien/Technicienne Service Après-Vente en bureautique, Technicien / Technicienne de help desk en informatique, Technicien / Technicienne de hot line en informatique, Technicien(ne) de maintenance de réseaux informatiques, Technicien(ne) de maintenance de réseaux télématiques, Technicien(ne) de maintenance de systèmes informatiques, Technicien / Technicienne de maintenance en bureautique, Technicien / Technicienne de maintenance en informatique, Technicien/Technicienne de maintenance en matériel de bureau, Technicien(ne) de maintenance en matériels informatiques, Technicien/Technicienne de maintenance en micro-informatique, Technicien(ne) de maintenance en microsystèmes informatiques, Technicien / Technicienne de maintenance en monétique, Technicien / Technicienne en micro réseaux et bureautique, Technicien/Technicienne en micro-informatique et bureautique, Technicien / Technicienne en micro-informatique et réseaux, Technicien / Technicienne en réseau local informatique, Technicien / Technicienne en téléassistance en informatique, Technicien / Technicienne support en bureautique, Technicien(ne) support en systèmes téléinformatiques

Fiche métier disponible à l'adresse :

http://www.orientation-pour-tous.fr/metier/maintenance-informatique-et-bureautique,12357.html

Ingénieur technico-commercial en informatique

Définition métier

Prospecte une clientèle de professionnels, propose des solutions techniques selon les besoins, impératifs du client et négocie les conditions commerciales de la vente. Peut coordonner une équipe commerciale et animer un réseau de commerciaux. Cas du Technico-Commercial informatique "Le champion de la solution informatique sur mesure pour les entreprises et les administrations, c'est l'ingénieur technico-commercial ! Son rôle : accompagner le projet, de sa négociation commerciale à sa réalisation technique."

Niveau

Bac+5

Code ROME

D1407

Formations

Bac +2 (BTS, DUT, ...) à Master (Master professionnel, diplôme d'ingénieur, ...) dans un secteur technique, scientifique ou industriel complété par une formation commerciale.

Fiche métier disponible à l'adresse :

http://recrutement.pole-emploi.fr/fichesrome/ficherome?codeRome=D1407&domaine=Candidat

Formation professionnelle

Définition métier

Réalise, dans le cadre de la formation continue, les apprentissages des savoirs et des savoir-faire de publics adultes ou jeunes afin de favoriser leur insertion professionnelle ou leur adaptation aux évolutions techniques et professionnelles. Peut réaliser l'analyse des besoins de formation d'une structure et concevoir des produits pédagogiques. Peut négocier la sous-traitance d'actions de formation. Peut coordonner une équipe. À l'heure où les technologies ne cessent d'évoluer, le formateur en informatique est partout. Connaissances affûtées et pédagogie en poche, il répond aux besoins en formation d'utilisateurs en tout genre.

Niveau

Bac+2 à Bac+5

Code ROME

K2111

Formations

Bac + 2 pour des formations dédiées aux outils bureautiques à bac + 5 pour des formations plus pointues ou pour créer des outils de formation. Voire plus, pour des expertises internationales par exemple

Appellations métier

Animateur / Animatrice de formateurs, Animateur / Animatrice de formation, Animateur-coordinateur/ Animatrice-coordinatrice de formation, Chargé / Chargée de formation en organisme de formation, Concepteur(trice) organisateur(trice) en formation, Concepteur-animateur / Conceptrice-animatrice de formation, Concepteur-formateur / Conceptrice-formatrice, Conseiller/Conseillère d'éducation populaire et de jeunesse, Didacticien / Didacticienne, E-formateur / E-formatrice, Formateur / Formatrice, Formateur / Formatrice bureautique, Formateur / Formatrice d'adultes, Formateur / Formatrice d'animateurs de formation, Formateur / Formatrice de formateurs, Formateur / Formatrice de formation professionnelle, Formateur / Formatrice de la formation continue, Formateur / Formatrice de langue vivante, Formateur / Formatrice e-learning, Formateur/ Formatrice en Institut Universitaire -IUFM- (ESPE), Formateur / Formatrice enseignement à distance, Formateur / Formatrice informatique, Formateur / Formatrice multimédia, Formateur / Formatrice remise à niveau, Formateur / Formatrice technique, Formateur animateur / Formatrice animatrice de formation, Formateur consultant / Formatrice consultante, Formateur coordinateur/ Formatrice coordinatrice de formation, Formateur coordonnateur / Formatrice coordonnatrice de stage, Formateur-conseil / Formatrice-conseil, Formateur-initiateur / Formatrice-initiatrice, Instituteur(trice) maître(sse) formateur(trice), Moniteur / Monitrice de formation professionnelle, Moniteur / Monitrice en formation continue, Professeur / Professeure en centre de formation pour adultes, Responsable ingénierie de la formation professionnelle, Téléformateur / Téléformatrice

Fiche métier disponible à l'adresse :

http://www.orientation-pour-tous.fr/metier/formateurtrice-en-informatique,11305.html

Administration de systèmes d'information

Définition métier

Administre et assure le fonctionnement et l'exploitation d'un ou plusieurs éléments matériels ou logiciels (outils, réseaux, bases de données, messagerie, ...) de l'entreprise ou d'une organisation. Veille à la cohérence, à l'accessibilité et à la sécurité des informations. Peut coordonner une équipe.

Niveau

Bac+2 à Bac+4

Code ROME

M1801

Formations

Bac+2 (BTS, DUT, ...) à Bac+4 (IUP, MIAGE, ...) dans le secteur de l'informatique ou des télécoms

Appellations métier

Administrateur / Administratrice de site Web, Administrateur / Administratrice de la messagerie, Administrateur / Administratrice de serveurs, Administrateur / Administratrice réseaux - télécoms, Administrateur / Administratrice de bases de données, Administrateur / Administratrice sécurité informatique, Administrateur / Administratrice de site internet, Administrateur / Administratrice système informatique, Administrateur / Administratrice réseau informatique

Fiche métier disponible à l'adresse :

http://www.orientation-pour-tous.fr/metier/administration-de-systemes-d-information,12617.html

Conseil et maîtrise d'ouvrage en systèmes d'information

Définition métier

Conseille la direction informatique, télécoms de l'entreprise sur des évolutions et solutions en techniques nouvelles (choix de logiciel, matériel, réseau, ...), dans un objectif d'optimisation et d'adéquation entre les moyens informatiques et télécoms et les besoins des utilisateurs. Assure un rôle de support (sécurité, qualité, méthode, ...) et d'assistance technique auprès des équipes informatiques ou télécoms (production, développement) de l'entreprise, des utilisateurs, des clients. Veille au respect des normes et des procédures de qualité et de sécurité. Peut intervenir directement sur tout ou partie d'un projet qui relève de son domaine d'expertise.

Niveau

Bac+4 à Bac+5

Code ROME

M1802

Formations

Master (M1, Master professionnel, diplôme d'ingénieur, ...) en informatique et télécoms, complété par une expérience professionnelle dans le secteur.

Appellations métier

Architecte multimédia, Architecte réseaux informatiques, Architecte système d'information, Architecte système informatique, Auditeur / Auditrice en système d'information, Auditeur informaticien / Auditrice informaticienne, Expert / Experte en communication et réseaux, Expert / Experte en sécurité des systèmes d'exploitation, Expert / Experte en technologie Internet et multimédia, Expert / Experte méthodes et qualité informatique, Expert / Experte qualité informatique, Expert / Experte réseaux et télécoms, Expert / Experte système d'exploitation, Expert / Experte système et réseaux, Expert / Experte sécurité informatique, Expert / Experte sécurité, méthode et qualité informatique, Ingénieur / Ingénieure méthodes informatiques, Ingénieur / Ingénieure réseau informatique, Ingénieur / Ingénieure système informatique, Ingénieur /, Ingénieure système réseau informatique, Ingénieur / Ingénieure sécurité informatique, Qualiticien / Qualiticienne logiciel en informatique, Responsable sécurité des systèmes d'information, Responsable sécurité informatique

Fiche métier disponible à l'adresse :

http://recrutement.pole-emploi.fr/fichesrome/ficherome?codeRome=M1802&domaine=Candidat

Direction des systèmes d'information

Définition métier

Dirige une organisation, des services, des structures informatiques, télécoms et fixe les évolutions des systèmes d'information et de télécommunications, selon les besoins fonctionnels et la stratégie de l'entreprise. Supervise la conception, la mise en œuvre et le maintien opérationnel (qualité, sécurité, fiabilité, coûts, délais) des prestations informatiques produites et des systèmes d'information et télécoms. Supervise et pilote des projets en systèmes d'information.

Niveau

Bac+4 à Bac+5

Code ROME

M1803

Formations

Master (M1, Master professionnel, diplôme d'ingénieur, ...) en informatique ou télécoms ou diplôme de niveau Bac+2 (BTS, DUT) ou une expertise du secteur d'activité de l'entreprise, complété par une expérience professionnelle en informatique.

Appellations métier

Chef de projet Web, Chef de projet développement logiciel, Chef de projet en linguistique informatique, Chef de projet informatique, Chef de projet internet, Chef de projet multimédia, Directeur / Directrice de département informatique, Directeur / Directrice de département télécoms, Directeur/Directrice Organisation et Systèmes d'Information, Directeur / Directrice de projet en informatique, Directeur / Directrice de projet télécoms, Directeur / Directrice de service télécoms, Directeur / Directrice des services informatiques -DSI-, Directeur / Directrice des systèmes d'information, Directeur/Directrice des systèmes d'information et télécoms, Directeur / Directrice informatique, Directeur / Directrice télécoms, Responsable d'exploitation informatique, Responsable d'un service informatique, Responsable d'un service télécoms, Responsable de division informatique, Responsable de division télécoms, Responsable de domaine en informatique, Responsable de domaine télécoms, Responsable de département informatique, Responsable de département télécoms, Responsable de la production informatique, Responsable projet architecture intégration grands systèmes, Responsable de projet architecture informatique, Responsable de projet architecture télécoms, Responsable de réseaux télécoms, Responsable des systèmes d'information, Responsable des systèmes informatiques, Responsable du management de la DSI, Responsable du réseau informatique, Responsable informatique, Responsable production informatique, Responsable télécoms

Fiche métier disponible à l'adresse :

http://recrutement.pole-emploi.fr/fichesrome/ficherome?codeRome=M1803&domaine=Candidat

Etudes et développement informatique

Définition métier

Conçoit, développe et met au point un projet d'application informatique, de la phase d'étude à son intégration, pour un client ou une entreprise selon des besoins fonctionnels et un cahier des charges. Peut conduire des projets de développement. Peut coordonner une équipe

Niveau

Bac+2 à Bac+5

Code ROME

M1805

Formations

Bac+2 (BTS, DUT) à Master (MIAGE, diplôme d'ingénieur, Master professionnel, ...) en informatique

Appellations métier

Analyste cogniticien / cogniticienne informatique, Analyste concepteur / conceptrice informatique, Analyste d'application, Analyste d'étude informatique, Analyste de gestion informatique, Analyste décisionnel - Business Intelligence, Analyste développeur / développeuse, Analyste fonctionnel / fonctionnelle informatique, Analyste organique informatique, Analyste responsable d'application informatique, Analyste réseau informatique, Analyste télématique, Analyste-programmeur / Analyste-programmeuse informatique, Analyste-programmeur(se) d'étude informatique, Analyste-programmeur(se) en informatique industrielle, Analyste-programmeur(se) gestion informatique, Analyste-programmeur(se) scientifique informatique, Assistant / Assistante chef de projet informatique, Chef de projet TMA - Tierce Maintenance Applicative, Chef de projet maîtrise d'œuvre informatique, Chef de projet étude et développement informatique, Concepteur / Conceptrice d'application informatique, Concepteur / Conceptrice logiciel informatique, Didacticien / Didacticienne informatique, Développeur / Développeuse - jeux vidéo, Développeur / Développeuse d'application, Développeur / Développeuse informatique, Développeur / Développeuse multimédia, Développeur / Développeuse web, Développeur / Développeuse web mobile, Développeur(se) décisionnel - Business Intelligence, Homologateur / Homologatrice logiciel, Informaticien / Informaticienne analyste, Informaticien / Informaticienne d'application, Informaticien / Informaticienne de développement, Informaticien chargé / Informaticienne chargée d'étude, Ingénieur / Ingénieure analyste en système d'information, Ingénieur / Ingénieure d'application informatique, Ingénieur / Ingénieure d'intégration applicative, Ingénieur / Ingénieure d'étude en informatique de gestion, Ingénieur / Ingénieure d'étude et développement informatique, Ingénieur / Ingénieure d'étude informatique, Ingénieur / Ingénieure de conception informatique, Ingénieur / Ingénieure de développement informatique, Ingénieur / Ingénieure de réalisation informatique, Ingénieur / Ingénieure logiciel informatique, Ingénieur informaticien / Ingénieure informaticienne, Ingénieur(e) analyse programmation en informatique gestion, Ingénieur(e) analyste-programmeur(se), Ingénieur(e) informatique développement en temps réel, Ingénieur(e) étude en application scientifique informatique, Intégrateur / Intégratrice d'application informatique, Lead programmeur / programmeuse - jeux vidéo, Paramétreur / Paramétreuse logiciel ERP, Programmeur / Programmeuse - jeux vidéo, Programmeur / Programmeuse d'études, Programmeur / Programmeuse de maintenance informatique, Programmeur / Programmeuse informatique, Programmeur industriel / Programmeuse industrielle, Responsable d'application informatique, Responsable d'atelier de génie logiciel, Responsable d'étude informatique, Responsable de gestion de configuration, Responsable de projet informatique, Responsable des développements informatiques, Technicien / Technicienne programmation, Testeur / Testeuse informatique, Webmaster développeur / développeuse

Fiche métier disponible à l'adresse :

http://recrutement.pole-emploi.fr/fichesrome/ficherome?codeRome=M1805&domaine=Candidat

Expertise et support technique en systèmes d'information

Définition métier

Traduit les besoins fonctionnels d'un système d'information d'un commanditaire, selon les objectifs du domaine métier (comptable, ressources humaines, logistique, commercial, production...) et les contraintes économiques et logistiques.

Négocie avec les informaticiens les composantes d'une application et d'un outil logiciel, tout au long de la conception et de la réalisation, dans l'intérêt de l'entreprise et des utilisateurs finaux.

Assiste la maîtrise d'ouvrage dans la définition des besoins, des solutions à mettre en œuvre et leurs intégrations dans le système d'information de l'entreprise. Participe à des projets de mise en œuvre de système d'information (implémentation).

Peut superviser un projet maîtrise d'ouvrage.

Niveau

Bac+4 à Bac+5

Code ROME

M1806

Formations

Master (M1, Master professionnel, diplôme d'ingénieur, ...) dans le secteur de l'organisation et du management des systèmes d'information, des ressources humaines, de la gestion, des finances, de la logistique, ... complété par une expérience professionnelle en conduite de projet et une connaissance des technologies des systèmes d'information.

Appellations métier

Architecte fonctionnel(le) de système d'information, Assistant(e) maîtrise d'ouvrage des systèmes d'information, Assistant(e) fonctionnel(le) des systèmes d'information, Chef de projet Maîtrise d'Ouvrage - MOA syst. D'information, Chef de projet maîtrise d'ouvrage des systèmes d'information, Chef de projet utilisateurs des systèmes d'information, Consultant / Consultante ERP - Enterprise Resource Planning, Consultant / Consultante SI CRM/GRC, Consultant / Consultante SI finance comptabilité, Consultant / Consultante SIRH ressources humaines, Consultant / Consultante décisionnel - Business Intelligence, Consultant / Consultante en accessibilité numérique, Consultant / Consultante en système d'information, Consultant / Consultante informatique, Consultant / Consultante réseaux informatiques, Consultant(e) fonctionnel(le) de progiciel, Consultant(e) fonctionnel(le) des systèmes d'information, Coordinateur(trice) Maîtrise d'ouvrage systèmes information, Coordinateur/Coordinatrice projet en Maîtrise d'Ouvrage MOA, Expert / Experte métier système d'information, Gestionnaire d'applications système d'information, Maître / Maîtresse d'ouvrage système d'information, Responsable de projets « métiers » système d'information, Responsable du système d'information « métier », Responsable utilisateurs des systèmes d'information, Urbaniste des systèmes d'information

Fiche métier disponible à l'adresse :

http://www.orientation-pour-tous.fr/metier/expertise-et-support-technique-en-systemes-d-information,12611.html

Production et exploitation de systèmes d'information

Définition métier

Met en œuvre et assure la disponibilité des ressources physiques (serveurs, disques, automates, ...) et des ressources logiques (logiciels, espaces disques, puissance...) nécessaires au fonctionnement des systèmes de production et d'exploitation informatiques et télécoms de l'entreprise. Surveille le fonctionnement des différents systèmes, réseaux, ... selon les normes et les méthodes d'exploitation et de sécurité. Peut coordonner une équipe.

Niveau

Bac+2

Code ROME

M1810

Formations

Bac+2 (BTS, DUT, ...) en informatique

Appellations métier

Adjoint / Adjointe d'exploitation informatique, Adjoint(e) technicien(ne) d'exploitation informatique, Agent / Agente d'exploitation informatique, Agent / Agente de planning informatique, Analyste d'exploitation, Assistant / Assistante d'exploitation informatique, Chargé / Chargée de mise en exploitation informatique, Chef d'exploitation informatique, Chef d'équipe de production informatique, Chef de salle informatique, Contrôleur / Contrôleuse de réseau informatique, Exploitant / Exploitante informatique, Exploitant / Exploitante réseau informatique, Gestionnaire de production informatique, Gestionnaire de ressources informatiques, Gestionnaire de ressources matérielles informatiques, Gestionnaire du parc informatique, Ingénieur / Ingénieure d'exploitation informatique, Ingénieur / Ingénieure de production informatique, Intégrateur / Intégratrice d'exploitation informatique, Opérateur / Opératrice d'exploitation informatique, Opérateur / Opératrice informatique, Opérateur pupitreur / Opératrice pupitreuse informatique, Pilote d'exploitation informatique, Pilote de ressources informatiques, Pilote multiserveur informatique, Pupitreur / Pupitreuse d'exploitation informatique, Pupitreur / Pupitreuse informatique , Pupitreur / Pupitreuse réseau informatique, Pupitreur / Pupitreuse système informatique, Technicien / Technicienne d'exploitation informatique, Technicien / Technicienne informatique, Technicien / Technicienne poste de travail en informatique, Technicien / Technicienne réseau informatique, Technicien / Technicienne système informatique

Fiche métier disponible à l'adresse :

http://www.orientation-pour-tous.fr/metier/production-et-exploitation-de-systemes-d-information,12630.html

Annexe D : Définitions

Audit de sécurité

Revue indépendante et examen des enregistrements et de l'activité du système afin de vérifier l'exactitude des contrôles du système pour s'assurer de leur concordance avec la politique de sécurité établie et les procédures d'exploitation, pour détecter les infractions à la sécurité et pour recommander les modifications appropriées des contrôles, de la politique et des procédures.

Auditabilité

Aptitude à fournir, à une autorité compétente, la preuve que la conception et le fonctionnement du système et de ses contrôles internes sont conformes aux exigences.

Authentification / identification

L'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.

Authentification de l'entité homologue

Confirmation qu'une entité homologue d'une association est bien l'entité déclarée.

Authentification de l'origine des données

Confirmation que la source des données reçues est telle que déclarée.

Confidentialité

Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

Cryptographie

Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification ne passe inaperçue et/ou d'empêcher leur utilisation non autorisée.

Cybersécurité

État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Disponibilité

Propriété d'être accessible et utilisable sur demande par une entité autorisée.

Intégrité

Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime.

Intégrité des données

Propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

Répudiation

Le fait, pour une des entités impliquées dans la communication, de nier avoir participé aux échanges, totalement ou en partie.

Système d'information

Ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information.

Annexe E : Glossaire

AES	Advanced Encryption Standard
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ADSL	Asymmetric Digital Subscriber Line
BIOS	Basic Input Output System
BAN	Body Area Network
BGP	Border Gateway Protocol
Botnets	Réseau d'ordinateurs infectés
BYOD	Bring Your Own Devices
CAN	Campus Are Network
CEH	Certified Ethical Hacker
CISSP	Certified Information System Security Professional
CASB	Cloud Access Security Brokers
CSG	Cloud Security Gateway
CLUSIF	Club de la Sécurité de l'Information Français
CMS	Content Management System
CCMP	Counter Cipher Mode Protocol
DMZ	Demilitarized Zone
DDoS	Distributed Denial of Service Attack
DNS	Domain Name System
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
GPG	GNU Privacy Guard
HTTPS	HyperText Transfer Protocol Secure
IGC	Infrastructure de Gestion de Clés (= PKI - Public Key Infrastructure)
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
LAN	Local Area Network
MOE	Maîtrise d'Œuvre
MOA	Maîtrise d'Ouvrage
MAC	Media Access Control
MEHARI	MÉthode Harmonisée d'Analyse de Risques
MAN	Metropolitan Area Network

OTP	One Time Password
OSPF	Open Shortest Path First
OCTAVE	Operationnaly Critical Threat, Asset, and Vulnerability Evaluation
PAN	Personal Area Network
PCA	Plan de Continuité d'Activité
PRA	Plan de Reprise d'Activité
PSSI	Politique de Sécurité des Systèmes d'Information
PSSIE	Politique de Sécurité des Systèmes d'Information de l'État
POP	Post Office Protocol
PSK	Pre-Shared Key
RGS	Référentiel Général de Sécurité
RAS	Remote Access Server
RSSI	Responsable de la sécurité des systèmes d'informatique
RSA	Rivest Shamir Adleman (initiales des trois inventeurs)
RIP	Routing Information Protocol
SCP	Secure copy
SFTP	Secure File Transfer Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
SIEM	Security Information and Event Management
SOC	Security Operating Center
SLA	Service Level Agreement
SSID	Service Set IDentifier
SMTP	Simple Mail Transfer Protocol
SSO	Single Sign-On
SaaS	Software as a Service
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
UDP	User Datagram Protocol
VLAN	Virtual LAN
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
WPAN	Wireless PAN

CyberEdu

Version 1.1 - Février 2017

Ce document a été rédigé par un consortium regroupant des enseignants-chercheurs et des professionnels du secteur de la cybersécurité.