

Administrateur systèmes, réseaux et bases de données

RNCP35594 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326
Formacode(s)	31034
Code(s) ROME	M1810, M1801
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	19/05/2021
Date d'échéance	19/05/2026

Certificateur(s)

ASS. POUR DEVELOPPEMENT INSERTION PROFES · SIRET : 40980167700017

INSTITUT DE GESTION SOCIALE (IGS) · SIRET : 31249509600157

Partenaires habilités

54 organismes habilités, d'après la liste publiée par France compétences : 54 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
AIX YNOV CAMPUS	52831294500033	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE	39350481600330	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE	39350481600348	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE	39350481600355	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE	39350481600363	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600090	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600215	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600223	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600249	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600272	Former et organiser l'évaluation

Liste complète des 54 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp35594-administrateur-systemes-reseaux-et-bases-de-donnees/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'administrateur systèmes réseaux et bases de données assure l'installation, l'administration et la surveillance de l'ensemble des équipements informatiques tant physiques que virtuels. Il veille à la cohérence et la qualité des données dans le respect des dispositions et procédures en vigueur dans l'entreprise. Il est le garant de la bonne exploitation des ressources informatiques qui lui sont confiées dans un objectif de qualité, de productivité, de disponibilité, avec une préoccupation constante quant à la sécurité de son système d'information.

ACTIVITÉS VISÉES

Administrer le Système d'Information

Assurer la gestion du Système d'information

Définir la politique de sécurisation du Système d'Information

Communiquer avec tous les acteurs internes ou externes au service informatique

COMPÉTENCES ATTESTÉES

Assurer l'exploitation du Système d'Information (SI) pour maintenir une opérationnalité constante grâce à un large spectre de savoir-faire associés aux systèmes

Concevoir l'infrastructure d'une plateforme virtuelle pour intégrer plusieurs machines physiques en une seule

Maintenir en conditions opérationnelles l'infrastructure de l'entreprise en utilisant des logiciels de gestion de la haute disponibilité

Identifier rapidement les systèmes qui nécessitent des correctifs et qui doivent être reconfigurés en fonction des préconisations constructeurs

Configurer les équipements réseaux pour assurer l'interconnexion physique et virtuelle des sites

Administrer les bases de données avec méthode selon la configuration requise pour leur mise en production

Mesurer et analyser les performances pour optimiser le stockage en vue de faciliter les accès

Améliorer les performances des bases de données en optimisant l'emplacement des stockages

Rationaliser les tâches quotidiennes en rédigeant des scripts et en les intégrant dans des procédures d'exploitation automatisées

Faciliter la résolution des problèmes par une analyse des journaux d'historiques systèmes

Automatiser les procédures de sauvegarde en rédigeant des scripts et en les intégrant avec des outils d'exploitation systèmes

Gérer les évolutions des infrastructures Informatiques en appliquant les principes et les limites de la norme IT Service Management ISO/CEI 20000

Assurer l'évolution des équipements en tenant compte des technologies émergentes

Comparer les solutions pour faire des propositions de renouvellement en tenant compte des contraintes budgétaires

Ordonnancer le plan de déploiement en tenant compte des disponibilités des différents acteurs concernés

Maquetter les solutions de déploiements pour le test et la validation des solutions retenues

Attribuer les ressources informatiques nécessaires au bon déroulement du plan en fonction du budget alloué

Superviser l'infrastructure informatique et le patrimoine applicatif pour identifier les anomalies, afin d'améliorer ses performances grâce aux outils spécifiques de monitoring installés

Recenser les ressources de l'infrastructure pour fournir des informations pertinentes sur l'architecture du SI

Migrer une architecture système ou réseau en optimisant les interventions et en gérant les risques

Organiser l'infrastructure pour permettre l'intégration permanente d'évolutions logicielles

Appliquer les évolutions des applications métiers en adoptant une approche incrémentielle et automatisée des modifications en production

Centraliser le traitement des incidents en un point unique d'accès au centre de support pour mieux prioriser les interventions

Elaborer un tableau de bord sur la résolution des tickets d'incidents par niveau de support pour améliorer l'efficacité de la résolution des incidents

Résoudre les tickets de niveau 3 & 4 en intervenant sur place ou à distance à l'aide d'outils de télédistribution

Concevoir un service numérique dans le but de réduire empreinte carbone en associant la transition écologique et numérique dans un contexte professionnel

Déterminer les indicateurs à utiliser dans la gestion informatique quotidienne en vue de permettre l'évaluation des impacts des solutions informatiques en termes de responsabilités sociales et environnementales

Agir avec méthode pour faire un état des lieux des risques de sécurité identifiables au sein du SI pour permettre aux

décideurs de définir leur politique de sécurité

Connaître et appliquer les normes ISO 27001 en adoptant une vue globale du SI dont le périmètre s'étend dans un contexte de télétravail massif

Configurer des solutions de sécurité classiques

Appliquer les techniques déployées afin de sécuriser les transactions numériques de l'entreprise en protégeant les transactions électroniques

Appliquer les procédures de sécurité liées aux accès physiques et logiques des données de l'entreprise en s'appuyant sur une stratégie d'identification et de protection des données sensibles

Mettre en place une gestion unique et commune des terminaux mobiles avec les autres matériels et logiciels, interfaçable avec les opérateurs sans fil et les solutions des constructeurs

Mettre en œuvre des règles et processus de sécurité

de gestion des identités et des accès pour gérer les habilitations

Déployer des éléments passifs de protection systématique ou actifs en appliquant un plan d'urgence en cas d'infection virale

Evaluer les perturbations de services grâce aux alertes émises par les sondes, pour identifier les correctifs à apporter

Déployer des solutions automatisées de mise à jour et de correctifs pour pallier aux attaques potentielles du SI

Identifier la criticité de l'interruption d'activité en fonction des métiers de l'entreprise, pour préconiser des solutions techniques adaptées

Crypter les canaux de transmissions des sauvegardes émises via le réseau pour éviter une dépréciation de la valeur des éléments immatériels de l'entreprise

Mettre en place un plan périodique de restauration permettant de vérifier l'intégrité des données

Identifier les éléments et applications critiques de l'entreprise en vue d'assurer la continuité opérationnelle

Prévoir la chaîne d'approvisionnement nécessaire au déploiement d'un télétravail de masse

Anticiper la disponibilité des ressources indispensables à la continuité minimale selon les différents métiers, garantissant la continuité du service aux utilisateurs.

Déployer des moyens de protections matériels et logiciels pour assurer la disponibilité des données et des applicatifs conformément au plan de continuité établi par la direction de l'entreprise

Mettre en œuvre un modèle opérationnel cohérent des politiques de sécurités sur site et dans le Cloud par un contrôle de l'infrastructure de bout en bout

Collecter des informations auprès de spécialistes techniques et d'utilisateurs, en analysant et synthétisant les problèmes décrits et leurs solutions

Concevoir la documentation technique, en français et en anglais, pour répondre aux besoins d'information des techniciens et des utilisateurs internes à l'entreprise

Former les équipes supports sur l'utilisation des outils de télédistribution en élaborant si besoin un support de formation associé

Identifier les compétences techniques attendues et le degré intégrabilité des futurs collaborateurs au sein de l'équipe afin de transmettre une fiche de poste au service RH

Conduire un entretien annuel en contrôlant l'atteinte des objectifs fixés et des besoins du collaborateur afin de proposer une montée des compétences

Mettre en place des outils collaboratifs pour transmettre des informations, des savoirs en vue d'améliorer l'efficacité et les résultats

Déléguer les tâches de niveau 1 & 2 à réaliser, en mobilisant son équipe par une estimation et une hiérarchisation les priorités

Définir les rôles en planifiant les interventions et missions de chacun pour la meilleure atteinte des objectifs par une bonne maîtrise des techniques de conduite de projet et de la législation du travail

Arbitrer les divergences ou les rivalités au sein de l'équipe par la pratique d'une écoute active pour éviter les tensions contre-productives

Diffuser les informations préparatoires nécessaires à la bonne tenue d'une réunion pour favoriser les prises de décisions en adaptant sa communication orale et écrite à ses interlocuteurs, tant en français qu'en anglais

Diffuser les informations aux utilisateurs des différents services de l'entreprise par écrit ou par l'animation d'actions de formation ou d'ateliers de travail, permettant de garantir l'engagement de tous les acteurs à la sécurité des données de l'entreprise

Mesurer les rapports qualité/prix du marché et inciter à fournir des services de qualité adaptés en tenant compte de l'étude d'opportunité et de faisabilité grâce à une maîtrise de l'environnement technique et fonctionnel

Renforcer les mesures de protection contre les erreurs humaines et opérationnelles en sensibilisant les utilisateurs

aux mesures techniques de sécurité

Favoriser l'adhésion des décideurs à la protection de l'entreprise aux dangers de la cybercriminalité

Faire respecter les ententes de niveau de service par une bonne connaissance des bonnes pratiques et des aspects commerciaux et juridiques d'un contrat de location, de maintenance, de service

Obtenir des rabais, remises et ristournes ou des améliorations de délais de livraison de la part de fournisseurs grâce à une bonne maîtrise des techniques de négociation

Blocs de compétences

RNCP35594BC01 — Administrer le Système d'Information

LISTE DE COMPÉTENCES

Assurer l'exploitation du Système d'Information (SI) pour maintenir une opérationnalité constante grâce à un large spectre de savoir-faire associés aux systèmes

Concevoir l'infrastructure d'une plateforme virtuelle pour intégrer plusieurs machines physiques en une seule

Maintenir en conditions opérationnelles l'infrastructure de l'entreprise en utilisant des logiciels de gestion de la haute disponibilité

Identifier rapidement les systèmes qui nécessitent des correctifs et qui doivent être reconfigurés en fonction des préconisations constructeurs

Configurer les équipements réseaux pour assurer l'interconnexion physique et virtuelle des sites

Administrer les bases de données avec méthode selon la configuration requise pour leur mise en production

Mesurer et analyser les performances pour optimiser le stockage en vue de faciliter les accès

Améliorer les performances des bases de données en optimisant l'emplacement des stockages

Rationaliser les tâches quotidiennes en rédigeant des scripts et en les intégrant dans des procédures d'exploitation automatisées.

Faciliter la résolution des problèmes par une analyse des journaux d'historiques systèmes.

Automatiser les procédures de sauvegarde en rédigeant des scripts et en les intégrant avec des outils d'exploitation systèmes

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle : À partir d'un cas réel d'entreprise le candidat doit administrer l'infrastructure informatique et mettre en œuvre une infrastructure réseau, administrer des bases de données ou d'entrepôts de données en cloud ou sur site, automatiser l'administration des serveurs, les remontées d'alertes, les procédures de sauvegarde.

Livrable : Dossier

composé d'un portefeuille de preuves comprenant entre autres un journal d'exploitation, un schéma topologique du Système d'Information, un tableau statistique des taux de disponibilité, la stratégie des mises à jours, un plan d'adressage du réseau. la méthodologie d'administration des bases, une interprétation des journaux, une topologie d'architecture des bases déployées, des statistiques d'exploitation, une procédure d'exploitation et des exemples de scripts d'automatisations.

Un certificat des compétences attestées selon les modalités d'évaluation décrites sera délivré à chaque candidat(e) à l'issue de la validation du bloc de compétences.

RNCP35594BC02 — Assurer la gestion du Système d'information

LISTE DE COMPÉTENCES

Gérer les évolutions des infrastructures Informatiques en appliquant les principes et les limites de la norme IT Service Management ISO/CEI 20000

Assurer l'évolution des équipements en tenant compte des technologies émergentes

Comparer les solutions pour faire des propositions de renouvellement en tenant compte des contraintes budgétaires

Ordonnancer le plan de déploiement en tenant compte des disponibilités des différents acteurs concernés

Maquetter les solutions de déploiements pour le test et la validation des solutions retenues

Attribuer les ressources informatiques nécessaires au bon déroulement du plan en fonction du budget alloué

Superviser l'infrastructure informatique et le patrimoine applicatif pour identifier les anomalies, afin d'améliorer ses performances grâce aux outils spécifiques de monitoring installés

Recenser les ressources de l'infrastructure pour fournir des informations pertinentes sur l'architecture du SI

Migrer une architecture système ou réseau en optimisant les interventions et en gérant les risques

- Organiser l'infrastructure pour permettre l'intégration permanente d'évolutions logicielles
- Appliquer les évolutions des applications métiers en adoptant une approche incrémentielle et automatisée des modifications en production
- Centraliser le traitement des incidents en un point unique d'accès au centre de support pour mieux prioriser les interventions
- Elaborer un tableau de bord sur la résolution des tickets d'incidents par niveau de support pour améliorer l'efficacité de la résolution des incidents
- Résoudre les tickets de niveau 3 & 4 en intervenant sur place ou à distance à l'aide d'outils de télédistribution
- Concevoir un service numérique dans le but de réduire empreinte carbone en associant la transition écologique et numérique dans un contexte professionnel
- Déterminer les indicateurs à utiliser dans la gestion informatique quotidienne en vue de permettre l'évaluation des impacts des solutions informatiques en termes de responsabilités sociales et environnementales

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle : À partir d'un cas réel d'entreprise le candidat doit recenser et proposer de solutions tant techniques qu'organisationnelles susceptibles de parfaire et faire évoluer le Système d'Information, concevoir un plan d'évolution des équipements informatique en tenant compte des contraintes budgétaires, superviser et contrôler la performance du Système d'information, présenter sa gestion opérationnelle au quotidien de l'urbanisation du SI guidée par les principes de l'agilité, présenter la gestion de l'assistance utilisateurs et participer à la conception responsable d'un service numérique.

Livrable : Dossier composé d'un portefeuille de preuves comprenant entre autres un tableau de bord de suivi du parc informatique, une Etude comparative de solutions, une proposition budgétaire, un plan de déploiement, un exemple de maquettage, une procédure de déploiement, un suivi budgétaire de déploiement l'utilisation d'un outil de supervision, une cartographie du SI, une procédure de migration, un schéma de mise en production, une procédure d'intégration et de signalement d'incidents, une statistique des résolutions d'incidents, les résultats de résolutions de tickets, les actions écoresponsables mises en place et une liste d'indicateurs retenus.

Un certificat des compétences attestées selon les modalités d'évaluation décrites sera délivré à chaque candidat(e) à l'issue de la validation du bloc de compétences.

RNCP35594BC03 — Définir la politique de sécurisation du Système d'Information

LISTE DE COMPÉTENCES

- Agir avec méthode pour faire un état des lieux des risques de sécurité identifiables au sein du SI pour permettre aux décideurs de définir leur politique de sécurité
- Connaître et appliquer les normes ISO 27001 en adoptant une vue globale du SI dont le périmètre s'étend dans un contexte de télétravail massif
- Configurer des solutions de sécurité classiques
- Appliquer les techniques déployées afin de sécuriser les transactions numériques de l'entreprise en protégeant les transactions électroniques
- Appliquer les procédures de sécurité liées aux accès physiques et logiques des données de l'entreprise en s'appuyant sur une stratégie d'identification et de protection des données sensibles
- Mettre en place une gestion unique et commune des terminaux mobiles avec les autres matériels et logiciels, interfaçable avec les opérateurs sans fil et les solutions des constructeurs
- Mettre en œuvre des règles et processus de sécurité de gestion des identités et des accès pour gérer les habilitations
- Déployer des éléments passifs de protection systématique ou actifs en appliquant un plan d'urgence en cas d'infection virale
- Evaluer les perturbations de services grâce aux alertes émises par les sondes, pour identifier les correctifs à apporter
- Déployer des solutions automatisées de mise à jour et de correctifs pour pallier aux attaques potentielles du SI
- Identifier la criticité de l'interruption d'activité en fonction des métiers de l'entreprise, pour préconiser des solutions techniques adaptées
- Crypter les canaux de transmissions des sauvegardes émises via le réseau pour éviter une dépréciation de la valeur des éléments immatériels de l'entreprise
- Mettre en place un plan périodique de restauration permettant de vérifier l'intégrité des données
- Identifier les éléments et applications critiques de l'entreprise en vue d'assurer la continuité opérationnelle
- Prévoir la chaîne d'approvisionnement nécessaire au déploiement d'un télétravail de masse

Anticiper la disponibilité des ressources indispensables à la continuité minimale selon les différents métiers, garantissant la continuité du service aux utilisateurs
Déployer des moyens de protections matériels et logiciels pour assurer la disponibilité des données et des applicatifs conformément au plan de continuité établi par la direction de l'entreprise
Mettre en œuvre un modèle opérationnel cohérent des politiques de sécurités sur site et dans le Cloud par un contrôle de l'infrastructure de bout en bout

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle : À partir d'un cas réel d'entreprise le candidat doit participer à la définition de la politique de sécurité informatique de l'entreprise, prévenir, détecter et traiter les risques informatiques, identifier et appliquer des mesures correctives aux failles de sécurité de l'infrastructure informatique, élaborer un plan de reprise d'activité après sinistre et un plan de continuité d'activité en cas de crise et contrôler l'utilisation du cloud et du web pour les utilisateurs sur sites, mobiles et distants.

Livrable : Dossier composé d'un portefeuille de preuves comprenant entre autres un rapport d'audit, une certification Cobit, un rapport d'identification des failles, une certification ISO 27001, une procédure d'accès physique et aux données, un plan d'évaluation des risques, une solution de gestion unique des accès aux périphériques, le règlement d'attribution des droits d'accès de l'entreprise., le résultat d'un scan périodique du réseau, un plan d'urgence un rapport d'alertes de failles, une procédure de prévention des risques, le plan de reprise et plan de sauvegarde, le planning des tests de restauration, le plan de continuité et une étude comparative des offres Cloud.

Un certificat des compétences attestées selon les modalités d'évaluation décrites sera délivré à chaque candidat(e) à l'issue de la validation du bloc de compétences

RNCP35594BC04 — Communiquer avec tous les acteurs internes ou externes au service informatique

LISTE DE COMPÉTENCES

Collecter des informations auprès de spécialistes techniques et d'utilisateurs, en analysant et synthétisant les problèmes décrits et leurs solutions

Concevoir la documentation technique, en français et en anglais, pour répondre aux besoins d'information des techniciens et des utilisateurs internes à l'entreprise

Former les équipes supports sur l'utilisation des outils de télédistribution en élaborant si besoin un support de formation associé

Identifier les compétences techniques attendues et le degré intégrabilité des futurs collaborateurs au sein de l'équipe afin de transmettre une fiche de poste au service RH

Conduire un entretien annuel en contrôlant l'atteinte des objectifs fixés et des besoins du collaborateur afin de proposer une montée des compétences

Mettre en place des outils collaboratifs pour transmettre des informations, des savoirs en vue d'améliorer l'efficacité et les résultats

Déléguer les tâches de niveau 1 & 2 à réaliser, en mobilisant son équipe par une estimation et une hiérarchisation les priorités

Définir les rôles en planifiant les interventions et missions de chacun pour la meilleure atteinte des objectifs par une bonne maîtrise des techniques de conduite de projet et de la législation du travail

Arbitrer les divergences ou les rivalités au sein de l'équipe par la pratique d'une écoute active pour éviter les tensions contre-productives

Diffuser les informations préparatoires nécessaires à la bonne tenue d'une réunion pour favoriser les prises de décisions en adaptant sa communication orale et écrite à ses interlocuteurs, tant en français qu'en anglais

Diffuser les informations aux utilisateurs des différents services de l'entreprise par écrit ou par l'animation d'actions de formation ou d'ateliers de travail, permettant de garantir l'engagement de tous les acteurs à la sécurité des données de l'entreprise

Mesurer les rapports qualité/prix du marché et inciter à fournir des services de qualité adaptés en tenant compte de l'étude d'opportunité et de faisabilité grâce à une maîtrise de l'environnement technique et fonctionnel

Renforcer les mesures de protection contre les erreurs humaines et opérationnelles en sensibilisant les utilisateurs aux mesures techniques de sécurité

Favoriser l'adhésion des décideurs à la protection de l'entreprise aux dangers de la cybercriminalité

Faire respecter les ententes de niveau de service par une bonne connaissance des bonnes pratiques et des aspects commerciaux et juridiques d'un contrat de location, de maintenance, de service, ...

Obtenir des rabais, remises et ristournes ou des améliorations de délais de livraison de la part de fournisseurs grâce à une bonne maîtrise des techniques de négociation

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle : À partir d'un cas réel d'entreprise le candidat doit communiquer avec les acteurs internes au service informatique, encadrer et animer d'une équipe de techniciens, communiquer avec les acteurs externes au service informatique, sensibiliser l'ensemble des dirigeants et des collaborateurs sur les risques liés à la cybercriminalité, gérer les négociations auprès de ses fournisseurs.

Livrable : Dossier

composé d'un portefeuille de preuves comprenant entre autres une réalisation ou enrichissement d'une base de connaissance, une documentation technique, un plan de formation équipes internes, une demande d'autorisation de recrutement, une préparation d'un entretien annuel, un outil de répartition des tâches un

cas conflictuel résolu, une charte Informatique de l'entreprise, un rapport de préconisations, une réclamation au service client du fournisseur et un devis ou une facture remisés.

Un certificat des compétences attestées selon les modalités d'évaluation décrites sera délivré à chaque candidat(e) à l'issue de la validation du bloc de compétences

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'administrateur systèmes et réseaux, bases de données peut travailler dans l'ensemble des secteurs d'activité et toute taille d'entreprise. Pour les entreprises de plus de 100 collaborateurs, tous les secteurs d'activités publics ou privés sont concernés.

TYPE D'EMPLOIS ACCESSIBLES

Administrateur systèmes et réseaux (et sécurité)

Administrateur systèmes (et sécurité)

Administrateur réseaux (et sécurité)

Administrateur d'infrastructures

Administrateur Cloud

Administrateur des systèmes d'informations

Superviseur infrastructure et réseaux

Responsable infrastructure systèmes et réseaux

Administrateur sécurité informatique

Administrateur de bases de données

Gestionnaire de systèmes informatiques et réseaux

Gestionnaire de réseau

Responsable réseaux et télécoms

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)	Modérée (3/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 4 sur 5.
Facteurs principaux	Intensité d'embauche, Inadéquation géographique
Salaire médian (mensuel)	2 419 €
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)
Projets de recrutement (BMO 2026)	9 549
Jugés difficiles à recruter	46 %

Emplois saisonniers	3 %
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

Voies d'accès

MODALITÉS D'ACCÈS

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

PRÉREQUIS À L'ENTRÉE EN FORMATION

- Pour un parcours en 3 ans, les candidats doivent être titulaires d'une certification de niveau 4

prioritairement scientifique ou informatique

- Pour un parcours en 1 ou 2 ans

(selon le profil du candidat) , les candidats doivent être titulaires d'une certification de niveau 5

(ou

avoir validé

deux années de formation post bac

) dans le domaine de l'informatique

- L'accès à la formation est également recevable pour les

candidats titulaires d'un niveau 4 ET

pouvant justifier d'une expérience de 3 ans minimum récente

dans le domaine de l'informatique

Dans tous les cas, le candidat devra avoir reçu un avis positif à l'issue du processus d'évaluation à l'entrée en formation .

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

Le jury est composé de quatre membres professionnels du secteur informatique et externe à l'organisme.

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	10 300 €
Selon la branche	6 500 € – 10 383 €
Prise en charge	Branches concernées
10 300 €	Valeur par défaut · 175 branches
10 383 €	CPNE Personnel navigant technique des exploitants d'hélicoptères, CPNE Transport aérien : personnel au sol, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms, CPNEF de la Branche des organismes de formation
10 380 €	CPNE industries alimentaires diverses, CPNEFP Transformation Laitière, CPNEFP de la branche des industries de produits alimentaires élaborés, CPNEFP des industries charcutières, CPNIEFP dans la coopération agricole
8 500 €	CPNE de l'immobilier, CPNEF de l'audiovisuel
7 702 €	CPNEFP Commerce à distance, CPNEFP des jardineries et graineteries
7 604 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement

7 000 €	CPNEFP de l'enseignement privé indépendant, CPNEFP de la métallurgie
6 500 €	CPNE du Commerce de détail et de gros à prédominance alimentaire, CPNEF inter-secteurs papier carton
10 283 €	CPNEF de la Publicité
9 500 €	CPNE Branche Caoutchouc
9 345 €	CPNE Travail Temporaire
9 000 €	CPNE chimie
8 400 €	CPNEFP de l'habillement, mercerie, chaussure et jouet
8 160 €	CPNE de la branche de l'hospitalisation privée à statut commercial et du thermalisme
8 090 €	CPNE FP Commerce de Détail de l'Horlogerie Bijouterie
7 720 €	CPNE de la branche des experts comptables et commissaires aux comptes
7 500 €	CPNE des industries de santé (CPNEIS)
7 300 €	CPNE Banque

Base légale

Date de décision	19/05/2021
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	19/05/2026

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2019	235	2	89 %	71 %
2018	160	4	76 %	76 %
2017	118	3	79 %	83 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP12112

NOUVELLE(S) CERTIFICATION(S)

RNCP41996

CORRESPONDANCES (PAR BLOCS)

RNCP35093

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/35594/>

Entrées et sorties de formation

Entrées en formation	4
----------------------	---

Parcours menés à terme	3
Taux d'achèvement	75 %
Période	02/2022 – 03/2025

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

Demande CPF — formations engagées

Dossiers CPF engagés	6
Montant total engagé	25 827 €
Coût moyen par dossier	4 305 €
Durée moyenne	212 h
Période	11/2021 – 02/2025
France compétences	51 %
Entreprise	26 %
OPCO	15 %
Reste à charge titulaire	4 %
État	4 %

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