

Technicien systèmes réseaux et sécurité

RNCP36462 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 5
Code(s) NSF	326r, 326
Formacode(s)	31034
Code(s) ROME	M1801, H1101, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	01/06/2022
Date d'échéance	01/06/2027

Certificateur(s)

ASS. POUR DEVELOPPEMENT INSERTION PROFES · SIRET : 40980167700017

INSTITUT DE GESTION SOCIALE (IGS) · SIRET : 31249509600157

Partenaires habilités

18 organismes habilités, d'après la liste publiée par France compétences : 18 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
APAVE EXPLOITATION FRANCE	90386961800012	Former et organiser l'évaluation
ASTON INSTITUT	49868549400029	Former et organiser l'évaluation
ASTON INSTITUT	49868549400052	Former et organiser l'évaluation
ASTON INSTITUT	49868549400060	Former et organiser l'évaluation
CIEFA DEPARTEMENT IPI	33264146300077	Former et organiser l'évaluation
EXPERNET	44276468400027	Former et organiser l'évaluation
EXPERNET CAMPUS INFORMATIQUE	44276468400035	Former et organiser l'évaluation
GROUPE IGS - CIEFA	33264146300028	Former et organiser l'évaluation
GROUPE IGS - CIEFA	33264146300051	Former et organiser l'évaluation
GROUPE IGS - CIEFA	33264146300135	Former et organiser l'évaluation

Liste complète des 18 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp36462-technicien-systemes-reseaux-et-securite/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le Technicien systèmes, réseaux et sécurité est le garant du bon fonctionnement des équipements informatiques et du réseau de l'entreprise. Son périmètre d'intervention peut s'étendre sur site, à distance et dans le Cloud. Il gère l'inventaire en appliquant une démarche écoresponsable, déploie le matériel, veille au maintien du parc informatique, recense les besoins des utilisateurs et préconise les solutions logicielles ou d'infrastructure. Il met en oeuvre les mesures de sécurité et sensibilise les utilisateurs afin de minimiser les risques cyber. Il participe à la transformation

digitale de l'entreprise en accompagnant les utilisateurs dans l'utilisation des nouveaux outils telles que les plateformes collaboratives.

ACTIVITÉS VISÉES

Déploiement des matériels, les systèmes et le réseau
Administration des serveurs hétérogènes et un réseau multi-sites
Sécurisation de l'environnement numérique d'exploitation
Entretien d'un parc informatique
Gestion du support technique auprès des utilisateurs

COMPÉTENCES ATTESTÉES

Vérifier le bon fonctionnement des matériels en effectuant des tests de pré-déploiement pour éviter les retours et dysfonctionnements.
Connaître l'architecture matérielle d'un poste de travail pour un déploiement adéquat aux besoins des services.
Déployer des serveurs physiques et virtuels pour centraliser les comptes des utilisateurs.
Intégrer les imprimantes dans le serveur d'impression afin de mutualiser leurs gestions.
Centraliser les connexions des téléphones IP et caméra des salles de réunions afin de faciliter leur gestion.
Intégrer la flotte des équipements mobiles en les interconnectant dans le réseau de l'entreprise en tenant compte des collaborateurs en situation de handicap.
Installer les systèmes d'exploitation hétérogènes grâce à un large spectre de savoir-faire associés en se référant rigoureusement aux notices techniques.
Se conformer strictement à des processus logiques et méthodologiques d'installation afin d'homogénéiser les processus de déploiement.
Automatiser la configuration des systèmes d'exploitation à l'aide de scripts afin de réduire les coûts et les délais de déploiement.
Se référer rigoureusement aux notices techniques en utilisant ses connaissances sur les protocoles réseaux afin d'identifier les différents équipements nécessaires à l'interconnexion des réseaux d'entreprise.
Brasser les liens réseaux pour assurer une connectivité de l'ensemble des équipements en respectant les plans et schémas réseaux.
Configurer le routage des différents réseaux pour assurer une communication optimale entre les différents sites de l'entreprise.
Appliquer le processus de déploiement des logiciels conformément à la gestion des licences et des autorisations de l'entreprise selon la demande du service tout en tenant compte des collaborateurs en situation de handicap.
Configurer des logiciels de prise en main à distance sur les postes clients afin d'assurer un support sur les postes nomades.
Automatiser l'installation des logiciels en fonction des besoins de l'utilisateur.
Configurer les plateformes collaboratives afin d'assurer la productivité de l'entreprise liée au travail hybride.
Utiliser les différents systèmes d'exploitation en tenant compte de leur interopérabilité.
Identifier les normes et protocoles réseaux nécessaire à l'installation et le paramétrage des serveurs physiques ou virtuels.
Utiliser les outils d'administration afin de centraliser la gestion des comptes utilisateurs et des droits d'accès aux applications métiers.
Optimiser les tâches récurrente d'administration des serveurs en produisant des scripts systèmes réutilisable.
Établir des règles d'administration afin de veiller au bon fonctionnement de la remontée des logs et des alertes.
Configurer les outils de sauvegardes et de restauration conformément au plan de reprise d'activité.
Se référer rigoureusement aux notices techniques en utilisant ses connaissances sur les protocoles réseaux.
Se conformer strictement à des processus logiques et méthodologiques en respectant les procédures établies.
Réaliser des maquettes réseaux pour simuler l'intégration de nouveaux équipements réseaux et réduire les erreurs potentielles de configurations.
Installer les solutions de sauvegarde grâce à un large spectre de savoir-faire technique associés aux politiques de sauvegarde.
Appliquer une gestion stricte des droits et des identités des utilisateurs en contrôlant l'annuaire de l'entreprise pour éviter un accès inapproprié aux données.
Tester régulièrement la redondance et l'opérationnalité des équipements du parc informatique.
Appliquer les directives du plan de reprise et de continuité d'activité en respectant son périmètre et les consignes.
Identifier le matériel, les systèmes d'exploitation ou les logiciels à mettre à jour (virtualisé ou physique) afin de

corriger les vulnérabilités.

Anticiper l'évolution de l'état des matériels, systèmes et logiciels pour minimiser les incidents de sécurité du parc informatique.

Vérifier que les terminaux gérés exécutent la version à jour des logiciels de sécurité en respectant les procédures d'entretien préventif.

Identifier les plateformes de mise à jour pour les matériels, systèmes et logiciels (virtualisées ou physiques) pour éviter les erreurs de configuration.

Configurer les outils de surveillance afin de filtrer l'accès au réseau de l'entreprise à l'aide de listes permettant de bloquer l'accès aux sites malveillants connus.

Chiffrer les équipements nomades (smartphone, tablettes, PC...) pour éviter l'exploitation frauduleuse des données de l'entreprise.

Créer des canaux de sécurisation en utilisant ses connaissances sur les protocoles de sécurité.

Limiter l'accès aux réseaux sans-fils public afin d'éviter les intrusions malveillantes.

Appliquer les procédures de sécurité liées aux accès physiques et logiques des données de l'entreprise afin de respecter la politique de sécurité de l'entreprise.

Tester l'opérationnalité des éléments constitutifs de sécurisation d'un parc informatique en respectant les processus méthodologiques préconisés.

Appliquer les processus de réception pour éviter les erreurs de livraisons.

Renseigner les documents de suivi afin de mettre à jour l'inventaire du parc informatique.

Mettre à jour des matériels, des systèmes d'exploitation et les logiciels clients pour garantir le fonctionnement optimal des équipements informatiques.

Renouveler le matériel informatique de l'utilisateur afin d'augmenter la durabilité des équipements du parc informatique.

Migrer des systèmes d'exploitation en fin de vie afin de maintenir leur opérationnalité pour répondre aux enjeux du développement durable.

Réparer et reconditionner des équipements informatiques garantissant un environnement numérique durable et écoresponsable.

Exploiter des méthodologies de recherche et d'organisation d'informations sur les nouvelles technologies.

Appliquer la méthode 4R (Réduire, réparer, réemployer et recycler) permettant d'augmenter le cycle de vie des postes utilisateurs.

Recycler le matériel usagé et obsolète du parc informatique dans le respect d'une démarche de transition écologique.

Collecter les informations permettant d'anticiper les innovations technologiques et de surveiller les nouvelles menaces informatiques en utilisant les différents outils de veille.

Analyser les nouvelles technologies émergentes avec leurs avantages et inconvénients sur le SI existant dans son périmètre d'intervention.

Rédiger des comparatifs des nouveaux matériels et logiciels par rapport à ceux utilisées par l'entreprise dans l'objectif d'augmenter les performances du SI.

Alerter et déclarer systématiquement toutes anomalies pouvant affecter le bon fonctionnement des éléments du parc informatique.

Respecter les niveaux de services inhérents aux contrats de maintenance afin de garantir les délais d'interventions.

Gérer les conflits utilisateurs afin d'établir une relation de confiance.

Analyser une situation en toute autonomie afin d'apporter une solution appropriée sur son périmètre.

Rédiger un rapport d'interventions sur la résolution d'incidents afin de garantir leurs suivis.

Développer son sens du service afin de résoudre les incidents des utilisateurs.

Se référer rigoureusement aux procédures d'entreprise permettant de hiérarchiser ses interventions.

Reformuler les requêtes des utilisateurs en faisant preuve d'empathie afin d'établir une relation de confiance dans l'objectif de faciliter la résolution de l'incident, en tenant compte des collaborateurs en situation de handicap.

Exposer une problématique technique ou organisationnelle en vue d'un partage d'informations au sein de l'équipe.

Prendre des notes et synthétiser l'information tant en français qu'en anglais pour diffusion en interne et externe au service informatique.

Respecter les règles de base de la communication écrite et orale tant en français qu'en anglais.

Synthétiser des informations d'ordre opérationnel afin de rédiger un compte rendu de réunion.

Assister l'utilisateur en facilitant la compréhension d'éléments techniques tout en s'assurant de la bonne compréhension par l'utilisateur des termes et procédures informatiques, en tenant compte des collaborateurs en situation de handicap.

Diffuser des bonnes pratiques pour un systèmes d'information plus responsable permettant de limiter l'impact sur l'environnement des usages du numérique.

Conseiller les utilisateurs sur les gestes écoresponsables en vue de réduire la pollution numérique.

Blocs de compétences

RNCP36462BC01 — Déployer les matériels, les systèmes et le réseau.

LISTE DE COMPÉTENCES

Vérifier le bon fonctionnement des matériels en effectuant des tests de pré-déploiement pour éviter les retours et dysfonctionnements.

Connaître l'architecture matérielle d'un poste de travail pour un déploiement adéquat aux besoins des services.

Déployer des serveurs physiques et virtuels pour centraliser les comptes des utilisateurs.

Intégrer les imprimantes dans le serveur d'impression afin de mutualiser leurs gestions.

Centraliser les connexions des téléphones IP et caméra des salles de réunions afin de faciliter leur gestion.

Intégrer la flotte des équipements mobiles en les interconnectant dans le réseau de l'entreprise en tenant compte des collaborateurs en situation de handicap.

Installer les systèmes d'exploitation hétérogènes grâce à un large spectre de savoir-faire associés en se référant rigoureusement aux notices techniques.

Se conformer strictement à des processus logiques et méthodologiques d'installation afin d'homogénéiser les processus de déploiement.

Automatiser la configuration des systèmes d'exploitation à l'aide de scripts afin de réduire les coûts et les délais de déploiement.

Se référer rigoureusement aux notices techniques en utilisant ses connaissances sur les protocoles réseaux afin d'identifier les différents équipements nécessaires à l'interconnexion des réseaux d'entreprise.

Brasser les liens réseaux pour assurer une connectivité de l'ensemble des équipements en respectant les plans et schémas réseaux.

Configurer le routage des différents réseaux pour assurer une communication optimale entre les différents sites de l'entreprise.

Appliquer le processus de déploiement des logiciels conformément à la gestion des licences et des autorisations de l'entreprise selon la demande du service tout en tenant compte des collaborateurs en situation de handicap.

Configurer des logiciels de prise en main à distance sur les postes clients afin d'assurer un support sur les postes nomades.

Automatiser l'installation des logiciels en fonction des besoins de l'utilisateur.

Configurer les plateformes collaboratives afin d'assurer la productivité de l'entreprise liée au travail hybride.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

À partir d'un cas réel d'entreprise le candidat doit déployer les matériels informatiques de production en conformité avec l'évolution de l'accessibilité numérique, installer les systèmes d'exploitation., déployer un réseau d'entrepisen déployer les logiciels.

Livrable : dossier de validation composé d'un portefeuille de preuves comprenant entre autres la procédures d'installation, plan de déploiement, plan de recette (...)

RNCP36462BC02 — Administrer des serveurs hétérogènes et un réseau multi-sites.

LISTE DE COMPÉTENCES

Utiliser les différents systèmes d'exploitation en tenant compte de leur interopérabilité.

Identifier les normes et protocoles réseaux nécessaire à l'installation et le paramétrage des serveurs physiques ou virtuels.

Utiliser les outils d'administration afin de centraliser la gestion des comptes utilisateurs et des droits d'accès aux applications métiers.

Optimiser les tâches récurrente d'administration des serveurs en produisant des scripts systèmes réutilisable.

Établir des règles d'administration afin de veiller au bon fonctionnement de la remontée des logs et des alertes.

Configurer les outils de sauvegardes et de restauration conformément au plan de reprise d'activité.

Se référer rigoureusement aux notices techniques en utilisant ses connaissances sur les protocoles réseaux.

Se conformer strictement à des processus logiques et méthodologiques en respectant les procédures établies.

Réaliser des maquettes réseaux pour simuler l'intégration de nouveaux équipements réseaux et réduire les erreurs potentielles de configurations.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

À partir d'un cas réel d'entreprise le candidat doit Installer et paramétrer les systèmes d'exploitation des serveurs physiques ou virtuels, administrer les serveurs de production, administrer les réseaux multi-sites.

Livrable : dossier de validation composé d'un portefeuille de preuves comprenant entre autres la procédure d'installation, le plan de migration, la politique de sauvegarde (...)

RNCP36462BC03 — Sécuriser l'environnement numérique d'exploitation.

LISTE DE COMPÉTENCES

Installer les solutions de sauvegarde grâce à un large spectre de savoir-faire technique associés aux politiques de sauvegarde.

Appliquer une gestion stricte des droits et des identités des utilisateurs en contrôlant l'annuaire de l'entreprise pour éviter un accès inapproprié aux données.

Tester régulièrement la redondance et l'opérationnalité des équipements du parc informatique.

Appliquer les directives du plan de reprise et de continuité d'activité en respectant son périmètre et les consignes.

Identifier le matériel, les systèmes d'exploitation ou les logiciels à mettre à jour (virtualisé ou physique) afin de corriger les vulnérabilités.

Anticiper l'évolution de l'état des matériels, systèmes et logiciels pour minimiser les incidents de sécurité du parc informatique.

Vérifier que les terminaux gérés exécutent la version à jour des logiciels de sécurité en respectant les procédures d'entretien préventif.

Identifier les plateformes de mise à jour pour les matériels, systèmes et logiciels (virtualisées ou physiques) pour éviter les erreurs de configuration.

Configurer les outils de surveillance afin de filtrer l'accès au réseau de l'entreprise à l'aide de listes permettant de bloquer l'accès aux sites malveillants connus.

Chiffrer les équipements nomades (smartphone, tablettes, PC...) pour éviter l'exploitation frauduleuse des données de l'entreprise.

Créer des canaux de sécurisation en utilisant ses connaissances sur les protocoles de sécurité.

Limiter l'accès aux réseaux sans-fils public afin d'éviter les intrusions malveillantes.

Appliquer les procédures de sécurité liées aux accès physiques et logiques des données de l'entreprise afin de respecter la politique de sécurité de l'entreprise.

Tester l'opérationnalité des éléments constitutifs de sécurisation d'un parc informatique en respectant les processus méthodologiques préconisés.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

À partir d'un cas réel d'entreprise le candidat doit Appliquer la politique de sécurité de l'entreprise à tous les niveaux (physique, système, logiciel, réseau), appliquer les mesures correctives des failles de sécurités des équipements informatiques, intégrer les logiciels de sécurité système et réseau.

Livrable : dossier de validation composé d'un portefeuille de preuves comprenant entre autres le plan de sauvegarde et de restauration, la politique de sécurité, la plan de veille sur les vulnérabilités (...)

RNCP36462BC04 — Entretenir un parc informatique.

LISTE DE COMPÉTENCES

Appliquer les processus de réception pour éviter les erreurs de livraisons.

Renseigner les documents de suivi afin de mettre à jour l'inventaire du parc informatique.

Mettre à jour des matériels, des systèmes d'exploitation et les logiciels clients pour garantir le fonctionnement optimal des équipements informatiques.

Renouveler le matériel informatique de l'utilisateur afin d'augmenter la durabilité des équipements du parc informatique.

Migrer des systèmes d'exploitation en fin de vie afin de maintenir leur opérationnalité pour répondre aux enjeux du développement durable.

Réparer et reconditionner des équipements informatiques garantissant un environnement numérique durable et

écoresponsable.

Exploiter des méthodologies de recherche et d'organisation d'informations sur les nouvelles technologies.

Appliquer la méthode 4R (Réduire, réparer, réemployer et recycler) permettant d'augmenter le cycle de vie des postes utilisateurs.

Recycler le matériel usagé et obsolète du parc informatique dans le respect d'une démarche de transition écologique.

Collecter les informations permettant d'anticiper les innovations technologiques et de surveiller les nouvelles menaces informatiques en utilisant les différents outils de veille.

Analyser les nouvelles technologies émergentes avec leurs avantages et inconvénients sur le SI existant dans son périmètre d'intervention.

Rédiger des comparatifs des nouveaux matériels et logiciels par rapport à ceux utilisés par l'entreprise dans l'objectif d'augmenter les performances du SI.

Alerter et déclarer systématiquement toutes anomalies pouvant affecter le bon fonctionnement des éléments du parc informatique.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

À partir d'un cas réel d'entreprise le candidat doit réceptionner les matériels ou les fournitures suivant les procédures d'entreprise, entretenir les matériels et systèmes informatiques, gérer l'inventaire des équipements du parc informatique, proposer des améliorations du parc informatique.

Livrable : dossier de validation composé d'un portefeuille de preuves comprenant entre autres

le documents de suivi, l'inventaire matériels et logiciels, l'état du stock, le plan de veille technologique, le rapports d'alertes (...)

RNCP36462BC05 — Assurer le support technique auprès des utilisateurs.

LISTE DE COMPÉTENCES

Respecter les niveaux de services inhérents aux contrats de maintenance afin de garantir les délais d'interventions.

Gérer les conflits utilisateurs afin d'établir une relation de confiance.

Analyser une situation en toute autonomie afin d'apporter une solution appropriée sur son périmètre.

Rédiger un rapport d'interventions sur la résolution d'incidents afin de garantir leurs suivis.

Développer son sens du service afin de résoudre les incidents des utilisateurs.

Se référer rigoureusement aux procédures d'entreprise permettant de hiérarchiser ses interventions.

Reformuler les requêtes des utilisateurs en faisant preuve d'empathie afin d'établir une relation de confiance dans l'objectif de faciliter la résolution de l'incident, en tenant compte des collaborateurs en situation de handicap.

Exposer une problématique technique ou organisationnelle en vue d'un partage d'informations au sein de l'équipe.

Prendre des notes et synthétiser l'information tant en français qu'en anglais pour diffusion en interne et externe au service informatique.

Respecter les règles de base de la communication écrite et orale tant en français qu'en anglais.

Synthétiser des informations d'ordre opérationnel afin de rédiger un compte rendu de réunion.

Assister l'utilisateur en facilitant la compréhension d'éléments techniques tout en s'assurant de la bonne compréhension par l'utilisateur des termes et procédures informatiques, en tenant compte des collaborateurs en situation de handicap.

Diffuser des bonnes pratiques pour un systèmes d'information plus responsable permettant de limiter l'impact sur l'environnement des usages du numérique.

Conseiller les utilisateurs sur les gestes écoresponsables en vue de réduire la pollution numérique.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle

À partir d'un cas réel d'entreprise le candidat doit diagnostiquer et résoudre des incidents techniques de niveau 1 & 2, réceptionner et gérer des incidents techniques en conformité avec la culture d'entreprise, participer aux réunions de travail de l'équipe informatique, former et communiquer auprès des utilisateurs.

Livrable : dossier de validation composé d'un portefeuille de preuves comprenant entre autres les fiches d'interventions, le contrat de service, l'historique d'interventions, le compte rendu d'activité, les rapports d'incidents, les apports d'intrusions et d'attaques informatiques, les résultats des enquêtes cybersécurité (...)

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Pour les entreprises de plus de 100 collaborateurs, tous les secteurs d'activités publics ou privés sont concernés.
Pour les entreprises de moins de 100 collaborateurs : Entreprise de services numériques (ESN), entreprises du secteur du tertiaire à haute valeur ajoutée.

TYPE D'EMPLOIS ACCESSIBLES

- Technicien système et réseau
- Technicien d'exploitation informatique
- Technicien réseau et télécom
- Adjoint technique informatique
- Technicien support et production
- Assistant administrateur systèmes et réseaux
- Technicien sécurité informatique
- Technicien d'exploitation Cloud
- Technicien service clients
- Techniciens des services aux utilisateurs en informatique

RÉGLEMENTATIONS D'ACTIVITÉ

Néant.

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	Intensité d'embauche, Inadéquation géographique
Salaire médian (mensuel)	2 468 €
Familles professionnelles (FAP)	G1X75 — Techniciens et agents de maîtrise en assistance et support technique client et en installation et maintenance télécoms et courants faibles · tension 5/5 (Très élevée) H1X92 — Ingénieurs en maintenance et support technique client · tension 5/5 (Très élevée) 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)	12 787
Jugés difficiles à recruter	47 %
Emplois saisonniers	3 %
Familles professionnelles (FAP)	G1X75 — Techniciens et agents de maîtrise en assistance et support technique client et en installation et maintenance télécoms et courants faibles H1X92 — Ingénieurs en maintenance et support technique client 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

PRÉREQUIS À L'ENTRÉE EN FORMATION

Formation initiale: le candidat doit avoir au moins un diplôme de niveau 4.

Formation continue:

avoir une expérience professionnelle de trois ans et plus.

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

Le jury est composé de deux professionnels de l'informatique, externes au certificateur ou des organismes partenaires

COMPOSITION DU JURY — VAE

Le jury est composé de trois professionnels de l'informatique, externes au certificateur

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	11 183 €
Selon la branche	6 000 € – 11 764 €
Prise en charge	Branches concernées
11 183 €	Valeur par défaut · 185 branches
11 764 €	CPNE Entreprises des activités du déchet et de la propreté urbaine, 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, CPNEFP Commerce à distance
11 374 €	CPNE du Commerce de détail et de gros à prédominance alimentaire, CPNEFP de l'enseignement privé indépendant
11 725 €	CPNEF de la Publicité
11 562 €	CPNEF de l'audiovisuel
11 160 €	CPNE de l'ingénierie, des services informatiques et du conseil
10 500 €	CPNE chimie
10 400 €	CPNEFP de la branche professionnelle des Entreprises du courtage d'assurances et/ou réassurances
10 000 €	CNPE de la Plasturgie et des Composites
9 120 €	CPNE de la branche de l'hospitalisation privée à statut commercial et du thermalisme
9 000 €	CPNE Branche Caoutchouc
8 730 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager
8 500 €	CPNE des industries de santé (CPNEIS)
8 000 €	CPNE de l'immobilier
6 000 €	CPNEFP de la métallurgie

Base légale

Date de décision	01/06/2022
Durée de l'enregistrement	5 ans

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2020	167	0	100 %	—
2019	128	0	91 %	83 %
2018	130	0	95 %	82 %

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP28668

CORRESPONDANCES (PAR BLOCS)
RNCP35583

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/36462/>

Où se former

Formations référencées	1
Organismes	1
Régions couvertes	0
Prix indicatif	9 000 €

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

Se former en apprentissage

Formations en apprentissage	6
Organismes gestionnaires (CFA)	5
Organismes formateurs	5
Régions couvertes	4
Départements couverts	5
Organismes certifiés Qualiopi	5
Formations à distance	2
Sessions	de 02/2024 à 08/2028

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	17
----------------------	----

Parcours menés à terme	7
Taux d'achèvement	41 %
Période	01/2024 – 09/2026

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

Demande CPF — formations engagées

Dossiers CPF engagés	18
Montant total engagé	100 020 €
Coût moyen par dossier	5 557 €
Durée moyenne	735 h
Période	12/2023 – 07/2026
France compétences	50 %
OPCO	40 %
Reste à charge titulaire	10 %
Compte d'engagement citoyen	0 %

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