

Administrateur systèmes, réseaux et bases de données

RNCP41996 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326
Formacode(s)	31034
Code(s) ROME	M1801
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	27/02/2026
Date d'échéance	27/02/2031

Certificateur(s)

INSTITUT DE GESTION SOCIALE (IGS) · SIRET : 31249509600157

Partenaires habilités

39 organismes habilités, d'après la liste publiée par France compétences : 39 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	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 (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
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600306	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600314	Former et organiser l'évaluation

Liste complète des 39 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp41996-administrateur-systemes-reseaux-et-bases-de-donnees/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

Avec le développement des communications et de l'informatique, l'administrateur systèmes et réseaux et bases de données a acquis un rôle majeur au sein de l'entreprise. Il est le garant du bon fonctionnement du système d'information. Son périmètre d'intervention peut s'étendre sur tout ou partie du S.I. de l'entreprise. Il recense les besoins puis prescrit des solutions logicielles ou d'infrastructure. Il conseille la direction. Il supervise et pilote les projets qui lui sont confiés. Il assure la mise en œuvre des mesures d'accompagnement du changement en matière d'organisation du travail et de la formation des utilisateurs. Il assure le plus souvent l'encadrement hiérarchique d'une équipe. Son métier évolue avec la montée en puissance du cloud, de la cybersécurité et de l'automatisation des processus IT et de l'Intelligence artificielle. Il doit s'adapter aux innovations technologiques et intégrer les enjeux de durabilité en assurant le recyclage et la gestion responsable des équipements numériques, en cohérence avec la politique RSE des entreprises.

ACTIVITÉS VISÉES

Administrer le système d'information :

- Mise en œuvre d'une architecture réseaux.
- Administration de l'infrastructure informatique en mode hybride.
- Administration des solutions de gouvernance et de gestion des données structurées ou non de l'entreprise et des volumes massifs de données (Big Data).
- Automatisation des processus informatiques.

Gérer le système d'information :

- Recensement et propositions de solutions tant techniques qu'organisationnelles susceptibles de faire évoluer le Système d'Information en lien avec les besoins métiers.
- Conception d'un plan d'évolution des équipements informatique.
- Supervision et contrôle de la performance du Système d'information.
- Gestion de l'urbanisation du Système d'Information guidée par les principes de l'agilité.
- Gestion de l'assistance utilisateurs.
- Conception d'un service numérique responsable.

Définir la politique de sécurisation du système d'information :

- Définition de la politique de sécurité informatique de l'entreprise.
- Identification et applications des mesures correctives aux failles de sécurité de l'infrastructure informatique.
- Prévention, détection et traitement des risques informatiques liés à : l'accès aux locaux et aux machines, l'accès aux données de l'entreprise, l'accès des et aux terminaux mobiles, l'activité des utilisateurs.
- Élaboration d'un plan de continuité d'activité en cas de crise.
- Élaboration d'un plan de reprise d'activité après sinistre.

Communiquer avec tous les acteurs internes ou externes au service informatique :

- Communication avec les acteurs internes au Service Informatique.
- Encadrement et animation d'une équipe de techniciens.
- Communication avec les acteurs externes au Service Informatique.
- Sensibilisation de l'ensemble des collaborateurs et des dirigeants à la protection des données informatique et à la prévention des risques liés aux cyberattaques.
- Gestion des négociations auprès des fournisseurs.

COMPÉTENCES ATTESTÉES

Configurer les équipements réseaux (routeurs, commutateurs, ...) des sites de l'entreprise selon les recommandations du responsable du systèmes d'information, ou des constructeurs, pour garantir la fluidité, la sécurité et la continuité des échanges de données en veillant à l'efficacité énergétique des équipements.

Installer et configurer des serveurs physiques ou virtuels (Cloud) et leurs systèmes d'exploitation afin de garantir la disponibilité, la stabilité, la performance des services numériques de l'entreprise (ERP) en respectant les besoins métiers exprimés et les politiques de sécurité, tout en optimisant la consommation énergétique (Green IT).

Concevoir et optimiser l'infrastructure de plateformes virtuelles en mutualisant les ressources (stockage, CPU, RAM, ...) des machines physiques dans un environnement centralisé (hyperviseurs), afin d'améliorer la flexibilité du système d'information et simplifier sa gestion.

Mettre en place une gestion unique et commune des terminaux mobiles (MDM) afin d'assurer une administration centralisée, cohérente et sécurisée de l'ensemble de l'infrastructure informatique.

Maintenir en conditions opérationnelles l'infrastructure de l'entreprise en utilisant des logiciels de gestion de haute disponibilité (clustering, load balancing, réplication, mises à jour), pour réduire les interruptions de services en appliquant les règles de santé et sécurité au travail lors des interventions.

Diagnostiquer les défaillances système ou réseau en analysant les logs, les symptômes et les dépendances entre services, afin d'assurer l'exploitation du Système d'Information, réduire les interruptions de service et limiter l'impact sur les utilisateurs.

Administrer les bases de données avec méthode en respectant les configurations requises (instances, paramètres système, schémas, droits d'accès, stockages, ...) et en appliquant les bonnes pratiques d'exploitation, afin d'assurer la disponibilité, l'intégrité et la performance des données en privilégiant les solutions économes en énergie.

Analyser les performances des bases de données installées sur la base des rapports d'usage collectés, afin d'accélérer les temps de traitement des requêtes.

Améliorer les performances des bases de données en optimisant l'emplacement des fichiers de stockage (données, journaux, index) sur les supports les plus adaptés pour garantir la réactivité des applications.

Automatiser les tâches d'exploitation courante (sauvegarde, mises à jour, déploiement) afin de fiabiliser les processus et gagner en productivité, en développant des scripts (Bash, PowerShell...) ou en utilisant des outils d'orchestration (Ansible, Python, IA, etc.), pour éviter les erreurs humaines et optimiser le temps d'administration.

Analyser les besoins techniques et métiers en identifiant les contraintes et opportunités, pour garantir la cohérence entre les choix techniques et les objectifs métiers, en intégrant les aspects d'accessibilité numérique pour tous les profils utilisateurs.

Gérer les évolutions des infrastructures Informatiques en appliquant les principes et les limites par la norme IT Service Management ISO/CEI 20000 pour garantir une évolution conforme aux standards de gestion des services informatiques et assurer leur alignement avec les besoins métiers et les exigences de qualité de service, dans le respect des standards environnementaux et de sobriété numérique.

Assurer l'évolution des équipements en tenant compte des technologies émergentes en anticipant les besoins futurs, pour garantir la pérennité des infrastructures, optimiser les investissements et accompagner les évolutions stratégiques de l'organisation.

Élaborer des propositions de renouvellement d'infrastructures, en analysant leurs performances et leur compatibilité, tout en tenant compte des contraintes budgétaires, en privilégiant des solutions à faible consommation énergétique, afin d'effectuer des choix d'investissement éclairés, durables et cohérents avec la stratégie de l'entreprise.

Élaborer un plan d'évolution des équipements informatique en identifiant les ressources, les étapes et les risques, pour garantir le bon déroulement du plan dans le respect des délais et des budgets afin de piloter la mise en œuvre des évolutions du Système d'Information.

Maquetter les solutions de déploiements dans un environnement de test (virtualisation, conteneurisation, sandbox, ...) pour détecter les incompatibilités et valider les choix techniques retenus avant leur mise en production, en s'assurant de l'accessibilité des interfaces testées pour les publics en situation de handicap.

Ordonnancer le plan de déploiement afin de coordonner efficacement les étapes d'installation ou de mise en production en tenant compte des disponibilités des différents acteurs concernés (équipes techniques, métiers, prestataires).

Attribuer les ressources informatiques nécessaires au bon déroulement du plan en tenant compte du budget alloué, des priorités opérationnelles, de la consommation énergétique et de la disponibilité des moyens (humains, matériels, logiciels), afin d'assurer la faisabilité technique et organisationnelle.

Suivre l'avancement des tâches et assurer la coordination avec les parties prenantes afin de maintenir la dynamique du projet, pour faciliter la réussite et la communication interservices.

Configurer les outils de supervision selon les indicateurs clés (taux de disponibilité, statuts du service, taux de perte de paquets, consommation énergétique, ...) en paramétrant des alertes adaptées, afin d'anticiper les dysfonctionnements.

Superviser l'infrastructure informatique et le patrimoine applicatif en utilisant les outils de supervision installés (supervision réseau, analyse de logs, alertes automatisées) afin d'améliorer les performances globales du système d'information.

Cartographier les composants du Système d'information (processus métiers, applications, fonctions, données, infrastructures...) pour faciliter la compréhension globale du SI, appuyer les prises de décision techniques et garantir la cohérence des évolutions à venir.

Organiser l'infrastructure en modélisant l'environnement technique (conteneurs, environnements de test, gestion des dépendances) pour accélérer les cycles de mise à jour, garantir la stabilité des services et soutenir l'agilité des équipes de développement et d'exploitation.

Accompagner les évolutions des applications métiers en adoptant une logique modulaire ou de composants (micro-services, APIs, ...) dans l'objectif de limiter les failles de sécurité, d'assurer la traçabilité des changements et de maintenir la continuité des services métiers, tout en veillant à la compatibilité avec les normes d'accessibilité numérique (RGAA).

Migrer une architecture système ou réseau dans le respect des principes d'urbanisation du SI en planifiant les interventions, en optimisant les opérations techniques et en identifiant les risques associés pour les anticiper afin de garantir la continuité de service, de limiter les interruptions et de sécuriser l'évolution du système d'information.

Maintenir un inventaire à jour des équipements et logiciels en intégrant les contraintes de maintenance, de licence, de durabilité, de recyclabilité et de sécurité pour optimiser les coûts et la performance du SI en cohérence avec la stratégie d'entreprise.

Centraliser le traitement des incidents en un point unique d'accès (ITSM, helpdesk) permettant de qualifier, affecter et historiser les incidents, pour mieux prioriser les interventions, optimiser la productivité des équipes support et améliorer la qualité du service rendu aux utilisateurs y compris ceux en situation de handicap.

Résoudre les tickets de niveau 3 & 4 à l'aide d'outils de prise en main à distance ou en intervenant sur place, pour limiter l'impact des incidents complexes sur l'activité de l'organisation et améliorer la satisfaction des utilisateurs.

Elaborer un tableau de bord sur la résolution des tickets d'incidents par niveau de support par la collecte et l'analyse des indicateurs clés (temps de réponse, taux de résolution, escalades, ...) afin d'identifier les points de blocage, d'améliorer l'efficacité de la résolution des incidents et de piloter la qualité du support utilisateur.

Concevoir un service numérique responsable en intégrant dès la phase de conception des principes d'écoconception (optimisation des ressources, sobriété énergétique, choix d'infrastructures durables) et en tenant compte des usages et contraintes du contexte professionnel, pour associer efficacement transition écologique et transition numérique, tout en répondant aux exigences fonctionnelles de l'organisation.

Gérer le parc informatique en identifiant les métriques (consommation énergétique, taux d'usage, recyclabilité, accessibilité numérique) adaptées aux activités de l'organisation, pour favoriser une gestion responsable du système d'information et orienter les choix techniques vers des pratiques durables et inclusives (RSE).

Rédiger ou mettre à jour la Politique de Sécurisation du Système d'Information (PSSI) en intégrant les recommandations internes (RSSI) et réglementaires (RGPD, ANSSI, ISO 27001 ...) pour formaliser les règles de sécurité, cadrer les pratiques et garantir un socle de protection cohérent.

Identifier les menaces et vulnérabilités du système d'information en réalisant une analyse de risques structurée (EBIOS, ISO 27005...) pour limiter l'exposition aux cyberattaques et renforcer la résilience du SI.

Déployer des solutions automatisées de mise à jour et de correctifs en configurant des outils de gestion centralisée des correctifs (WSUS, Ansible, scripts de déploiement, solutions EDR, IA) et en planifiant leur diffusion de manière contrôlée, pour limiter les surfaces d'attaque, assurer la conformité aux politiques de sécurité.

Évaluer les perturbations de services en exploitant les alertes émises par les sondes de supervision (réseau, système, base de données), en croisant les données collectées (logs, métriques, seuils) et en analysant l'impact sur la qualité de service pour identifier les correctifs à déployer rapidement.

Appliquer les procédures de sécurité liées aux accès physiques de l'entreprise en s'appuyant sur une stratégie d'identification (badges, registres d'accès, vidéosurveillance, droits d'entrée différenciés) afin de limiter les intrusions non autorisées dans les zones sensibles, en respectant les règles d'accessibilité aux bâtiments pour tous les utilisateurs (PMR, ...).

Configurer les dispositifs de sécurité (pare-feu, VPN, MFA, antivirus, etc.) pour garantir l'intégrité, la confidentialité et la disponibilité des données de l'entreprise et protéger les infrastructures contre les intrusions ou les fuites de données.

Gérer les comptes utilisateurs et les groupes dans un service d'annuaire en appliquant les politiques internes (mot de passe, rotation, GPO, ...) et en respectant les habilitations définies pour chaque utilisateur afin de permettre et tracer l'accès aux données de l'entreprise, tout en s'assurant que les procédures d'authentification restent accessibles.

Mettre en place une journalisation et un suivi d'activité en exploitant les outils de supervision de sécurité (SIEM, log, ...), pour assurer une réactivité en cas de comportements suspects ou d'incident et de conserver une traçabilité complète.

Identifier les éléments et applications critiques de l'entreprise en vue d'assurer la continuité opérationnelle en prévoyant un site de repli ou une infrastructure de secours adaptée pour maintenir les services essentiels en cas de sinistre, en prenant en compte les besoins spécifiques des utilisateurs en situation de handicap.

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, en privilégiant des solutions à faible consommation énergétique et éco-conçues.

Identifier la criticité de l'interruption d'activité en fonction des métiers de l'entreprise en analysant l'impact d'éventuels dysfonctionnements pour préconiser des mesures de redondance et garantir une bonne reprise d'activités.

Prioriser les besoins de continuité en évaluant les impacts potentiels d'interruption et en classant la reprise selon la criticité de l'activité, en intégrant les contraintes de santé au travail des équipes mobilisées lors des reprises (horaires, stress, charge).

Crypter les canaux de transmissions des sauvegardes émises via le réseau pour éviter une perte de données.

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

Collecter des informations auprès de spécialistes techniques en analysant et synthétisant les problèmes décrits afin d'envisager des solutions, en veillant à inclure les besoins spécifiques des utilisateurs en situation de handicap.

Alimenter la base de connaissances interne en documentant les incidents et les solutions apportées afin de faciliter la résolution des incidents similaires avec des contenus clairs, structurés et accessibles à tous les profils d'utilisateurs.

Concevoir la documentation technique, en français et en anglais, pour répondre aux besoins d'information des techniciens et faciliter l'usage des logiciels de support déployés dans l'entreprise.

Identifier les compétences techniques et relationnelles attendues et le degré intégrabilité des futurs collaborateurs au sein de l'équipe en analysant les besoins opérationnels du service afin d'élaborer une fiche de poste précise en vue de conduire un entretien d'embauche, en intégrant des critères favorisant l'inclusion.

Conduire un entretien annuel en contrôlant l'atteinte des objectifs fixés et des besoins du collaborateur afin de proposer une montée des compétences, en prenant en compte les besoins spécifiques liés à la santé ou au handicap du collaborateur.

Former l'équipe de techniciens en élaborant un plan de formation pour garantir l'autonomie des équipes, standardiser les pratiques et sécuriser les interventions dans le respect des procédures de l'entreprise et des conditions de travail adaptées (rythme, fatigue cognitive, stress, ergonomie, etc...).

Coordonner l'activité de son équipe en mettant en place des outils collaboratifs pour fluidifier le partage des instructions en vue d'améliorer l'efficacité, les résultats et la montée en compétence des techniciens.

Déléguer les tâches de niveau 1 & 2 à réaliser de façon équitable, en hiérarchisant les priorités afin de mobiliser efficacement son équipe, tout en préservant la santé mentale et physique des collaborateurs.

Définir les rôles en planifiant les interventions et missions de chacun pour la meilleure atteinte des objectifs afin de garantir une organisation opérationnelle et efficace, dans le respect des obligations de santé au 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 et préserver un climat de travail serein, propice à l'inclusion de profils divers et à la prévention des RPS (risques psychosociaux).

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, en veillant à l'accessibilité des supports pour tous les profils d'interlocuteurs tant en français qu'en anglais.

Produire des supports documentaires à destination des utilisateurs en utilisant un langage accessible pour formaliser les procédures et garantir leur applicabilité.

Diffuser les informations liées à l'exploitation de l'environnement numériques de travail aux utilisateurs des différents services de l'entreprise afin de permettre l'engagement de tous les acteurs à une meilleure productivité de l'entreprise, en utilisant des formats inclusifs et compréhensibles.

Former les utilisateurs aux nouvelles procédures en fonction des enjeux et besoins métiers pour favoriser leur adhésion et limiter les résistances aux changements, en tenant compte des personnes en situation de handicap.

Informers les collaborateurs aux menaces courantes telles que les ransomware, le phishing, la compromission des e-mails professionnels (BEC) à l'aide de supports adaptés (volet sécurité de la charte informatique, campagnes de sensibilisation, newsletters sécurités, webinaires, ...) afin qu'ils aient les bonnes pratiques pour protéger les données de l'entreprise dans l'environnement de travail.

Renforcer les mesures de protection contre les erreurs humaines et opérationnelles en sensibilisant les utilisateurs aux mesures techniques de sécurité (authentification forte, sauvegarde, gestion des accès, usage des équipements, ...) afin de réduire les risques liés aux usages non maîtrisés du système d'information.

Favoriser l'adhésion des décideurs à la protection de l'entreprise aux dangers de la cybercriminalité en communiquant de manière pédagogique sur les risques, les enjeux réglementaires et les impacts économiques d'une cyberattaque afin de mobiliser les moyens humains, techniques, financiers et organisationnels nécessaires à la sécurité du système d'information.

Faire respecter les ententes de niveau de service (contrat de services) par une bonne connaissance des bonnes pratiques (ITIL) et des aspects commerciaux et juridiques d'un contrat (de location, de maintenance, de service, etc...) afin de maintenir des bonnes relations avec les fournisseurs et prestataires, et protéger les intérêts de

l'entreprise.

Mesurer les rapports qualité/prix du marché et inciter à fournir des services de qualité adaptés en s'appuyant sur une étude d'opportunité et de faisabilité pour faire des choix pertinents et maîtriser les coûts, en tenant compte de la durabilité des solutions proposées (recyclabilité, maintenance responsable, ...).

Négocier avec les fournisseurs en mobilisant les techniques et les leviers de discussion pour obtenir de meilleures offres et contribuer à la performance économique du service informatique.

Blocs de compétences

RNCP41996BC01 — Administrer le système d'information

LISTE DE COMPÉTENCES

Configurer les équipements réseaux (routeurs, commutateurs, ...) des sites de l'entreprise selon les recommandations du responsable du système d'information, ou des constructeurs, pour garantir la fluidité, la sécurité et la continuité des échanges de données en veillant à l'efficacité énergétique des équipements.

Installer et configurer des serveurs physiques ou virtuels (Cloud) et leurs systèmes d'exploitation afin de garantir la disponibilité, la stabilité, la performance des services numériques de l'entreprise (ERP) en respectant les besoins métiers exprimés et les politiques de sécurité, tout en optimisant la consommation énergétique (Green IT).

Concevoir et optimiser l'infrastructure de plateformes virtuelles en mutualisant les ressources (stockage, CPU, RAM, ...) des machines physiques dans un environnement centralisé (hyperviseurs), afin d'améliorer la flexibilité du système d'information et simplifier sa gestion.

Mettre en place une gestion unique et commune des terminaux mobiles (MDM) afin d'assurer une administration centralisée, cohérente et sécurisée de l'ensemble de l'infrastructure informatique.

Maintenir en conditions opérationnelles l'infrastructure de l'entreprise en utilisant des logiciels de gestion de haute disponibilité (clustering, load balancing, réplication, mises à jour), pour réduire les interruptions de services en appliquant les règles de santé et sécurité au travail lors des interventions.

Diagnostiquer les défaillances système ou réseau en analysant les logs, les symptômes et les dépendances entre services, afin d'assurer l'exploitation du Système d'Information, réduire les interruptions de service et limiter l'impact sur les utilisateurs.

Administrer les bases de données avec méthode en respectant les configurations requises (instances, paramètres système, schémas, droits d'accès, stockages, ...) et en appliquant les bonnes pratiques d'exploitation, afin d'assurer la disponibilité, l'intégrité et la performance des données en privilégiant les solutions économes en énergie.

Analyser les performances des bases de données installées sur la base des rapports d'usage collectés, afin d'accélérer les temps de traitement des requêtes.

Améliorer les performances des bases de données en optimisant l'emplacement des fichiers de stockage (données, journaux, index) sur les supports les plus adaptés pour garantir la réactivité des applications.

Automatiser les tâches d'exploitation courante (sauvegarde, mises à jour, déploiement) afin de fiabiliser les processus et gagner en productivité, en développant des scripts (Bash, PowerShell...) ou en utilisant des outils d'orchestration (Ansible, Python, IA, etc.), pour éviter les erreurs humaines et optimiser le temps d'administration.

MODALITÉS D'ÉVALUATION

Rédaction d'un dossier et soutenance orale.

RNCP41996BC02 — Gérer le système d'information

LISTE DE COMPÉTENCES

Analyser les besoins techniques et métiers en identifiant les contraintes et opportunités, pour garantir la cohérence entre les choix techniques et les objectifs métiers, en intégrant les aspects d'accessibilité numérique pour tous les profils utilisateurs.

Gérer les évolutions des infrastructures Informatiques en appliquant les principes et les limites par la norme IT Service Management ISO/CEI 20000 pour garantir une évolution conforme aux standards de gestion des services informatiques et assurer leur alignement avec les besoins métiers et les exigences de qualité de service, dans le respect des standards environnementaux et de sobriété numérique.

Assurer l'évolution des équipements en tenant compte des technologies émergentes en anticipant les besoins futurs, pour garantir la pérennité des infrastructures, optimiser les investissements et accompagner les évolutions stratégiques de l'organisation.

Élaborer des propositions de renouvellement d'infrastructures, en analysant leurs performances et leur compatibilité,

tout en tenant compte des contraintes budgétaires, en privilégiant des solutions à faible consommation énergétique, afin d'effectuer des choix d'investissement éclairés, durables et cohérents avec la stratégie de l'entreprise.

Élaborer un plan d'évolution des équipements informatique en identifiant les ressources, les étapes et les risques, pour garantir le bon déroulement du plan dans le respect des délais et des budgets afin de piloter la mise en œuvre des évolutions du Système d'Information.

Maquetter les solutions de déploiements dans un environnement de test (virtualisation, conteneurisation, sandbox, ...) pour détecter les incompatibilités et valider les choix techniques retenus avant leur mise en production, en s'assurant de l'accessibilité des interfaces testées pour les publics en situation de handicap.

Ordonnancer le plan de déploiement afin de coordonner efficacement les étapes d'installation ou de mise en production en tenant compte des disponibilités des différents acteurs concernés (équipes techniques, métiers, prestataires).

Attribuer les ressources informatiques nécessaires au bon déroulement du plan en tenant compte du budget alloué, des priorités opérationnelles, de la consommation énergétique et de la disponibilité des moyens (humains, matériels, logiciels), afin d'assurer la faisabilité technique et organisationnelle.

Suivre l'avancement des tâches et assurer la coordination avec les parties prenantes afin de maintenir la dynamique du projet, pour faciliter la réussite et la communication interservices.

Configurer les outils de supervision selon les indicateurs clés (taux de disponibilité, statuts du service, taux de perte de paquets, consommation énergétique, ...) en paramétrant des alertes adaptées, afin d'anticiper les dysfonctionnements.

Superviser l'infrastructure informatique et le patrimoine applicatif en utilisant les outils de supervision installés (supervision réseau, analyse de logs, alertes automatisées) afin d'améliorer les performances globales du système d'information.

Cartographier les composants du Système d'information (processus métiers, applications, fonctions, données, infrastructures...) pour faciliter la compréhension globale du SI, appuyer les prises de décision techniques et garantir la cohérence des évolutions à venir.

Organiser l'infrastructure en modélisant l'environnement technique (conteneurs, environnements de test, gestion des dépendances) pour accélérer les cycles de mise à jour, garantir la stabilité des services et soutenir l'agilité des équipes de développement et d'exploitation.

Accompagner les évolutions des applications métiers en adoptant une logique modulaire ou de composants (micro-services, APIs, ...) dans l'objectif de limiter les failles de sécurité, d'assurer la traçabilité des changements et de maintenir la continuité des services métiers, tout en veillant à la compatibilité avec les normes d'accessibilité numérique (RGAA).

Migrer une architecture système ou réseau dans le respect des principes d'urbanisation du SI en planifiant les interventions, en optimisant les opérations techniques et en identifiant les risques associés pour les anticiper afin de garantir la continuité de service, de limiter les interruptions et de sécuriser l'évolution du système d'information.

Maintenir un inventaire à jour des équipements et logiciels en intégrant les contraintes de maintenance, de licence, de durabilité, de recyclabilité et de sécurité pour optimiser les coûts et la performance du SI en cohérence avec la stratégie d'entreprise.

Centraliser le traitement des incidents en un point unique d'accès (ITSM, helpdesk) permettant de qualifier, affecter et historiser les incidents, pour mieux prioriser les interventions, optimiser la productivité des équipes support et améliorer la qualité du service rendu aux utilisateurs y compris ceux en situation de handicap.

Résoudre les tickets de niveau 3 & 4 à l'aide d'outils de prise en main à distance ou en intervenant sur place, pour limiter l'impact des incidents complexes sur l'activité de l'organisation et améliorer la satisfaction des utilisateurs.

Elaborer un tableau de bord sur la résolution des tickets d'incidents par niveau de support par la collecte et l'analyse des indicateurs clés (temps de réponse, taux de résolution, escalades, ...) afin d'identifier les points de blocage, d'améliorer l'efficacité de la résolution des incidents et de piloter la qualité du support utilisateur.

Concevoir un service numérique responsable en intégrant dès la phase de conception des principes d'écoconception (optimisation des ressources, sobriété énergétique, choix d'infrastructures durables) et en tenant compte des usages et contraintes du contexte professionnel, pour associer efficacement transition écologique et transition numérique, tout en répondant aux exigences fonctionnelles de l'organisation.

Gérer le parc informatique en identifiant les métriques (consommation énergétique, taux d'usage, recyclabilité, accessibilité numérique) adaptées aux activités de l'organisation, pour favoriser une gestion responsable du système d'information et orienter les choix techniques vers des pratiques durables et inclusives (RSE).

MODALITÉS D'ÉVALUATION

Rédaction d'un dossier et soutenance orale.

RNCP41996BC03 — Définir la politique de sécurisation du système d'information

LISTE DE COMPÉTENCES

Rédiger ou mettre à jour la Politique de Sécurisation du Système d'Information (PSSI) en intégrant les recommandations internes (RSSI) et réglementaires (RGPD, ANSSI, ISO 27001 ...) pour formaliser les règles de sécurité, cadrer les pratiques et garantir un socle de protection cohérent.

Identifier les menaces et vulnérabilités du système d'information en réalisant une analyse de risques structurée (EBIOS, ISO 27005...) pour limiter l'exposition aux cyberattaques et renforcer la résilience du SI.

Déployer des solutions automatisées de mise à jour et de correctifs en configurant des outils de gestion centralisée des correctifs (WSUS, Ansible, scripts de déploiement, solutions EDR, IA) et en planifiant leur diffusion de manière contrôlée, pour limiter les surfaces d'attaque, assurer la conformité aux politiques de sécurité.

Évaluer les perturbations de services en exploitant les alertes émises par les sondes de supervision (réseau, système, base de données), en croisant les données collectées (logs, métriques, seuils) et en analysant l'impact sur la qualité de service pour identifier les correctifs à déployer rapidement.

Appliquer les procédures de sécurité liées aux accès physiques de l'entreprise en s'appuyant sur une stratégie d'identification (badges, registres d'accès, vidéosurveillance, droits d'entrée différenciés) afin de limiter les intrusions non autorisées dans les zones sensibles, en respectant les règles d'accessibilité aux bâtiments pour tous les utilisateurs (PMR, ...).

Configurer les dispositifs de sécurité (pare-feu, VPN, MFA, antivirus, etc.) pour garantir l'intégrité, la confidentialité et la disponibilité des données de l'entreprise et protéger les infrastructures contre les intrusions ou les fuites de données.

Gérer les comptes utilisateurs et les groupes dans un service d'annuaire en appliquant les politiques internes (mot de passe, rotation, GPO, ...) et en respectant les habilitations définies pour chaque utilisateur afin de permettre et tracer l'accès aux données de l'entreprise, tout en s'assurant que les procédures d'authentification restent accessibles.

Mettre en place une journalisation et un suivi d'activité en exploitant les outils de supervision de sécurité (SIEM, log, ...), pour assurer une réactivité en cas de comportements suspects ou d'incident et de conserver une traçabilité complète.

Identifier les éléments et applications critiques de l'entreprise en vue d'assurer la continuité opérationnelle en prévoyant un site de repli ou une infrastructure de secours adaptée pour maintenir les services essentiels en cas de sinistre, en prenant en compte les besoins spécifiques des utilisateurs en situation de handicap.

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, en privilégiant des solutions à faible consommation énergétique et éco-conçues.

Identifier la criticité de l'interruption d'activité en fonction des métiers de l'entreprise en analysant l'impact d'éventuels dysfonctionnements pour préconiser des mesures de redondance et garantir une bonne reprise d'activités.

Prioriser les besoins de continuité en évaluant les impacts potentiels d'interruption et en classant la reprise selon la criticité de l'activité, en intégrant les contraintes de santé au travail des équipes mobilisées lors des reprises (horaires, stress, charge).

Crypter les canaux de transmissions des sauvegardes émises via le réseau pour éviter une perte de données.

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

MODALITÉS D'ÉVALUATION

Rédaction d'un dossier et soutenance orale.

RNCP41996BC04 — Communiquer avec tous les acteurs internes ou externes au service informatique

LISTE DE COMPÉTENCES

Collecter des informations auprès de spécialistes techniques en analysant et synthétisant les problèmes décrits afin d'envisager des solutions, en veillant à inclure les besoins spécifiques des utilisateurs en situation de handicap.

Alimenter la base de connaissances interne en documentant les incidents et les solutions apportées afin de faciliter la résolution des incidents similaires avec des contenus clairs, structurés et accessibles à tous les profils d'utilisateurs.

Concevoir la documentation technique, en français et en anglais, pour répondre aux besoins d'information des techniciens et faciliter l'usage des logiciels de support déployés dans l'entreprise.

Identifier les compétences techniques et relationnelles attendues et le degré intégrabilité des futurs collaborateurs au sein de l'équipe en analysant les besoins opérationnels du service afin d'élaborer une fiche de poste précise en vue de conduire un entretien d'embauche, en intégrant des critères favorisant l'inclusion.

Conduire un entretien annuel en contrôlant l'atteinte des objectifs fixés et des besoins du collaborateur afin de proposer une montée des compétences, en prenant en compte les besoins spécifiques liés à la santé ou au handicap du collaborateur.

Former l'équipe de techniciens en élaborant un plan de formation pour garantir l'autonomie des équipes, standardiser les pratiques et sécuriser les interventions dans le respect des procédures de l'entreprise et des conditions de travail adaptées (rythme, fatigue cognitive, stress, ergonomie, etc...).

Coordonner l'activité de son équipe en mettant en place des outils collaboratifs pour fluidifier le partage des instructions en vue d'améliorer l'efficacité, les résultats et la montée en compétence des techniciens.

Déléguer les tâches de niveau 1 & 2 à réaliser de façon équitable, en hiérarchisant les priorités afin de mobiliser efficacement son équipe, tout en préservant la santé mentale et physique des collaborateurs.

Définir les rôles en planifiant les interventions et missions de chacun pour la meilleure atteinte des objectifs afin de garantir une organisation opérationnelle et efficace, dans le respect des obligations de santé au 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 et préserver un climat de travail serein, propice à l'inclusion de profils divers et à la prévention des RPS (risques psychosociaux).

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, en veillant à l'accessibilité des supports pour tous les profils d'interlocuteurs tant en français qu'en anglais.

Produire des supports documentaires à destination des utilisateurs en utilisant un langage accessible pour formaliser les procédures et garantir leur applicabilité.

Diffuser les informations liées à l'exploitation de l'environnement numériques de travail aux utilisateurs des différents services de l'entreprise afin de permettre l'engagement de tous les acteurs à une meilleure productivité de l'entreprise, en utilisant des formats inclusifs et compréhensibles.

Former les utilisateurs aux nouvelles procédures en fonction des enjeux et besoins métiers pour favoriser leur adhésion et limiter les résistances aux changements, en tenant compte des personnes en situation de handicap.

Informers les collaborateurs aux menaces courantes telles que les ransomware, le phishing, la compromission des e-mails professionnels (BEC) à l'aide de supports adaptés (volet sécurité de la charte informatique, campagnes de sensibilisation, newsletters sécurités, webinaires, ...) afin qu'ils aient les bonnes pratiques pour protéger les données de l'entreprise dans l'environnement de travail.

Renforcer les mesures de protection contre les erreurs humaines et opérationnelles en sensibilisant les utilisateurs aux mesures techniques de sécurité (authentification forte, sauvegarde, gestion des accès, usage des équipements, ...) afin de réduire les risques liés aux usages non maîtrisés du système d'information.

Favoriser l'adhésion des décideurs à la protection de l'entreprise aux dangers de la cybercriminalité en communiquant de manière pédagogique sur les risques, les enjeux réglementaires et les impacts économiques d'une cyberattaque afin de mobiliser les moyens humains, techniques, financiers et organisationnels nécessaires à la sécurité du système d'information.

Faire respecter les ententes de niveau de service (contrat de services) par une bonne connaissance des bonnes pratiques (ITIL) et des aspects commerciaux et juridiques d'un contrat (de location, de maintenance, de service, etc...) afin de maintenir des bonnes relations avec les fournisseurs et prestataires, et protéger les intérêts de l'entreprise.

Mesurer les rapports qualité/prix du marché et inciter à fournir des services de qualité adaptés en s'appuyant sur une étude d'opportunité et de faisabilité pour faire des choix pertinents et maîtriser les coûts, en tenant compte de la durabilité des solutions proposées (recyclabilité, maintenance responsable, ...).

Négocier avec les fournisseurs en mobilisant les techniques et les leviers de discussion pour obtenir de meilleures offres et contribuer à la performance économique du service informatique.

MODALITÉS D'ÉVALUATION

Rédaction d'un dossier et soutenance orale.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

L'Administrateur systèmes réseaux et bases de données exerce son activité :

- au sein d'entreprises et organisations privées de tout secteur d'activité et de taille diversifiée (PME/PMI ou ETI et grands groupes nationaux ou internationaux)

- au sein d'organisations et administrations publiques et collectivités territoriales
- au sein d'ESN
- en Freelance

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
Gestionnaire de Parc
Responsable Informatique
Administrateur datacenter
Administrateur informatique
Administrateur système Linux
Administrateur système Microsoft
Ingénieur systèmes et réseaux
Gestionnaire d'infrastructure

RÈGLEMENTATIONS D'ACTIVITÉ

Le métier en lui-même n'est pas réglementé mais s'exerce dans un contexte règlementaire :

- la loi n° 78-17 du 6 janvier 1978 (LIL, Loi Informatique et Liberté) portant sur l'informatique, les fichiers et les libertés qui régit ce domaine. Elle réglemente le traitement de données personnelles ainsi que les droits et obligations des personnes qui prennent en charge ce processus et a donné naissance à la CNIL ;
- l'ordonnance du 12 décembre 2018 destinée à prendre en compte le RGPD et à simplifier l'architecture globale du texte.

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

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

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

Le jury est composé de trois membres : 2 professionnels du secteur informatique, externes à l'organisme certificateur et 1 représentant de l'organisme 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	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	27/02/2026
Durée de l'enregistrement	5 ans
Date d'échéance de l'enregistrement	27/02/2031
Date de dernière délivrance possible	27/02/2035

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2024	440	1	78 %	78 %
2023	437	3	70 %	82 %
2022	354	0	73 %	87 %
2021	361	1	91 %	92 %

Liens avec d'autres certifications

ANCIENNES VERSIONS
RNCP35594

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/41996/>

Où se former

Formations référencées	1
Organismes	1
Régions couvertes	0
Prix indicatif	9 600 €

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

Se former en apprentissage

Formations en apprentissage	6
Organismes gestionnaires (CFA)	4

Organismes formateurs	4
Régions couvertes	3
Départements couverts	4
Organismes certifiés Qualiopi	4
Sessions	de 09/2026 à 09/2027

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