

Administrateur systèmes, réseaux et cybersécurité

RNCP39611 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326n
Formacode(s)	31034, 31045, 24220, 24273, 31008
Code(s) ROME	M1802, M1801
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	01/10/2024
Date d'échéance	01/10/2029

Certificateur(s)

ASSOCIATION POUR LA GESTION DE 3IL · SIRET : 39770462800015

Partenaires habilités

29 organismes habilités, d'après la liste publiée par France compétences : 29 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ASSOCIATION O.R.T.	77568810400063	Former et organiser l'évaluation
CAMPUS DE MONTPELLIER	92369614000022	Former et organiser l'évaluation
CCCLX	88343992900059	Former et organiser l'évaluation
CFT Tunis	—	Former et organiser l'évaluation
CHAMBRE COMMERCE ET INDUSTRIE LA NIEVRE	18580003400067	Former et organiser l'évaluation
CHAMBRE DE COMMERCE ET D INDUSTRIE	18280001100047	Former et organiser l'évaluation
CHAMBRE DE COMMERCE ET D INDUSTRIE	18974211700097	Former et organiser l'évaluation
CHAMBRE DE COMMERCE ET D INDUSTRIE DU TARN (CCI) - SITE DE CASTRES MAZAMET	13001278400026	Former et organiser l'évaluation
CODA	92219486500031	Former et organiser l'évaluation
CODA	92219486500049	Former et organiser l'évaluation

Liste complète des 29 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp39611-administrateur-systemes-reseaux-et-cybersecurite/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'Administrateur Systèmes, Réseaux et Cybersécurité est un professionnel IT essentiel qui assure le bon fonctionnement, la sécurité et l'efficacité des infrastructures technologiques au sein des organisations.

Il gère et maintient les systèmes d'exploitation en s'assurant de leur mise à jour, leur sécurité et leur optimisation pour garantir une performance optimale.

ACTIVITÉS VISÉES

Administration et optimisation des systèmes d'exploitation et la virtualisation pour la sécurité et la performance

Administration des serveurs, de la virtualisation et Gestion de la qualité de services

Maintien de la haute disponibilité et automatisation des systèmes

Configuration et administration de l'infrastructure réseau et des solutions cloud.

Configuration de l'infrastructure Réseaux

Conception et réalisation de l'intégration et le déploiement continu (Cloud & Devops)

Sécurisation et mise en place de stratégies de cybersécurité et protection des données

Mise en œuvre des politiques de sécurité et gestion des risques par l'Ethical Hacking

Administration des systèmes de sécurité et des contrôles d'accès

Supervision et contrôle de la protection des données et de la conformité réglementaire

Conduite de projet d'infrastructure systèmes et réseaux sécurisée

Étude de faisabilité et définition des exigences techniques

Planification et suivi de projet selon les méthodologies agiles

Recherche documentaire et veille technologique en contexte multilingue

COMPÉTENCES ATTESTÉES

Administrer et optimiser les systèmes d'exploitation Unix, Linux et Windows en tenant compte des bonnes pratiques de la qualité de service (QoS), en collaboration avec les équipes techniques, pour assurer les exigences de performance et de fiabilité de l'entreprise

Concevoir des topologies systèmes à l'aide d'un annuaire, en structurant efficacement les ressources informatiques et la gestion des identités et des accès aux différentes ressources, pour répondre aux besoins opérationnels, et respecter les politiques d'accès et sécurité de l'entreprise

Concevoir et déployer des environnements virtualisés à l'aide de plateformes spécialisées On-Premise ou sur un cloud provider, en coopération avec les architectes système, pour rationaliser l'utilisation des ressources informatiques et répondre à l'évolutivité des besoins de l'entreprise

Concevoir, gérer et administrer les systèmes de gestion de bases de données relationnelles et NoSQL, en appliquant les principes d'optimisation des bases de données et en collaboration avec les développeurs et les analystes de données, pour garantir la cohérence, la qualité, la sécurité et l'accessibilité permanente des informations

Mettre en œuvre des solutions de redondance, de réplication et de clustering, en tenant compte des contraintes de sécurité et de performance, afin la continuité de l'activité de l'entreprise

Surveiller et optimiser les performances des systèmes informatiques en utilisant des outils de monitoring et d'analyse, en coordination avec les équipes d'exploitation, pour détecter et résoudre proactivement les problèmes techniques et améliorer la performance des systèmes

Manager le processus de gestion des incidents informatiques en utilisant un système de ticketing pour conduire, hiérarchiser ou escalader les incidents en collaboration avec les équipes techniques et en respectant les SLA définis pour assurer une reprise ou continuité des activités de l'entreprise

Automatiser les tâches d'administration en développant et en appliquant des scripts en Python, Shell, et Bash, pour augmenter l'efficacité opérationnelle et réduire les délais de réponse en cas de problèmes ou de besoins de maintenance

Configurer l'infrastructure réseau à l'aide de protocoles et d'équipements adaptés aux besoins fonctionnels et en collaboration avec l'équipe réseau, pour assurer une connectivité fluide et sécurisée du système d'information

Déployer les solutions de télécommunications, de réseaux de données et voix, en supervisant l'installation et la configuration dans l'environnement de production, en collaboration avec les équipes techniques et les fournisseurs, pour garantir l'efficacité des communications internes et externes et assurer la continuité des services

Superviser et assurer la maintenance du réseau en utilisant des systèmes de monitoring, en collaboration avec les équipes de sécurité informatique et d'exploitation, pour maintenir une performance réseau optimale

Développer des environnements virtualisés en utilisant une plateforme conteneurisation pour standardiser et simplifier

le déploiement d'applications sur tous types d'infrastructure

Coordonner les conteneurs avec des logiciels d'orchestration en garantissant l'activité des pipelines d'intégration et de déploiement continus pour optimiser la résilience et la performance des applications

Intégrer et déployer les pratiques de sécurité dans les processus de développement et d'exploitation en collaborant avec les équipes de développement et en utilisant des outils DevOps, pour maîtriser les risques et assurer la conformité des applications sur des plateformes cloud

Développer, documenter et mettre en œuvre des politiques de sécurité informatique, en évaluant les risques et en établissant des stratégies de mitigation en collaboration avec les équipes de gouvernance et de conformité, et en se servant d'outils d'analyse de risques et en réalisant des procédures pour renforcer la posture de sécurité de l'entreprise et protéger les actifs informationnels

Conduire des audits de sécurité réguliers pour évaluer l'efficacité des mesures de sécurité en place, en utilisant des méthodologies d'audit standardisées et en collaboration avec les équipes internes et les auditeurs externes, afin de détecter les faiblesses et de recommander des améliorations

Élaborer et mettre en œuvre des actions correctives en analysant les résultats des audits de sécurité et en identifiant les vulnérabilités et les non-conformités, en coopération avec les équipes de sécurité et de conformité, afin d'améliorer continuellement les mesures de sécurité de l'organisation et de garantir la conformité réglementaire

Implémenter les outils et systèmes de sécurité tels que les pare-feux, les IDS/IPS, en s'assurant de leur configuration optimale et de leur mise à jour, en travaillant de concert avec l'équipe réseau et les spécialistes de la sécurité, pour prévenir les intrusions et protéger les réseaux de l'entreprise

Administrer les systèmes de gestion des identités et des accès (IAM), en mettant en œuvre des politiques d'accès rigoureuses et en utilisant des technologies d'authentification avancées (MFA) et tenant compte de personnes en situation de handicap, pour garantir que seul le personnel autorisé a accès aux systèmes critiques et aux données sensibles

Superviser les opérations de sauvegarde et de restauration des données, en élaborant des plans de reprise après sinistre, en coopération avec les équipes IT et les parties prenantes opérationnelles, pour assurer la continuité des activités et la protection des données

Assurer le support et le suivi des incidents IT en supervisant les équipes techniques à l'aide d'outils de gestion d'incidents et en communiquant avec les utilisateurs et différentes parties prenantes, afin de respecter les objectifs en RTO et RPO établis par les SLA dans le Plan de Reprise d'Activité sous la Direction des Systèmes d'Information

Assurer la conformité aux réglementations de protection des données, telles que le RGPD, en menant des évaluations et des audits de conformité, en collaboration avec les conseillers juridiques et les experts en réglementation, et en mettant en place des actions correctives, pour éviter les sanctions et renforcer la confiance des parties prenantes dans la gouvernance des données de l'entreprise

Analyser les besoins opérationnels et les traduire en exigences fonctionnelles et techniques détaillées, en conduisant des études de faisabilité et en évaluant les options technologiques, pour définir des solutions informatiques qui s'alignent avec les objectifs stratégiques de l'entreprise

Rédiger des documents de spécification technique qui serviront de référence pour les décisions technologiques et les investissements, en assurant que les solutions choisies soient viables, rentables et conformes aux normes de l'industrie

Orchestrer et animer des projets informatiques en utilisant des méthodologies agiles pour planifier, exécuter et surveiller le travail de développement, et en facilitant la communication entre toutes les parties prenantes y compris en situation de handicap pour atteindre les objectifs définis

Optimiser la gestion des projets en termes d'avancement, gestion des priorités et ajustements grâce à des outils de gestion de projet tels que JIRA ou Trello afin de maximiser l'efficacité de l'équipe, respecter les délais et garantir la qualité des livrables

Gérer le budget de projet en utilisant des outils de gestion financière (ex. Microsoft Project, Excel, ou des logiciels spécialisés comme SAP) et des techniques de budgétisation (ex. répartition des coûts, analyse de la valeur acquise), en respectant les contraintes financières et temporelles du projet, afin d'assurer une utilisation optimale des ressources et de garantir la rentabilité et le succès du projet

Analyser des contenus de diverses sources d'informations spécialisés, en mobilisant ses connaissances technologiques et sa maîtrise de l'anglais, pour résoudre des incidents ou répondre à des besoins précis et ponctuels en soutien du Système d'Information (SI)

Mettre en place une veille technologique et réglementaire en relation avec l'activité de l'entreprise en sélectionnant des sources d'information multilingues, en s'assurant de la véracité de leurs contenus et en utilisant des outils de collecte avancés pour un stockage et une organisation efficace des données récoltées dans une base de

connaissance

Analyser les données brutes collectées dans la base de connaissances technologiques en comparant les différents résultats afin d'établir différentes hypothèses ou scénarii d'évolution, d'optimisation et de sécurisation des infrastructures

Diffuser les hypothèses ou scénarii aux collaborateurs du département IT (Information Technology) en utilisant des outils collaboratifs et en déterminant une fréquence idéale de diffusion pour améliorer les connaissances et une montée en compétence de l'équipe et le soutien du processus décisionnel et l'innovation au sein du projet

Blocs de compétences

RNCP39611BC01 — Administrer et optimiser les systèmes d'exploitation et la virtualisation pour la sécurité et la performance

LISTE DE COMPÉTENCES

Administrer et optimiser les systèmes d'exploitation Unix, Linux et Windows en tenant compte des bonnes pratiques de la qualité de service (QoS), en collaboration avec les équipes techniques, pour assurer les exigences de performance et de fiabilité de l'entreprise

Concevoir des topologies systèmes à l'aide d'un annuaire, en structurant efficacement les ressources informatiques et la gestion des identités et des accès aux différentes ressources, pour répondre aux besoins opérationnels, et respecter les politiques d'accès et sécurité de l'entreprise

Concevoir et déployer des environnements virtualisés à l'aide de plateformes spécialisées On-Premise ou sur un cloud provider, en coopération avec les architectes système, pour rationaliser l'utilisation des ressources informatiques et répondre à l'évolutivité des besoins de l'entreprise

Concevoir, gérer et administrer les systèmes de gestion de bases de données relationnelles et NoSQL, en appliquant les principes d'optimisation des bases de données et en collaboration avec les développeurs et les analystes de données, pour garantir la cohérence, la qualité, la sécurité et l'accessibilité permanente des informations

Mettre en œuvre des solutions de redondance, de réplication et de clustering, en tenant compte des contraintes de sécurité et de performance, afin la continuité de l'activité de l'entreprise

Surveiller et optimiser les performances des systèmes informatiques en utilisant des outils de monitoring et d'analyse, en coordination avec les équipes d'exploitation, pour détecter et résoudre proactivement les problèmes techniques et améliorer la performance des systèmes

Manager le processus de gestion des incidents informatiques en utilisant un système de ticketing pour conduire, hiérarchiser ou escalader les incidents en collaboration avec les équipes techniques et en respectant les SLA définis pour assurer une reprise ou continuité des activités de l'entreprise

Automatiser les tâches d'administration en développant et en appliquant des scripts en Python, Shell, et Bash, pour augmenter l'efficacité opérationnelle et réduire les délais de réponse en cas de problèmes ou de besoins de maintenance

MODALITÉS D'ÉVALUATION

Mise en situation reconstituée

: Dossier d'architecture technique + Mise en place de la solution mise en œuvre

Mise en situation reconstituée : Analyser une architecture et son PCA pour proposer des améliorations et des outils de monitoring adaptés

Compte-rendu d'amélioration de l'architecture

PRÉREQUIS À L'ENTRÉE

Être titulaire d'une certification de niveau 5 dans le domaine informatique.

PRÉREQUIS À LA VALIDATION

Avoir suivi la formation de préparation du bloc concerné.

RNCP39611BC02 — Configurer et administrer l'infrastructure réseau et les solutions cloud

LISTE DE COMPÉTENCES

Configurer l'infrastructure réseau à l'aide de protocoles et d'équipements adaptés aux besoins fonctionnels et en collaboration avec l'équipe réseau, pour assurer une connectivité fluide et sécurisée du système d'information

Déployer les solutions de télécommunications, de réseaux de données et voix, en supervisant l'installation et la configuration dans l'environnement de production, en collaboration avec les équipes techniques et les fournisseurs, pour garantir l'efficacité des communications internes et externes et assurer la continuité des services

Superviser et assurer la maintenance du réseau en utilisant des systèmes de monitoring, en collaboration avec les équipes de sécurité informatique et d'exploitation, pour maintenir une performance réseau optimale

Développer des environnements virtualisés en utilisant une plateforme conteneurisation pour standardiser et simplifier le déploiement d'applications sur tous types d'infrastructure

Coordonner les conteneurs avec des logiciels d'orchestration en garantissant l'activité des pipelines d'intégration et de déploiement continus pour optimiser la résilience et la performance des applications

Intégrer et déployer les pratiques de sécurité dans les processus de développement et d'exploitation en collaborant avec les équipes de développement et en utilisant des outils DevOps, pour maîtriser les risques et assurer la conformité des applications sur des plateformes cloud

MODALITÉS D'ÉVALUATION

Mise en situation reconstituée à travers une étude de cas: Dossier technique de la solution (Topologie, Fiches de test, ...) + Mise en service de la solutions

Mise en situation reconstituée : Mise en place d'un système d'automatisation d'intégration et de déploiement continu. (Individuelle)

PRÉREQUIS À L'ENTRÉE

Être titulaire d'une certification de niveau 5 dans le domaine informatique.

PRÉREQUIS À LA VALIDATION

Avoir suivi la formation de préparation du bloc concerné.

RNCP39611BC03 — Élaborer et mettre en œuvre des stratégies de cybersécurité et de protection des données

LISTE DE COMPÉTENCES

Développer, documenter et mettre en œuvre des politiques de sécurité informatique, en évaluant les risques et en établissant des stratégies de mitigation en collaboration avec les équipes de gouvernance et de conformité, et en se servant d'outils d'analyse de risques et en réalisant des procédures pour renforcer la posture de sécurité de l'entreprise et protéger les actifs informationnels

Conduire des audits de sécurité réguliers pour évaluer l'efficacité des mesures de sécurité en place, en utilisant des méthodologies d'audit standardisées et en collaboration avec les équipes internes et les auditeurs externes, afin de détecter les faiblesses et de recommander des améliorations

Élaborer et mettre en œuvre des actions correctives en analysant les résultats des audits de sécurité et en identifiant les vulnérabilités et les non-conformités, en coopération avec les équipes de sécurité et de conformité, afin d'améliorer continuellement les mesures de sécurité de l'organisation et de garantir la conformité réglementaire

Implémenter les outils et systèmes de sécurité tels que les pare-feux, les IDS/IPS, en s'assurant de leur configuration optimale et de leur mise à jour, en travaillant de concert avec l'équipe réseau et les spécialistes de la sécurité, pour prévenir les intrusions et protéger les réseaux de l'entreprise

Administrer les systèmes de gestion des identités et des accès (IAM), en mettant en œuvre des politiques d'accès rigoureuses et en utilisant des technologies d'authentification avancées (MFA) et tenant compte de personnes en situation de handicap, pour garantir que seul le personnel autorisé a accès aux systèmes critiques et aux données sensibles

Superviser les opérations de sauvegarde et de restauration des données, en élaborant des plans de reprise après sinistre, en coopération avec les équipes IT et les parties prenantes opérationnelles, pour assurer la continuité des activités et la protection des données

Assurer le support et le suivi des incidents IT en supervisant les équipes techniques à l'aide d'outils de gestion d'incidents et en communiquant avec les utilisateurs et différentes parties prenantes, afin de respecter les objectifs en RTO et RPO établis par les SLA dans le Plan de Reprise d'Activité sous la Direction des Systèmes d'Information

Assurer la conformité aux réglementations de protection des données, telles que le RGPD, en menant des évaluations et des audits de conformité, en collaboration avec les conseillers juridiques et les experts en réglementation, et en mettant en place des actions correctives, pour éviter les sanctions et renforcer la confiance des parties prenantes dans la gouvernance des données de l'entreprise

MODALITÉS D'ÉVALUATION

Mise en situation reconstituée : Rapport d'analyse et préconisations

Mise en situation reconstituée :

A partir d'une étude de cas d'une infrastructure réseau d'entreprise, le candidat proposera un rapport d'analyse et de préconisations d'amélioration de l'existant

Mise en situation reconstituée : Mise en place d'un plan de sauvegarde à partir de l'étude de cas

PRÉREQUIS À L'ENTRÉE

Être titulaire d'une certification de niveau 5 dans le domaine informatique.

PRÉREQUIS À LA VALIDATION

Avoir suivi la formation de préparation du bloc concerné.

RNCP39611BC04 — Conduire la gestion de projets d'infrastructure systèmes et réseaux sécurisée

LISTE DE COMPÉTENCES

Analyser les besoins opérationnels et les traduire en exigences fonctionnelles et techniques détaillées, en conduisant des études de faisabilité et en évaluant les options technologiques, pour définir des solutions informatiques qui s'alignent avec les objectifs stratégiques de l'entreprise

Rédiger des documents de spécification technique qui serviront de référence pour les décisions technologiques et les investissements, en assurant que les solutions choisies soient viables, rentables et conformes aux normes de l'industrie.

Orchestrer et animer des projets informatiques en utilisant des méthodologies agiles pour planifier, exécuter et surveiller le travail de développement, et en facilitant la communication entre toutes les parties prenantes y compris en situation de handicap pour atteindre les objectifs définis

Optimiser la gestion des projets en termes d'avancement, gestion des priorités et ajustements grâce à des outils de gestion de projet tels que JIRA ou Trello afin de maximiser l'efficacité de l'équipe, respecter les délais et garantir la qualité des livrables

Gérer le budget de projet en utilisant des outils de gestion financière (ex. Microsoft Project, Excel, ou des logiciels spécialisés comme SAP) et des techniques de budgétisation (ex. répartition des coûts, analyse de la valeur acquise), en respectant les contraintes financières et temporelles du projet, afin d'assurer une utilisation optimale des ressources et de garantir la rentabilité et le succès du projet

Analyser des contenus de diverses sources d'informations spécialisés, en mobilisant ses connaissances technologiques et sa maîtrise de l'anglais, pour résoudre des incidents ou répondre à des besoins précis et ponctuels en soutien du Système d'Information (SI)

Mettre en place une veille technologique et règlementaire en relation avec l'activité de l'entreprise en sélectionnant des sources d'information multilingues, en s'assurant de la véracité de leurs contenus et en utilisant des outils de collecte avancés pour un stockage et une organisation efficace des données récoltées dans une base de connaissance

Analyser les données brutes collectées dans la base de connaissances technologiques en comparant les différents résultats afin d'établir différentes hypothèses ou scénarii d'évolution, d'optimisation et de sécurisation des infrastructures

Diffuser les hypothèses ou scénarii aux collaborateurs du département IT (Information Technology) en utilisant des outils collaboratifs et en déterminant une fréquence idéale de diffusion pour améliorer les connaissances et une montée en compétence de l'équipe et le soutien du processus décisionnel et l'innovation au sein du projet

MODALITÉS D'ÉVALUATION

Mise en situation reconstituée : Rédaction d'une étude d'avant-projet

Mise en situation professionnelle reconstituée : Compte rendu d'activité (livrables collectifs) + Soutenance individuelle

Mise en situation reconstituée:

Rédaction d'un rapport de veille multilingue + Présentation orale de son rapport de veille multilingue

PRÉREQUIS À L'ENTRÉE

Être titulaire d'une certification de niveau 5 dans le domaine informatique.

PRÉREQUIS À LA VALIDATION

Avoir suivi la formation de préparation du bloc concerné.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Les "Administrateurs Systèmes, Réseaux et Cybersécurité" trouvent leur place dans une multitude de secteurs, reflétant leur polyvalence et leur importance cruciale. Ils sont indispensables dans les domaines de la finance, de la santé, de l'éducation, des technologies de l'information, et bien plus encore. Chaque secteur compte sur ces professionnels pour maintenir une infrastructure informatique robuste, sécurisée, et adaptative, capable de soutenir

des opérations complexes et de protéger des données critiques. Opter pour une certification dans ce domaine ouvre des portes à des carrières dynamiques et essentielles, dotées de perspectives d'évolution et d'innovation constantes dans un environnement technologique en évolution rapide.

TYPE D'EMPLOIS ACCESSIBLES

- Administrateur systèmes et réseaux (et sécurité)
- Administrateur systèmes (et sécurité)
- Administrateur réseaux (et sécurité)
- Administrateur infrastructures
- Administrateur d'infrastructures et cloud
- Administrateur cybersécurité
- Responsable infrastructure systèmes et réseaux

RÉGLEMENTATIONS D'ACTIVITÉ

En France, les métiers d'Administrateur Systèmes, Réseaux et Cybersécurité sont encadrés par plusieurs réglementations spécifiques, en particulier dans les domaines de la cybersécurité et de la protection des données. Ces réglementations incluent des exigences de souveraineté pour les fournisseurs de services cloud, des normes strictes contre la corruption, ainsi que des mesures de protection des lanceurs d'alerte et de régulation des pratiques de lobbying.

Les cadres juridiques comme la loi Sapin II imposent aux entreprises des obligations en matière de lutte contre la corruption, tandis que des régulations comme SecNumCloud spécifient des conditions de contrôle et de propriété pour les entreprises de services cloud, limitant notamment la participation étrangère pour assurer que les données soient stockées et traitées au sein de l'UE.

De plus, des autorités régulatrices telles que la Commission Nationale de l'Informatique et des Libertés (CNIL) et l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) jouent un rôle crucial. La CNIL assure la conformité au Règlement Général sur la Protection des Données (RGPD), qui fixe les règles de traitement des données personnelles dans l'UE. L'ANSSI, quant à elle, offre des directives pour la sécurisation des systèmes d'information, essentielles pour les administrateurs systèmes, réseaux et cybersécurité dans leur mission de protection des infrastructures critiques.

Les réglementations n'imposent pas à un "administrateur systèmes, réseaux et cybersécurité" d'être de posséder des diplômes spécifiques supplémentaire. Cependant, elles requièrent que les pratiques et les procédures de gestion des données et de la sécurité soient conformes aux standards imposés.

Ainsi, bien qu'une certification ou une formation spécifique ne soit pas une obligation légale, elles sont fortement recommandées pour assurer la conformité et pour démontrer la compétence dans la gestion sécurisée des systèmes d'information et la protection des données personnelles. Des certifications peuvent aider les professionnels à prouver leur connaissance et leur engagement envers ces pratiques, augmentant leur crédibilité et leur valeur sur le marché du travail.

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	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 704 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % 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) 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)	14 307
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 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

Cursus en 3 ans, être titulaire d'un baccalauréat

Cursus en 1 an : être titulaire d'une certification de niveau 5 dans le domaine informatique

COMPOSITION DU JURY — FORMATION INITIALE

Le jury de certification est composé de 4 membres dont 2 professionnels (externes)

travaillant dans le domaine d'activité de la certification

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

Le jury de certification est composé de 4 membres dont 2 professionnels (externes) travaillant dans le domaine d'activité de la certification

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	8 800 €
Selon la branche	6 600 € – 9 149 €
Prise en charge	Branches concernées
8 800 €	Valeur par défaut · 178 branches
9 149 €	CPNE Casinos, CPNE Travail Temporaire, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms, CPNEF de l'audiovisuel
8 000 €	CPNE des MFR, CPNE des Métiers de la Transformation des Grains, CPNE des Vins et Spiritueux, CPNE des centres de gestion agréés et habilités agricoles, CPNEFP Transformation Laitière
8 535 €	CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP Habillement succursaliste, CPNEFP du Négoce de l'ameublement
8 990 €	CPNEF branche retraite complémentaire et prévoyance, CPNEFP Mutualité
8 417 €	CPNE Branche Caisse d'Epargne, CPNE de la branche Banque Populaire
9 115 €	CPNEFP du négoce des matériaux de construction
8 583 €	CPNEFP Coopératives de consommateurs

8 057 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 050 €	CPNEFP Commerce à distance
7 500 €	CPNE des industries de santé (CPNEIS)
7 374 €	CPNE FP Branche des magasins du Bricolage
7 200 €	CPNEFP de la branche des prestataires de services du secteur tertiaire
7 000 €	CPNEFP de la métallurgie
6 600 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager

Base légale

Date de décision	01/10/2024
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	01/10/2029
Date de dernière délivrance possible	01/10/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2022	134	1	94 %	69 %
2021	104	2	90 %	56 %
2020	78	0	86 %	75 %
2019	35	0	80 %	55 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP34412

CORRESPONDANCES (PAR BLOCS)

RNCP34206, RNCP34237, RNCP34412, RNCP34474, RNCP35093, RNCP35587, RNCP36075, RNCP36370, RNCP38108

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/39611/>

Où se former

Formations référencées	4
Organismes	4
Régions couvertes	4
Prix indicatif	4 000 € – 7 466 €
Durée	504 – 1043 h

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

Se former en apprentissage

Formations en apprentissage	15
Organismes gestionnaires (CFA)	11
Organismes formateurs	12
Régions couvertes	8
Départements couverts	12
Organismes certifiés Qualiopi	12
Sessions	de 09/2025 à 09/2029

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

Entrées et sorties de formation

Entrées en formation	3
Parcours menés à terme	0
Taux d'achèvement	0 %
Période	10/2025 – 09/2026

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	5
Montant total engagé	21 300 €
Coût moyen par dossier	4 260 €
Durée moyenne	393 h
Période	09/2025 – 09/2026
France compétences	69 %
Reste à charge titulaire	30 %
Entreprise	0 %

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