

Expert en ingénierie et cybersécurité des systèmes d'information

RNCP41988 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 326t
Formacode(s)	31006, 31008
Code(s) ROME	M1801, M1802, M1803
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	27/02/2026
Date d'échéance	27/02/2029

Certificateur(s)

H3 · SIRET : 70202279900028

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification : expert en ingénierie et cybersécurité des systèmes d'information forme des professionnels capables de concevoir, sécuriser et piloter des projets numériques complexes, de l'architecture au déploiement en passant par le développement, l'intégration cloud et la supervision. Elle répond aux besoins croissants des entreprises, administrations et ESN de garantir la performance, la conformité réglementaire (RGPD, NIS2, DORA), la continuité de service et la résilience face aux cybermenaces. L'expert certifié agit à la fois comme concepteur technique, garant de la cybersécurité et conseil stratégique auprès des directions métiers et des DSI, en intégrant les contraintes budgétaires, fonctionnelles et environnementales. Son rôle transverse, mobilisant des méthodes agiles, DevOps/DevSecOps et ITIL, permet d'accompagner la transformation numérique des organisations tout en assurant la protection de leurs actifs numériques critiques et leur alignement avec les enjeux de souveraineté et de durabilité numériques.

ACTIVITÉS VISÉES

- Diagnostic du SI existant et identification des besoins d'évolution
- Réalisation d'une veille stratégique et technologique
- Élaboration des orientations d'évolution du SI
- Définition des objectifs et des moyens du projet
- Organisation et suivi de la mise en œuvre
- Management des ressources humaines et organisationnelles du projet
- Maintenir et faire évoluer le SI en conditions opérationnelles
- Optimisation de la performance et de la conformité du SI
- Proposition d'axes d'amélioration continue du SI
- Implémentation des pratiques DevSecOps de gestion du code, d'intégration et de traçabilité documentaire
- Sécurisation applicative, durcissement des environnements et conformité réglementaire
- Supervision de la performance, la fiabilité et la qualité des solutions numériques dans une approche de cybersécurité opérationnelle
- Conception d'applications robustes et évolutives
- Conception et intégration des solutions d'analyse et d'IA
- Maintien, supervision et mise à jour des solutions intelligentes

COMPÉTENCES ATTESTÉES

- Identifier les besoins métiers, utilisateurs et data-driven en exploitant des techniques de modélisation des processus, des outils de collecte et d'analyse des données structurées et non structurées, ainsi que des méthodes de co-conception afin de produire un cahier des charges aligné, robuste et conforme.
- Évaluer l'architecture, les performances, les usages et les vulnérabilités du SI en mobilisant des outils d'analyse de trafic, de benchmarks applicatifs, d'audit de code et de tests de sécurité afin de produire un diagnostic orienté décision et sécurisé.
- Évaluer la maturité numérique de l'organisation en mobilisant des référentiels de diagnostic, des indicateurs de performance et des outils d'analyse systémique afin d'orienter l'évolution du SI selon les capacités de l'organisation.
- Modéliser la cartographie fonctionnelle, stratégique, technique, data et de sécurité du SI en combinant l'analyse des dépendances internes et externes, des ateliers de co-construction avec les parties prenantes, des audits documentaires et des outils de modélisation afin de sécuriser les scénarios d'évolution et de maîtriser les risques.
- Anticiper les évolutions technologiques, métiers et réglementaires impactant le SI en qualifiant les sources d'innovation pertinentes, en analysant leurs effets sur la trajectoire du SI et en intégrant les exigences de conformité et d'agilité afin de structurer une veille stratégique opérationnelle à forte valeur décisionnelle.
- Structurer la restitution des résultats de veille technologique, métier et réglementaire en mobilisant des outils de visualisation stratégique, des synthèses analytiques orientées décision et des formats adaptés aux parties prenantes afin d'éclairer les arbitrages dans la définition et la priorisation des orientations d'évolution du SI.
- Construire les orientations stratégiques d'évolution du SI en élaborant des scénarios d'urbanisation et en intégrant une stratégie de gouvernance des données fondée sur l'analyse des usages, des contraintes de conformité et des enjeux de qualité, de sécurité et d'éthique, afin de proposer une trajectoire évolutive, fiable et responsable pour le SI.
- Aligner la vision stratégique du SI avec les engagements RSE de l'organisation en évaluant les impacts environnementaux, sociaux et éthiques des orientations technologiques afin de soutenir une transformation numérique durable, inclusive et conforme aux exigences sociétales.
- Projeter l'architecture cible du SI en alignant les objectifs métier et technologiques, en mobilisant des référentiels d'architecture (TOGAF, Zachman), des principes de scalabilité, d'interopérabilité et de résilience, ainsi que des modèles de gouvernance intégrée afin de structurer une trajectoire cohérente, soutenable et pilotable de transformation du SI.
- Définir la stratégie de cybersécurité de l'organisation en alignant les exigences techniques, réglementaires et métiers avec les référentiels (ISO 27001, NIST, EBIOS RM), en structurant les dispositifs de pilotage et en mesurant la maturité afin d'assurer la conformité, la résilience et la gouvernance globale du SI
- Formaliser une note de cadrage du projet de transformation du SI en analysant les besoins exprimés et implicites des parties prenantes, les enjeux métier, les contraintes techniques et réglementaires, à l'aide d'outils de clarification des objectifs, de matrice d'analyse de la valeur et de grille d'arbitrage stratégique afin de structurer un référentiel de pilotage cohérent et aligné.
- Qualifier les parties prenantes, les risques et les impacts métiers d'un projet de transformation du SI en mobilisant des outils d'analyse d'enjeux, de cartographie d'acteurs, de matrices de criticité et de simulation d'impact organisationnel afin de sécuriser les choix de conception, de structuration et de pilotage du projet.
- Structurer le planning et le budget d'un projet de transformation du SI en mobilisant des méthodes de découpage en lots (WBS), des outils de planification (PERT, GANTT), des grilles d'estimation des charges et des référentiels de coûts afin d'optimiser l'allocation des ressources, de maîtriser les délais.
- Piloter l'avancement d'un projet de transformation du SI en analysant les écarts entre prévisionnel et réalisé à l'aide d'indicateurs techniques, financiers, data et ROI, en mobilisant des outils de reporting dynamique, de tableaux de bord et de revues de jalons afin d'ajuster les plans d'action et garantir l'atteinte des objectifs.
- Évaluer les impacts et les résultats d'un projet de transformation du SI en mobilisant des indicateurs de performance, des matrices d'impact, des analyses de parcours utilisateur et des revues de gouvernance des données afin de fiabiliser les arbitrages, garantir la valeur délivrée et de capitaliser les apprentissages pour les projets futurs.
- Définir les rôles, les responsabilités et les compétences nécessaires à la réussite d'un projet de transformation du SI en mobilisant des matrices de responsabilités (RACI, MOF), des référentiels de compétences, des analyses de charge et des entretiens avec les parties prenantes afin de structurer une organisation projet efficace, lisible et adaptée aux exigences du projet.
- Encadrer une équipe technique ou projet mobilisée sur un SI en définissant les objectifs collectifs et individuels, en

structurant les modes de fonctionnement collaboratif, les rituels de pilotage et les parcours de montée en compétences afin de garantir la performance collective et la motivation durable.

- Coordonner les interactions entre les équipes internes, les partenaires et les fournisseurs impliqués dans un projet de transformation du SI en définissant les responsabilités, les modalités de collaboration, les engagements contractuels et les outils de pilotage collaboratif afin d'assurer la cohésion opérationnelle, la performance collective et la conformité aux objectifs du projet.
- Mettre en œuvre des méthodes d'organisation du travail adaptées aux projets de transformation du SI en combinant des approches agiles, hybrides ou itératives, des outils de pilotage par la valeur, des dispositifs de gestion de la charge et des rituels de coordination afin d'optimiser la fluidité, l'engagement et la performance projet.
- Résoudre les incidents techniques, applicatifs et data affectant le SI en mobilisant des outils d'observabilité, d'analyse de logs, de supervision temps réel et de traçabilité des flux afin de restaurer la disponibilité des services, d'identifier les causes racines et de fiabiliser le fonctionnement opérationnel du SI.
- Automatiser la gestion des incidents et des actions de remédiation dans les environnements SI en structurant des procédures déclenchables (runbooks), en configurant des outils d'orchestration (SOAR, scripts, workflows) et en intégrant des seuils d'alerte déclencheurs afin de réduire les délais, renforcer la réactivité et assurer la continuité de service.
- Déployer des évolutions correctives ou adaptatives du SI en analysant les causes techniques, fonctionnelles ou data des écarts de performance, en mobilisant des outils de gestion des versions, de tests de non-régression, de documentation et de supervision continue afin d'assurer la stabilité et la conformité du SI.
- Formaliser la documentation des actions de maintenance du SI en structurant les procédures, les journaux d'intervention, les historiques de configuration, les matrices de conformité et les enseignements post-incidents afin de garantir la traçabilité, la capitalisation et le respect des obligations.
- Réaliser des audits de performance, de sécurité et de conformité du SI en mobilisant des outils d'analyse de vulnérabilités, de métrologie applicative, de contrôle des flux de données et de conformité réglementaire (RGPD, SLA, ISO) afin d'identifier les écarts et formuler des recommandations.
- Configurer des outils de supervision et d'alerte du SI en intégrant en y intégrant des dashboards DevOps, des métriques CI/CD, des outils d'analyse de logs unifiés, des indicateurs de performance, de sécurité et de disponibilité, en mobilisant des solutions de monitoring temps réel, des tableaux de bord dynamiques et des scripts d'automatisation afin d'anticiper les défaillances et garantir la continuité des services.
- Définir et suivre la politique de sécurité du SI et de protection des données en structurant les dispositifs de contrôle d'accès, de gestion des vulnérabilités, de chiffrement, de journalisation et de gouvernance des données personnelles à l'aide de référentiels normatifs (ISO 27001, NIS2, RGPD) et d'outils de supervision afin de maîtriser les risques et garantir la conformité.
- Réaliser des benchmarks de solutions ou de services numériques en définissant des critères comparatifs techniques, fonctionnels, économiques et réglementaires, en mobilisant des grilles d'analyse multicritères, des retours d'expérience utilisateurs et des référentiels sectoriels afin d'objectiver les choix technologiques.
- Formuler des plans d'amélioration continue du SI en analysant les retours d'expérience, les incidents et les écarts de performance, en mobilisant des outils d'évaluation, des revues post-mortem, des indicateurs de pilotage et des boucles de rétroaction afin de structurer des trajectoires mesurables et alignées sur les objectifs qualité.
- Administrer la gestion du code source et des configurations du SI dans un environnement collaboratif en structurant les workflows de versioning, les politiques de branche, les systèmes d'intégration continue, les règles de revue de code et de traçabilité via des plateformes telles que Git ou GitLab afin de garantir la qualité, la maintenabilité et la sécurité applicative.
- Déployer des pipelines d'intégration et de déploiement automatisé en configurant les étapes critiques du cycle CI/CD et des jobs automatisés de compilation, de tests, de packaging et de déploiement à l'aide d'outils d'orchestration afin d'optimiser la qualité, la traçabilité et la résilience des livraisons et améliorer la performance du cycle de développement.
- Documenter les environnements, les livrables et les évolutions du SI en structurant les référentiels techniques, les guides de déploiement, les journaux de version et les procédures de changement à l'aide d'outils collaboratifs et de normes de structuration documentaire afin d'assurer la traçabilité et la conformité.
- Identifier les vulnérabilités des systèmes, applications et flux de données en mobilisant des outils d'analyse de vulnérabilités, de scans automatisés, de tests d'intrusion manuels ou scriptés et d'audits de configuration afin de réduire les surfaces d'attaque, de prioriser les actions correctives et de garantir la robustesse du SI face aux menaces.
- Sécuriser la gestion des accès, des secrets et des certificats au sein du SI en configurant des politiques de contrôle

d'accès (RBAC, ABAC), des coffres-forts de secrets, des outils de rotation automatique, de gestion du cycle de vie des certificats et de journalisation cryptographique afin de garantir la confidentialité et l'intégrité des échanges.

- Intégrer la sécurité dans toutes les phases du cycle de vie des projets SI en définissant des exigences de sécurité dès les phases de spécification, en automatisant les contrôles de conformité, en automatisant la validation des règles de sécurité dans les pipelines CI/CD, en documentant les arbitrages de sécurité et en mobilisant des outils DevSecOps afin de garantir une protection continue et une conformité réglementaire.
- Déployer des outils de supervision, d'observabilité et de contrôle de la qualité des données dans les environnements applicatifs et techniques en configurant des solutions de monitoring applicatif (APM), de collecte et d'analyse de logs, de métriques systèmes et de règles de data quality afin d'anticiper les dégradations et fiabiliser les systèmes.
- Concevoir des scénarios de tests techniques et de performance du SI en définissant des cas de test représentatifs des charges réelles, en mobilisant des outils de test automatisés, de simulation de montée en charge, de profiling et d'analyse comparative afin de valider la robustesse et la conformité des solutions aux exigences de service.
- Suivre les indicateurs de fiabilité, d'usage et de valeur ajoutée métier d'une solution numérique en définissant des métriques pertinentes, en exploitant des outils de monitoring applicatif, d'analyse comportementale et de business intelligence afin d'orienter les actions d'optimisation continue.
- Renforcer la sécurité des environnements d'exécution des solutions numériques en appliquant des politiques de durcissement (bastion, sandbox, chroot, conteneurs isolés), en configurant des systèmes de détection d'anomalies comportementales et en intégrant des profils de sécurité adaptés afin de réduire les risques et garantir l'intégrité des environnements critiques.
- Intégrer les exigences d'accessibilité numérique, d'inclusivité et de prise en compte des besoins spécifiques dans la conception, le développement et la supervision des solutions numériques en appliquant les référentiels RGAA/WCAG, en analysant les parcours utilisateurs et en mobilisant les outils de test adaptés afin de garantir l'équité d'usage et la conformité.
- Modéliser une architecture logicielle scalable et data-centric en sélectionnant des styles architecturaux adaptés, en structurant les flux de données, les mécanismes de persistance, de transformation et d'exposition adaptés aux exigences de performance, d'accessibilité et de personnalisation des parcours utilisateurs afin de garantir la performance et la valorisation stratégique du SI.
- Développer des applications web, mobiles ou backend exploitant les données en implémentant des interfaces responsives, des services REST ou GraphQL, des connecteurs d'accès aux sources de données structurées ou non structurées et des mécanismes de traitement applicatif optimisé afin d'assurer cohérence, fluidité et performance
- Intégrer des API, des frameworks applicatifs et les contraintes de sécurité, de performance, de conformité et d'accessibilité numérique dans la conception d'applications en sélectionnant des bibliothèques éprouvées, en configurant les règles d'authentification et de gestion des accès, en implémentant des tests de performance, de conformité RGPD et d'accessibilité afin de garantir leur robustesse, leur inclusivité et leur conformité réglementaire.
- Préparer des données en vue d'analyse en collectant les jeux de données multi-sources, en nettoyant les anomalies, doublons ou valeurs manquantes, en transformant et structurant les données à l'aide d'outils de data wrangling, d'ETL ou de scripts automatisés afin de garantir leur qualité, leur intégrité et leur exploitabilité dans des pipelines d'analyse avancée ou d'IA.
- Réaliser un modèle d'apprentissage automatique en sélectionnant les algorithmes adaptés à la nature des données et aux objectifs d'analyse, en préparant les jeux d'entraînement et de validation, en paramétrant les hyperparamètres, en évaluant les performances à l'aide de métriques appropriées et en analysant les biais afin de garantir la robustesse, la fiabilité et la pertinence des résultats.
- Intégrer un modèle d'analyse ou d'apprentissage automatique dans une solution logicielle en exposant les résultats via des API sécurisées, des composants d'interface ou des tableaux de bord dynamiques, en mobilisant des outils de déploiement, de visualisation et de monitoring des performances afin d'en assurer l'exploitabilité, la valeur métier et la maintenabilité technique
- Superviser les performances, les biais et les dérives des modèles d'analyse ou d'apprentissage automatique en instrumentant des métriques de suivi en configurant des outils de monitoring de production, en analysant les comportements du modèle face à de nouvelles données et en détectant les écarts de comportement statistique et les tentatives d'attaques ciblées sur les modèles afin de garantir leur équité, leur fiabilité et leur adaptation dans le temps.
- Documenter les modèles, jeux de données et traitements d'apprentissage automatique en structurant les métadonnées, les fiches de version, les fiches d'explicabilité, les journaux d'expérimentation et les conditions d'usage à l'aide d'outils collaboratifs et de référentiels de gouvernance afin de garantir leur transparence, leur traçabilité et leur conformité.

- Proposer des axes d'amélioration continue des solutions intelligentes en analysant les écarts de performance, les retours d'usage, les métriques d'équité et de robustesse, en mobilisant des outils de visualisation, des audits de gouvernance, des revues de cycle de vie et des benchmarks de pratiques afin de renforcer la valeur métier des dispositifs data, IA et UX.
- Industrialiser le cycle de vie des modèles d'intelligence artificielle en orchestrant les processus de mise en production, de réentraînement automatisé, de suivi de version, de validation continue et de retraitement périodique à l'aide d'outils de MLOps et de gouvernance afin d'en garantir la fiabilité, la reproductibilité et la conformité durable.
- Déployer des environnements virtualisés, conteneurisés ou cloud en sélectionnant des architectures adaptées aux exigences d'élasticité, de haute disponibilité et de sécurité, en configurant des outils d'orchestration et des services managés afin de garantir leur scalabilité, portabilité et résilience.
- Administrer les ressources réseau, systèmes, stockage et base de données en configurant des environnements virtualisés ou physiques, en mobilisant des outils d'automatisation, de supervision et de gestion de la performance afin d'assurer la disponibilité, la fiabilité et la performance des services.
- Optimiser la disponibilité, la scalabilité et la résilience des infrastructures numériques en configurant des mécanismes de redondance, de load balancing, d'auto-scaling et de reprise après sinistre à l'aide d'architectures distribuées, de services managés et de solutions multi-régions afin de garantir la continuité de service.
- Mettre en place des outils de supervision, de sauvegarde et d'alerte dans des environnements hybrides ou cloud en configurant des sondes de collecte, des tableaux de bord dynamiques, des politiques de sauvegarde automatisées, des scripts de vérification d'intégrité et des mécanismes d'alerte multicritères afin d'anticiper les incidents et garantir la résilience du SI.
- Automatiser la gestion des infrastructures numériques en développant des scripts d'administration et en mobilisant des outils d'infrastructure as code pour provisionner, configurer et maintenir les ressources systèmes, réseaux et cloud afin de provisionner, maintenir et tracer les ressources dans des environnements hybrides ou cloud.
- Gérer les identités, les accès et les permissions au sein d'infrastructures hybrides ou cloud en configurant des politiques d'authentification forte, des mécanismes d'autorisation granulaire, des services IAM et des solutions de fédération d'identités afin d'assurer la sécurité et la conformité des accès.
- Réaliser des audits de sécurité et des tests d'intrusion sur les infrastructures numériques en mobilisant des outils de scanning de vulnérabilités, des techniques de pentest manuels ou automatisés, des sondes d'analyse comportementale, des plateformes SOC et des solutions SIEM afin d'identifier les failles et formuler des recommandations correctives.
- Piloter une réponse à incident de cybersécurité en activant les plans de continuité et de reprise d'activité, en coordonnant les parties prenantes internes et externes, et en appliquant les référentiels (NIS2, ISO 27035) afin de minimiser les impacts opérationnels, réglementaires et réputationnels.
- Mettre en œuvre des politiques de conformité et de durcissement des environnements d'exécution en appliquant des benchmarks de sécurité, des principes Zero Trust et des contrôles de configuration automatisés afin de réduire la surface d'attaque et renforcer la sécurité.

Blocs de compétences

RNCP41988BC01 — Définir la vision stratégique du système d'information (SI)

LISTE DE COMPÉTENCES

- Identifier les besoins métiers, utilisateurs et data-driven en exploitant des techniques de modélisation des processus, des outils de collecte et d'analyse des données structurées et non structurées, ainsi que des méthodes de co-conception afin de produire un cahier des charges aligné, robuste et conforme.
- Évaluer l'architecture, les performances, les usages et les vulnérabilités du SI en mobilisant des outils d'analyse de trafic, de benchmarks applicatifs, d'audit de code et de tests de sécurité afin de produire un diagnostic orienté décision et sécurisé.
- Évaluer la maturité numérique de l'organisation en mobilisant des référentiels de diagnostic, des indicateurs de performance et des outils d'analyse systémique afin d'orienter l'évolution du SI selon les capacités de l'organisation.
- Modéliser la cartographie fonctionnelle, stratégique, technique, data et de sécurité du SI en combinant l'analyse des dépendances internes et externes, des ateliers de co-construction avec les parties prenantes, des audits documentaires et des outils de modélisation afin de sécuriser les scénarios d'évolution et de maîtriser les risques.
- Anticiper les évolutions technologiques, métiers et réglementaires impactant le SI en qualifiant les sources d'innovation pertinentes, en analysant leurs effets sur la trajectoire du SI et en intégrant les exigences de conformité

et d'agilité afin de structurer une veille stratégique opérationnelle à forte valeur décisionnelle.

- Structurer la restitution des résultats de veille technologique, métier et réglementaire en mobilisant des outils de visualisation stratégique, des synthèses analytiques orientées décision et des formats adaptés aux parties prenantes afin d'éclairer les arbitrages dans la définition et la priorisation des orientations d'évolution du SI.
- Construire les orientations stratégiques d'évolution du SI en élaborant des scénarios d'urbanisation et en intégrant une stratégie de gouvernance des données fondée sur l'analyse des usages, des contraintes de conformité et des enjeux de qualité, de sécurité et d'éthique, afin de proposer une trajectoire évolutive, fiable et responsable pour le SI.
- Aligner la vision stratégique du SI avec les engagements RSE de l'organisation en évaluant les impacts environnementaux, sociaux et éthiques des orientations technologiques afin de soutenir une transformation numérique durable, inclusive et conforme aux exigences sociétales.
- Projeter l'architecture cible du SI en alignant les objectifs métier et technologiques, en mobilisant des référentiels d'architecture (TOGAF, Zachman), des principes de scalabilité, d'interopérabilité et de résilience, ainsi que des modèles de gouvernance intégrée afin de structurer une trajectoire cohérente, soutenable et pilotable de transformation du SI.
- Définir la stratégie de cybersécurité de l'organisation en alignant les exigences techniques, réglementaires et métiers avec les référentiels (ISO 27001, NIST, EBIOS RM), en structurant les dispositifs de pilotage et en mesurant la maturité afin d'assurer la conformité, la résilience et la gouvernance globale du SI

MODALITÉS D'ÉVALUATION

Une étude de cas stratégique individuelle contextualisée

Le candidat reçoit un dossier entreprise incluant :

- Des données stratégiques, métiers, data et réglementaires ;
- Un schéma d'architecture SI existant ;
- Des documents de veille et de benchmark ;
- Des indicateurs d'usage et de maturité numérique.

Il lui est demandé de produire dans un dossier rédigé comprenant :

- Un diagnostic structuré du SI (cartographie, performance, alignement stratégique, maturité) ;
- Des orientations d'évolution justifiées (urbanisation, gouvernance data, sobriété numérique) ;
- Un plan d'architecture cible argumenté, intégrant des éléments de gouvernance, de sécurité et de RSE ;
- Une restitution graphique et une présentation des arbitrages au format note de synthèse ou soutenance professionnelle.

Des aménagements spécifiques sont prévus pour les candidats en situation de handicap, sur demande formalisée et justifiée.

RNCP41988BC02 — Piloter un projet de transformation ou de développement du système d'information (SI)

LISTE DE COMPÉTENCES

- Formaliser une note de cadrage du projet de transformation du SI en analysant les besoins exprimés et implicites des parties prenantes, les enjeux métier, les contraintes techniques et réglementaires, à l'aide d'outils de clarification des objectifs, de matrice d'analyse de la valeur et de grille d'arbitrage stratégique afin de structurer un référentiel de pilotage cohérent et aligné.
- Qualifier les parties prenantes, les risques et les impacts métiers d'un projet de transformation du SI en mobilisant des outils d'analyse d'enjeux, de cartographie d'acteurs, de matrices de criticité et de simulation d'impact organisationnel afin de sécuriser les choix de conception, de structuration et de pilotage du projet.
- Structurer le planning et le budget d'un projet de transformation du SI en mobilisant des méthodes de découpage en lots (WBS), des outils de planification (PERT, GANTT), des grilles d'estimation des charges et des référentiels de coûts afin d'optimiser l'allocation des ressources, de maîtriser les délais.
- Piloter l'avancement d'un projet de transformation du SI en analysant les écarts entre prévisionnel et réalisé à l'aide d'indicateurs techniques, financiers, data et ROI, en mobilisant des outils de reporting dynamique, de tableaux de bord et de revues de jalons afin d'ajuster les plans d'action et garantir l'atteinte des objectifs.
- Évaluer les impacts et les résultats d'un projet de transformation du SI en mobilisant des indicateurs de performance, des matrices d'impact, des analyses de parcours utilisateur et des revues de gouvernance des données afin de fiabiliser les arbitrages, garantir la valeur délivrée et de capitaliser les apprentissages pour les projets futurs.
- Définir les rôles, les responsabilités et les compétences nécessaires à la réussite d'un projet de transformation du SI en mobilisant des matrices de responsabilités (RACI, MOF), des référentiels de compétences, des analyses de charge et des entretiens avec les parties prenantes afin de structurer une organisation projet efficace, lisible et

adaptée aux exigences du projet.

- Encadrer une équipe technique ou projet mobilisée sur un SI en définissant les objectifs collectifs et individuels, en structurant les modes de fonctionnement collaboratif, les rituels de pilotage et les parcours de montée en compétences afin de garantir la performance collective et la motivation durable.
- Coordonner les interactions entre les équipes internes, les partenaires et les fournisseurs impliqués dans un projet de transformation du SI en définissant les responsabilités, les modalités de collaboration, les engagements contractuels et les outils de pilotage collaboratif afin d'assurer la cohésion opérationnelle, la performance collective et la conformité aux objectifs du projet.
- Mettre en œuvre des méthodes d'organisation du travail adaptées aux projets de transformation du SI en combinant des approches agiles, hybrides ou itératives, des outils de pilotage par la valeur, des dispositifs de gestion de la charge et des rituels de coordination afin d'optimiser la fluidité, l'engagement et la performance projet.

MODALITÉS D'ÉVALUATION

Projet tutoré de conduite de projet SI

En groupe

Évaluation individualisée

Sur la base d'un cahier des charges partiellement défini, les candidats :

- Formalisent la note de cadrage complète,
- Élaborent le planning et le budget avec outils adaptés (PERT, GANTT, WBS),
- Pilotent l'avancement et les indicateurs ROI/data.

L'équipe produit un dossier projet complet et chaque candidat soutient une séquence du projet devant un jury professionnel.

Les livrables attendus sont :

Note de cadrage, planning, budget, jalons suivis, livrables projet.

Soutenance orale individuelle devant un jury extérieur constitué à minima de 2 professionnels du secteur, comprenant une partie en langue anglaise (contexte du projet)

Cette soutenance s'appuie sur un dossier projet constitué des preuves et de la description de la mise en œuvre des différentes compétences

Des aménagements spécifiques sont prévus pour les candidats en situation de handicap, sur demande formalisée et justifiée.

RNCP41988BC03 — Maintenir la performance et la sécurité opérationnelle du système d'information (SI)

LISTE DE COMPÉTENCES

- Résoudre les incidents techniques, applicatifs et data affectant le SI en mobilisant des outils d'observabilité, d'analyse de logs, de supervision temps réel et de traçabilité des flux afin de restaurer la disponibilité des services, d'identifier les causes racines et de fiabiliser le fonctionnement opérationnel du SI.
- Automatiser la gestion des incidents et des actions de remédiation dans les environnements SI en structurant des procédures déclenchables (runbooks), en configurant des outils d'orchestration (SOAR, scripts, workflows) et en intégrant des seuils d'alerte déclencheurs afin de réduire les délais, renforcer la réactivité et assurer la continuité de service.
- Déployer des évolutions correctives ou adaptatives du SI en analysant les causes techniques, fonctionnelles ou data des écarts de performance, en mobilisant des outils de gestion des versions, de tests de non-régression, de documentation et de supervision continue afin d'assurer la stabilité et la conformité du SI.
- Formaliser la documentation des actions de maintenance du SI en structurant les procédures, les journaux d'intervention, les historiques de configuration, les matrices de conformité et les enseignements post-incidents afin de garantir la traçabilité, la capitalisation et le respect des obligations.
- Réaliser des audits de performance, de sécurité et de conformité du SI en mobilisant des outils d'analyse de vulnérabilités, de métrologie applicative, de contrôle des flux de données et de conformité réglementaire (RGPD, SLA, ISO) afin d'identifier les écarts et formuler des recommandations.
- Configurer des outils de supervision et d'alerte du SI en intégrant en y intégrant des dashboards DevOps, des métriques CI/CD, des outils d'analyse de logs unifiés, des indicateurs de performance, de sécurité et de disponibilité, en mobilisant des solutions de monitoring temps réel, des tableaux de bord dynamiques et des scripts d'automatisation afin d'anticiper les défaillances et garantir la continuité des services.
- Définir et suivre la politique de sécurité du SI et de protection des données en structurant les dispositifs de contrôle d'accès, de gestion des vulnérabilités, de chiffrement, de journalisation et de gouvernance des données personnelles à l'aide de référentiels normatifs (ISO 27001, NIS2, RGPD) et d'outils de supervision afin de maîtriser les risques et

garantir la conformité.

- Réaliser des benchmarks de solutions ou de services numériques en définissant des critères comparatifs techniques, fonctionnels, économiques et réglementaires, en mobilisant des grilles d'analyse multicritères, des retours d'expérience utilisateurs et des référentiels sectoriels afin d'objectiver les choix technologiques.
- Formuler des plans d'amélioration continue du SI en analysant les retours d'expérience, les incidents et les écarts de performance, en mobilisant des outils d'évaluation, des revues post-mortem, des indicateurs de pilotage et des boucles de rétroaction afin de structurer des trajectoires mesurables et alignées sur les objectifs qualité.

MODALITÉS D'ÉVALUATION

Une mise en situation technique avec dossier d'incident

Le candidat analyse un incident critique (technique, applicatif, data) sur un SI fictif, en mobilisant :

- Outils d'analyse de logs, de supervision et d'audit ;
- Scénarios d'évolution correctives ;
- Documentation et reporting réglementaire (conformité RGPD/SLA).

Il propose également un benchmark de solutions et un plan structuré d'amélioration continue.

Livrables :

Rapport d'intervention technique (50 à 60 pages) + documentation de maintenance + benchmark et plan d'optimisation.

Soutenance orale devant un jury extérieur constitué à minima de 2 professionnels du secteur.

Des aménagements spécifiques sont prévus pour les candidats en situation de handicap, sur demande formalisée et justifiée notamment pour des profils ayant des limitations physiques ou cognitives (aménagements logiciels, format de code, démonstration orale, etc.)

RNCP41988BC04 — Superviser la cybersécurité et la conformité des solutions numériques

LISTE DE COMPÉTENCES

- Administrer la gestion du code source et des configurations du SI dans un environnement collaboratif en structurant les workflows de versioning, les politiques de branche, les systèmes d'intégration continue, les règles de revue de code et de traçabilité via des plateformes telles que Git ou GitLab afin de garantir la qualité, la maintenabilité et la sécurité applicative.
- Déployer des pipelines d'intégration et de déploiement automatisé en configurant les étapes critiques du cycle CI/CD et des jobs automatisés de compilation, de tests, de packaging et de déploiement à l'aide d'outils d'orchestration afin d'optimiser la qualité, la traçabilité et la résilience des livraisons et améliorer la performance du cycle de développement.
- Documenter les environnements, les livrables et les évolutions du SI en structurant les référentiels techniques, les guides de déploiement, les journaux de version et les procédures de changement à l'aide d'outils collaboratifs et de normes de structuration documentaire afin d'assurer la traçabilité et la conformité.
- Identifier les vulnérabilités des systèmes, applications et flux de données en mobilisant des outils d'analyse de vulnérabilités, de scans automatisés, de tests d'intrusion manuels ou scriptés et d'audits de configuration afin de réduire les surfaces d'attaque, de prioriser les actions correctives et de garantir la robustesse du SI face aux menaces.
- Sécuriser la gestion des accès, des secrets et des certificats au sein du SI en configurant des politiques de contrôle d'accès (RBAC, ABAC), des coffres-forts de secrets, des outils de rotation automatique, de gestion du cycle de vie des certificats et de journalisation cryptographique afin de garantir la confidentialité et l'intégrité des échanges.
- Intégrer la sécurité dans toutes les phases du cycle de vie des projets SI en définissant des exigences de sécurité dès les phases de spécification, en automatisant les contrôles de conformité, en automatisant la validation des règles de sécurité dans les pipelines CI/CD, en documentant les arbitrages de sécurité et en mobilisant des outils DevSecOps afin de garantir une protection continue et une conformité réglementaire.
- Déployer des outils de supervision, d'observabilité et de contrôle de la qualité des données dans les environnements applicatifs et techniques en configurant des solutions de monitoring applicatif (APM), de collecte et d'analyse de logs, de métriques systèmes et de règles de data quality afin d'anticiper les dégradations et fiabiliser les systèmes.
- Concevoir des scénarios de tests techniques et de performance du SI en définissant des cas de test représentatifs des charges réelles, en mobilisant des outils de test automatisés, de simulation de montée en charge, de profiling et d'analyse comparative afin de valider la robustesse et la conformité des solutions aux exigences de service.
- Suivre les indicateurs de fiabilité, d'usage et de valeur ajoutée métier d'une solution numérique en définissant des métriques pertinentes, en exploitant des outils de monitoring applicatif, d'analyse comportementale et de business

intelligence afin d'orienter les actions d'optimisation continue.

- Renforcer la sécurité des environnements d'exécution des solutions numériques en appliquant des politiques de durcissement (bastion, sandbox, chroot, conteneurs isolés), en configurant des systèmes de détection d'anomalies comportementales et en intégrant des profils de sécurité adaptés afin de réduire les risques et garantir l'intégrité des environnements critiques.
- Intégrer les exigences d'accessibilité numérique, d'inclusivité et de prise en compte des besoins spécifiques dans la conception, le développement et la supervision des solutions numériques en appliquant les référentiels RGAA/WCAG, en analysant les parcours utilisateurs et en mobilisant les outils de test adaptés afin de garantir l'équité d'usage et la conformité.

MODALITÉS D'ÉVALUATION

Atelier technique encadré (type DevSecOps Lab/ Hackathon)

Le candidat reçoit une chaîne applicative à auditer et sécuriser.

Il doit :

- Intégrer des contrôles CI/CD ;
- Implémenter des mesures de sécurité (vulnérabilités, RBAC, chiffrement, DevSecOps) ;
- Vérifier la conformité RGPD, accessibilité, durcissement environnement.

Le candidat devra justifier le respect des obligations de sécurité applicative et réglementaire à travers l'intégration documentée d'outils de contrôle automatisé, la référence aux normes en vigueur (RGPD, ISO, OWASP), et l'évaluation des risques résiduels.

L'épreuve inclut aussi une restitution synthétique des choix faits.

Livrables :

Configuration technique + document de conformité + Présentation orale individuelle de la réalisation et démonstration devant un professionnel

Des aménagements spécifiques sont prévus pour les candidats en situation de handicap, sur demande formalisée et justifiée notamment pour des profils ayant des limitations physiques ou cognitives (aménagements logiciels, format de code, démonstration orale, etc.)

RNCP41988BC05 — Développer et déployer des solutions logicielles, Data & IA

LISTE DE COMPÉTENCES

- Modéliser une architecture logicielle scalable et data-centric en sélectionnant des styles architecturaux adaptés, en structurant les flux de données, les mécanismes de persistance, de transformation et d'exposition adaptés aux exigences de performance, d'accessibilité et de personnalisation des parcours utilisateurs afin de garantir la performance et la valorisation stratégique du SI.
- Développer des applications web, mobiles ou backend exploitant les données en implémentant des interfaces responsives, des services REST ou GraphQL, des connecteurs d'accès aux sources de données structurées ou non structurées et des mécanismes de traitement applicatif optimisé afin d'assurer cohérence, fluidité et performance
- Intégrer des API, des frameworks applicatifs et les contraintes de sécurité, de performance, de conformité et d'accessibilité numérique dans la conception d'applications en sélectionnant des bibliothèques éprouvées, en configurant les règles d'authentification et de gestion des accès, en implémentant des tests de performance, de conformité RGPD et d'accessibilité afin de garantir leur robustesse, leur inclusivité et leur conformité réglementaire.
- Préparer des données en vue d'analyse en collectant les jeux de données multi-sources, en nettoyant les anomalies, doublons ou valeurs manquantes, en transformant et structurant les données à l'aide d'outils de data wrangling, d'ETL ou de scripts automatisés afin de garantir leur qualité, leur intégrité et leur exploitabilité dans des pipelines d'analyse avancée ou d'IA.
- Réaliser un modèle d'apprentissage automatique en sélectionnant les algorithmes adaptés à la nature des données et aux objectifs d'analyse, en préparant les jeux d'entraînement et de validation, en paramétrant les hyperparamètres, en évaluant les performances à l'aide de métriques appropriées et en analysant les biais afin de garantir la robustesse, la fiabilité et la pertinence des résultats.
- Intégrer un modèle d'analyse ou d'apprentissage automatique dans une solution logicielle en exposant les résultats via des API sécurisées, des composants d'interface ou des tableaux de bord dynamiques, en mobilisant des outils de déploiement, de visualisation et de monitoring des performances afin d'en assurer l'exploitabilité, la valeur métier et la maintenabilité technique
- Superviser les performances, les biais et les dérives des modèles d'analyse ou d'apprentissage automatique en instrumentant des métriques de suivi en configurant des outils de monitoring de production, en analysant les comportements du modèle face à de nouvelles données et en détectant les écarts de comportement statistique et les

tentatives d'attaques ciblées sur les modèles afin de garantir leur équité, leur fiabilité et leur adaptation dans le temps.

- Documenter les modèles, jeux de données et traitements d'apprentissage automatique en structurant les métadonnées, les fiches de version, les fiches d'explicabilité, les journaux d'expérimentation et les conditions d'usage à l'aide d'outils collaboratifs et de référentiels de gouvernance afin de garantir leur transparence, leur traçabilité et leur conformité.
- Proposer des axes d'amélioration continue des solutions intelligentes en analysant les écarts de performance, les retours d'usage, les métriques d'équité et de robustesse, en mobilisant des outils de visualisation, des audits de gouvernance, des revues de cycle de vie et des benchmarks de pratiques afin de renforcer la valeur métier des dispositifs data, IA et UX.
- Industrialiser le cycle de vie des modèles d'intelligence artificielle en orchestrant les processus de mise en production, de réentraînement automatisé, de suivi de version, de validation continue et de retraitement périodique à l'aide d'outils de MLOps et de gouvernance afin d'en garantir la fiabilité, la reproductibilité et la conformité durable.

MODALITÉS D'ÉVALUATION

Projet technique individuel

Le candidat reçoit :

- Un jeu de données métier,
- Un besoin utilisateur
- Des contraintes techniques (RGPD, performance, IA).

Il développe une solution applicative data-driven intégrant :

- Collecte, nettoyage, structuration des données ;
- Modélisation IA (training + métriques) ;
- Visualisation ou intégration métier (dashboard/API) ;
- Documentation explicable, accessible et traçable.

Livrables :

Code source + note technique + présentation fonctionnelle.

Des aménagements spécifiques sont prévus pour les candidats en situation de handicap, sur demande formalisée et justifiée.

RNCP41988BC06 — Concevoir et superviser des infrastructures numériques et cloud

LISTE DE COMPÉTENCES

- Déployer des environnements virtualisés, conteneurisés ou cloud en sélectionnant des architectures adaptées aux exigences d'élasticité, de haute disponibilité et de sécurité, en configurant des outils d'orchestration et des services managés afin de garantir leur scalabilité, portabilité et résilience.
- Administrer les ressources réseau, systèmes, stockage et base de données en configurant des environnements virtualisés ou physiques, en mobilisant des outils d'automatisation, de supervision et de gestion de la performance afin d'assurer la disponibilité, la fiabilité et la performance des services.
- Optimiser la disponibilité, la scalabilité et la résilience des infrastructures numériques en configurant des mécanismes de redondance, de load balancing, d'auto-scaling et de reprise après sinistre à l'aide d'architectures distribuées, de services managés et de solutions multi-régions afin de garantir la continuité de service.
- Mettre en place des outils de supervision, de sauvegarde et d'alerte dans des environnements hybrides ou cloud en configurant des sondes de collecte, des tableaux de bord dynamiques, des politiques de sauvegarde automatisées, des scripts de vérification d'intégrité et des mécanismes d'alerte multicritères afin d'anticiper les incidents et garantir la résilience du SI.
- Automatiser la gestion des infrastructures numériques en développant des scripts d'administration et en mobilisant des outils d'infrastructure as code pour provisionner, configurer et maintenir les ressources systèmes, réseaux et cloud afin de provisionner, maintenir et tracer les ressources dans des environnements hybrides ou cloud.
- Gérer les identités, les accès et les permissions au sein d'infrastructures hybrides ou cloud en configurant des politiques d'authentification forte, des mécanismes d'autorisation granulaire, des services IAM et des solutions de fédération d'identités afin d'assurer la sécurité et la conformité des accès.
- Réaliser des audits de sécurité et des tests d'intrusion sur les infrastructures numériques en mobilisant des outils de scanning de vulnérabilités, des techniques de pentest manuels ou automatisés, des sondes d'analyse comportementale, des plateformes SOC et des solutions SIEM afin d'identifier les failles et formuler des recommandations correctives.
- Piloter une réponse à incident de cybersécurité en activant les plans de continuité et de reprise d'activité, en coordonnant les parties prenantes internes et externes, et en appliquant les référentiels (NIS2, ISO 27035) afin de

minimiser les impacts opérationnels, réglementaires et réputationnels.

- Mettre en œuvre des politiques de conformité et de durcissement des environnements d'exécution en appliquant des benchmarks de sécurité, des principes Zero Trust et des contrôles de configuration automatisés afin de réduire la surface d'attaque et renforcer la sécurité.

MODALITÉS D'ÉVALUATION

Projet technique individuel sur environnement cloud

Le candidat reçoit un cahier des charges pour déployer une infrastructure résiliente.

Il est évalué sur sa capacité à :

- Configurer des environnements hybrides (cloud, conteneurs, supervision) ;
- Implémenter des mécanismes de sécurité et de supervision ;
- Réaliser des audits et tests d'intrusion ;
- Documenter les choix, risques et plans de reprise.

Livrables :

Infrastructure fonctionnelle + rapport de sécurisation + soutenance orale.

Des aménagements spécifiques sont prévus pour les candidats en situation de handicap, sur demande formalisée et justifiée.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les grandes entreprises et groupes internationaux comme le secteur banque/assurance, énergie, défense, télécoms, industrie, santé

Les Entreprises de Services du Numérique (ESN) et cabinets de conseil spécialisés en cybersécurité

Les startups technologiques

Le secteur public comme les ministères, collectivités, hôpitaux, établissements publics

Les Opérateurs d'Importance Vitale (OIV) et les Opérateurs de Services Essentiels (OSE)

TYPE D'EMPLOIS ACCESSIBLES

Administrateur/trice Système et réseau

Ingénieur Étude et développement

Ingénieur Système et réseau

Consultant (e) IT

Responsable informatique

Ingénieur DEVOPS

Consultant (e) sécurité, Ingénieur Sécurité

CTO : Chief Technical Officer

RÉGLEMENTATIONS D'ACTIVITÉ

Le métier d'expert en ingénierie et cybersécurité des systèmes d'information n'est pas une activité réglementée au sens juridique.

Son exercice n'est soumis à aucune obligation légale de détention d'un diplôme d'État, d'autorisation administrative ou d'appartenance à un ordre professionnel.

En revanche, les professionnels intervenant dans ce domaine doivent maîtriser un ensemble de référentiels techniques et réglementaires et respecter des obligations de conformité strictes, en particulier lorsqu'ils opèrent dans des secteurs critiques (finance, santé, administration, infrastructures essentielles).

La certification visée prépare donc à exercer un métier non réglementé, mais exposé à de fortes exigences normatives, notamment en matière de cybersécurité, de protection des données personnelles et de gouvernance des systèmes d'information.

Le professionnel mobilise, selon les contextes, les référentiels suivants :

- Référentiels en cybersécurité
- Référentiels réglementaires et légaux
- Référentiels d'architecture, gouvernance et management SI
- Référentiels techniques, DevSecOps, cloud et data
- Accessibilité, inclusion, durabilité

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)	2 942 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (19 % des actifs en emploi)
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (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)	16 497
Jugés difficiles à recruter	46 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X91 — Chefs de projet et directeurs de service informatique 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, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

Etre titulaire d'une certification de niveau 6 type "Licence" ou "titre professionnel", spécialisé dans les métiers de l'informatique, avec une spécialité/option en développement/programmation (Titre professionnel Concepteur Développeur d'Applications, Licence Professionnelle Métiers de l'informatique).

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

Le jury est composé de 4 membres dont 3 professionnels externes

COMPOSITION DU JURY — VAE

Le jury est composé de 2 professionnels externes

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	7 141 €
Selon la branche	5 850 € – 7 669 €

Prise en charge	Branches concernées
7 141 €	Valeur par défaut · 196 branches
7 669 €	CPNEFP Commerce à distance, CPNEFP dans les établissements d'enseignement privés sous contrat, CPNEFP des jardineries et graineteries
6 979 €	CPNE des industries de santé (CPNEIS), CPNEFP de la branche des prestataires de services du secteur tertiaire, CPNEFP des commerces de gros
7 650 €	CPNE Branche Caoutchouc, CPNEFP de la métallurgie
6 930 €	CPNEF de l'audiovisuel, CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
7 533 €	CPNE de l'ingénierie, des services informatiques et du conseil
7 335 €	CPNEFP de la branche des industries de produits alimentaires élaborés
7 154 €	CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique
7 126 €	CPNE des Télécoms
6 889 €	CPNEF de la Publicité
6 390 €	CPNE Banque
5 850 €	CPNEF inter-secteurs papier carton

Base légale

Date de décision	27/02/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	27/02/2029
Date de dernière délivrance possible	27/02/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2024	70	0	73 %	—
2023	75	0	93 %	74 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP35726

CORRESPONDANCES (PAR BLOCS)

RNCP35275, RNCP35284, RNCP35726, RNCP36469, RNCP36912, RNCP38004, RNCP38823, RNCP38951, RNCP39582, RNCP39765, RNCP40147, RNCP40363

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.h3hitema.fr/h3-hitema/debouches-issue-formation-informatique/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/41988/>