

Expert DevOps

RNCP42520 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 326n, 326p
Formacode(s)	31006, 31009, 31094, 31087, 24273
Code(s) ROME	M1802, M1805, M1806, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	26/06/2026
Date d'échéance	26/06/2029

Certificateur(s)

CODA · SIRET : 92219486500031

THE PROGRESS FACTORY · SIRET : 85118370700047

<https://theprogressfactory.fr/>

Partenaires habilités

3 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation et 1 à former.

Organisme	SIRET	Habilitation
EF2C	91516491700030	Former et organiser l'évaluation
EF2C	91516491700048	Former et organiser l'évaluation
EF2C	—	Former

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le secteur numérique français traverse une transformation profonde, marquée par l'adoption massive du cloud computing, la généralisation de la conteneurisation et l'évolution des modèles de sécurité vers le Zero Trust. Cette mutation, accélérée par les crises sanitaires, géopolitiques et cybersécuritéaires de la période 2020-2025, génère un besoin critique en compétences capables d'embrasser simultanément la conception d'architectures cloud-natives, l'automatisation des cycles de livraison, la fiabilité des services en production et la sécurité intégrée.

Le métier d'Expert DevOps répond à cette complexité croissante. Il désigne un rôle qui a naturellement évolué pour englober ce qui est couramment appelé DevSecOps, ingénierie cloud-native et Site Reliability Engineering - non pas des spécialités distinctes, mais les expressions contemporaines d'une même discipline en constante évolution.

ACTIVITÉS VISÉES

Analyser les besoins et évaluer la faisabilité technique des projets

Concevoir l'architecture logicielle et sélectionner les technologies

Modéliser les systèmes et valider les solutions avec les parties prenantes

Rédiger les spécifications techniques détaillées

Planifier et coordonner les équipes techniques multi-profils

Piloter la performance et respecter les contraintes projet

Résoudre les problèmes complexes et incidents critiques

Organiser la montée en compétences et produire la documentation technique

Concevoir les chaînes d'intégration et déploiement continu
Développer l'infrastructure as code pour les environnements
Automatiser les tests et interconnecter les outils
Évaluer le niveau de sécurité d'un système de cycle de vie applicatif
Automatiser la détection des vulnérabilités dans les cycles de développement
Sécuriser les architectures et gérer les configurations sensibles
Assurer la conformité réglementaire des solutions déployées
Déployer des infrastructures cloud-native résilientes et optimisées
Définir les objectifs de service et métriques de performance (SLI/SLO/Error Budget)
Optimiser la disponibilité et superviser les systèmes en production

COMPÉTENCES ATTESTÉES

Mener une veille technologique et stratégique sur les écosystèmes cloud, les pratiques DevOps et les nouvelles architectures en évaluant leur pertinence technique et métier pour orienter les choix de solutions et les propositions d'innovation

Conduire une analyse des besoins utilisateurs en mobilisant des techniques d'entretien et d'atelier participatif afin d'identifier les objectifs fonctionnels, non-fonctionnels (performance, sécurité) et les impératifs d'accessibilité, du système d'information

Auditer les systèmes techniques et les processus existants en s'appuyant sur l'analyse documentaire et les entretiens avec les parties prenantes, afin d'éclairer les choix d'évolution et orienter la stratégie d'architecture future

Évaluer la faisabilité technique d'un projet en analysant les contraintes technologiques, budgétaires, temporelles et environnementales afin de valider ou ajuster le périmètre d'intervention

Concevoir une architecture cloud-native en appliquant les patterns d'architecture cloud adaptés, afin de garantir la résilience, la scalabilité horizontale et la maintenabilité dans des environnements dynamiques et élastiques

Sélectionner les modèles de service cloud (IaaS, CaaS, PaaS, FaaS, SaaS) et les technologies associées, en comparant leurs performances, coûts, compatibilités et leur efficacité énergétique, afin d'optimiser l'adéquation avec les besoins métier dans une démarche de sobriété numérique

Définir les principes de sécurité dès la conception en conciliant contraintes réglementaires et bonnes pratiques de cybersécurité pour assurer la protection des systèmes et des données

Modéliser les architectures et flux de données en utilisant les outils de modélisation appropriés (UML, diagrammes d'architecture) afin de s'aligner avec les équipes et les parties prenantes autour d'une architecture cible

Présenter et argumenter les choix architecturaux auprès des interlocuteurs techniques et métier en adaptant le niveau de communication pour obtenir la validation des solutions

Produire la documentation d'architecture de référence (notes de cadrage, spécifications techniques, schémas) en formalisant les principes, les choix et les contraintes pour guider les équipes et assurer la maintenabilité de la solution

Documenter les interfaces et protocoles d'échanges en précisant les formats, sécurisations et modalités techniques pour permettre l'intégration des composants

Planifier les projets techniques en appliquant les méthodologies adaptées au contexte (ex: agile) afin de définir les livrables, les étapes clés et ressources nécessaires

Orchestrer le flux de travail des équipes en animant les sessions collaboratives, en procédant aux arbitrages techniques pour lever les points de blocage, et en s'appuyant sur les outils de gestion partagés, afin d'assurer la fluidité des activités et la prévisibilité des livraisons

Définir et piloter le système de mesure de la performance projet, en instrumentant son cycle de vie avec des indicateurs actionnables, afin d'aider à la prise de décision et de communiquer efficacement sur sa progression

Piloter les risques projet (techniques, humains, organisationnels) en procédant aux arbitrages nécessaires sur les contraintes de qualité, coût et délai, afin de garantir le respect des engagements et de sécuriser l'atteinte des objectifs

Piloter la résolution d'incidents et de problèmes complexes en mobilisant une expertise technique pour diagnostiquer les causes racines et mettre en œuvre les plans d'action appropriés afin de rétablir et de fiabiliser le service

Organiser la gestion de crise en définissant les procédures d'escalade et de communication pour minimiser l'impact sur les activités métier

Élaborer la documentation technique opérationnelle (playbooks, runbooks, procédures) en formalisant les bonnes pratiques et processus pour faciliter l'autonomie des équipes

Organiser le transfert de compétences en animant des sessions de formation et d'accompagnement technique, en adaptant les modalités pédagogiques et les outils aux besoins spécifiques des collaborateurs, y compris ceux en

situation de handicap, tout en respectant les principes d'ergonomie et de prévention des risques professionnels, pour développer l'expertise des équipes dans des conditions de travail saines

Mettre en place les outils et processus d'accompagnement à l'adoption des bonnes pratiques DevOps, y compris celles relatives à l'accessibilité numérique, en créant les supports et cadres de travail appropriés pour accélérer la montée en maturité

Concevoir des pipelines CI/CD adaptés aux projets en analysant les besoins de déploiement et les contraintes techniques afin d'automatiser le cycle de vie applicatif de bout en bout

Définir les stratégies de déploiement (blue-green, canary, rolling) en évaluant les risques et les exigences de disponibilité pour minimiser l'impact sur la production

Implémenter les mécanismes de rollback et de monitoring des déploiements en intégrant les outils d'observabilité pour garantir la réversibilité et la traçabilité des livraisons

Développer l'infrastructure as code en utilisant les outils appropriés (tel que Terraform ou Ansible) pour provisionner et gérer les ressources de manière reproductible

Versionner et organiser le code d'infrastructure en appliquant les bonnes pratiques de développement et de gestion de configuration pour assurer la maintenabilité et la collaboration

Gérer les environnements multi-cloud et hybrides en adaptant les templates et configurations pour optimiser la portabilité et l'efficacité des déploiements

Intégrer les tests automatisés dans les pipelines en orchestrant les tests unitaires, d'intégration, de performance et d'accessibilité (a11y) pour valider la qualité du code et des déploiements

Interconnecter les outils de la chaîne CI/CD via APIs et webhooks en configurant les flux d'échanges de données pour créer une chaîne outillée cohérente et automatisée

Automatiser les tâches opérationnelles récurrentes en développant des scripts et workflows personnalisés pour limiter les interventions manuelles, réduire la charge de travail répétitive et améliorer l'efficacité et les conditions de travail des équipes

Conduire un audit de sécurité d'un système (application, infrastructure, pipeline) en s'appuyant sur des référentiels de bonnes pratiques (ex: OWASP, CIS) et des analyses techniques, afin d'identifier et de hiérarchiser les vulnérabilités, les défauts de configuration et les écarts de conformité

Élaborer un plan de remédiation priorisé en traduisant les vulnérabilités identifiées en actions correctives techniques et organisationnelles, afin de proposer une feuille de route claire pour l'amélioration de la sécurité et d'éclairer la prise de décision

Mettre en œuvre une stratégie de "Shift Left Security" en intégrant des outils d'analyse (SAST, DAST, SCA) au cœur des pipelines CI/CD, afin de détecter et de permettre la correction des vulnérabilités au plus tôt du cycle de vie logiciel

Automatiser l'analyse des vulnérabilités des conteneurs et images en utilisant les scanners spécialisés (tel que Trivy, Clair ou Snyk) pour sécuriser les artefacts avant leur déploiement

Mettre en place les politiques de remédiation automatisée en définissant les seuils critiques et les actions correctives pour traiter les vulnérabilités selon leur criticité

Gérer les secrets et données sensibles en implémentant les coffres-forts numériques (avec des outils tel que Vault ou AWS Secrets Manager) et les mécanismes de rotation automatique pour protéger les informations critiques

Sécuriser les communications réseau en configurant les politiques de segmentation, chiffrement et contrôle d'accès pour garantir la confidentialité, l'intégrité et la segmentation des flux de données

Durcir les configurations systèmes et applicatives en appliquant les benchmarks de sécurité (CIS, OWASP) et les principes de moindre privilège pour réduire la surface d'attaque

Mettre en œuvre une approche de "Compliance as Code" en traduisant les exigences réglementaires (telles que RGPD, PCI-DSS, HDS) et préparer les audits de conformité (tels que SOC 2 ou ISO 27001), en traduisant ces exigences en règles et contrôles automatisés afin de garantir et de prouver la conformité en continu tout au long du cycle de livraison

Documenter et tracer les mesures de sécurité mises en œuvre en produisant les preuves d'audit et rapports de conformité pour faciliter les contrôles réglementaires

Maintenir la gouvernance sécuritaire en définissant les politiques de sécurité, procédures d'incident et plans de continuité, en intégrant la gestion du stress lié aux incidents de sécurité, pour assurer la sécurité opérationnelle continue sans compromettre le bien-être des équipes

Orchestrer des applications conteneurisées avec Kubernetes en configurant les ressources, services et politiques de résilience pour garantir la scalabilité automatique et la haute disponibilité

Concevoir des architectures multi-zones et multi-régions en exploitant les services cloud managés (AWS, GCP, Azure) pour assurer la continuité de service et la reprise après sinistre

Implémenter les patterns de résilience applicative (circuit breaker, retry, timeout) en intégrant les mécanismes de tolérance aux pannes pour maintenir la performance en cas de défaillance partielle

Définir les Service Level Indicators (SLI) en identifiant les métriques critiques de performance, disponibilité et latence pour mesurer objectivement la qualité de service

Établir les Service Level Objectives (SLO) en fixant les seuils de performance acceptables basés sur les besoins métier pour contractualiser les niveaux de service attendus

Contribuer à la négociation des Service Level Agreements (SLA) en traduisant les SLO en engagements contractuels réalisables, afin de garantir l'alignement entre les attentes métier et les capacités techniques

Architecturer la supervision complète des systèmes en déployant les solutions de monitoring, logging et alerting (tel que Prometheus, Grafana ou ELK) pour assurer l'observabilité en temps réel

Optimiser les performances et les coûts d'infrastructure (FinOps) en analysant les métriques d'utilisation, en mesurant l'empreinte carbone (GreenOps) et en ajustant le dimensionnement pour maximiser l'efficacité opérationnelle et environnementale

Gérer les incidents de production en appliquant les méthodes SRE (post-mortem, error budget, chaos engineering) en préservant l'équilibre et la charge de travail des équipes pour améliorer continuellement la fiabilité des services

Blocs de compétences

RNCP42520BC01 — Définir la stratégie technique et l'architecture des solutions Cloud

LISTE DE COMPÉTENCES

Mener une veille technologique et stratégique sur les écosystèmes cloud, les pratiques DevOps et les nouvelles architectures en évaluant leur pertinence technique et métier pour orienter les choix de solutions et les propositions d'innovation

Conduire une analyse des besoins utilisateurs en mobilisant des techniques d'entretien et d'atelier participatif afin d'identifier les objectifs fonctionnels, non-fonctionnels (performance, sécurité) et les impératifs d'accessibilité, du système d'information

Auditer les systèmes techniques et les processus existants en s'appuyant sur l'analyse documentaire et les entretiens avec les parties prenantes, afin d'éclairer les choix d'évolution et orienter la stratégie d'architecture future

Évaluer la faisabilité technique d'un projet en analysant les contraintes technologiques, budgétaires, temporelles et environnementales afin de valider ou ajuster le périmètre d'intervention

Concevoir une architecture cloud-native en appliquant les patterns d'architecture cloud adaptés, afin de garantir la résilience, la scalabilité horizontale et la maintenabilité dans des environnements dynamiques et élastiques

Sélectionner les modèles de service cloud (IaaS, CaaS, PaaS, FaaS, SaaS) et les technologies associées, en comparant leurs performances, coûts, compatibilités et leur efficacité énergétique, afin d'optimiser l'adéquation avec les besoins métier dans une démarche de sobriété numérique

Définir les principes de sécurité dès la conception en conciliant contraintes réglementaires et bonnes pratiques de cybersécurité pour assurer la protection des systèmes et des données

Modéliser les architectures et flux de données en utilisant les outils de modélisation appropriés (UML, diagrammes d'architecture) afin de s'aligner avec les équipes et les parties prenantes autour d'une architecture cible

Présenter et argumenter les choix architecturaux auprès des interlocuteurs techniques et métier en adaptant le niveau de communication pour obtenir la validation des solutions

Produire la documentation d'architecture de référence (notes de cadrage, spécifications techniques, schémas) en formalisant les principes, les choix et les contraintes pour guider les équipes et assurer la maintenabilité de la solution

Documenter les interfaces et protocoles d'échanges en précisant les formats, sécurisations et modalités techniques pour permettre l'intégration des composants

MODALITÉS D'ÉVALUATION

Étude de cas, soutenance orale

RNCP42520BC02 — Piloter les projets de déploiement des solutions Cloud natives

LISTE DE COMPÉTENCES

Planifier les projets techniques en appliquant les méthodologies adaptées au contexte (ex: agile) afin de définir les livrables, les étapes clés et ressources nécessaires

Orchestrer le flux de travail des équipes en animant les sessions collaboratives, en procédant aux arbitrages techniques pour lever les points de blocage, et en s'appuyant sur les outils de gestion partagés, afin d'assurer la

fluidité des activités et la prévisibilité des livraisons

Définir et piloter le système de mesure de la performance projet, en instrumentant son cycle de vie avec des indicateurs actionnables, afin d'aider à la prise de décision et de communiquer efficacement sur sa progression

Piloter les risques projet (techniques, humains, organisationnels) en procédant aux arbitrages nécessaires sur les contraintes de qualité, coût et délai, afin de garantir le respect des engagements et de sécuriser l'atteinte des objectifs

Piloter la résolution d'incidents et de problèmes complexes en mobilisant une expertise technique pour diagnostiquer les causes racines et mettre en œuvre les plans d'action appropriés afin de rétablir et de fiabiliser le service

Organiser la gestion de crise en définissant les procédures d'escalade et de communication pour minimiser l'impact sur les activités métier

Élaborer la documentation technique opérationnelle (playbooks, runbooks, procédures) en formalisant les bonnes pratiques et processus pour faciliter l'autonomie des équipes

Organiser le transfert de compétences en animant des sessions de formation et d'accompagnement technique, en adaptant les modalités pédagogiques et les outils aux besoins spécifiques des collaborateurs, y compris ceux en situation de handicap, tout en respectant les principes d'ergonomie et de prévention des risques professionnels, pour développer l'expertise des équipes dans des conditions de travail saines

Mettre en place les outils et processus d'accompagnement à l'adoption des bonnes pratiques DevOps, y compris celles relatives à l'accessibilité numérique, en créant les supports et cadres de travail appropriés pour accélérer la montée en maturité

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle, soutenance orale

RNCP42520BC03 — Industrialiser le cycle de vie logiciel par l'automatisation (CI/CD)

LISTE DE COMPÉTENCES

Concevoir des pipelines CI/CD adaptés aux projets en analysant les besoins de déploiement et les contraintes techniques afin d'automatiser le cycle de vie applicatif de bout en bout

Définir les stratégies de déploiement (blue-green, canary, rolling) en évaluant les risques et les exigences de disponibilité pour minimiser l'impact sur la production

Implémenter les mécanismes de rollback et de monitoring des déploiements en intégrant les outils d'observabilité pour garantir la réversibilité et la traçabilité des livraisons

Développer l'infrastructure as code en utilisant les outils appropriés (tel que Terraform ou Ansible) pour provisionner et gérer les ressources de manière reproductible

Versionner et organiser le code d'infrastructure en appliquant les bonnes pratiques de développement et de gestion de configuration pour assurer la maintenabilité et la collaboration

Gérer les environnements multi-cloud et hybrides en adaptant les templates et configurations pour optimiser la portabilité et l'efficacité des déploiements

Intégrer les tests automatisés dans les pipelines en orchestrant les tests unitaires, d'intégration, de performance et d'accessibilité (a11y) pour valider la qualité du code et des déploiements

Interconnecter les outils de la chaîne CI/CD via APIs et webhooks en configurant les flux d'échanges de données pour créer une chaîne outillée cohérente et automatisée

Automatiser les tâches opérationnelles récurrentes en développant des scripts et workflows personnalisés pour limiter les interventions manuelles, réduire la charge de travail répétitive et améliorer l'efficacité et les conditions de travail des équipes

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle, soutenance orale

RNCP42520BC04 — Intégrer la sécurité et la conformité dans le cycle de vie applicatif (SSDLC)

LISTE DE COMPÉTENCES

Conduire un audit de sécurité d'un système (application, infrastructure, pipeline) en s'appuyant sur des référentiels de bonnes pratiques (ex: OWASP, CIS) et des analyses techniques, afin d'identifier et de hiérarchiser les vulnérabilités, les défauts de configuration et les écarts de conformité

Élaborer un plan de remédiation priorisé en traduisant les vulnérabilités identifiées en actions correctives techniques et organisationnelles, afin de proposer une feuille de route claire pour l'amélioration de la sécurité et d'éclairer la prise de décision

Mettre en œuvre une stratégie de "Shift Left Security" en intégrant des outils d'analyse (SAST, DAST, SCA) au cœur des pipelines CI/CD, afin de détecter et de permettre la correction des vulnérabilités au plus tôt du cycle de vie logiciel
Automatiser l'analyse des vulnérabilités des conteneurs et images en utilisant les scanners spécialisés (tel que Trivy, Clair ou Snyk) pour sécuriser les artefacts avant leur déploiement

Mettre en place les politiques de remédiation automatisée en définissant les seuils critiques et les actions correctives pour traiter les vulnérabilités selon leur criticité

Gérer les secrets et données sensibles en implémentant les coffres-forts numériques (avec des outils tel que Vault ou AWS Secrets Manager) et les mécanismes de rotation automatique pour protéger les informations critiques

Sécuriser les communications réseau en configurant les politiques de segmentation, chiffrement et contrôle d'accès pour garantir la confidentialité, l'intégrité et la segmentation des flux de données

Durcir les configurations systèmes et applicatives en appliquant les benchmarks de sécurité (CIS, OWASP) et les principes de moindre privilège pour réduire la surface d'attaque

Mettre en œuvre une approche de "Compliance as Code" en traduisant les exigences réglementaires (telles que RGPD, PCI-DSS, HDS) et préparer les audits de conformité (tels que SOC 2 ou ISO 27001), en traduisant ces exigences en règles et contrôles automatisés afin de garantir et de prouver la conformité en continu tout au long du cycle de livraison

Documenter et tracer les mesures de sécurité mises en œuvre en produisant les preuves d'audit et rapports de conformité pour faciliter les contrôles réglementaires

Maintenir la gouvernance sécuritaire en définissant les politiques de sécurité, procédures d'incident et plans de continuité, en intégrant la gestion du stress lié aux incidents de sécurité, pour assurer la sécurité opérationnelle continue sans compromettre le bien-être des équipes

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle, soutenance orale

RNCP42520BC05 — Garantir la fiabilité et l'efficience des services en production (SRE)

LISTE DE COMPÉTENCES

Orchestrer des applications conteneurisées avec Kubernetes en configurant les ressources, services et politiques de résilience pour garantir la scalabilité automatique et la haute disponibilité

Concevoir des architectures multi-zones et multi-régions en exploitant les services cloud managés (AWS, GCP, Azure) pour assurer la continuité de service et la reprise après sinistre

Implémenter les patterns de résilience applicative (circuit breaker, retry, timeout) en intégrant les mécanismes de tolérance aux pannes pour maintenir la performance en cas de défaillance partielle

Définir les Service Level Indicators (SLI) en identifiant les métriques critiques de performance, disponibilité et latence pour mesurer objectivement la qualité de service

Établir les Service Level Objectives (SLO) en fixant les seuils de performance acceptables basés sur les besoins métier pour contractualiser les niveaux de service attendus

Contribuer à la négociation des Service Level Agreements (SLA) en traduisant les SLO en engagements contractuels réalisables, afin de garantir l'alignement entre les attentes métier et les capacités techniques

Architecturer la supervision complète des systèmes en déployant les solutions de monitoring, logging et alerting (tel que Prometheus, Grafana ou ELK) pour assurer l'observabilité en temps réel

Optimiser les performances et les coûts d'infrastructure (FinOps) en analysant les métriques d'utilisation, en mesurant l'empreinte carbone (GreenOps) et en ajustant le dimensionnement pour maximiser l'efficience opérationnelle et environnementale

Gérer les incidents de production en appliquant les méthodes SRE (post-mortem, error budget, chaos engineering) en préservant l'équilibre et la charge de travail des équipes pour améliorer continuellement la fiabilité des services

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle, soutenance orale

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'Expert DevOps évolue au sein d'un écosystème économique diversifié : Entreprises de Services du Numérique (ESN), éditeurs de logiciels, scale-ups technologiques et grands groupes engagés dans leur transformation numérique.

Les secteurs fortement réglementés représentent un débouché privilégié : services financiers et assurance (DORA, PCI-DSS), santé et pharma (HDS, RGPD), énergie et industries critiques (NIS2, SecNumCloud), administrations et collectivités (souveraineté numérique, référentiels ANSSI). L'expertise s'étend à tout secteur dont la compétitivité repose sur des systèmes numériques sécurisés et résilients.

TYPE D'EMPLOIS ACCESSIBLES

- Expert DevOps
- Expert DevSecOps
- Platform Engineer
- Site Reliability Engineer (SRE)
- Lead DevOps
- Consultant DevOps

RÉGLEMENTATIONS D'ACTIVITÉ

Le métier d'Expert DevOps ne nécessite aucune habilitation particulière pour être exercé. Cette profession valorise la maîtrise de compétences complexes plutôt qu'un statut légal spécifique. L'expert évolue néanmoins dans un environnement réglementaire dense et évolutif, nécessitant une maîtrise approfondie des obligations de conformité pour traduire les exigences légales en solutions techniques.

Réglementations européennes :

- Directive NIS2 (UE) 2022/2555 du 14 décembre 2022 : étend les obligations de cybersécurité à de nouveaux secteurs et impose des délais stricts de notification d'incidents, impactant directement la conception des systèmes d'observabilité et des processus de gestion d'incidents.
- RGPD (UE) 2016/679 du 27 avril 2016 : impose des obligations de protection des données personnelles qui impactent les choix architecturaux et les pratiques de développement (Privacy by Design).
- Cyber Resilience Act : règlement européen en cours d'adoption imposant des exigences de sécurité obligatoires pour les produits numériques, renforçant le besoin d'une approche "Compliance as Code".

Réglementations nationales et sectorielles :

- Qualification SecNumCloud (ANSSI) : référentiels de sécurité pour les services cloud destinés aux secteurs critiques et enjeux de souveraineté numérique.
- Obligations HDS (Code de la santé publique, art. L. 1111-8) : hébergement agréé des données de santé.
- Réglementations du secteur financier : PCI-DSS pour les données de paiement, règlement DORA pour la résilience opérationnelle.

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

MODALITÉS D'ACCÈS

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

PRÉREQUIS À L'ENTRÉE EN FORMATION

Être titulaire d'une certification de niveau 6 dans le domaine de l'informatique (développement, systèmes et réseaux, gestion de projet technique).

ou

Justifier d'une expérience professionnelle d'au moins 3 ans sur des fonctions en lien avec les compétences visées par la certification, notamment en développement, systèmes et réseaux, ou en gestion de projet technique.

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

Minimum 3 membres, dont au moins 2 professionnels externes qualifiés (experts DevOps, DevSecOps, Architecture Cloud ou SRE, justifiant d'au moins 3 ans d'expérience)

Base légale

Date de décision	26/06/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	26/06/2029
Date de dernière délivrance possible	26/06/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2024	17	0	88 %	100 %
2023	17	0	88 %	93 %

Liens avec d'autres certifications

CORRESPONDANCES (PAR BLOCS)

RNCP40165, RNCP40757

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/42520/>

Où se former

Formations référencées	7
Organismes	1
Régions couvertes	1
Prix indicatif	4 000 € – 11 500 €
Durée	120 – 1345 h

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.