Annexe I.B – Référentiel de compétences

Bloc de compétences n°1 - Support et mise à disposition de services informatiques

Conditions de réalisation et ressources nécessaires

Contexte

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.

Ressources

- Description de l'organisation cliente : son métier, ses processus, ses acteurs (internes et externes), son système d'information et sa politique de communication.
- Description du prestataire informatique : ses compétences, ses méthodes, ses outils, ses procédures et référentiels.
- Description du système informatique de l'organisation cliente : infrastructure de communication, cartographie des applications, règles de sécurité.
- Référentiels, normes, réglementations, chartes, standards et méthodes mobilisées dans le cadre de la mise à disposition d'un service.
- Contrat de prestation de services.
- Environnement de production opérationnel et conforme à l'environnement technologique décrit dans l'annexe II.E du diplôme.
- Cahier des charges (avec les spécifications fonctionnelles et éventuellement techniques du service à mettre à disposition).

Degré d'autonomie, responsabilités

La personne titulaire du diplôme est en charge, pour le compte des utilisateurs et des clients, de tout ou partie du support et de la mise à disposition des services informatiques. Elle travaille dans un périmètre donné en respectant les étapes du processus de prise en compte des demandes d'intervention, ou bien, au sein d'une équipe projet, à la mise à disposition d'un nouveau service. Pour ce faire elle est consciente des enjeux liés à la gestion des actifs informatiques.

Elle écoute et interprète les demandes des utilisateurs et des clients. Elle prend en compte ces demandes, les qualifie et les traite ou les relaie vers une personne ou une entité habilitée et compétente. Elle informe et sensibilise les utilisateurs et les clients concernant le support et la mise à disposition des services informatiques. Elle rend compte de ses activités afin de constituer une documentation (FAQ, banque de connaissances, etc.).		
Compétences	**Indicateurs de performance**	**Savoirs associés**
Gérer le patrimoine informatique ▪ Recenser et identifier les ressources numériques ▪ Exploiter des référentiels, normes et standards adoptés par le prestataire informatique ▪ Mettre en place et vérifier les niveaux d'habilitation associés à un service ▪ Vérifier les conditions de la continuité d'un service informatique ▪ Gérer des sauvegardes ▪ Vérifier le respect des règles d'utilisation des ressources numériques	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.	<u>Savoirs technologiques</u> Patrimoine informatique : définition, outils de gestion Système informatique Système d'exploitation : gestion des utilisateurs, habilitations et droits d'accès Disponibilité d'un service informatique : enjeux techniques, économiques et juridiques Plans de continuité et de reprise d'activité Typologie et techniques de sauvegarde et de restauration Typologie des supports de sauvegarde <u>Savoirs économiques, juridiques et managériaux</u> Typologie des acteurs de l'industrie informatique Normes et standards : enjeux techniques et économiques Typologie des licences logicielles, modalités de tarification Gestion des actifs informatiques : méthodes, enjeux techniques, financiers, organisationnels et juridiques pour l'organisation Contrat de prestation de service informatique et autres

		contrats liés à la gestion du patrimoine informatique Obligations légales en matière de conservation et d'archivage des données Charte informatique et sa valeur juridique Responsabilités du salarié utilisateur des ressources informatiques
Répondre aux incidents et aux demandes d'assistance et d'évolution ▪ Collecter, suivre et orienter des demandes ▪ Traiter des demandes concernant les services réseau et système, applicatifs ▪ Traiter des demandes concernant les applications	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.	<u>Savoirs technologiques</u> 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 Normes et standards concernant la gestion des configurations et la gestion d'incidents 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 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 <u>Savoirs économiques, juridiques et managériaux</u> Entente de niveau de service et contrat d'assistance : obligations et responsabilités
Développer la présence en ligne de l'organisation ▪ Participer à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques ▪ 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.	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.	<u>Savoirs technologiques</u> Référencement et mesure d'audience d'un service en ligne Conventions d'écriture électronique Charte graphique 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 <u>Savoirs économiques, juridiques et managériaux</u> E-réputation d'une organisation : modalités de construction, atteintes, protection juridique et enjeux économiques Responsabilité de l'éditeur et de l'hébergeur du site *Web* Mentions légales et conditions générales d'utilisation d'un site *Web* Réglementation en matière de collecte, de traitement et

		de conservation des données à caractère personnel Droit d'utilisation des contenus externes Nom de domaine : formalisme, organismes d'attribution et de gestion, conflits et résolution
Travailler en mode projet ▪ Analyser les objectifs et les modalités d'organisation d'un projet ▪ Planifier les activités ▪ Évaluer les indicateurs de suivi d'un projet et analyser les écarts	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.	<u>Savoirs technologiques</u> Planification de projet : approche prédictive et séquentielle, approche agile. Outil de gestion de projet : fonctionnalités et paramétrage
Mettre à disposition des utilisateurs un service informatique ▪ Réaliser les tests d'intégration et d'acceptation d'un service ▪ Déployer un service ▪ Accompagner les utilisateurs dans la mise en place d'un service	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.	<u>Savoirs technologiques</u> Service informatique : prestations, moyens techniques, rôles des parties prenantes Principes d'architecture d'un service Services et protocoles réseaux standard et de base Techniques et outils de déploiement des services informatiques

	Les modalités d'accompagnement sont définies. Le service déployé est opérationnel et donne satisfaction à l'utilisateur.	Techniques et outils de test des services informatiques
Organiser son développement professionnel ▪ Mettre en place son environnement d'apprentissage personnel ▪ Mettre en œuvre des outils et stratégies de veille informationnelle ▪ Gérer son identité professionnelle ▪ Développer son projet professionnel	Les besoins de formation sont identifiés pour assurer le support ou mettre à disposition un service. 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 ; - d'utiliser de manière approfondie des moyens de recherche d'information ; - de renforcer de ses compétences. L'identité professionnelle est pertinente et visible sur un réseau social professionnel.	<u>Savoirs technologiques</u> 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) Veille informationnelle et curation : sources d'information, stratégies et outils. Panorama des métiers de l'informatique

Bloc de compétences n°2 option B « Solutions logicielles et applications métiers » - Conception et développement d'applications

Conditions de réalisation et ressources nécessaires

Contexte

La personne titulaire du diplôme exerce des activités de conception et de développement d'applications pour répondre aux besoins d'une organisation cliente. Elle travaille pour le compte de l'entité informatique interne à une organisation cliente, entreprise de services du numérique, une société de conseil en technologies ou encore 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 met en œuvre l'environnement technologique nécessaire à la conception et au développement des applications informatiques : environnement de développement, de tests, outil collaboratif de suivi et de gestion des versions ou encore système de gestion de bases de données.

Ressources

- Description de l'organisation cliente : son métier, ses processus, ses acteurs (internes et externes) et son système d'information.
- Description du prestataire informatique de l'organisation cliente : ses compétences, ses méthodes, ses outils, ses procédures et référentiels.
- Description du système informatique de l'organisation cliente : infrastructure de communication, cartographie des applications, règles de sécurité.
- Référentiels, normes, réglementations, chartes, standards et méthodes mobilisées dans le cadre d'un développement informatique.
- Contrat de prestation de services.
- Environnement de conception d'applications opérationnel et conforme à l'environnement technologique décrit dans l'annexe II.E du diplôme.
- Outils de génération et rétro-conception de base de données, de correspondance (*mapping*) objet-relationnel, de modélisation et de maquettage.
- Cahier des charges fourni par l'organisation cliente (avec les spécifications fonctionnelles et éventuellement techniques du service à concevoir).
- Cadre du développement de l'application : cadre applicatif (*framework*) retenu, bibliothèque de composants spécifiques, schéma de données spécifique.

Degré d'autonomie, responsabilités

La personne titulaire du diplôme est en charge de la conception et de la programmation de composants applicatifs ainsi que de la gestion des données

persistantes nécessaires à la production ou à la maintenance d'une solution logicielle. En lien avec différents interlocuteurs, elle participe aux spécifications techniques et fonctionnelles de l'application et s'adapte au contexte technologique et organisationnel de l'organisation cliente. Sa veille technologique lui permet de choisir les technologies pertinentes pour implémenter les fonctionnalités techniques qui lui ont été confiées, dans le respect de la législation en vigueur et des principes éthiques de la profession. La personne titulaire du diplôme rend compte de ses activités à son responsable ou au client final. Elle assure des activités de formation auprès des utilisateurs et leur fournit une documentation d'utilisation du service développé ou amélioré.		
Compétences	**Indicateurs de performance**	**Savoirs associés**
Concevoir et développer une solution applicative ▪ Analyser un besoin exprimé et son contexte juridique ▪ Participer à la conception de l'architecture d'une solution applicative ▪ Modéliser une solution applicative ▪ Exploiter les ressources du cadre applicatif (*framework)* ▪ Identifier, développer, utiliser ou adapter des composants logiciels ▪ Exploiter les technologies *Web* pour mettre en œuvre les échanges entre applications, y compris de mobilité ▪ Utiliser des composants d'accès aux données ▪ Intégrer en continu les versions d'une	La proposition de la solution applicative répond au besoin exprimé dans le cahier des charges y compris dans sa dimension contractuelle : - 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	<u>Savoirs technologiques</u> 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 Composition du coût d'une solution applicative Interfaces homme-machine : principes ergonomiques, techniques de conception, d'évaluation et de validation. Concepts de la programmation objet : classe, objet, abstraction, interface, héritage, polymorphisme, annotations, patrons de conception, interface de programmation d'applications Concepts de la programmation événementielle : techniques de gestion des événements et exploitation de

solution applicative ▪ Réaliser les tests nécessaires à la validation ou à la mise en production d'éléments adaptés ou développés ▪ Rédiger des documentations technique et d'utilisation d'une solution applicative ▪ Exploiter les fonctionnalités d'un environnement de développement et de tests	correspondance objet-relationnel ou toute autre solution de persistance. La solution est développée dans les règles de l'art : - 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.	bibliothèques de composants graphiques Programmation au sein d'un cadre applicatif (*framework)* : structure, outil d'aide au développement et de gestion des dépendances, techniques d'injection des dépendances Architectures et techniques d'interopérabilité entre applications. Caractéristiques des formats de données : structurées ou non Persistance et couche d'accès aux données Techniques et outils de documentation. Techniques de gestion des erreurs et des exceptions Fonctionnalités d'un outil de gestion de projets. Concepts et techniques de développement agile Fonctionnalités avancées d'un environnement de développement. Techniques de gestion de versions Techniques et outils d'intégration continue Techniques et outils de tests et d'intégration de composants logiciels
Assurer la maintenance corrective ou évolutive d'une solution applicative ▪ Recueillir, analyser et mettre à jour les informations sur une version d'une solution applicative ▪ Évaluer la qualité d'une solution applicative	L'évolution de la solution applicative répond aux besoins exprimés dans le cahier des charges. 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	<u>Savoirs économiques, juridiques et managériaux</u> Contraintes éthiques et environnementales dans la conception d'une solution applicative Cahier des charges et ses enjeux juridiques Contrat de développement et de maintenance applicative (formation, exécution, inexécution) et ses clauses spécifiques

▪ Analyser et corriger un dysfonctionnement ▪ Mettre à jour des documentations technique et d'utilisation d'une solution applicative ▪ Élaborer et réaliser les tests des éléments mis à jour	contraintes ergonomiques. Un outil collaboratif de gestion des versions est utilisé. 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. 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. Les tests de non régression sont réalisés. Les composants logiciels sont documentés de manière à être réutilisés. 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.	Réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel Responsabilité civile et pénale du concepteur de solutions applicatives Protection juridique des productions de solutions applicatives : droit d'auteur, modes de protection indirects et conditions de brevetabilité Typologie des licences logicielles et droits des utilisateurs
Gérer les données ▪ Exploiter des données à l'aide d'un langage de requêtes ▪ Développer des fonctionnalités	L'exploitation des données permet de construire l'information attendue. Les accès aux données sont contrôlés conformément	<u>Savoirs technologiques</u> Typologie des bases de données Caractéristiques des formats de données structurées ou non

applicatives au sein d'un système de gestion de base de données (relationnel ou non) ▪ Concevoir ou adapter une base de données ▪ Administrer et déployer une base de données	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.	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 de définition des données, des contraintes et de contrôle des données. Langage et outils de manipulation et d'interrogation d'une base de données Langage d'automatisation des actions dans une base de données 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. Modèles de référence de représentation des données. Méthodes et outils de modélisation des données. <u>Savoirs économiques, juridiques et managériaux</u> 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

Bloc de compétences n°3 - Cybersécurité des services informatiques

Conditions de réalisation et ressources nécessaires

Contexte

La personne titulaire du diplôme exerce des activités pour répondre aux besoins de sécurité des services informatiques d'une organisation cliente notamment au regard du développement des menaces et attaques en provenance du cybermonde et des risques liés aux usages numériques. Elle travaille pour le compte de l'entité informatique interne à 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 participe à la mise en œuvre de l'environnement technologique nécessaire à la sécurité des services informatiques.

Ressources

- Description de l'organisation cliente : son métier, le caractère sensible des activités conduites, ses processus, ses acteurs (internes et externes) et son système d'information.
- Description du prestataire informatique de l'organisation cliente : ses compétences, ses méthodes, ses outils, ses procédures et ses référentiels.
- Description du système informatique de l'organisation cliente : infrastructure de communication, cartographie des applications, règles de sécurité et de sûreté.
- Référentiels, normes, réglementations, chartes, standards et méthodes mobilisées dans le cadre de la mise à disposition d'un service sécurisé.
- Contrat de prestation de services.
- Environnement de production opérationnel et conforme à l'environnement technologique décrit dans l'annexe II.E du diplôme.
- Cahier des charges fourni par l'organisation cliente : spécifications fonctionnelles et éventuellement techniques, définition du périmètre d'intervention, exigences en termes de protection des données, des applications et des équipements.

Degré d'autonomie, responsabilités

La personne titulaire du diplôme participe à la mise en œuvre de la politique de gestion de la sécurité informatique de l'organisation cliente, en veillant à documenter ses actions. Elle travaille dans un périmètre donné en respectant les méthodes, normes et standards qui prévalent au sein de cette organisation.

Elle participe notamment à l'information et à la sensibilisation des utilisateurs aux risques en recommandant les pratiques adaptées. Elle contribue à la sécurisation des accès aux services informatiques : protection des accès aux ressources numériques, aux données, aux équipements et aux applications. En fonction de sa spécialité, elle intervient plus particulièrement sur la sécurité des infrastructures ou des développements d'application.

Dans une petite structure, elle peut travailler en autonomie en tenant compte des risques spécifiques identifiés pour l'organisation cliente. Elle prend en charge l'information, la sensibilisation et la formation des utilisateurs aux questions de sécurité informatique.

Dans une structure plus importante, elle travaille au sein d'une équipe en rendant compte de ses activités.

Compétences	**Indicateurs de performance**	**Savoirs associés**
Protéger les données à caractère personnel ▪ 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	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 à caractère personnel en tenant compte des risques identifiés.	<u>Savoirs technologiques</u> Typologie des risques et leurs impacts. Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve. Sécurité et sûreté : périmètre respectif. 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. Sécurité des communications numériques : rôle des protocoles, segmentation, administration, restriction

Préserver l'identité numérique de l'organisation ▪ Protéger l'identité numérique d'une organisation ▪ Déployer les moyens appropriés de preuve électronique	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.	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.
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	Des supports de communication interne sont accessibles aux utilisateurs et adaptés à leurs destinataires. 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.	<u>Savoirs économiques, juridiques et managériaux</u> Les données à caractère personnel : définition, réglementation, rôle de la CNIL. L'identité numérique de l'organisation : risques et protection juridique. Droit de la preuve électronique. La sécurité des équipements personnels des utilisateurs et de leurs usages : prise en compte des nouvelles modalités de travail, rôle de la charte informatique. Les risques des cyberattaques pour l'organisation : économique, juridique, atteinte à l'identité de l'entreprise. Obligations légales de notification en cas de faille de sécurité. Réglementation en matière de lutte contre la fraude informatique : infractions, sanctions. Les organisations de lutte contre la cybercriminalité.

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

Option SLAM **Assurer la cybersécurité d'une solution applicative et de son développement** ▪ 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	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.	<u>Savoirs technologiques</u> 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. <u>Savoir économique, juridique et managérial</u> Responsabilité du concepteur de solutions applicatives.