

Administrateur systèmes, réseaux et cybersécurité

RNCP40356 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326
Formacode(s)	31034, 31032, 31006, 24231, 31008
Code(s) ROME	M1801
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	28/03/2025
Date d'échéance	28/03/2030

Certificateur(s)

OPENCLASSROOMS · SIRET : 49386136300080

OPENCLASSROOMS · SIRET : 49386136300098

Partenaires habilités

7 organismes habilités, d'après la liste publiée par France compétences : 1 à former et organiser l'évaluation et 6 à former.

Organisme	SIRET	Habilitation
GRETA COTES NORMANDES	19501219000029	Former
GRETA PORTES NORMANDES	19270016900027	Former
LYCEE ENS GEN TECHNO GUSTAVE FLAUBERT	19760096800022	Former
LYCEE GENERAL ET TECHNOLOGIQUE CAMILLE JULLIAN	19330023300031	Former
LYCEE TECHNIQUE REGIONAL LES EUCALYPTUS	19060075900020	Former
OPENCLASSROOMS	49386136300098	Former et organiser l'évaluation
ORGANISME DE GESTION DE L'ECOLE SCHNEIDER ELECTRIC	87838051800026	Former

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'administrateur systèmes, réseaux et sécurité est responsable de la performance et de la sécurité du système d'information de l'entreprise pour laquelle il travaille. Il doit être en mesure d'identifier et de mettre en œuvre les solutions qui répondent aux besoins et aux contraintes du SI sous sa responsabilité. Il fait évoluer le SI en cohérence avec les évolutions du contexte sans transiger sur le niveau de performance et de sécurité requis. Il intervient pour cela sur toutes les étapes du cycle de vie du SI, de sa conception initiale à son amélioration continue : en passant par sa mise en production, son administration et sa maintenance au quotidien.

En fonction de son cadre d'intervention, il pourra être amené soit à concentrer ses activités sur un périmètre donné dont il deviendra spécialiste (réseaux, systèmes, etc.), soit à endosser plusieurs casquettes nécessitant une certaine polyvalence et par conséquent, des savoir-faire variés et moins spécialisés. Il est donc important qu'un administrateur réseaux, systèmes et sécurité sache agir sur toutes les couches et tout le cycle de vie du SI.

Pour réussir ses missions, l'administrateur systèmes, réseaux et sécurité doit s'appuyer sur de solides compétences techniques et posséder des savoir-être (compétences comportementales) pour collaborer au quotidien avec ses

interlocuteurs.

ACTIVITÉS VISÉES

Veille informationnelle (principalement réglementaire technologique et sécurité)
Collecte et analyse des besoins
Recherche d'une solution technique
Conseil auprès des décideurs
Établissement / formalisation du plan projet
Conception des infrastructures systèmes / réseaux
Mise en place des infrastructures systèmes / réseaux
Gestion des accès aux ressources
Gestion des actifs informatiques et configuration, des mises à jour et des sauvegardes
Supervision du bon fonctionnement des infrastructures informatiques
Surveillance du degré de sécurité des infrastructures informatiques

COMPÉTENCES ATTESTÉES

Définir et mettre en place un système de veille automatisée ou non afin de repérer les évolutions en lien avec son activité (Information Technology / technologies de l'information)
Analyser les informations collectées afin d'identifier les opportunités (ex : nouvelles technologies, nouveaux services cloud) et les éventuelles menaces (ex : cybermenaces, mise en conformité nécessaire) Le cas échéant, les partager avec ses pairs (communauté / réseau) ou bien des collaborateurs au sein d'une organisation
Analyser, le cas échéant préciser / affiner, et formaliser les besoins informatiques, afin d'identifier les objectifs (résultats attendus) et les éventuelles contraintes techniques, matérielles, budgétaires et réglementaires
Identifier une solution en termes d'infrastructure informatique, adaptée et conforme aux besoins / contraintes, à l'aide d'une recherche ponctuelle ciblée ou bien à partir de la veille, et la représenter visuellement, à l'aide d'un outil de modélisation adapté, afin d'en illustrer son implémentation, ses actions et ses éventuels impacts / risques
Estimer les coûts associés (humains et matériels) à la solution technique afin de déterminer le budget nécessaire à sa mise en production et à son exploitation
Présenter la solution technique, expliquer / argumenter ses choix techniques / financiers auprès des décideurs dans un objectif de validation
Organiser (définir / planifier / attribuer) les tâches nécessaires à la conception et à la mise en production de la solution dans le système d'information en cohérence avec les contraintes de l'organisation (notamment un minimum d'impact sur la continuité du service)
Définir / structurer / modéliser l'architecture technique de l'infrastructure cible, à l'aide d'un logiciel adapté, selon l'agencement des briques fonctionnelles (utilisateurs / données / traitements souhaités) et les critères fournis (performance, sécurité, évolutivité, etc), afin de définir l'organisation et les caractéristiques des équipements / composants et leurs interactions
Identifier les configurations à appliquer sur les équipements / composants de l'infrastructure cible, à partir des ressources adaptées (ex : documentation fournisseur) et selon le modèle d'architecture défini afin d'en disposer selon l'usage voulu
Créer un prototype ou bien une version pilote (une maquette test) de l'infrastructure système / réseau, à l'aide d'un outil de simulation adapté, afin de visualiser et de tester les équipements / composants, leurs interactions et les fonctionnalités associées Valider ou non la mise en production selon les résultats
Identifier les règles de durcissement (suppression des services inutiles, forcer la robustesse des mots de passe, etc), à partir des guides externes (ANSSI, fournisseurs, etc), les adapter si besoin aux contraintes de l'organisation afin de sécuriser les infrastructures
Installer et effectuer les réglages (configurations / sécurisation) sur les équipements / composants réseaux / systèmes, quel que soit le type d'infrastructure et le mode de déploiement, dans le respect des règles de l'art et selon les caractéristiques techniques et fonctionnelles définies
Élaborer et mettre en œuvre une procédure de test afin de valider la conformité et la fonctionnalité de l'infrastructure déployée
Rédiger l'ensemble des procédures nécessaires à la mise en production / au déploiement de la solution
Former les utilisateurs ou bien communiquer les bonnes pratiques liées à l'utilisation d'un nouveau service afin d'accompagner le changement
Organiser / mettre à jour un annuaire des rôles / des autorisations associées à l'aide d'un outil adapté selon les droits définis, dans le respect de la politique de sécurité de l'organisation et de la réglementation en vigueur (sur les

données) afin de centraliser la gestion des identités / accès

Concevoir, mettre en place et planifier des solutions d'automatisation (ex : scripts, applications) sur des tâches préalablement identifiées à l'aide d'outils adaptés afin de lancer et d'exécuter de manière automatisée les opérations

Mettre en place un système d'authentification au SI et à ses services afin de permettre un accès sécurisé, conforme et différencié au système d'information (et à ses services)

Mettre en place (installer / configurer / tester / sécuriser) un outil de gestion des actifs et des configurations automatisé, partagé selon les droits définis et accessible, afin de mettre à jour [bénéficier en temps réel des informations sur] les composants du système d'information, préalablement inventoriés, et leurs relations

Définir (choix des méthodes, outils, techniques), installer, configurer et tester une stratégie opérationnelle de sauvegarde en cohérence avec les données (nature / type / criticité) et les contraintes de l'organisation afin d'enregistrer / de dupliquer / de répliquer et d'archiver les données dans un ou plusieurs lieux de stockage selon les critères définis au sein du plan de sauvegarde (classification des données, fréquence souhaitée, etc)

Automatiser les tâches (les opérations) de sauvegarde à l'aide des outils (de planification / d'exécution) et des langages de programmation adaptés (ex : PowerShell, Python, Bash)

Sécuriser, à l'aide des configurations adaptées au plan de sauvegarde et préconisées (ANSSI, fournisseurs, etc), les sauvegardes lors des enregistrements / duplications / réplifications / archivage, afin de réduire les risques d'altération ou de disparition des données

Documenter le système de sauvegarde et établir / formaliser une procédure de restauration des données afin de fournir la démarche à appliquer en cas d'incident

Prioriser et affecter les tickets selon le type / le niveau de support, à l'aide d'un outil de gestion (ex : outil de ticketing / d'assistance) adapté, afin d'organiser les interventions

Effectuer des interventions de support niveaux 2 et/ou 3 afin de rétablir le service fourni au niveau attendu Les enregistrer (demande, réponse apportée, le cas échéant, documentation fournie) afin d'assurer la traçabilité et de clôturer les tickets

Intégrer un outil de supervision, le paramétrer selon le niveau de service attendu (observation des indicateurs de performance / sécurité / disponibilité et seuils) et le tester afin de monitorer les infrastructures informatiques (enregistrer l'activité) et d'émettre une alerte en cas de dysfonctionnements (franchissement du seuil d'alerte)

Établir une procédure afin de présenter le système de supervision auprès de l'équipe en charge de la maintenance du système d'information et les actions à entreprendre en cas de dysfonctionnement / d'alerte (points de contrôles, indicateurs, actions à entreprendre en cas de dysfonctionnement)

Exploiter les remontées (logs / journaux) des activités enregistrées via l'outil de supervision afin d'analyser la performance et la disponibilité des infrastructures informatiques selon les différentes utilisations (spécifiques ou non) au regard des indicateurs définis (ex : taux de disponibilité, charges de calcul, temps de réponse, etc)

Structurer et outiller les différentes étapes d'une intervention portant sur l'évaluation de la sécurité informatique (collecte d'informations, inventaire des actifs, recherche de vulnérabilité, exploitation, élévation des privilèges, propagation, nettoyage) en cohérence avec un périmètre cible

Mettre en œuvre une évaluation de la sécurité informatique sur un périmètre cible, selon la méthodologie préalablement définie et à l'aide des outils adaptés (outils d'énumération / scanner, test d'intrusion, etc) afin d'identifier et de caractériser les vulnérabilités et les failles de sécurité selon leur niveau de criticité

Documenter les vulnérabilités et les failles de sécurité afin de les partager au commanditaire (client interne / externe) Le cas échéant, rédiger des supports à destination d'un public plus élargi (non technique) afin de rendre accessibles les conclusions de l'évaluation

Proposer des mesures ou bien des règles, en cohérence avec les vulnérabilités / failles observées, afin de renforcer la sécurité du SI (mieux protéger / mieux surveiller) Les traduire au sein d'un plan d'action

Blocs de compétences

RNCP40356BC01 — Optimiser (faire évoluer) les infrastructures informatiques

LISTE DE COMPÉTENCES

Définir et mettre en place un système de veille automatisée ou non afin de repérer les évolutions en lien avec son activité (Information Technology / technologies de l'information)

Analyser les informations collectées afin d'identifier les opportunités (ex : nouvelles technologies, nouveaux services cloud) et les éventuelles menaces (ex : cybermenaces, mise en conformité nécessaire) Le cas échéant, les partager avec ses pairs (communauté / réseau) ou bien des collaborateurs au sein d'une organisation

Analyser, le cas échéant préciser / affiner, et formaliser les besoins informatiques, afin d'identifier les objectifs (résultats attendus) et les éventuelles contraintes techniques, matérielles, budgétaires et réglementaires

Identifier une solution en termes d'infrastructure informatique, adaptée et conforme aux besoins / contraintes, à l'aide d'une recherche ponctuelle ciblée ou bien à partir de la veille, et la représenter visuellement, à l'aide d'un outil de modélisation adapté, afin d'en illustrer son implémentation, ses actions et ses éventuels impacts / risques

Estimer les coûts associés (humains et matériels) à la solution technique afin de déterminer le budget nécessaire à sa mise en production et à son exploitation

Présenter la solution technique, expliquer / argumenter ses choix techniques / financiers auprès des décideurs dans un objectif de validation

Organiser (définir / planifier / attribuer) les tâches nécessaires à la conception et à la mise en production de la solution dans le système d'information en cohérence avec les contraintes de l'organisation (notamment un minimum d'impact sur la continuité du service)

MODALITÉS D'ÉVALUATION

Projets (mises en situation professionnelle réelles ou reconstituées, cas pratiques) - Soutenances orales

RNCP40356BC02 — Concevoir et déployer les infrastructures informatiques

LISTE DE COMPÉTENCES

Définir / structurer / modéliser l'architecture technique de l'infrastructure cible, à l'aide d'un logiciel adapté, selon l'agencement des briques fonctionnelles (utilisateurs / données / traitements souhaités) et les critères fournis (performance, sécurité, évolutivité, etc), afin de définir l'organisation et les caractéristiques des équipements / composants et leurs interactions

Identifier les configurations à appliquer sur les équipements / composants de l'infrastructure cible, à partir des ressources adaptées (ex : documentation fournisseur) et selon le modèle d'architecture défini afin d'en disposer selon l'usage voulu

Créer un prototype ou bien une version pilote (une maquette test) de l'infrastructure système / réseau, à l'aide d'un outil de simulation adapté, afin de visualiser et de tester les équipements / composants, leurs interactions et les fonctionnalités associées

Valider ou non la mise en production selon les résultats

Identifier les règles de durcissement (suppression des services inutiles, forcer la robustesse des mots de passe, etc), à partir des guides externes (ANSSI, fournisseurs, etc), les adapter si besoin aux contraintes de l'organisation afin de sécuriser les infrastructures

Installer et effectuer les réglages (configurations / sécurisation) sur les équipements / composants réseaux / systèmes, quel que soit le type d'infrastructure et le mode de déploiement, dans le respect des règles de l'art et selon les caractéristiques techniques et fonctionnelles définies

Élaborer et mettre en œuvre une procédure de test afin de valider la conformité et la fonctionnalité de l'infrastructure déployée

Rédiger l'ensemble des procédures nécessaires à la mise en production / au déploiement de la solution

Former les utilisateurs ou bien communiquer les bonnes pratiques liées à l'utilisation d'un nouveau service afin d'accompagner le changement

MODALITÉS D'ÉVALUATION

Projets (mises en situation professionnelle réelles ou reconstituées, cas pratiques) - Soutenances orales

RNCP40356BC03 — Administrer (exploiter / maintenir) les infrastructures informatiques

LISTE DE COMPÉTENCES

Organiser / mettre à jour un annuaire des rôles / des autorisations associées à l'aide d'un outil adapté selon les droits définis, dans le respect de la politique de sécurité de l'organisation et de la réglementation en vigueur (sur les données) afin de centraliser la gestion des identités / accès

Concevoir, mettre en place et planifier des solutions d'automatisation (ex : scripts, applications) sur des tâches préalablement identifiées à l'aide d'outils adaptés afin de lancer et d'exécuter de manière automatisée les opérations

Mettre en place un système d'authentification au SI et à ses services afin de permettre un accès sécurisé, conforme et différencié au système d'information (et à ses services)

Mettre en place (installer / configurer / tester / sécuriser) un outil de gestion des actifs et des configurations automatisé, partagé selon les droits définis et accessible, afin de mettre à jour [bénéficier en temps réel des informations sur] les composants du système d'information, préalablement inventoriés, et leurs relations

Définir (choix des méthodes, outils, techniques), installer, configurer et tester une stratégie opérationnelle de

sauvegarde en cohérence avec les données (nature / type / criticité) et les contraintes de l'organisation afin d'enregistrer / de dupliquer / de répliquer et d'archiver les données dans un ou plusieurs lieux de stockage selon les critères définis au sein du plan de sauvegarde (classification des données, fréquence souhaitée, etc)

Automatiser les tâches (les opérations) de sauvegarde à l'aide des outils (de planification / d'exécution) et des langages de programmation adaptés (ex : PowerShell, Python, Bash)

Sécuriser, à l'aide des configurations adaptées au plan de sauvegarde et préconisées (ANSSI, fournisseurs, etc), les sauvegardes lors des enregistrements / duplications / répliquions / archivage, afin de réduire les risques d'altération ou de disparition des données

Documenter le système de sauvegarde et établir / formaliser une procédure de restauration des données afin de fournir la démarche à appliquer en cas d'incident

Prioriser et affecter les tickets selon le type / le niveau de support, à l'aide d'un outil de gestion (ex : outil de ticketing / d'assistance) adapté, afin d'organiser les interventions

Effectuer des interventions de support niveaux 2 et/ou 3 afin de rétablir le service fourni au niveau attendu Les enregistrer (demande, réponse apportée, le cas échéant, documentation fournie) afin d'assurer la traçabilité et de clôturer les tickets

MODALITÉS D'ÉVALUATION

Projets (mises en situation professionnelle réelles ou reconstituées, cas pratiques) - Soutenances orales

RNCP40356BC04 — Superviser et surveiller les infrastructures informatiques

LISTE DE COMPÉTENCES

Intégrer un outil de supervision, le paramétrer selon le niveau de service attendu (observation des indicateurs de performance / sécurité / disponibilité et seuils) et le tester afin de monitorer les infrastructures informatiques (enregistrer l'activité) et d'émettre une alerte en cas de dysfonctionnements (franchissement du seuil d'alerte)

Établir une procédure afin de présenter le système de supervision auprès de l'équipe en charge de la maintenance du système d'information et les actions à entreprendre en cas de dysfonctionnement / d'alerte (points de contrôles, indicateurs, actions à entreprendre en cas de dysfonctionnement)

Exploiter les remontées (logs / journaux) des activités enregistrées via l'outil de supervision afin d'analyser la performance et la disponibilité des infrastructures informatiques selon les différentes utilisations (spécifiques ou non) au regard des indicateurs définis (ex : taux de disponibilité, charges de calcul, temps de réponse, etc)

Structurer et outiller les différentes étapes d'une intervention portant sur l'évaluation de la sécurité informatique (collecte d'informations, inventaire des actifs, recherche de vulnérabilité, exploitation, élévation des privilèges, propagation, nettoyage) en cohérence avec un périmètre cible

Mettre en œuvre une évaluation de la sécurité informatique sur un périmètre cible, selon la méthodologie préalablement définie et à l'aide des outils adaptés (outils d'énumération / scanner, test d'intrusion, etc) afin d'identifier et de caractériser les vulnérabilités et les failles de sécurité selon leur niveau de criticité

Documenter les vulnérabilités et les failles de sécurité afin de les partager au commanditaire (client interne / externe) Le cas échéant, rédiger des supports à destination d'un public plus élargi (non technique) afin de rendre accessibles les conclusions de l'évaluation

Proposer des mesures ou bien des règles, en cohérence avec les vulnérabilités / failles observées, afin de renforcer la sécurité du SI (mieux protéger / mieux surveiller) Les traduire au sein d'un plan d'action

MODALITÉS D'ÉVALUATION

Projets (mises en situation professionnelle réelles ou reconstituées, cas pratiques) - Soutenances orales

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Tous secteurs d'activité.

TYPE D'EMPLOIS ACCESSIBLES

Administrateur informatique

Administrateur systèmes et réseaux

Administrateur sécurité informatique

Administrateur de serveurs

Administrateur infrastructures

Administrateur Linux / Windows

RÉGLEMENTATIONS D'ACTIVITÉ

La profession n'est pas réglementée. L'administrateur systèmes, réseaux et cybersécurité exerce toutefois ses activités dans le respect des bonnes pratiques de la profession (sécurité, confidentialité, qualité, numérique responsable...) ainsi que de la législation en vigueur (RGPD, Loi Informatique et Libertés, normes ISO 27000, directives de l'ANSSI...).

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

Être titulaire d'une certification professionnelle de niveau 5 (ou équivalent) en informatique et systèmes d'information ;
OU être titulaire du baccalauréat ou d'une certification de niveau 4 (ou équivalent) et justifier d'une expérience professionnelle d'au moins deux ans en informatique et systèmes d'information.

Tout autre profil relève d'une procédure dérogatoire.

PRÉREQUIS À LA VALIDATION

?Pour bénéficier de la certification professionnelle complète, le candidat doit valider les quatre blocs de compétences.

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

Le jury de délivrance de la certification est composé du responsable pédagogique de la filière et deux professionnels du métier visé extérieurs 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	8 255 €
Selon la branche	7 000 € – 9 112 €

Prise en charge	Branches concernées
8 255 €	Valeur par défaut · 186 branches
9 112 €	CPNE Casinos, CPNE Services de l'eau, CPNE Travail Temporaire, CPNE autoroutes, CPNE de l'ingénierie, des services informatiques et du conseil
7 923 €	CPNE FP Branche des magasins du Bricolage, CPNEFP Commerce succursaliste de la Chaussure, CPNEFP Commerce à distance, CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager
7 500 €	CPNE des industries de santé (CPNEIS), CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
8 591 €	CPNEF de l'Exploitation cinématographique et de la Distribution de films
8 400 €	CPNEFP de l'habillement, mercerie, chaussure et jouet
8 136 €	CPNE de la branche de la Distribution Directe
8 134 €	CPNE FP Commerce de Détail de l'Horlogerie Bijouterie
7 967 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
7 124 €	CPNEFP de la blanchisserie, laverie, location de linge, nettoyage à sec, pressing et teinturerie
7 000 €	CPNEFP de la métallurgie

Base légale

Date de décision	28/03/2025
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	28/03/2030
Date de dernière délivrance possible	27/03/2034

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2023	101	8	83 %	—
2022	127	0	89 %	76 %
2021	34	0	91 %	76 %

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP36370

CORRESPONDANCES (PAR BLOCS)
RNCP36370

Pour plus d'informations

LIEN VERS LE DESCRIPTIF
<https://openclassrooms.com/fr/paths/734-administrateur-systemes-reseaux-et-securite>

Fiche officielle (France Compétences)
<https://www.francecompetences.fr/recherche/rncp/40356/>

Où se former

Formations référencées	3
Organismes	2
Régions couvertes	1
Prix indicatif	6 600 € – 13 200 €
Durée	1200 h

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

Se former en apprentissage

Formations en apprentissage	1
Organismes gestionnaires (CFA)	1
Organismes formateurs	1
Régions couvertes	1
Départements couverts	1
Organismes certifiés Qualiopi	1
Formations à distance	1
Sessions	de 04/2025 à 10/2028

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	82
Parcours menés à terme	13
Taux d'achèvement	16 %
Période	05/2025 – 09/2026

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

Demande CPF — formations engagées

Dossiers CPF engagés	93
Montant total engagé	578 740 €
Coût moyen par dossier	6 223 €
Durée moyenne	981 h
Période	04/2025 – 09/2026
France compétences	44 %
France Travail	23 %
Reste à charge titulaire	15 %
Entreprise	9 %

OPCO	5 %
-------------	-----

Régions	4 %
----------------	-----

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