

Développeur de solutions numériques sécurisées

RNCP42620 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326t
Formacode(s)	31067, 31006
Code(s) ROME	M1805, M1801, M1810, M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	17/07/2026
Date d'échéance	17/07/2029

Certificateur(s)

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

Partenaires habilités

3 organismes habilités, d'après la liste publiée par France compétences : 3 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
CHAMBRE COMMERCE ET INDUSTRIE VAUCLUSE	18840001400018	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

La généralisation des usages numériques, combinée à la montée des menaces cyber, renforce la nécessité pour les organisations de disposer de professionnels capables d'intégrer la sécurité dès la conception des solutions informatiques. Les exigences réglementaires et normatives en matière de protection des données et de sécurité des systèmes d'information accentuent encore cette demande.

La certification «?Développeur de Solutions Numériques Sécurisées?» a pour objectif de valider les compétences techniques permettant de concevoir, développer, sécuriser et maintenir des solutions numériques conformes aux bonnes pratiques de développement sécurisé et aux exigences de sécurité en vigueur.

À l'issue du parcours, le titulaire est en mesure de contribuer à des projets de développement de solutions numériques sécurisées au sein d'équipes techniques et dans des environnements variés. Il applique les règles de sécurité, de qualité et de conformité attendues d'un professionnel de niveau 6.

ACTIVITÉS VISÉES

Analyse des besoins et des risques de sécurité associés à la solution numérique

Clarification du besoin et du contexte d'usage/exploitation, incluant contraintes techniques, dépendances, parties prenantes et responsabilités.

Cartographie des actifs, du périmètre et des flux, avec classification/criticité, frontières de confiance, interfaces et points d'exposition.

Modélisation des menaces et évaluation/hiérarchisation des risques (scénarios d'attaque, impacts, probabilité, risques résiduels et priorités de traitement).

Formalisation des exigences fonctionnelles et de sécurité, critères d'acceptation et décisions de traitement du risque.

Conception d'une solution logicielle sécurisée

Définition de l'architecture cible et des choix de conception, intégrant les exigences de sécurité, les contraintes d'exploitation et les dépendances.

Conception des mécanismes de sécurité "by design", incluant gestion des identités et des accès, contrôle d'accès, chiffrement, protections applicatives...

Elaboration d'un plan de sécurisation, incluant schémas d'architecture, spécifications techniques, modèles de données et flux, critères de sécurité testables dans une logique DevSecOps.

Préparation et organisation du développement de la solution numérique.

Développement sécurisé de la solution numérique

Mise en œuvre des pratiques de développement, appliquant les standards de code sécurisé, les conventions d'architecture logicielle, et les règles de gestion d'erreurs.

Gestion sécurisée des dépendances et composants, incluant sélection/validation des bibliothèques et configuration sécurisée.

Traçabilité et production des preuves de conformité du développement, incluant documentation technique minimale, enregistrement des décisions/écarts, justification des compromis, et constitution des éléments de preuve nécessaires aux étapes de tests, de validation et d'audit.

Réalisation des tests de sécurité et validation avant mise en production

Définition de la stratégie de tests de sécurité et des critères de validation de la solution numérique.

Réalisation et automatisation des vérifications de sécurité, incluant tests applicatifs (DAST), tests sur APIs, contrôles des dépendances/containers, validation des configurations et analyses ciblées.

Conduite des investigations et tests approfondis, incluant reproduction des failles, analyse d'impact, priorisation et, le cas échéant, coordination de tests d'intrusion/évaluations externes.

Décision de validation pré-production, incluant reporting, mise à jour du backlog sécurité, vérification des correctifs, gestion des dérogations acceptées et constitution des preuves de conformité.

Intégration et déploiement sécurisés de la solution numérique.

Conception et sécurisation de la chaîne d'intégration et de déploiement (CI/CD).

Industrialisation des configurations et de l'infrastructure de déploiement de façon sécurisée.

Exécution des déploiements et mise en service sécurisée, incluant vérifications post-déploiement, validation de la configuration effective, activation de la journalisation/monitoring et gestion des accès.

Maintien en conditions opérationnelles sécurisées et gestion des vulnérabilités de la solution numérique

Maintenance et exploitation de la solution, incluant qualité de service (performance/disponibilité), supervision (observabilité) et sécurité.

Organisation et exécution du processus de gestion des vulnérabilités, incluant veille/alertes, qualification (sévérité, exploitabilité, impact), priorisation, planification des correctifs et gestion des dépendances.

Réalisation des actions de remédiation et de durcissement continu, et gestion des événements de sécurité.

Accompagnement des projets de développement, de modernisation et de sécurisation des outils de l'organisation intégrant les innovations technologiques

Cadrage et appui à la définition des trajectoires de modernisation incluant une technologie innovante.

Analyse de l'existant, identification des écarts (techniques, sécurité, conformité), priorisation et recommandation de scénarios.

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.

Sensibilisation des parties prenantes aux enjeux de sécurité

Analyse des profils de parties prenantes (métiers, IT, produit, direction, prestataires), de leurs interactions avec la solution et les principaux scénarios de risque

Ciblage des messages et des priorités de sensibilisation.

Conception de contenus et de dispositifs de sensibilisation adaptés, incluant supports et formats appropriés.

Animation d'actions de sensibilisation et accompagnement des comportements.

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, en les traduisant en exigences fonctionnelles, afin d'élaborer ou

de valider un cahier des charges fonctionnel et technique de la solution numérique à développer.

Modéliser les menaces et qualifier les exigences de sécurité de la solution numérique à développer, en analysant les actifs, flux, surfaces d'attaque et scénarios d'abus à partir du besoin et du contexte d'usage, afin d'orienter les choix de conception et de réduire le risque dès l'amont.

Participer au prototypage 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)

Sélectionner les technologies et les données adaptées à la réalisation de la solution numérique, 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 l'architecture et les composants de la solution numérique projetée, en intégrant les exigences de protection et de sécurisation des données dans les choix d'architecture, de fonctionnalité et de technologies, afin d'assurer sa résilience, sa maintenabilité et sa sécurisation durable.

Planifier le projet de développement, en ordonnant et en organisant ses étapes, et en répartissant les responsabilités et les tâches en fonction des compétences disponibles, tout en prenant les dispositions favorisant l'inclusion et maintien dans l'équipe projet des personnes en situation de handicap, afin de répondre aux exigences des parties prenantes en optimisant les délais, les coûts et l'efficacité collective.

Développer les composants applicatifs de la solution numérique selon des pratiques de codage sécurisé, en appliquant les principes secure-by-design/secure-by-default et les référentiels de vulnérabilités usuels (Web/API), afin de prévenir l'introduction de failles dès le développement.

Protéger les données sensibles utilisées par la solution numérique, en appliquant les exigences de chiffrement et de gestion des clés et en mettant en œuvre des mesures contre les attaques courantes visant les bases de données, afin d'en préserver la confidentialité et de les prémunir de toute tentative de piratage.

Intégrer la maîtrise des dépendances et composants logiciels utilisés par le code, en contrôlant versions, intégrité, provenance, licences et mises à jour, et en traitant les alertes de sécurité associées, afin de limiter l'exposition aux vulnérabilités connues et aux risques de chaîne d'approvisionnement logicielle.

Elaborer un plan de tests de sécurité, en définissant le périmètre, les scénarios et les critères d'acceptation, afin de sécuriser la décision de mise en production.

Mettre en œuvre des tests de sécurité outillés, incluant des tests d'intrusion/résilience, en paramétrant et exécutant les contrôles adaptés au contexte, afin d'identifier et de qualifier les vulnérabilités de la solution développée.

Corriger les vulnérabilités et vérifier la non-régression des fonctionnalités de la solution numérique, en appliquant des correctifs et en re-testant, afin de réduire le risque résiduel d'atteindre le niveau de sécurité attendu.

Industrialiser l'intégration et la livraison en sécurisant la chaîne CI/CD, afin de produire des livraisons reproductibles et conformes au niveau de sécurité attendu.

Déployer la solution sur des environnements cibles, en appliquant des procédures d'installation/mise à jour, en vérifiant l'état de santé post-déploiement et en assurant la réversibilité, afin de garantir la disponibilité du service et la maîtrise du risque opérationnel.

Gérer la configuration applicative et les secrets de déploiement, en séparant configuration et code, en utilisant des mécanismes de stockage/rotation sécurisés, et en contrôlant les droits d'accès, afin de limiter les erreurs de configuration et les expositions accidentelles.

Mettre en œuvre la maintenance et le traitement continu des vulnérabilités de la solution numérique, en déployant des correctifs et des éléments de sécurité supplémentaires (patchs correctifs, mises à jour, protocoles, ...), afin d'en garantir les fonctionnalités en toute sécurité.

Contribuer au traitement d'un incident de sécurité sur la solution numérique, en collectant les éléments utiles, en appliquant les actions nécessaires et en produisant un retour d'expérience, afin d'en limiter l'impact et de prévenir sa récurrence.

Réaliser un audit technique de sécurité de la solution et de son infrastructure associée, en vérifiant la configuration, l'exposition, les droits, la gestion des secrets, la journalisation et les composants déployés au moyen de référentiels et d'outils adaptés, afin d'identifier les écarts, de prioriser les actions correctives et de réduire les risques en exploitation. Identifier l'opportunité et la pertinence de faire appel à des technologies avancées et innovantes (Cybersécurité, IA, VR, Blockchain...) pour l'évolution de la solution numérique, 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.

Communiquer les exigences et risques de sécurité du produit, en traduisant les enjeux techniques en messages compréhensibles et actionnables pour les parties prenantes (produit, développement, QA, exploitation), afin d'aligner les décisions de conception, de développement et de déploiement sur un niveau de sécurité attendu.

Documenter les exigences et mécanismes de sécurité de la solution développée, en produisant une documentation technique et d'exploitation (contrôles d'accès, flux, gestion des secrets, règles de validation, journalisation, limites connues), afin de garantir la compréhension des choix de conception et la mise en œuvre correcte des mesures de sécurité par les parties prenantes.

Animer des actions de sensibilisation et d'accompagnement, en organisant des ateliers ciblés (revue de risques, démo de vulnérabilités, retour d'expérience d'incidents, revue de code orientée sécurité) et en aidant les équipes à mettre en œuvre les mesures attendues, afin d'améliorer l'appropriation, la conformité et la qualité de réalisation dans la durée.

Blocs de compétences

RNCP42620BC01 — Concevoir une solution numérique sécurisée

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, en les traduisant en exigences fonctionnelles et en intégrant les contraintes d'accessibilité conformément au RGAA, afin d'élaborer ou de valider un cahier des charges fonctionnel et technique de la solution numérique à développer.

Modéliser les menaces et qualifier les exigences de sécurité de la solution numérique à développer, en analysant les actifs, flux, surfaces d'attaque et scénarios d'abus à partir du besoin et du contexte d'usage, afin d'orienter les choix de conception et de réduire le risque dès l'amont.

Participer au prototypage 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).

Sélectionner les technologies et les données adaptées à la réalisation de la solution numérique, 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 l'architecture et les composants de la solution numérique projetée, en intégrant les exigences de protection et de sécurisation des données et d'accessibilité imposées par le RGAA

dans les choix d'architecture, de fonctionnalité et de technologies, afin d'assurer sa résilience, sa maintenabilité et sa sécurisation durable.

Planifier le projet de développement, en ordonnant et en organisant ses étapes, et en répartissant les responsabilités et les tâches en fonction des compétences disponibles, tout en prenant les dispositions favorisant l'inclusion et maintien dans l'équipe projet des personnes en situation de handicap, afin de répondre aux exigences des parties prenantes en optimisant les délais, les coûts et l'efficacité collective.

MODALITÉS D'ÉVALUATION

Dans le cadre d'une mise en situation professionnelle reconstituée, à partir d'une étude de cas réel ou fictif, le candidat assure la conception d'une solution logicielle, restituée par l'analyse des besoins fonctionnelles associés à la solution, l'identification et l'analyse des risques associés à la solution logicielle, le prototype de la solution logicielle, les choix d'architecture et de technologies pour la réalisation de la solution logicielle, et le plan de développement de la solution logicielle.

Les livrables sont réalisés individuellement et présentés oralement devant un jury d'évaluation.

RNCP42620BC02 — Développer une solution numérique sécurisée

LISTE DE COMPÉTENCES

Développer les composants applicatifs de la solution numérique selon des pratiques de codage sécurisé, en appliquant les principes secure-by-design/secure-by-default et les référentiels de vulnérabilités usuels (Web/API), afin

de prévenir l'introduction de failles dès le développement.

Protéger les données sensibles utilisées par la solution numérique, en appliquant les exigences de chiffrement et de gestion des clés et en mettant en œuvre des mesures contre les attaques courantes visant les bases de données, afin d'en préserver la confidentialité et de les prémunir de toute tentative de piratage.

Intégrer la maîtrise des dépendances et composants logiciels utilisés par le code, en contrôlant versions, intégrité, provenance, licences et mises à jour, et en traitant les alertes de sécurité associées, afin de limiter l'exposition aux vulnérabilités connues et aux risques de chaîne d'approvisionnement logicielle.

Elaborer un plan de tests de sécurité, en définissant le périmètre, les scénarios et les critères d'acceptation, afin de sécuriser la décision de mise en production.

Mettre en œuvre des tests de sécurité outillés, incluant des tests d'intrusion/résilience, en paramétrant et exécutant les contrôles adaptés au contexte, afin d'identifier et de qualifier les vulnérabilités de la solution développée.

Corriger les vulnérabilités et vérifier la non-régression des fonctionnalités de la solution numérique, en appliquant des correctifs et en re-testant, afin de réduire le risque résiduel d'atteindre le niveau de sécurité attendu

MODALITÉS D'ÉVALUATION

Dans le cadre d'une mise en situation professionnelle reconstituée, à partir d'une étude de cas réel ou fictif, le candidat assure la conception d'une solution logicielle, restituée par la solution développée, le plan de tests de la solution, et la restitution des résultats des tests, incluant les correctifs opérés pour remédier aux vulnérabilités de la solution identifiées.

Les livrables sont réalisés individuellement et présentés oralement devant un jury d'évaluation

RNCP42620BC03 — Déployer et maintenir en conditions sécurisées une solution numérique et son infrastructure associée

LISTE DE COMPÉTENCES

Industrialiser l'intégration et la livraison en sécurisant la chaîne CI/CD, afin de produire des livraisons reproductibles et conformes au niveau de sécurité attendu.

Déployer la solution sur des environnements cibles, en appliquant des procédures d'installation/mise à jour, en vérifiant l'état de santé post-déploiement et en assurant la réversibilité, afin de garantir la disponibilité du service et la maîtrise du risque opérationnel.

Gérer la configuration applicative et les secrets de déploiement, en séparant configuration et code, en utilisant des mécanismes de stockage/rotation sécurisés, et en contrôlant les droits d'accès, afin de limiter les erreurs de configuration et les expositions accidentelles.

Mettre en œuvre la maintenance et le traitement continu des vulnérabilités de la solution numérique, en déployant des correctifs et des éléments de sécurité supplémentaires (patches correctifs, mises à jour, protocoles, ...), afin d'en garantir les fonctionnalités en toute sécurité.

Contribuer au traitement d'un incident de sécurité sur la solution numérique, en collectant les éléments utiles, en appliquant les actions nécessaires et en produisant un retour d'expérience, afin d'en limiter l'impact et de prévenir sa récurrence.

Réaliser un audit technique de sécurité de la solution et de son infrastructure associée, en vérifiant la configuration, l'exposition, les droits, la gestion des secrets, la journalisation et les composants déployés au moyen de référentiels et d'outils adaptés, afin d'identifier les écarts, de prioriser les actions correctives et de réduire les risques en exploitation.

MODALITÉS D'ÉVALUATION

Dans le cadre d'une mise en situation professionnelle reconstituée, à partir d'une étude de cas réel ou fictif, le candidat assure le déploiement d'une solution logicielle et sa maintenance, restitués par l'intégration de la solution dans son infrastructure et son environnement d'utilisation, la configuration applicative et la sécurisation de l'utilisation de la solution, la réalisation d'une action de maintenance évolutive contribuant au maintien de la sécurité de la solution, le traitement d'un incident de sécurité affectant la solution, et l'audit de sécurité de l'infrastructure de la solution.

Les livrables sont réalisés individuellement et présentés oralement devant un jury d'évaluation.

RNCP42620BC04 — 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...) pour l'évolution de la solution numérique, 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.

Communiquer les exigences et risques de sécurité du produit, en traduisant les enjeux techniques en messages compréhensibles et actionnables pour les parties prenantes (produit, développement, QA, exploitation), afin d'aligner les décisions de conception, de développement et de déploiement sur un niveau de sécurité attendu.

Documenter les exigences et mécanismes de sécurité de la solution développée, en produisant une documentation technique et d'exploitation (contrôles d'accès, flux, gestion des secrets, règles de validation, journalisation, limites connues), accessible et adaptée aux personnes en situation de handicap, afin de garantir la compréhension des choix de conception et la mise en œuvre correcte des mesures de sécurité par les parties prenantes.

Animer des actions de sensibilisation et d'accompagnement, intégrant les besoins spécifiques des personnes en situation de handicap, en organisant des ateliers ciblés (revue de risques, démo de vulnérabilités, retour d'expérience d'incidents, revue de code orientée sécurité) et en aidant les équipes à mettre en œuvre les mesures attendues, afin d'améliorer l'appropriation, la conformité et la qualité de réalisation dans la durée.

MODALITÉS D'ÉVALUATION

Dans le cadre d'une mise en situation professionnelle reconstituée, à partir d'une étude de cas réel ou fictif, le candidat propose l'implémentation d'une solution intégrant une technologie émergente, restituée par une étude de faisabilité de la solution, les dispositions assurant la sécurisation de la solution, les exigences et risques de sécurité de la solution et la sensibilisation de ses parties prenantes, et la documentation de la solution.

Les livrables sont réalisés individuellement et présentés oralement devant un jury d'évaluation.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le développeur de solutions numériques sécurisées intervient au sein de toute organisation qui conçoit, développe ou exploite des produits informatiques. Il peut exercer son activité dans des contextes professionnels variés, notamment au sein d'une ESN (Entreprise de services du numérique), avec des missions réalisées pour le compte de clients, dans une start-up en participant à la création et au lancement de nouveaux produits innovants, ou au sein d'un grand groupe, en tant que développeur interne, quel que soit le secteur d'activité. Cette diversité d'environnements permet au candidat d'adapter ses compétences techniques et méthodologiques à des projets et des enjeux multiples.

TYPE D'EMPLOIS ACCESSIBLES

Développeur sécurité - Développeur de solutions numériques sécurisées - Développeur de solutions de sécurité - Développeur applicatif orienté sécurité - Développeur web sécurisé - Développeur logiciel avec spécialisation sécurité - Développeur DevSecOps junior. Ces fonctions s'exercent généralement sous la supervision d'un responsable ou d'un expert confirmé et peuvent évoluer, avec l'expérience, vers des postes à plus forte responsabilité.

RÈGLEMENTATIONS D'ACTIVITÉ

Le métier de Développeur de Solutions Numériques Sécurisées relève d'une activité non réglementée. Toutefois, son exercice s'effectue dans le respect des dispositions réglementaires en vigueur et des normes de référence suivantes : Protection des données personnelles : Règlement (UE) 2016/679 (RGPD), loi n° 78-17 du 6 janvier 1978 modifiée (Informatique et Libertés), loi n° 2018-493 du 20 juin 2018 et ordonnance n° 2018-1125 du 12 décembre 2018.

Cybersécurité et gestion des services : normes ISO 27001 et ISO 20000, bonnes pratiques reconnues (CISA, EBIOS, ANSSI).

La loi n°2022-309 du 4 mars 2022

(Application 1er octobre 2023).

Responsabilité numérique : loi n° 2021-1485 du 15 novembre 2021 (loi REEN) et Référentiel Général d'Écoconception des Services Numériques (RGESN) & le projet de loi SREN (Sécuriser et Réguler l'Espace Numérique).

Principes professionnels : respect de l'éthique, de l'écoresponsabilité, de l'accessibilité numérique, des droits d'auteur et de la protection des logiciels et du code de la cybersécurité 2024.

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)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 781 €
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) M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	41 765
Jugés difficiles à recruter	50 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X80 — Techniciens d'étude et de développement en informatique M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Pour un public en formation initiale ou en alternance : être titulaire d'une certification de niveau 4 pour une entrée en 1^{re} année,

ou être titulaire d'une certification de niveau 5 à dominante scientifique et/ou informatique, pour une entrée directe en 3^e année.

Pour un public en reconversion professionnelle : être titulaire au minimum d'une certification de niveau 4 en informatique ; pour les candidats issus d'une autre spécialité, la réalisation d'un test de positionnement est requise afin d'évaluer les connaissances préalables, notamment dans le domaine scientifique et informatique.

PRÉREQUIS À LA VALIDATION

Pour pouvoir se présenter aux épreuves de certification, le candidat doit avoir été assidu en formation et 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), et le responsable de la certification professionnelle (ou son représentant).

Base légale

Date de décision	17/07/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	17/07/2029
Date de dernière délivrance possible	17/07/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2025	144	0	73 %	0 %
2024	111	0	54 %	25 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP37778

CORRESPONDANCES (PAR BLOCS)

RNCP37300, RNCP37778, RNCP37873, RNCP37987, RNCP39609, RNCP41238, RNCP41285, RNCP41586

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.esiee-it.fr/fr>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42620/>

Se former en apprentissage

Formations en apprentissage	8
Organismes gestionnaires (CFA)	1
Organismes formateurs	2
Régions couvertes	1
Départements couverts	2
Organismes certifiés Qualiopi	2
Sessions	de 09/2025 à 08/2029

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