

Manager en infrastructures et cybersécurité des systèmes d'information

RNCP38779 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 326m, 326n
Formacode(s)	31009, 31045, 24231, 31094, 24293
Code(s) ROME	M1801, M1802, M1803, M1804, M1810
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	27/03/2024
Date d'échéance	27/03/2029

Certificateur(s)

CESI · SIRET : 77572257201109<http://www.cesi.fr>

Partenaires habilités

59 organismes habilités, d'après la liste publiée par France compétences : 59 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
CENTRE DE FORMATION-CFSA CAMPUS CENTRE	18360001400058	Former et organiser l'évaluation
C E SI	77572257200366	Former et organiser l'évaluation
C E SI	77572257200820	Former et organiser l'évaluation
C E SI	77572257200838	Former et organiser l'évaluation
C E SI	77572257200846	Former et organiser l'évaluation
C E SI	77572257200911	Former et organiser l'évaluation
C E SI	77572257200929	Former et organiser l'évaluation
C E SI	77572257200960	Former et organiser l'évaluation
C E SI	77572257200978	Former et organiser l'évaluation
C E SI	77572257201018	Former et organiser l'évaluation

Liste complète des 59 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp38779-manager-en-infrastructures-et-cybersecurite-des-systemes-d-information/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le Manager en infrastructures et cybersécurité des SI a pour fonction principale de concevoir et mettre en œuvre des architectures réseaux sécurisées dans le respect des normes et règlements en vigueur, de gérer des projets de migration ou de sécurisation des SI, d'évaluer, au travers de différentes méthodes et outils d'audit, les vulnérabilités et le niveau de résilience du SI, de manager une équipe et de conduire le changement au sein de son organisation

ACTIVITÉS VISÉES

Manager les équipes et la transformation du SI

Superviser le portefeuille projets de la DSI et sa mise en œuvre

Concevoir l'infrastructure du système d'information

Sécuriser les infrastructures du système d'information (accès, réseaux et données)

COMPÉTENCES ATTESTÉES

Gérer et encadrer son équipe (responsabilité hiérarchique) pour développer les compétences et optimiser l'organisation du système d'information en s'assurant que les tâches affectées soient accessibles et en cohérence avec les compétences des membres de l'équipe

Organiser et piloter une équipe (responsabilité fonctionnelle) pour optimiser la réalisation des projets IT en utilisant des outils collaboratifs et en adaptant son style de management

Manager les relations clients/fournisseurs pour optimiser la mise en œuvre des projets IT en utilisant les moyens de communications et les outils collaboratifs adaptés et accessibles

Analyser l'environnement technique et métier utilisant le système d'information pour en identifier les processus, les workflows et les technologies existantes en exploitant les données disponibles (documentations techniques, rapports d'activités, audits, interviews, etc.)

Modéliser le SI en synthétisant les données utiles pour le rendre compréhensible par les décideurs

Identifier les améliorations possibles du SI pour optimiser les flux métiers en répondant aux enjeux stratégiques de l'entreprise

Identifier une méthode de gestion du changement pour garantir l'adhésion des parties prenantes en s'appuyant sur les leviers de motivation et d'engagement identifiés

Définir et conduire le plan d'accompagnement en identifiant les acteurs et les actions à mener (formation, communication, régulation, mesure, etc.) pour s'assurer de l'appropriation par tous de la transformation induite par la stratégie de la DSI

Élaborer le référentiel documentaire des projets IT afin de garantir son appropriation par les acteurs des projets et d'harmoniser la formalisation et la gestion des projets (réception de la demande, analyse de faisabilité, etc.) en se basant sur les pratiques de l'entreprise et les référentiels existants (méthodologies de type cycle en V, méthodologies agiles, etc.)

Définir des critères de choix pertinents pour gérer les priorités du portefeuille projets du SI et ordonnancer l'ensemble des projets proposés en tenant compte des règles applicables (législatives, normatives, culturelles, éthiques, etc.)

Exposer et défendre les choix effectués pour permettre une lecture claire et cohérente auprès des hiérarchiques et des fonctionnels lors de la sélection des projets informatiques grâce à une présentation des cotations réalisées

S'approprier le contexte et le périmètre de chaque projet IT en identifiant ses objectifs, ses enjeux et ses contraintes spécifiés afin d'apporter une réponse au besoin exprimé par la maîtrise d'ouvrage

Établir le plan de management (gestion des risques, planification, organisation, budget, indicateurs, parties prenantes, plan de communication, etc.) de chaque projet IT à conduire afin de pouvoir en suivre l'avancée en s'appuyant sur les outils de management de projet

Contrôler et valider les différents livrables des projets IT pour respecter le triangle d'or (qualité, coût, délai) attendu en mettant à jour les tableaux de bord de suivi du projet

Organiser les recettes (fonctionnelle et technique) de chaque projet IT pour livrer un produit conforme aux exigences du client en établissant les cahiers de recette

Établir les documents administratifs, contractuels et techniques des projets IT (solde des contrats, procès-verbaux de recette, documentations techniques, etc.) pour formaliser la clôture du projet dans le respect des règlements en vigueur (RGPD, droit commercial, etc.) et aux exigences fonctionnelles et techniques

Organiser et animer la capitalisation de l'expérience à l'issue des projets IT au sein des équipes projet (réunions, documentation, etc.) en analysant les indicateurs de performance du projet (État d'avancement, économie réalisée, avancée technique, etc.) dans un objectif d'amélioration continue

Auditer l'infrastructure du SI pour identifier les limites et points faibles en vérifiant la conformité par rapport aux standards technologiques, organisationnels et de cybersécurité (Préconisation ANSSI et principaux éditeurs)

Étudier et comparer les différentes solutions technologiques afin de réaliser les choix adaptés aux besoins métiers de l'entreprise

Concevoir une infrastructure informatique sécurisée (réseaux, cloud, ERP, data, sauvegarde, etc.) en s'appuyant sur les besoins clients, les standards d'architecture des SI et les bonnes pratiques en terme de cybersécurité

Identifier les projets qui composeront le portefeuille projet d'évolution et de migration de l'architecture du SI

Organiser et animer un système de veille active sur les technologies des SI et les menaces en cybersécurité en s'informant auprès des éditeurs, prestataires et organismes de référence de type ANSSI

Analyser les solutions implantées pour identifier les besoins de mises à jour ou d'évolutions du SI en définissant des indicateurs d'activité ou de détection de problèmes de sécurité

Conseiller la direction sur les projets et investissements à conduire pour aider à la prise de décision et à la gouvernance du SI en présentant des indicateurs formalisés sous forme de tableaux de bord par exemple

Auditer l'infrastructure du SI afin d'identifier les éléments nécessitant une sécurisation ainsi que le niveau de sécurité nécessaire (accès, données, etc.) en utilisant des outils de pentesting associés à une méthodologie d'audit

Identifier les droits, les obligations et normes applicables en matière de sécurisation du SI afin de garantir sa conformité réglementaire et normative en s'appuyant sur les standards et normes relatives à la cybersécurité (RGPD, ISO27001, CNIL, etc.)

Concevoir le plan de sécurisation et de supervision du SI pour répondre au niveau de sécurisation attendu en s'appuyant sur les résultats de l'audit et dans le respect des obligations réglementaires et normatives (RGPD, CNIL, etc.) ainsi que sur les bonnes pratiques de sécurisation des SI

Identifier les opérations et les parties prenantes pour organiser et planifier les projets de sécurisation du SI en s'appuyant sur une méthodologie de gestion de projet de type AGILE

Suivre et superviser la mise en œuvre des solutions de sécurisation pour mesurer leur efficacité et garantir le niveau de sécurisation requis en définissant des indicateurs de suivis appropriés et des outils de surveillance de type SIEM

Organiser et animer un système de veille active pour se tenir à jour sur les menaces en cybersécurité et solutions de sécurisation en s'informant auprès des éditeurs, prestataires et organismes de référence (ANSSI, CERT, etc.)

Analyser les indicateurs d'activité pour identifier les besoins de mises à jour, évolutions ou failles de sécurité en s'appuyant sur les informations de veille

Conseiller la direction sur les projets et investissements à conduire en terme de cybersécurité et aider à la mise en œuvre d'une gouvernance de la sécurité SI en présentant des indicateurs formalisés sous forme de tableaux de bord par exemple

Anticiper la crise cyber pour réagir rapidement et gérer ses impacts en mettant en place une évaluation des risques, un plan de continuité d'activité, un plan de communication et une identification des rôles et responsabilités

Détecter et identifier l'attaque pour adapter la réponse en analysant les données de surveillance et les incidents de sécurité

Gérer l'incident et répondre à la crise pour stopper sa progression et rétablir un système d'information sain en rendant le plan de communication accessible à tous les acteurs internes et externes ainsi qu'en activant les solutions de restauration

Evaluer les dommages pour améliorer la résilience du SI en analysant l'attaque, les pertes subies et en mettant à jour les solutions techniques et le plan de crise cyber

Blocs de compétences

RNCP38779BC01 — Manager les équipes et la transformation du SI

LISTE DE COMPÉTENCES

Gérer et encadrer son équipe (responsabilité hiérarchique) pour développer les compétences et optimiser l'organisation du système d'information en s'assurant que les tâches affectées soient accessibles et en cohérence avec les compétences des membres de l'équipe

Organiser et piloter une équipe (responsabilité fonctionnelle) pour optimiser la réalisation des projets IT en utilisant des outils collaboratifs et en adaptant son style de management

Manager les relations clients/fournisseurs pour optimiser la mise en œuvre des projets IT en utilisant les moyens de communications et les outils collaboratifs adaptés et accessibles

Analyser l'environnement technique et métier utilisant le système d'information pour en identifier les processus, les workflows et les technologies existantes en exploitant les données disponibles (documentations techniques, rapports d'activités, audits, interviews, etc.)

Modéliser le SI en synthétisant les données utiles pour le rendre compréhensible par les décideurs

Identifier les améliorations possibles du SI pour optimiser les flux métiers en répondant aux enjeux stratégiques de l'entreprise

Identifier une méthode de gestion du changement pour garantir l'adhésion des parties prenantes en s'appuyant sur les leviers de motivation et d'engagement identifiés

Définir et conduire le plan d'accompagnement en identifiant les acteurs et les actions à mener (formation, communication, régulation, mesure, etc.) pour s'assurer de l'appropriation par tous de la transformation induite par la stratégie de la DSI

MODALITÉS D'ÉVALUATION

Application professionnelle (réelle ou simulée) de management de la transformation du SI donnant lieu à une soutenance orale

RNCP38779BC02 — Superviser le portefeuille projets de la DSI et sa mise en œuvre

LISTE DE COMPÉTENCES

Élaborer le référentiel documentaire des projets IT afin de garantir son appropriation par les acteurs des projets et d'harmoniser la formalisation et la gestion des projets (réception de la demande, analyse de faisabilité, etc.) en se basant sur les pratiques de l'entreprise et les référentiels existants (méthodologies de type cycle en V, méthodologies agiles, etc.)

Définir des critères de choix pertinents pour gérer les priorités du portefeuille projets du SI et ordonnancer l'ensemble des projets proposés en tenant compte des règles applicables (législatives, normatives, culturelles, éthiques, etc.)

Exposer et défendre les choix effectués pour permettre une lecture claire et cohérente auprès des hiérarchiques et des fonctionnels lors de la sélection des projets informatiques grâce à une présentation des cotations réalisées

S'approprier le contexte et le périmètre de chaque projet IT en identifiant ses objectifs, ses enjeux et ses contraintes spécifiés afin d'apporter une réponse au besoin exprimé par la maîtrise d'ouvrage

Établir le plan de management (gestion des risques, planification, organisation, budget, indicateurs, parties prenantes, plan de communication, etc.) de chaque projet IT à conduire afin de pouvoir en suivre l'avancée en s'appuyant sur les outils de management de projet

Contrôler et valider les différents livrables des projets IT pour respecter le triangle d'or (qualité, coût, délai) attendu en mettant à jour les tableaux de bord de suivi du projet

Organiser les recettes (fonctionnelle et technique) de chaque projet IT pour livrer un produit conforme aux exigences du client en établissant les cahiers de recette

Établir les documents administratifs, contractuels et techniques des projets IT (solde des contrats, procès-verbaux de recette, documentations techniques, etc.) pour formaliser la clôture du projet dans le respect des règlements en vigueur (RGPD, droit commercial, etc.) et aux exigences fonctionnelles et techniques

Organiser et animer la capitalisation de l'expérience à l'issue des projets IT au sein des équipes projet (réunions, documentation, etc.) en analysant les indicateurs de performance du projet (État d'avancement, économie réalisée, avancée technique, etc.) dans un objectif d'amélioration continue

MODALITÉS D'ÉVALUATION

Application professionnelle (réelle ou simulée) sur la supervision d'un portefeuille projets donnant lieu à la production d'un document écrit

RNCP38779BC03 — Concevoir l'infrastructure du système d'Information

LISTE DE COMPÉTENCES

Auditer l'infrastructure du SI pour identifier les limites et points faibles en vérifiant la conformité par rapport aux standards technologiques, organisationnels et de cybersécurité (Préconisation ANSSI et principaux éditeurs)

Étudier et comparer les différentes solutions technologiques afin de réaliser les choix adaptés aux besoins métiers de l'entreprise

Concevoir une infrastructure informatique sécurisée (réseaux, cloud, ERP, data, sauvegarde, etc.) en s'appuyant sur les besoins clients, les standards d'architecture des SI et les bonnes pratiques en terme de cybersécurité

Identifier les projets qui composeront le portefeuille projet d'évolution et de migration de l'architecture du SI

Organiser et animer un système de veille active sur les technologies des SI et les menaces en cybersécurité en s'informant auprès des éditeurs, prestataires et organismes de référence de type ANSSI

Analyser les solutions implantées pour identifier les besoins de mises à jour ou d'évolutions du SI en définissant des indicateurs d'activité ou de détection de problèmes de sécurité

Conseiller la direction sur les projets et investissements à conduire pour aider à la prise de décision et à la gouvernance du SI en présentant des indicateurs formalisés sous forme de tableaux de bord par exemple

MODALITÉS D'ÉVALUATION

Application professionnelle (réelle ou simulée) sur la conception d'une infrastructure informatique sécurisée donnant lieu à une soutenance orale

RNCP38779BC04 — Sécuriser les infrastructures du système d'Information (accès, réseaux et données)

LISTE DE COMPÉTENCES

Auditer l'infrastructure du SI afin d'identifier les éléments nécessitant une sécurisation ainsi que le niveau de sécurité nécessaire (accès, données, etc.) en utilisant des outils de pentesting

associés à une méthodologie d'audit

Identifier les droits, les obligations et normes applicables en matière de sécurisation du SI afin de garantir sa conformité réglementaire et normative en s'appuyant sur les standards et normes relatives à la cybersécurité (RGPD, ISO27001, CNIL, etc.)

Concevoir le plan de sécurisation et de supervision du SI pour répondre au niveau de sécurisation attendu en s'appuyant sur les résultats de l'audit et dans le respect des obligations réglementaires et normatives (RGPD, CNIL, etc.) ainsi que sur les bonnes pratiques de sécurisation des SI

Identifier les opérations et les parties prenantes pour organiser et planifier les projets de sécurisation du SI en s'appuyant sur une méthodologie de gestion de projet de type AGILE

Suivre et superviser la mise en œuvre des solutions de sécurisation pour mesurer leur efficacité et garantir le niveau de sécurisation requis en définissant des indicateurs de suivis appropriés et des outils de surveillance de type SIEM

Organiser et animer un système de veille active pour se tenir à jour sur les menaces en cybersécurité et solutions de sécurisation en s'informant auprès des éditeurs, prestataires et organismes de référence (ANSSI, CERT, etc.)

Analyser les indicateurs d'activité pour identifier les besoins de mises à jour, évolutions ou failles de sécurité en s'appuyant sur les informations de veille

Conseiller la direction sur les projets et investissements à conduire en terme de cybersécurité et aider à la mise en œuvre d'une gouvernance de la sécurité SI en présentant des indicateurs formalisés sous forme de tableaux de bord par exemple

Anticiper la crise cyber pour réagir rapidement et gérer ses impacts en mettant en place une évaluation des risques, un plan de continuité d'activité, un plan de communication et une identification des rôles et responsabilités

Détecter et identifier l'attaque pour adapter la réponse en analysant les données de surveillance et les incidents de sécurité

Gérer l'incident et répondre à la crise pour stopper sa progression et rétablir un système d'information sain en rendant le plan de communication accessible à tous les acteurs internes et externes ainsi qu'en activant les solutions de restauration

Evaluer les dommages pour améliorer la résilience du SI en analysant l'attaque, les pertes subies et en mettant à jour les solutions techniques et le plan de crise cyber

MODALITÉS D'ÉVALUATION

Application professionnelle (réelle ou simulée) sur la sécurisation d'une infrastructure informatique donnant lieu à la production d'un document écrit

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le Manager en infrastructures et cybersécurité des systèmes d'information exerce sa fonction, pour tous les secteurs d'activité, au sein d'organisations dotées d'un système d'information. Ce métier répond particulièrement aux besoins des ESN

dont la particularité est d'intervenir en sous-traitance pour des clients d'activités et de structures variées.

TYPE D'EMPLOIS ACCESSIBLES

Ingénieur système et réseaux et/ou cybersécurité

Chef de projet infrastructures / systèmes d'information / cybersécurité

Consultant en système d'information ou cybersécurité

Responsable des systèmes d'information

Responsable de la sécurité du système d'information

Ingénieur Infrastructures

Architecte en systèmes d'information ou en cybersécurité

Expert technique (cybersécurité ou Infrastructures informatiques)
Manager du système d'information
Directeur des systèmes d'information
Responsable informatique

RÈGLEMENTATIONS D'ACTIVITÉ

Le Manager en infrastructures et cybersécurité des SI exerce dans un cadre réglementaire très précis. En fonction de l'environnement dans lequel il évolue, il ne peut se soustraire :

Aux règlements :

Règlement (UE) « eIDAS » n°910/2014 du 23 juillet 2014 relatif aux transactions électroniques au sein du marché intérieur permettant d'établir un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques

Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité)

Aux directives :

Directive (UE) 2016/1148 du Parlement Européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (Texte présentant de l'intérêt pour l'EEE)

Aux lois :

Loi de programmation militaire (loi n° 2013-1168 du 18 décembre 2013) - article 22 - qui impose aux opérateurs d'importance vitale le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent : les systèmes d'information d'importance vitale (SIIV)

Loi n°2018-607 relative à la programmation militaire pour les années 2019 - 2025 promulguée par la Président de la République le 13 juillet 2018. Elle comporte des dispositions relatives au renforcement des capacités de détection des attaques informatiques, aujourd'hui indispensables pour élever le niveau de sécurité de la Nation

Aux décrets :

Décret n°2015-351 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale

Décret n°2015-350 relatif à la qualification des produits de sécurité et des prestataires de services de confiance pour les besoins de la sécurité nationale

Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique

Aux instructions :

Instruction générale interministérielle n°2100 du 1er décembre 1975 pour l'application en France du système de sécurité de l'Organisation du traité de l'Atlantique nord

Instruction interministérielle n°920 du 12 janvier 2005 relative aux systèmes traitant des informations classifiées de défense de niveau confidentiel-défense

Instruction générale interministérielle n°2102 du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union Européenne

Instruction interministérielle n° 910 du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI).

Instruction interministérielle n° 300 du 23 juin 2014 relative à la protection contre les signaux compromettants

Instruction interministérielle n° 901 du 28 janvier 2015 relative à la protection des systèmes d'information sensibles, notamment ceux traitant des informations portant la mention Diffusion Restreinte

Instruction générale interministérielle n°1300 du 9 août 2021 sur la protection du secret de la défense nationale

Au référentiel :

Référentiel général de sécurité pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives

A la circulaire :

Circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 relative à la politique de sécurité des systèmes d'information (PSSIE)

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible, Lien formation-emploi
Salaire médian (mensuel)	2 962 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (41 % des actifs en emploi)
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique · tension 4/5 (Élevée) M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom · tension 5/5 (Très élevée) M2X91 — Chefs de projet et directeurs de service informatique · tension 4/5 (Élevée) M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	34 624
Jugés difficiles à recruter	52 %
Emplois saisonniers	1 %
Familles professionnelles (FAP)	M1X81 — Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique M2X90 — Ingénieurs et cadres d'étude, recherche et développement en informatique et télécom M2X91 — Chefs de projet et directeurs de service informatique M2X92 — Responsables et cadres de la production, de l'exploitation et de la maintenance informatique et télécom M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Le candidat doit être titulaire :

ou d'un niveau 5 en informatique pour le cycle de préparation en 36 mois ;

ou d'un niveau 6 en informatique pour le cycle de préparation en 24 mois ;

ou d'un niveau 6 en informatique avec 3 ans d'expérience professionnelle en informatique pour le cycle de préparation en 12 mois.

Tout autre profil relève du dérogatoire.

La sélection des candidats comprend un dossier de candidature avec CV et lettre de motivation - des tests de positionnement - un entretien individuel de sélection.

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

Le jury national unique est composé de 4 membres professionnels externes dont 50% en activité dans le métier ou qui supervisent des personnes l'exerçant

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	7 611 €
Selon la branche	6 500 € – 7 614 €
Prise en charge	Branches concernées
7 611 €	Valeur par défaut · 208 branches
6 500 €	CPNEF inter-secteurs papier carton, CPNEFP Carrières et matériaux
7 614 €	CPNEFP de la Mutualité Sociale Agricole
7 536 €	CPNE Banque
7 500 €	CPNE des industries de santé (CPNEIS)

Base légale

Date de décision	27/03/2024
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	27/03/2029
Date de dernière délivrance possible	27/03/2033

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2022	416	6	98 %	—
2021	178	2	93 %	99 %
2020	169	1	93 %	96 %

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP35588

CORRESPONDANCES (PAR BLOCS)

RNCP34471, RNCP34553, RNCP34561, RNCP35435, RNCP35584, RNCP35588, RNCP35612, RNCP35620, RNCP36297, RNCP36469, RNCP36909, RNCP37259, RNCP37744, RNCP38105, RNCP38293, RNCP38457, RNCP38599, RNCP40168, RNCP40239, RNCP41450, RNCP41880

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.cesi.fr/formation/mastere-professionnel-manager-en-infrastructures-et-cybersecurite-des-si-en-alternance-2371644/>

<https://www.cesi.fr/formation/manager-en-infrastructures-et-cybersecurite-des-si-2336504/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/38779/>

Où se former

Formations référencées	61
------------------------	----

Organismes	24
Régions couvertes	12
Prix indicatif	3 360 € – 18 060 €
Durée	16 – 301 h

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

Se former en apprentissage

Formations en apprentissage	25
Organismes gestionnaires (CFA)	14
Organismes formateurs	22
Régions couvertes	12
Départements couverts	22
Organismes certifiés Qualiopi	22
Sessions	de 10/2024 à 10/2029

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	34
Parcours menés à terme	13
Taux d'achèvement	38 %
Période	05/2024 – 09/2026

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

Demande CPF — formations engagées

Dossiers CPF engagés	46
Montant total engagé	221 063 €
Coût moyen par dossier	4 806 €
Durée moyenne	80 h
Période	04/2024 – 09/2026
France compétences	69 %
Entreprise	12 %
Reste à charge titulaire	8 %
OPCO	6 %
France Travail	5 %

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