

Développeur de solutions numériques sécurisées

RNCP37778 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326t
Formacode(s)	31067, 31006
Code(s) ROME	M1805
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	19/07/2023
Date d'échéance	19/07/2026

Certificateur(s)

ESIEE IT - CCI PARIS ILE DE FRANCE · SIRET : 88931074400020

Partenaires habilités

5 organismes habilités, d'après la liste publiée par France compétences : 5 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
CHAMBRE COMMERCE ET INDUSTRIE VAUCLUSE	18840001400018	Former et organiser l'évaluation
CHAMBRE COMMERCE & INDUSTRIE HTE SAVOI	18743001200067	Former et organiser l'évaluation
CHAMBRE DE COMMERCE ET D'INDUSTRIE MARSEILLE-PROVENCE	18130002100019	Former et organiser l'évaluation
ESIEE IT - CCI PARIS ILE DE FRANCE	88931074400038	Former et organiser l'évaluation
ESIEE IT - CCI PARIS ILE DE FRANCE	88931074400061	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le risque cyber a considérablement augmenté ces dernières années, en particulier depuis le début du Covid-19, concomitant à la numérisation des processus et du mode de travail, dans tous les secteurs. La cybersécurité doit donc suivre et faire face à ce mouvement afin de protéger les installations sur notre territoire: hôpitaux, sites industriels...Le développeur de solutions numériques sécurisées, ou développeur sécurité, est celui qui analyse les menaces et les besoins en cybersécurité qui en découlent afin de pouvoir développer des logiciels et applications sûrs. Sa mission est donc particulièrement sensible au sein de l'entreprise et du service IT.

ACTIVITÉS VISÉES

- Analyser un besoin, conceptualiser et maquetter une solution numérique, et établir la planification et le plan de sécurisation de la solution
 - o Analyse technique des besoins de sécurisation
 - o Conceptualisation d'une solution logicielle
 - o Mise en place du projet de solution logicielle

- Concevoir, développer, mettre en production et maintenir une solution numérique
 - o Choix des outils et technologies
 - o Développement de la solution logicielle
 - o Mise en production et réalisation de la maintenance de la solution logicielle
- Concevoir et mettre en œuvre des projets de développement, de modernisation et de sécurisation des solutions numériques intégrant des innovations technologiques
 - o Accompagnement des projets de développement, de modernisation et de sécurisation des outils de l'organisation
 - o Sensibilisation des parties prenantes aux enjeux de sécurité

COMPÉTENCES ATTESTÉES

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.

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.

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

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, sécurisation des interfaces en limitant la surface d'attaques possibles).

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

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

Sélectionner les technologies et les données adaptées à la réalisation de la solution numérique sécurisée, 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.

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 la solution et de simplifier les évolutions futures

Développer et intégrer les différents éléments qui composent la solution, en écrivant son propre code, et en utilisant des bibliothèques 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

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

Préparer la documentation nécessaire, afin de permettre aux parties prenantes de tester, valider et d'effectuer la recette de la solution

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

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

Assurer un traitement continu des vulnérabilités, en déployant des éléments de sécurité (patches correctifs, mises à jour, protocoles, ...), afin de garantir une sécurité permanente et optimale de la solution

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

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

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

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

Blocs de compétences

RNCP37778BC01 — Analyser un besoin, conceptualiser et maquetter une solution numérique, et établir la planification et le plan de sécurisation de la solution

LISTE DE COMPÉTENCES

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.

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.

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

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, sécurisation des interfaces en limitant la surface d'attaques possibles).

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

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

MODALITÉS D'ÉVALUATION

Etude de cas / mise en situation professionnelle.

Evaluation en contrôles continus.

RNCP37778BC02 — Concevoir, développer, mettre en production et maintenir une solution numérique

LISTE DE COMPÉTENCES

Sélectionner les technologies et les données adaptées à la réalisation de la solution numérique sécurisée, 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.

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 la solution et de simplifier les évolutions futures.

Développer et intégrer les différents éléments qui composent la solution, en écrivant son propre code, et en utilisant des bibliothèques 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.

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.

Préparer la documentation nécessaire, afin de permettre aux parties prenantes de tester, valider et d'effectuer la recette de la solution.

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.

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.

Assurer un traitement continu des vulnérabilités, en déployant des éléments de sécurité (patches correctifs, mises à jour, protocoles, ...), afin de garantir une sécurité permanente et optimale de la solution.

MODALITÉS D'ÉVALUATION

Etude de cas / mise en situation professionnelle.

Evaluation en contrôles continus.

RNCP37778BC03 — Concevoir et mettre en œuvre des projets de développement, de modernisation et de sécurisation des solutions numériques intégrant des innovations technologiques

LISTE DE COMPÉTENCES

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.

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.

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.

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.

MODALITÉS D'ÉVALUATION

Etude de cas / mise en situation professionnelle.

Evaluation en contrôles continus.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le développeur de solutions numériques sécurisées peut travailler dans toute entreprise développant des produits informatiques. Il peut exercer son métier aussi bien dans une ESN (Entreprise de services du numérique) et être envoyé chez des clients, dans une start-up lançant un tout nouveau produit, ou encore choisir d'intégrer un grand groupe ayant besoin de ses propres développeurs en interne, quel que soit le secteur.

TYPE D'EMPLOIS ACCESSIBLES

Développeur sécurité - Développeur Cybersécurité - Développeur de solutions numériques sécurisées - Développeur de solutions de sécurité - SysOps & Security - Post auditeur en sécurité des systèmes d'information -

Auditeur en sécurité des systèmes d'information - Expert en test d'intrusion /sécurité des systèmes d'information

RÈGLEMENTATIONS D'ACTIVITÉ

L'accès au métier n'est pas réglementé. Néanmoins, dans l'exercice de ses fonctions, le développeur de solutions

numériques sécurisées est tenu de respecter un cadre réglementaire. Dans le cadre de ses activités et notamment pour la partie conception et sécurisation des applications, le développeur de solutions numériques sécurisées est soumis au respect du RGPD permettant la protection des données personnelles. Dans la rédaction du cahier des charges et dans le maquettage de l'interface utilisateur, il doit prendre en compte le référentiel général d'amélioration de l'accessibilité (RGAA).

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Très élevée (5/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 4 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 864 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	27 458
Jugés difficiles à recruter	53 %
Emplois saisonniers	1 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

- Pour un public formation initiale ou alternance : Niveau 4 pour une entrée en 1ère année ou niveau 5 (avec une dominante scientifique et/ou informatique) pour une entrée en 2ème 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.

PRÉREQUIS À LA VALIDATION

Pour pouvoir se présenter aux épreuves de certification, le candidat doit satisfaire aux exigences suivantes :

- avoir été assidu en formation
- avoir participé aux évaluations de contrôle continu.

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE

Le jury est composé au minimum de 4 personnes, parmi lesquelles :

- Au minimum deux professionnels dont 1 représentant des salariés de la profession et 1 représentant des employeurs de la profession. Le président du jury est choisi parmi eux.
- Un rapporteur (le responsable pédagogique de la promotion)
- Le responsable de la certification professionnelle (ou son représentant).

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	9 475 €
Selon la branche	7 000 € – 12 000 €
Prise en charge	Branches concernées
9 475 €	Valeur par défaut · 175 branches
12 000 €	CPNE Entreprises des activités du déchet et de la propreté urbaine, CPNE autoroutes, CPNE de l'ingénierie, des services informatiques et du conseil, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNEF de la Branche des organismes de formation
11 055 €	CPNE Transport aérien : personnel au sol, CPNEFP de l'enseignement privé indépendant, CPNEFP de la Restauration rapide
9 500 €	CPNE Branche Caisse d'Epargne, CPNE de la branche Banque Populaire
8 990 €	CPNEF branche retraite complémentaire et prévoyance, CPNEFP Mutualité
7 923 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
7 353 €	CPNEFP de la branche professionnelle des Entreprises du courtage d'assurances et/ou réassurances, CPNFPE des sociétés d'assurances
7 000 €	CPNE chimie, CPNEFP de la métallurgie
11 845 €	CPNE des Télécoms
11 844 €	CPNE Travail Temporaire
11 601 €	CPNE de la branche de la Distribution Directe
10 500 €	CPNEFP des industries des tuiles et briques
9 672 €	CPNEFP de la Mutualité Sociale Agricole
9 480 €	CPNEF de l'audiovisuel
9 000 €	CPNEFP de la branche des prestataires de services du secteur tertiaire
8 285 €	CPNEFP Commerce à distance
8 057 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 036 €	CPNE FP Branche des magasins du Bricolage
8 029 €	CPNEFP des jardineries et graineteries
7 585 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
7 300 €	CPNE Banque

Base légale

Date de décision	19/07/2023
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	19/07/2026
Date de dernière délivrance possible	19/07/2030

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP42620

CORRESPONDANCES (PAR BLOCS)
RNCP36490, RNCP38038

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.esi-ee-it.fr/fr/formation-bac3-entree-l3-developpeur-de-solutions-numeriques-securisees-parcours-cybersecurite-en>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/37778/>

Se former en apprentissage

Formations en apprentissage	4
Organismes gestionnaires (CFA)	2
Organismes formateurs	3
Régions couvertes	2
Départements couverts	2
Organismes certifiés Qualiopi	3
Sessions	de 09/2024 à 07/2029

Catalogue des formations en apprentissage — réseau des Carif-Oref. Sans frais pour l'alternant : formation financée par l'OPCO de la branche (NPEC).

Demande CPF — formations engagées

Dossiers CPF engagés	1
Montant total engagé	3 500 €
Coût moyen par dossier	3 500 €
Durée moyenne	90 h
Période	10/2025
France compétences	100 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.