Référentiel de certification RNCP

Développeur de solutions numériques sécurisées

Intitulé : Développeur de solutions numériques sécurisées, **niveau 6**

Prérequis (hors VAE) :

- ⇨ Pour un public formation initiale ou alternance : Niveau 4 pour une entrée en 1ere année ou niveau 5 (avec une dominante scientifique et/ou informatique) pour une entrée en 2eme année.
- ⇨ Pour un public en reconversion : un niveau 4 au minimum, en informatique, si autre spécialité : réalisation d'un test de positionnement pour évaluer les connaissances préalables dans le domaine scientifique.

REFERENTIELS – ACTIVITES / CERTIFICATION

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
<u>BLOC 1</u> : Analyser un besoin, conceptualiser et maquetter une solution numérique, et établir la planification et le plan de sécurisation de la solution **A1. Analyse technique des besoins de sécurisation** • Activité de veille / technique / juridique / concurrentielle • Analyse ou rédaction d'un cahier des charges **A2. Conceptualisation d'une solution logicielle** • Exploration des solutions logicielles possibles • Maquettage de l'interface utilisateur	**C1 - Organiser un système de veille** en termes juridique, technique, concurrentiel, écologique, et de sécurité, en identifiant les ressources et les bonnes pratiques afin d'être force de proposition et d'anticiper les opportunités de développement et de sécurisation des projets. **C2** - **Analyser** les besoins des parties prenantes du projet afin d'élaborer ou de valider un cahier des charges fonctionnel et technique, en identifiant et en ayant une bonne compréhension des risques et menaces numériques auxquels la solution va être exposée. **C3** – **Conceptualiser** une solution adaptée aux usages des utilisateurs finaux, intégrant les enjeux de sécurité identifiés (*secure by design*) en mettant en place une méthode de travail collective favorisant la créativité (design thinking, approche de design, lean startup), en prenant en compte les problématiques d'accessibilité à la solution pour tous les publics, y compris en situation de handicap, afin d'explorer toutes les possibilités et de répondre aux besoins des utilisateurs finaux **C4 – Concevoir** la maquette de la solution envisagée, en respectant le cahier des charges afin de répondre aux besoins des parties prenantes et prendre en compte les exigences légales et de sécurité (respect de la vie privée,	**M1. Mise en situation professionnelle à partir de :** • **Un projet fictif ou réel :** proposé par une entreprise, un formateur ou par les apprenants eux-mêmes, en réponse à une problématique donnée. **Ou** • **Une étude de cas :** issue d'une situation réelle, dont l'objectif est de réaliser une solution logicielle équivalente à une solution existante, ou de proposer une solution plus évoluée, afin de répondre à une problématique donnée. Dans les deux cas, le candidat doit réaliser une analyse des besoins, passer par une phase d'idéation et conceptualiser une solution à mettre en place**.** En mettant en place une méthodologie de gestion et de pilotage de son projet. Ce travail peut être réalisé individuellement ou en équipe mais évalué individuellement. Ce projet fait l'objet d'une restitution écrite et d'une restitution orale devant un jury d'évaluation.	- (C1) Une veille et une analyse de l'existant sont réalisées. Les textes ayant un impact sur le domaine sont identifiés. Une analyse de l'impact est réalisée. - (C2, C4) L'expérience utilisateur est prise en compte (le choix de la langue, de la devise, …). Un persona est établi, et ses caractéristiques sont analysées et prises en compte. - (C1, C4) Prise en compte des aspects juridiques, techniques, concurrentiels, écologiques, et de sécurité, en lien avec la solution à développer. - (C2) Les parties prenantes sont identifiées, et leurs besoins analysés à l'aide des outils d'exploration adéquats. - (C3) Une méthodologie permettant la prise en compte des attentes des utilisateurs finaux et de l'inclusion a été déterminée. L'ergonomie et les fonctionnalités sont adaptées à la méthodologie décrite. Les dispositions prises pour permettre l'accessibilité des informations prennent en compte les bonnes pratiques des normes WCAG et RGAA. - (C2, C4) Les fonctionnalités principales, répondant aux besoins sont identifiées et le choix est justifié.

A3. Mise en place du projet de solution logicielle • Elaboration d'un plan de sécurisation • Planification du projet de développement	sécurisation des interfaces en limitant la surface d'attaques possibles). **C5 – Elaborer** un plan de sécurisation et de réduction du risque, en analysant les risques de sécurité identifiés dans les systèmes utilisés, y compris dans les dispositifs spécifiques (applications d'accessibilités ou les dispositifs de communication utilisés par les personnes en situation de handicap), afin de préconiser des évolutions et des solutions correctives **C6 – Planifier** le projet de développement, en ordonnant et en organisant les étapes de développement, et en mettant en place un environnement de pilotage d'un projet de développement en répartissant les responsabilités et les tâches en fonction des compétences disponibles, tout en prenant les dispositions nécessaires pour permettre aux membres de l'équipe projet en situation de handicap de réaliser ces tâches, afin de répondre aux exigences des parties prenantes en optimisant les délais, les coûts et l'efficacité collective.	**M2. Evaluation en contrôles continus** En parallèle, des contrôles sont effectués sous forme de contrôles continues ou de travaux pratiques portant sur : - La conceptualisation d'une solution logicielle - La prise en compte de la sécurité dans un projet	- (C4) Une maquette est réalisée en utilisant des outils adaptés. - (C5) Les enjeux de sécurité sont identifiés et analysés (vulnérabilité, …). - (C5) Des recommandations de sécurisation et de réduction du risque identifié sont proposées. Une première liste est dressée avec les recommandations associées. - (C6) Un planning du projet de développement, ainsi que des activités sont mis en place. Les méthodologies et les outils adaptés à la gestion de projets sont définis et utilisées. La répartition des tâches est adaptée aux ressources allouées et les dispositions nécessaires pour l'inclusion des membres de l'équipe projet en situation de handicap sont prises, le cas échéant.
<u>BLOC 2</u> : Concevoir, développer, mettre en production et maintenir une solution numérique **A4. Choix des outils et technologies** • Choix des technologies adaptées à la réalisation de la solution logicielle • Modélisation et conception de la solution logicielle	**C7- Sélectionner** les technologies et les données adaptées à la réalisation de la solution logicielle, en prenant en compte l'infrastructure nécessaire et les enjeux liés à la sécurité, afin de répondre aux exigences des parties prenantes et de la solution à développer. **C8- Concevoir** la solution, en identifiant les différents éléments qui la composent et leurs interactions, tout en définissant les actions à mettre en place pour sécuriser les échanges de données, en définissant les modalités d'accessibilité à la solution pour tous les publics, y compris en situation de handicap, et en identifiant les moyens de réduire la consommation énergétique d'un programme afin de garantir la pérennisation et la sécurisation de	**M3. Mise en situation professionnelle à partir de :** • **Un projet fictif ou réel :** proposé par une entreprise, un formateur ou par les apprenants eux-mêmes, en réponse à une problématique donnée. **Ou** • **Une étude de cas :** issue d'une situation réelle, dont l'objectif est de réaliser une solution logicielle équivalente à une solution existante, ou de proposer une solution plus évoluée, afin de répondre à une problématique donnée. **Dans les deux cas, l'apprenant doit :** - Choisir les technologies appropriées, concevoir et développer la solution	- (C7) Les technologies sélectionnées sont adaptées pour la réalisation de la solution. - (C7) L'architecture et les infrastructures choisies sont adaptées aux besoins présents et futurs de la solution. - (C7, C8, C9) Le choix des bibliothèques et/ou frameworks techniques est justifié et est adapté aux besoins présents et futurs de la solution. - (C8) La conception du programme intègre la sécurisation de la solution. - (C8) La conception de la solution comprend des modalités techniques conformes au référentiel général d'amélioration de l'accessibilité (RGAA) : les critères relatifs aux images, cadres, couleurs, multimédia, tableaux, liens, scripts, éléments obligatoires, structuration de l'information,

A5. Développement de la solution logicielle • Ecriture du code • Test et vérification de la solution développée • Validation de la solution développée et recette **A6. Mise en production et réalisation de la maintenance de la solution logicielle** • Déploiement de la solution • Réalisation de la maintenance corrective et évolutive de la solution • Réalisation de la maintenance corrective et évolutive de la sécurité de la solution	la solution et de simplifier les évolutions futures. **C9- Développer et intégrer** les différents éléments qui composent la solution, en écrivant son propre code, et en utilisant des librairies et/ou des frameworks existants**,** en prenant les précautions nécessaires vis-à-vis des outils et services tiers, afin de livrer une solution fonctionnelle, sécurisée et respectant les standards du métier. **C10- Tester** la solution, en réalisation des tests unitaires et fonctionnels, dans des environnements maîtrisés et reproductibles (Dev et préprod), afin de garantir le bon fonctionnement de la solution avant sa livraison. **C11- Préparer** la documentation nécessaire, afin de permettre aux parties prenantes de tester, valider et d'effectuer la recette de la solution**.** **C12- Déployer** la solution, en élaborant et en mettant en place un plan de déploiement dans un environnement de production, comprenant la mise en œuvre des processus d'intégration et de déploiement continue (CI /CD), afin de prévoir la maintenance évolutive et sécuritaire de la solution. **C13**- **Mettre en œuvre** la maintenance évolutive, corrective, en réaction à des bugs identifiés par les utilisateurs ou à des demandes d'évolution, afin de garantir une solution fonctionnelle au regard des évolutions d'usage. **C14**- **Assurer** un traitement continu des vulnérabilités, en déployant des éléments de sécurité (patchs correctifs, mises à jour, protocoles, …), afin de garantir une sécurité permanente et optimale de la solution.	- Tester la solution de point de vue fonctionnelle et de sécurité - Déployer et documenter la solution - Assurer un traitement continu des vulnérabilités de sécurité Ce travail peut être réalisé individuellement ou en équipe mais évalué individuellement. Ce projet fait l'objet d'une restitution écrite et d'une restitution orale devant un jury d'évaluation. **M4. Evaluation en contrôles continus** En parallèle, des contrôles sont effectués sous forme de contrôles continus ou de travaux pratiques portant sur les différents éléments qui constituent le cycle de vie de développement et de sécurisation d'une solution logicielle.	présentation de l'information, formulaires, navigation, consultation, sont pris en compte de manière adaptée à la nature du projet et des besoins des utilisateurs. - (C8) Le projet intègre l'efficacité énergétique comme critère de qualité : il limite le nombre de calcul, il privilégie les technologies permettant des traitements plus rapides et moins énergivores. - (C11) Une documentation technique des différentes versions du code est établie en respectant les pratiques de rédaction de la réglementation en vigueur (entrée sortie, règles de nommage, règles de versionnage, nom de l'auteur du programme, …). - (C10) Le code est testé et corrigé d'un point de vue fonctionnel. - (C9) Les écrans d'interface sont réalisés et répondent aux contraintes du marché et des parties prenantes préalablement définies dans le cahier des charges. - (C9, C10, C12) La solution est conçue de manière agile (intégration, livraison et déploiement continue : CI/CD) à l'aide de système de contrôle de version (versionning). - (C9) Les échanges et les accès aux données sont sécurisés (reconnaissance d'empreinte, mot de passe, login, …). - (C10) Les écritures de tests unitaires et fonctionnels sont établies et répondent aux enjeux de sécurité. - (C10) La solution est déployée sur un serveur accessible par internet. - (C12) Le plan de déploiement de la solution est établi dans le respect des aspects sécuritaires préalablement définies. - (C12, C13, C14) Un plan de déploiement est établi et prend en compte la maintenance évolutive, corrective et sécurité de la solution mise en place.

BLOC 3 : Concevoir et mettre en œuvre des projets de développement, de modernisation et de sécurisation des solutions numériques intégrant des innovations technologiques **A7. Accompagnement des projets de développement, de modernisation et de sécurisation des outils de l'organisation** • Analyse du projet de développement pour identifier les opportunités d'intégration des technologies avancées et innovantes. • Adaptation de l'architecture de la solution en vue de l'intégration des innovations identifiées. • Préconisation des évolutions nécessaires pour maintenir la sécurité de la solution, durant le processus d'intégration de l'innovation. **A8. Sensibilisation des parties prenantes aux enjeux de sécurité** • Accompagnement des parties prenantes dans l'appréhension des enjeux de l'innovation intégrée et des enjeux de sécurité induits	**C15- Identifier** l'opportunité et la pertinence de faire appel à des technologies avancées et innovantes (Cybersécurité, IA, VR, Blockchain …), en étudiant leur faisabilité et en analysant les enjeux de sécurité associés, afin d'apporter de la valeur ajoutée pour le produit ou la partie prenante. **C16- Proposer** une architecture adéquate, pour intégrer des technologies et des usages innovants en respectant une éthique de développement durable, en analysant et en étudiant les différentes possibilités, afin d'assurer la cohérence de la solution finale au regard des différents modules qui la composent. **C17- Faire évoluer** la sécurité de la solution au regard des innovations technologiques introduites en améliorant les règles de sécurisation ou en apportant des solutions de sécurisation innovantes, afin de rester en adéquation avec la stratégie de sécurité des parties prenantes. **C18- Sensibiliser** les différentes parties prenantes du projet aux impacts et risques liés à l'intégration d'une innovation technologique ou d'usage dans la solution, en les accompagnant dans les différentes phases du projet, et en veillant à communiquer sur les enjeux de l'accessibilité aux personnes en situation de handicap et de confidentialité, afin de s'assurer de l'intégration des bonnes pratiques.	**M5. Mise en situation professionnelle à partir de :** • **Un projet fictif ou réel :** proposé par une entreprise, un formateur ou par les apprenants eux-mêmes, en réponse à une problématique donnée. **Ou** • **Une étude de cas :** issue d'une situation réelle, dont l'objectif est de réaliser une solution logicielle équivalente à une solution existante, ou de proposer une solution plus évoluée, afin de répondre à une problématique donnée. **Dans les deux cas, l'apprenant doit :** - Présenter un dossier d'étude de faisabilité de la solution Ce travail peut être réalisé individuellement ou en équipe mais évalué individuellement. Ce projet fait l'objet d'une restitution écrite et d'une restitution orale devant un jury d'évaluation. **M6. Evaluation en contrôles continus** En parallèle, des contrôles sont effectués sous forme de contrôles continus ou de travaux pratiques portant la capacité d'identifier les innovations adaptées à intégrer dans le projet et de les mettre en œuvre en maintenant la sécurité globale du système.	- (C15) Les tendances émergentes de la tech (RV, IA, cybersécurité, …) sont identifiées. - (C15-C16) Des technologies innovantes adaptées à la solution sont intégrées au projet (objets connectés, reconnaissance faciale, …). - (C15) Les enjeux de sécurité associés à ces nouvelles tendances/technologies sont identifiés et analysés (protection et intégrité des données, identification, …). - (C16) Les différentes architectures techniques possibles pour le projet sont analysées et comparées. - (C16) Les critères de comparaison sont identifiés et adaptés au projet. L'architecture retenue est justifiée, répond aux critères préalablement établis et respecte une éthique de développement durable. - (C17) La solution proposée respecte les exigences de sécurité des parties prenantes (respect de la vie privé des salariés d'une entreprise, nécessité de la double authentification, …). - (C17) La solution est en adéquation avec le cadre réglementaire (RGPD, RSE, CNIL, ...). - (C18) Un plan de sensibilisation des parties prenantes est prévu. Les actions mises en place sont adaptées aux parties prenantes identifiées. Elles comprennent la sensibilisation aux enjeux d'accessibilité aux personnes en situation de handicap, en s'appuyant sur les bonnes pratiques du RGAA et, le cas échéant, en appliquant les normes internationales WCAG. - (C18) La sensibilisation des parties prenantes est mesurée avec les outils adaptés (satisfaction, …).

Pour obtenir la certification, outre la validation des 3 blocs de compétences, la rédaction et la soutenance d'un mémoire professionnel est obligatoire.

Ce mémoire professionnel consiste à la description et l'analyse des missions réalisées en entreprise (Apprentissage ou Stage).

Ce travail est encadré par un tuteur école ainsi que par un tuteur professionnel (Maitre d'Apprentissage ou tuteur entreprise). En fonction du degré de confidentialité, les mémoires professionnels peuvent faire l'objet d'une version restreinte (accessible uniquement aux membres du jury), accompagnée d'une version publique qui est systématiquement déposée sur la plateforme pédagogique de l'école à l'issue de la soutenance.
Le mémoire professionnel est présenté en fin de cursus devant un jury de professionnels qui inclut l'équipe pédagogique et un professionnel expérimenté ayant au moins 5 ans d'expérience dans le domaine informatique). Le candidat présente son travail devant le jury (environ 20 minutes) et c'est d'un suivi d'une session de questions/réponses. A l'issue de cette séance, le jury délibère sur la note finale en prenant en compte la qualité du rapport écrit ainsi que de la présentation orale selon une grille d'évaluation préétablie.

Le candidat désirant obtenir la certification par la voie de la VAE devra faire la preuve qu'il a acquis les compétences de chacun des blocs de compétences sur la base d'un livret de preuves présenté oralement devant le jury.