

Expert en systèmes d'information sécurisés (Cloud ou Big Data)

RNCP38837 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	31023, 31032, 31006, 31096
Code(s) ROME	M1805, M1810, M1802, M1806, M1803
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	27/03/2024
Date d'échéance	27/03/2027

Certificateur(s)

IP-FORMATION · SIRET : 42079370500047

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'objectif principal de cette certification est de former des professionnels hautement qualifiés dans le domaine de la cyber sécurité et du Big data (selon l'option choisie). Les apprenants acquerront une expertise approfondie en matière de protection des systèmes d'information, de gestion des risques, de détection et de réponse aux incidents de sécurité, ainsi que de conformité réglementaire mais également, les principes fondamentaux de la gestion des données, les techniques d'analyse avancées et les méthodologies pour extraire des informations utiles à partir de grandes quantités de données.

Les apprenants doivent être en mesure de concevoir des architectures sécurisées pour les systèmes d'information, en prenant en compte les aspects liés à la cyber sécurité et au big data. Ils doivent être capables d'identifier les vulnérabilités potentielles, de mettre en place des mécanismes de prévention et de détection des attaques, et de proposer des solutions adaptées pour garantir la protection des données tout en développant des compétences de leadership et management pour diriger efficacement des équipes, de gérer des projets complexes et de prendre des décisions stratégiques dans le domaine de la cyber sécurité et du big data.

La certification met l'accent sur la compréhension des enjeux actuels forts. Les apprenants doivent être conscients des menaces émergentes, des nouvelles technologies et des tendances du secteur. Ils doivent également être capables de s'adapter rapidement aux évolutions technologiques et aux changements réglementaires.

Cette certification répond à la demande croissante de professionnels hautement qualifiés dans ces domaines. Le contexte actuel est marqué par une augmentation significative des cyberattaques, des violations de données et des exigences réglementaires en matière de protection des informations.

Les organisations sont de plus en plus conscientes des risques liés à la cyber sécurité et cherchent à renforcer leur posture de sécurité. Parallèlement, la quantité de données générées et stockées par les entreprises continue de croître de manière exponentielle, offrant des opportunités d'analyse approfondie pour soutenir la prise de décision et l'innovation.

Les diplômés seront prêts à travailler dans différents secteurs tels que la finance, la santé, les services gouvernementaux, l'e-commerce et les entreprises technologiques, où la protection des données et la gestion des risques sont essentielles.

ACTIVITÉS VISÉES

Analyse et évaluation des besoins de l'organisation

- Audit de la structure fonctionnelle d'un SI
- Identification avec la direction générale des informations sensibles et des risques
- Cartographie des risques techniques, sécuritaires et réglementaires
- Recommandations en terme de sécurisation, d'optimisation réseau et d'impact écologique

Conception de la stratégie d'évolution du SI de l'organisation

- Analyse des outils opérationnels de création d'un schéma d'intégration existants sur le marché et répondant au besoin de l'organisation
- Préconisations sur la sélection des solutions à retenir
- Choix des solutions techniques à intégrer lors de l'évolution du SI
- Conception et proposition des solutions d'intégration et d'évolution du SI
- Anticipation des impacts liés aux changements d'orientation des décideurs sur les technologies de l'information- Anticipation des impacts liés à la capacité de traitement des services fournis (croissance forte du nombre de collaborateurs, réplcation de services, exposition d'interconnexion entre les sites d'une même organisation...)
- Conception d'un plan de continuité ou de reprise d'activité

Élaboration d'une stratégie de veille technologique

- Analyse des besoins fonctionnels et opérationnels des utilisateurs du système d'information en interne
- Recueil des informations sur les nouveaux usages et les innovations (Robotique, IoT, Intelligence Artificielle, Blockchain...)
- Choix des outils et détermination des critères de collecte (choix des filtres, élaboration des équations de recherche)
- Mise en place d'alerte sur des sujets spécifiques (ex : Google Alert, ...)

Identification et formalisation du périmètre du projet SI

- Communication avec les membres du SI sur les informations techniques actuelles et historiques
- Étude de l'environnement et des composants techniques adaptés aux besoins attendus
- Rédaction des spécificités organisationnelles et fonctionnelles
- Rédaction des cahiers des charges conformes aux besoins et aux orientations stratégiques définies

Élaboration du dossier technique d'un projet SI

- Identification des dispositifs du SI existants
- Étude d'évolution et de changement des dispositifs (serveurs, logiciels, langages de programmation, composants de sécurité...)
- Formalisation des modifications à apporter sur le SI

Pilotage des phases de développement, de recette (tests unitaires et tests utilisateurs) et d'implémentation

- Respect et suivi du budget
- Respect des délais
- Étude des coûts de projet IT
- Choix des fournisseurs
- Coopération avec les fournisseurs extérieurs
- Réalisation d'un organigramme de développement et définition d'un rétroplanning des points d'avancée
- Pilotage des équipes et définition des rôles de chacun
- Définition et organisation des protocoles de tests

Évaluation de la performance post projet et amélioration continue

- Suivi des retours utilisateurs
- Utilisation des outils de mesure de performance
- Analyse des indicateurs d'utilisation et de performance post intégration
- Interprétation des résultats des indicateurs
- Définition et mise en place d'actions correctives si nécessaire

Analyse et interprétation des données dans un environnement soumis à des contraintes légales et techniques

- Caractérisation d'une donnée
- Cartographie et classification des données
- Définition du circuit de traitement et de diffusion d'une donnée
- Interprétation des contraintes légales liées au RGPD et techniques appliquées à la classification d'une donnée

Conception de la politique de protection des données

- Définition des dispositifs de protection des données
- Conception d'un plan d'actions intégrant le cadre technique, réglementaire et sécuritaire
- Identification des ressources techniques, matérielles et humaines pour la réalisation du plan d'actions

Management des équipes et suivi de la politique de protection des données

- Identification des compétences manquantes dans les équipes et communication de l'information auprès des ressources humaines
- Définition du rôle et des responsabilités de chaque partie prenante de la politique appliquée
- Définition et interprétation des indicateurs de réalisation du plan d'actions
- Suivi de l'avancée des étapes du plan d'actions
- Respect du délai imposé

Les activités relatives à la première option sont :

Création d'une architecture de services Cloud sécurisé

- Analyse et benchmark des différentes plateformes de Cloud
- Définition de la stratégie Cloud public, privé, hybride
- Création d'infrastructures

virtualisées, conteneurisées et en Cloud Computing

- Suivi en continu des outils de monitoring (applicatifs et logiciels, bases de données, couches logiciel, espaces disques, réseaux de télécoms, réseaux informatiques, serveurs, systèmes)
- Identification et diagnostic des dysfonctionnements et des incidents (lié aux ressources d'exploitation)
- Mise en œuvre de mesures correctives
- Assurance de la qualité du service Cloud par des tests

Sécurisation préventive et corrective du système d'information

- Anticipation des comportements d'attaques (usurpation, détournement, interception...) et conception d'une stratégie de sécurisation dans le cadre éthique et légal des réglementations en vigueur
- Audit de sécurité de type test d'intrusion (whitebox, greybox et blackbox)
- Audit de sécurité de type analyse après incident (forensic)
- Analyse et interprétation des logs
- Présentation des résultats de l'audit de sécurité
- Intégration et utilisation des preuves numériques dans le système d'information
- Élaboration de recommandations de sécurisation du système d'information et de la stratégie de défense

Les activités relatives à la seconde option sont :

Collecte, analyse et manipulation des données massives

- Récupération et mise en forme exploitable des données (nettoyage) provenant de sources hétérogènes en respectant la réglementation en vigueur
- Exploration et analyse des données (EDA)
- Développement et utilisation des technologies de récupération et de manipulation de données
- Analyse des données et des datas en présence via des API, de l'Open Data et des technologies spécifiques
- Classement des données par catégorie avec des règles de classification
- Création d'interfaces de visualisation des données (outils de business intelligence, technologies web...)
- Élaboration d'algorithmes et de méthodologies de détection des tendances dans un ensemble de données (analyse statistique)
- Conception et développement d'algorithmes d'intelligence artificielle (Machine Learning, Deep learning,...)

Conception d'architectures Big Data

- Interprétation d'un schéma de Data Lake
- Conception d'un modèle de Data Warehouse
- Définition de la politique de transfert des données entre les différents dispositifs de stockage
- Conception, intégration et utilisation de bases de données
- Création d'outils de transfert de données

COMPÉTENCES ATTESTÉES

- Diagnostiquer et interpréter la structure fonctionnelle d'un SI en identifiant les informations sensibles et les risques techniques, sécuritaires et réglementaires en collaborant avec les décideurs afin de proposer des mesures en accord avec les objectifs généraux et le schéma directeur informatique.
- Réaliser un benchmark des solutions existantes sur le marché, en réalisant une matrice fonctionnelle et budgétaire relative aux différentes fonctionnalités des outils et des besoins de l'organisation afin de sélectionner les solutions les plus adaptées à la problématique métier.
- Conceptualiser et proposer un schéma d'intégration et d'évolution d'un SI en tenant compte des contraintes fonctionnelles, techniques et budgétaires actuelles et à venir afin de proposer des projets d'évolutions, d'adaptations

ou de migration du système d'information en accord avec le développement de l'organisation et les besoins en matière de ressources matérielles, organisationnelles, réglementaires et sécuritaires.

- Définir la politique de continuité ou de reprise d'activité de l'organisation en élaborant un schéma directeur et en intégrant des solutions de réplication afin d'anticiper une paralysie totale ou partielle des services du SI.
- Mettre en place un dispositif de veille technologique, en français et en anglais, en analysant les besoins des destinataires et en sélectionnant les outils concordant aux besoins afin d'anticiper les technologies émergentes (robotique, IOT, intelligence artificielle, blockchain...) qui pourraient participer à une évolution du système d'information de l'organisation.
- Réaliser un benchmark en analysant le système d'information actuel et les solutions techniques existantes répondant au besoin afin de proposer un environnement de composants techniques en adéquation avec le projet.
- Constituer le cahier des charges de conception ou d'évolution du système d'information à partir des propositions validées par les décideurs afin d'accompagner le développement de l'organisation.
- Rédiger les spécificités techniques et fonctionnelles en prenant en compte le cahier des charges du maître d'ouvrage et en étudiant la faisabilité des évolutions techniques souhaitées afin de répondre aux objectifs définis par le cahier des charges.
- Organiser le pilotage et le management des équipes projet en menant à bien les phases de développement, de recette et d'implémentation tout en s'assurant du respect du budget et des délais et en prenant en compte les différentes situation de handicap le cas échéant afin de mettre en œuvre les plans d'évolution du système et les schémas directeurs de la réalisation du projet.
- Organiser et formuler les différents protocoles de tests en collaboration avec les équipes techniques, en rédigeant un dossier technique détaillant ces protocoles afin d'assurer la qualité du fonctionnement des recettes.
- Mesurer la performance du système d'information suite à son évolution, son changement ou la fusion des systèmes d'information en suivant les retours utilisateurs et en analysant les indicateurs d'utilisation et de performance afin de mettre en place des actions correctives si nécessaire.
- Collecter et recenser les données présentes et utilisées au sein d'un système d'information en interprétant le schéma de base de données et en échangeant avec le responsable du SI afin d'énumérer les données stockées par le SI et les données en transition dans le SI.
- Caractériser et classifier les données exploitées dans un SI en interprétant la nature et la forme de chaque donnée et en prenant en compte les contraintes légales liées au RGPD et techniques applicables à la classification afin de réaliser une cartographie complète sur l'utilisation, le stockage et la transition d'une donnée.
- Élaborer un plan d'actions sur la protection des données d'un SI en définissant les dispositifs répondant au cadre technique, réglementaire et sécuritaire adaptés aux données du SI afin de concevoir une politique de protection des données adaptée à l'organisation.
- Répartir les rôles et les objectifs des parties prenantes en réalisant une cartographie des compétences existantes et de celles manquantes par rapport aux besoins du plan d'actions et en prenant en compte les différentes situations de handicap le cas échéant afin d'assurer la réalisation du plan d'actions dans les délais impartis.
- Assurer le suivi du plan d'actions en respectant le budget et la planification des étapes clés afin de veiller à la bonne réalisation du plan d'actions et d'anticiper d'éventuelles adaptations.
- Réaliser un benchmark des plateformes de Cloud en comparant les différents services proposés afin de définir la meilleure stratégie Cloud public, privé, hybride adaptée au besoin.
- Concevoir une stratégie Cloud en interprétant les résultats du benchmark et en prenant en compte les contraintes du système d'information afin de créer une architecture sécurisée uniforme ou répartie.
- Créer l'architecture sécurisée et automatisée en cloud en déployant des services sur les plateformes choisies et garantissant la communication avec le système d'information afin d'assurer le bon fonctionnement et son adaptation aux évolutions.
- Assurer le suivi fonctionnel des services Cloud en intégrant des solutions de monitoring et de diagnostic afin de garantir la qualité de service et d'appliquer d'éventuelles mesures correctives.
- Auditer la sécurité du système d'information à travers des tests d'intrusion et d'analyse de façon automatisée afin de protéger le système d'information de l'entreprise et assurer sa qualité.
- Élaborer une stratégie de sécurisation du système d'information (hardening) en interprétant les résultats de l'audit de sécurité afin de renforcer la sécurité du système d'information.
- Réaliser un audit après incident (forensic) en analysant les logs, preuves numériques et empreintes d'attaques afin d'identifier les failles de sécurité exploitées, ainsi que les ressources impactées.
- Rédiger un rapport d'audit en utilisant les résultats des tests d'intrusion et de l'analyse forensicafin de synthétiser

les résultats d'analyse et des incidents et de recommander une stratégie d'évolution ou de remédiation.

- Collecter et nettoyer des ensembles volumineux de données structurées et non structurées issues de sources internes et externes de l'entreprise à l'aide des technologies de récupération, d'interprétation et de manipulation de données afin d'alimenter l'environnement de Big Data.
- Analyser et visualiser des données volumineuses en utilisant des outils de visualisation et de synthétisation afin de simplifier l'interprétation des données.
- Concevoir et développer des algorithmes d'intelligence artificielle en utilisant un langage informatique et des méthodes d'amélioration de performance du modèle afin de développer des outils intelligents répondant au besoin des métiers.
- Élaborer une architecture de stockage de type Data Lake en analysant l'environnement métier et en intégrant des structures de bases de données adaptées afin de concevoir une stratégie de traitement et de transformation de données.
- Développer des outils de transfert de données en utilisant des langages de programmation et des données stockées en Data Lake afin de procéder à la transformation vers un Data Warehouse.

Blocs de compétences

RNCP38837BC01 — Définir la stratégie des systèmes d'information

LISTE DE COMPÉTENCES

Diagnostiquer et interpréter la structure fonctionnelle d'un SI en identifiant les informations sensibles et les risques techniques, sécuritaires et réglementaires en collaborant avec les décideurs afin de proposer des mesures en accord avec les objectifs généraux et le schéma directeur informatique.

Réaliser un benchmark des solutions existantes sur le marché, en réalisant une matrice fonctionnelle et budgétaire relative aux différentes fonctionnalités des outils et des besoins de l'organisation afin de sélectionner les solutions les plus adaptées à la problématique métier.

Conceptualiser et proposer un schéma d'intégration et d'évolution d'un SI en tenant compte des contraintes fonctionnelles, techniques et budgétaires actuelles et à venir afin de proposer des projets d'évolutions, d'adaptations ou de migration du système d'information en accord avec le développement de l'organisation et les besoins en matière de ressources matérielles, organisationnelles, réglementaires et sécuritaires.

Définir la politique de continuité ou de reprise d'activité de l'organisation en élaborant un schéma directeur et en intégrant des solutions de réplication afin d'anticiper une paralysie totale ou partielle des services du SI.

Mettre en place un dispositif de veille technologique, en français et en anglais, en analysant les besoins des destinataires et en sélectionnant les outils concordant aux besoins afin d'anticiper les technologies émergentes (robotique, IOT, intelligence artificielle, blockchain...) qui pourraient participer à une évolution du système d'information de l'organisation.

MODALITÉS D'ÉVALUATION

- Mise en situation professionnelle
- Etudes de cas

PRÉREQUIS À L'ENTRÉE

- Avoir un diplôme de niveau 6 dans un domaine en relation avec la certification ou justifier d'une expérience de plus de 5 ans dans le domaine concerné par le bloc.
- Répondre favorablement à l'entretien de motivation ainsi qu'aux tests techniques d'entrée en formation (minimum 10/20).

PRÉREQUIS À LA VALIDATION

- Obtenir, a minima, la note de 10/20 à la mise en situation professionnelle
- Obtenir, a minima, la note de 10/20 à l'étude de cas

RNCP38837BC02 — Piloter le projet du système d'information

LISTE DE COMPÉTENCES

Réaliser un benchmark en analysant le système d'information actuel et les solutions techniques existantes répondant au besoin afin de proposer un environnement de composants techniques en adéquation avec le projet.

Constituer le cahier des charges de conception ou d'évolution du système d'information à partir des propositions validées par les décideurs afin d'accompagner le développement de l'organisation.

Rédiger les spécificités techniques et fonctionnelles en prenant en compte le cahier des charges du maître d'ouvrage

et en étudiant la faisabilité des évolutions techniques souhaitées afin de répondre aux objectifs définis par le cahier des charges.

Organiser le pilotage et le management des équipes projet en menant à bien les phases de développement, de recette et d'implémentation tout en s'assurant du respect du budget et des délais et en prenant en compte les différentes situation de handicap le cas échéant afin de mettre en œuvre les plans d'évolution du système et les schémas directeurs de la réalisation du projet.

Organiser et formuler les différentes protocoles de tests en collaboration avec les équipes techniques, en rédigeant un dossier technique détaillant ces protocoles afin d'assurer la qualité du fonctionnement des recettes.

Mesurer la performance du système d'information suite à son évolution, son changement ou la fusion des systèmes d'information en suivant les retours utilisateurs et en analysant les indicateurs d'utilisation et de performance afin de mettre en place des actions correctives si nécessaire.

MODALITÉS D'ÉVALUATION

- Mises en situation professionnelle
- Etudes de cas

PRÉREQUIS À L'ENTRÉE

- Avoir un diplôme de niveau 6 dans un domaine en relation avec la certification ou justifier d'une expérience de plus de 5 ans dans le domaine concerné par le bloc.
- Répondre favorablement à l'entretien de motivation ainsi qu'aux tests techniques d'entrée en formation (minimum 10/20).

PRÉREQUIS À LA VALIDATION

- Obtenir, a minima, la note de 10/20 à la mise en situation professionnelle
- Obtenir, a minima, la note de 10/20 à l'étude de cas

RNCP38837BC03 — Définir et appliquer la politique et les dispositifs de protection de données

LISTE DE COMPÉTENCES

Collecter et recenser les données présentes et utilisées au sein d'un système d'information en interprétant le schéma de base de données et en échangeant avec le responsable du SI afin d'énumérer les données stockées par le SI et les données en transition dans le SI.

Caractériser et classer les données exploitées dans un SI en interprétant la nature et la forme de chaque donnée et en prenant en compte les contraintes légales liées au RGPD et techniques applicables à la classification afin de réaliser une cartographie complète sur l'utilisation, le stockage et la transition d'une donnée.

Elaborer un plan d'actions sur la protection des données d'un SI en définissant les dispositifs répondant au cadre technique, réglementaire et sécuritaire adaptés aux données du SI afin de concevoir une politique de protection des données adaptée à l'organisation.

Répartir les rôles et les objectifs des parties prenantes en réalisant une cartographie des compétences existantes et de celles manquantes par rapport aux besoins du plan d'actions et en prenant en compte les différentes situations de handicap le cas échéant afin d'assurer la réalisation du plan d'actions dans les délais impartis.

Assurer le suivi du plan d'actions en respectant le budget et la planification des étapes clés afin de veiller à la bonne réalisation du plan d'actions et d'anticiper d'éventuelles adaptations.

MODALITÉS D'ÉVALUATION

- Etude de cas
- Mises en situation

PRÉREQUIS À L'ENTRÉE

- Avoir un diplôme de niveau 6 dans un domaine en relation avec la certification ou justifier d'une expérience de plus de 5 ans dans le domaine concerné par le bloc.
- Répondre favorablement à l'entretien de motivation ainsi qu'aux tests techniques d'entrée en formation (minimum 10/20).

PRÉREQUIS À LA VALIDATION

- Obtenir, a minima, la note de 10/20 à la mise en situation professionnelle
- Obtenir, a minima, la note de 10/20 à l'étude de cas

RNCP38837BC04 — (Optionnel) Concevoir et sécuriser les architectures des systèmes d'information (Cybersécurité et Cloud Computing)

LISTE DE COMPÉTENCES

Réaliser un benchmark des plateformes de Cloud en comparant les différents services proposés afin de définir la meilleure stratégie Cloud public, privé, hybride adaptée au besoin.

Concevoir une stratégie Cloud en interprétant les résultats du benchmark et en prenant en compte les contraintes du système d'information afin de créer une architecture sécurisée uniforme ou répartie.

Créer l'architecture sécurisée et automatisée en cloud en déployant des services sur les plateformes choisies et garantissant la communication avec le système d'information afin d'assurer le bon fonctionnement et son adaptation aux évolutions.

Assurer le suivi fonctionnel des services Cloud en intégrant des solutions de monitoring et de diagnostic afin de garantir la qualité de service et d'appliquer d'éventuelles mesures correctives.

Auditer la sécurité du système d'information à travers des tests d'intrusion et d'analyse de façon automatisée afin de protéger le système d'information de l'entreprise et assurer sa qualité.

Elaborer une stratégie de sécurisation du système d'information (hardening) en interprétant les résultats de l'audit de sécurité afin de renforcer la sécurité du système d'information.

Réaliser un audit après incident (forensic) en analysant les logs, preuves numériques et empreintes d'attaques afin d'identifier les failles de sécurité exploitées, ainsi que les ressources impactées.

Rédiger un rapport d'audit en utilisant les résultats des tests d'intrusion et de l'analyse forensic afin de synthétiser les résultats d'analyse et des incidents et de recommander une stratégie d'évolution ou de remédiation.

MODALITÉS D'ÉVALUATION

- Etudes de cas
- Mise en situation

PRÉREQUIS À L'ENTRÉE

- Avoir un diplôme de niveau 6 dans un domaine en relation avec la certification ou justifier d'une expérience de plus de 5 ans dans le domaine concerné par le bloc.
- Répondre favorablement à l'entretien de motivation ainsi qu'aux tests techniques d'entrée en formation (minimum 10/20).

PRÉREQUIS À LA VALIDATION

- Obtenir, a minima, la note de 10/20 à la mise en situation professionnelle
- Obtenir, a minima, la note de 10/20 à l'étude de cas

RNCP38837BC05 — (Optionnel) Concevoir et développer des architectures Big Data

LISTE DE COMPÉTENCES

Collecter et nettoyer des ensembles volumineux de données structurées et non structurées issues de sources internes et externes de l'entreprise à l'aide des technologies de récupération, d'interprétation et de manipulation de données afin d'alimenter l'environnement de Big Data.

Analyser et visualiser des données volumineuses en utilisant des outils de visualisation et de synthétisation afin de simplifier l'interprétation des données.

Concevoir et développer des algorithmes d'intelligence artificielle en utilisant un langage informatique et des méthodes d'amélioration de performance du modèle afin de développer des outils intelligents répondant au besoin des métiers.

Elaborer une architecture de stockage de type data lake en analysant l'environnement métier et en intégrant des structures de bases de données adaptées afin de concevoir une stratégie de traitement et de transformation de données.

Développer des outils de transfert de données en utilisant des langages de programmation et des données stockées en data lake afin de procéder à la transformation vers un data warehouse.

MODALITÉS D'ÉVALUATION

Mises en situation professionnelle

PRÉREQUIS À L'ENTRÉE

- Avoir un diplôme de niveau 6 dans un domaine en relation avec la certification ou justifier d'une expérience de plus de 5 ans dans le domaine concerné par le bloc.

- Répondre favorablement à l'entretien de motivation ainsi qu'aux tests techniques d'entrée en formation (minimum 10/20).

PRÉREQUIS À LA VALIDATION

Obtenir, a minima, la note de 10/20 aux mises en situation professionnelle

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les titulaires de la certification travaillent essentiellement pour des entreprises du secteur informatique, c'est-à-dire des sociétés de services en ingénierie informatique (ESN), des éditeurs de logiciels, des constructeurs informatiques, des opérateurs en télécommunications etc. en relation avec différentes services. Ils opèrent également dans des cabinets de conseil comme consultants pour des grands comptes. Ils peuvent travailler dans tous les secteurs d'activité : du secteur de la production télévisuelle, à l'énergie, en passant par les télécommunications.

TYPE D'EMPLOIS ACCESSIBLES

- Responsable de projet / de projet technique informatique
- Responsable de département informatique
- Responsable des services informatiques / Responsable des systèmes d'information
- Consultant en systèmes d'information / Consultant informatique / Consultant IT / Consultant devops / Consultant cybersécurité / Consultant IT / Consultant big data
- Maître d'ouvrage / Maitrise d'œuvre des systèmes d'informations (MOA / MOE)
- Architecte des systèmes d'information
- Expert des systèmes d'information
- Ingénieur systèmes et réseaux / Ingénieur d'études informatiques / Ingénieur de poste de travail
- Responsable qualité IT / informatique
- Architecte web
- Expert en infrastructure big data

RÈGLEMENTATIONS D'ACTIVITÉ

L'activité n'est pas réglementée. Si le métier n'est soumis à aucune réglementation, ces professionnels sont des acteurs clefs du respect par l'entreprise de la législation française et européenne sur la protection des données.

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)	2 912 €
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) 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)	43 955
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 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

PRÉREQUIS À L'ENTRÉE EN FORMATION

- Avoir un diplôme de niveau 6 dans un domaine en relation avec la certification
- Répondre favorablement à l'entretien de motivation ainsi qu'aux tests techniques d'entrée en formation (minimum 10/20).

PRÉREQUIS À LA VALIDATION

- Ne pas totaliser plus de 20% d'absences justifiées ou injustifiées sur l'intégralité du cursus
- Obtenir, a minima, la moyenne de 10/20 en contrôle continu au travers des évaluations réalisées tout au long de l'année
- Rendre obligatoirement son mémoire d'expertise dans les délais imposés

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, VAE

Le jury de certification est composé d'un membre de la direction de l'école et de 3 professionnels du secteur dont le président, ayant été audités et validés par la direction pédagogique. Un président de jury est choisi parmi les 3 jurés, en l'occurrence le profil qui a l'expérience et la maturité la plus à même d'animer la session et les délibérations.

COMPOSITION DU JURY — CONTRAT DE PROFESSIONNALISATION

Le jury de certification est composé d'un membre de la direction de l'école et de 3 professionnels du secteur dont le président, ayant été audités et validés par la direction pédagogique. Un président de jury est choisi parmi les 3 jurés, en l'occurrence le profil qui a l'expérience et la maturité la plus à même d'animer la session et les délibérations.

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	8 500 €
--------------------------------	---------

Selon la branche

4 172 € – 8 585 €

Prise en charge	Branches concernées
8 500 €	Valeur par défaut · 191 branches
8 585 €	CPNE de l'ingénierie, des services informatiques et du conseil, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Métiers de la Transformation des Grains, CPNE des Télécoms, CPNEFP Import-Export
7 368 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
7 225 €	CPNE Branche Caoutchouc, CPNEFP de la métallurgie
7 727 €	CPNE Travail Temporaire
7 565 €	CPNE FP Commerce de Détail de l'Horlogerie Bijouterie
7 310 €	CPNEFP de l'habillement, mercerie, chaussure et jouet
7 297 €	CPNEF de l'audiovisuel
7 296 €	CPNEFP Commerce à distance
6 885 €	CPNE Banque
6 800 €	CPNE des industries de santé (CPNEIS)
4 172 €	CPNEFP des commerces de gros

Base légale

Date de décision	27/03/2024
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	27/03/2027
Date de dernière délivrance possible	27/03/2031

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2022	164	0	99 %	94 %
2021	143	0	99 %	73 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP34567

CORRESPONDANCES (PAR BLOCS)

RNCP34567

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/38837/>

Se former en apprentissage

Formations en apprentissage	1
Organismes gestionnaires (CFA)	1
Organismes formateurs	1
Régions couvertes	1
Départements couverts	1
Organismes certifiés Qualiopi	1
Sessions	de 11/2025 à 11/2028

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