# Technicien d'infrastructures informatiques sécurisées

RNCP42933 · RNCP · Publiée

## L'essentiel

| | |
|---|---|
| **Niveau de qualification** | Niveau 5 |
| **Code(s) NSF** | 326, 326r, 326u |
| **Formacode(s)** | 31034, 24220, 31008, 31051 |
| **Code(s) ROME** | I1401, M1810, M1801 |
| **Type d'enregistrement** | Enregistrement sur demande |
| **Date d'enregistrement** | 30/10/2026 |
| **Date d'échéance** | 30/10/2031 |

## Certificateur(s)

**CESI · SIRET : 77572257201109**
http://www.cesi.fr

## Partenaires habilités

56 organismes habilités, d'après la liste publiée par France compétences : 56 à former et organiser l'évaluation.

| Organisme | SIRET | Habilitation |
|---|---|---|
| C E SI | 77572257200366 | Former et organiser l'évaluation |
| C E SI | 77572257200820 | 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 |
| C E SI | 77572257201034 | Former et organiser l'évaluation |
| C E SI | 77572257201042 | Former et organiser l'évaluation |

Liste complète des 56 partenaires habilités : https://data.aktaconseil.fr/certifications/rncp42933-technicien-d-infrastructures-informatiques-securisees/partenaires

## Résumé de la certification

### OBJECTIFS ET CONTEXTE

Le Technicien d'infrastructures informatiques sécurisées est un professionnel de l'informatique chargé d'assurer le bon fonctionnement et la maintenance des systèmes informatiques et des réseaux de l'entreprise. Il intervient sur l'ensemble des éléments d'un système d'information (postes de travail, équipements réseaux, serveurs, applications métiers). Il joue un rôle essentiel dans la continuité d'activité de l'entreprise en garantissant la disponibilité et la performance du système d'information tout en intégrant les enjeux de cybersécurité dans le monde professionnel.

### ACTIVITÉS VISÉES

Installer et configurer les ordinateurs clients de l’entreprise
Diagnostiquer et dépanner les ordinateurs clients de l’entreprise
Assurer les interventions informatiques
Virtualiser l’infrastructure serveur et les services de l’entreprise
Installer et configurer les serveurs Microsoft Windows et Linux et les services de l’entreprise
Administrer les ressources informatiques de l’entreprise
Optimiser de façon sécurisée l’accès aux ressources du parc informatique
Connecter les différents éléments du réseau avec les supports de transmission correspondants
Déployer et administrer les éléments actifs (routeur, commutateur, etc.) du réseau
Réaliser le suivi opérationnel des différents équipements informatiques
Préserver l’intégrité des données de l’entreprise
Participer à la configuration les outils permettant la continuité de service et la reprise d’activité
Intégrer les outils de protection des interconnexions de réseaux (pare-feu, proxy, etc.)

### COMPÉTENCES ATTESTÉES

Identifier les caractéristiques des postes clients à partir des besoins métier et des besoins spécifiques, tout en prenant en compte les situations de handicap, afin de fournir à tous un poste utilisateur
Intégrer les postes clients dans le service d’annuaire (par exemple Active Directory) pour appliquer les paramètres de session utilisateur dans le respect de la politique de l’entreprise
Elaborer une image de référence (master) configurée à partir des besoins métier et des besoins spécifiques, tout en prenant en compte l’accessibilité, pour préparer le déploiement rapide d’un environnement homogène
Déployer l’image du système en mobilisant les différentes solutions de déploiement pour garantir l’installation rapide d’environnements homogènes
Etablir le diagnostic de la panne informatique du poste client dans le respect des bonnes pratiques afin de mettre en œuvre une stratégie de réparation et/ou de remplacement des matériels
Identifier les solutions de recyclage des matériels informatiques obsolètes ou défectueux pour respecter la directive européenne DEEE en s’appuyant sur la politique numérique responsable de l’entreprise
Planifier ses interventions avec les utilisateurs en les priorisant afin de limiter le temps d’indisponibilité des équipements informatiques
Assurer la traçabilité des interventions en utilisant un outil de support informatique (helpdesk) dans le respect de la politique de renseignement des données client (conformité avec le RGPD) pour alimenter la base de connaissance et permettre la facturation client
Installer la solution de virtualisation (ou hyperviseur) sélectionnée par sa hiérarchie afin d’optimiser les ressources matérielles, les opérations de maintenance et la consommation énergétique de l’infrastructure serveur
Virtualiser les serveurs Microsoft Windows et Linux et les services (par exemple Azure) de l’entreprise sur l’hyperviseur pour centraliser l’infrastructure serveur
Migrer les systèmes virtualisés vers l’hyperviseur de back-up et/ou spare pour programmer des opérations de maintenance (préventive et corrective) et garantir la continuité de service (dont PCA/PRA) de l’entreprise
Configurer les serveurs Microsoft Windows, les rôles et/ou les services (DHCP, DFS, DNS, etc.) définis par la hiérarchie afin de répondre aux besoins de l’entreprise
Configurer les protocoles de communication (SSH, RDP, etc.) pour administrer à distance les serveurs de façon sécurisée
Configurer, en CLI, les serveurs Linux et les rôles (FTP, SMB) définis par la hiérarchie afin d’optimiser les ressources matérielles et de répondre aux besoins de l’entreprise
Configurer les espaces de stockage dans le respect de la politique de gestion d’accès aux données et de la législation en vigueur (RGPD, HDS, etc.) pour garantir l’intégrité et la confidentialité des données de l’entreprise
Configurer un service d’annuaire (par exemple Active Directory) au sein de l’infrastructure serveur pour centraliser et optimiser la gestion des utilisateurs et matériels finaux
Administrer les comptes utilisateurs de l’entreprise dans le service d’annuaire (par exemple Active Directory) pour assurer la connexion de chaque poste utilisateur à l’infrastructure serveur
Configurer les stratégies de groupe (GPO) afin de fournir les ressources logicielles nécessaires aux utilisateurs et limiter l’accès aux fonctionnalités définies en conformité avec la PSSI (dont confidentialité, traçabilité, éthique, etc.) de l’entreprise
Affecter les groupes de sécurité aux utilisateurs en fonction des besoins du métier afin d’optimiser la gestion des

accès aux ressources partagées (Dossiers partagés, imprimantes, etc.)
Configurer les limitations (volume, horaires, etc.) de l'utilisation des ressources pour être conforme avec la politique de l'entreprise
Schématiser le plan du réseau selon la topologie définie par la hiérarchie pour assurer la maintenance et la mise à jour et permettre les évolutions de l'infrastructure réseau
Réaliser les nouvelles connexions réseaux physiques au sein des baies de brassage et dans le respect des bonnes pratiques du « cable management » pour interconnecter les espaces au sein de l'entreprise
Effectuer les opérations de recettage pour référencer les prises réseaux en utilisant les outils de tests adaptés au câblage utilisé
Installer les bornes sans-fil en tenant compte de l'infrastructure existante et des besoins pour assurer l'activité nomade au sein de l'entreprise
Configurer les éléments actifs du réseau (commutateurs, points d'accès sans-fil, routeurs, etc.) en conformité avec le plan de l'infrastructure réseau afin d'assurer la communication des matériels entre eux, en interne et en externe à l'entreprise
Activer les interfaces de gestion des éléments actifs du réseau pour les administrer à distance en utilisant des protocoles de communication sécurisés (SSH, HTTPS, etc.)
Séparer les réseaux en utilisant des réseaux virtuels (VLAN) afin de cloisonner et de sécuriser les transmissions de données
Assurer la sécurité d'accès physique aux éléments actifs du réseau dans le respect de la PSSI de l'entreprise pour éviter les intrusions physiques dans son réseau
Identifier les causes des dysfonctionnements en suivant le modèle OSI pour dépanner les utilisateurs et restaurer la fluidité du réseau
Suivre l'état et l'utilisation du parc informatique en activant la journalisation pour assurer la maintenance préventive et curative du matériel
Configurer la solution de supervision sélectionnée par sa hiérarchie pour automatiser les alertes liées au matériel informatique
Assurer l'état du stock de matériel de remplacement pour anticiper les interventions auprès de l'utilisateur
Configurer une solution de stockage sécurisée et redondée afin d'assurer la disponibilité, l'intégrité et la confidentialité des données dans le respect des règlements en vigueur (dont le RGPD) et des guides essentiels et préconisations diffusées par l'ANSSI
Configurer la solution de sauvegarde dans le respect de la PSSI et/ou des PCA et/ou PRA définis dans l'entreprise afin de pouvoir récupérer les données altérées, supprimées ou perdues
Restaurer des fichiers à partir de l'outil de sauvegarde en cas d'altération, de suppression ou de perte de données pour pouvoir garantir le fonctionnement des processus métier de l'entreprise
Réaliser les opérations d'extractions de données des boîtes de messagerie des utilisateurs pour assurer la migration des services de messagerie dans le respect de la législation en vigueur (dont RGPD)
Identifier les actions à mener, à partir des PCA et/ou PRA de l'entreprise, en cas de crise ou de sinistre ayant un impact sur le système d'information, pour permettre la continuité de service en mode dégradé
Restaurer la configuration des éléments actifs du système d'information (routeurs, commutateurs, serveurs, etc.) à partir des sauvegardes des configurations pour optimiser la reprise d'activité en cas de crise ou de sinistre
Assurer la redondance des éléments actifs du système d'information en cas de crise ou de sinistre (double alimentation, RAID, réplication de machines virtuelles, etc.) pour permettre la continuité de service en mode dégradé et la mise à jour documentaire
Installer une solution de pare-feu matériel en le connectant au réseau avec l'extérieur et anticiper la mise en place des règles de filtrage
Créer des règles de filtrage dans le respect de la PSSI de l'entreprise et en configurant des règles de pare-feu sans état (stateless) pour améliorer le niveau de sécurité des connexions
Configurer le proxy pour limiter l'accès aux sites externes non conformes avec la PSSI de l'entreprise

## Blocs de compétences

### RNCP42933BC01 — Maintenir et dépanner le parc informatique de l’entreprise

**LISTE DE COMPÉTENCES**

Identifier les caractéristiques des postes clients à partir des besoins métier et des besoins spécifiques, tout en prenant en compte les situations de handicap, afin de fournir à tous un poste utilisateur

Intégrer les postes clients dans le service d’annuaire (par exemple Active Directory) pour appliquer les paramètres de session utilisateur dans le respect de la politique de l’entreprise

Elaborer une image de référence (master) configurée à partir des besoins métier et des besoins spécifiques, tout en prenant en compte l’accessibilité, pour préparer le déploiement rapide d’un environnement homogène

Déployer l’image du système en mobilisant les différentes solutions de déploiement pour garantir l’installation rapide d’environnements homogènes

Etablir le diagnostic de la panne informatique du poste client dans le respect des bonnes pratiques afin de mettre en œuvre une stratégie de réparation et/ou de remplacement des matériels

Identifier les solutions de recyclage des matériels informatiques obsolètes ou défectueux pour respecter la directive européenne DEEE en s’appuyant sur la politique numérique responsable de l’entreprise

Planifier ses interventions avec les utilisateurs en les priorisant afin de limiter le temps d’indisponibilité des équipements informatiques

Assurer la traçabilité des interventions en utilisant un outil de support informatique (helpdesk) dans le respect de la politique de renseignement des données client (conformité avec le RGPD) pour alimenter la base de connaissance et permettre la facturation client

**MODALITÉS D'ÉVALUATION**

Application professionnelle réelle ou simulée sur la base de la gestion d’un parc informatique donnant lieu à la production d'un document écrit

### RNCP42933BC02 — Installer et administrer l’infrastructure serveur et les services de l’entreprise

**LISTE DE COMPÉTENCES**

Installer la solution de virtualisation (ou hyperviseur) sélectionnée par sa hiérarchie afin d’optimiser les ressources matérielles, les opérations de maintenance et la consommation énergétique de l’infrastructure serveur

Virtualiser les serveurs Microsoft Windows et Linux et les services (par exemple Azure) de l’entreprise sur l’hyperviseur pour centraliser l’infrastructure serveur

Migrer les systèmes virtualisés vers l’hyperviseur de back-up et/ou spare pour programmer des opérations de maintenance (préventive et corrective) et garantir la continuité de service (dont PCA/PRA) de l’entreprise

Configurer les serveurs Microsoft Windows, les rôles et/ou les services (DHCP, DFS, DNS, etc.) définis par la hiérarchie afin de répondre aux besoins de l’entreprise

Configurer les protocoles de communication (SSH, RDP, etc.) pour administrer à distance les serveurs de façon sécurisée

Configurer, en CLI, les serveurs Linux et les rôles (FTP, SMB) définis par la hiérarchie afin d’optimiser les ressources matérielles et de répondre aux besoins de l’entreprise

Configurer les espaces de stockage dans le respect de la politique de gestion d’accès aux données et de la législation en vigueur (RGPD, HDS, etc.) pour garantir l’intégrité et la confidentialité des données de l’entreprise

Configurer un service d’annuaire (par exemple Active Directory) au sein de l’infrastructure serveur pour centraliser et optimiser la gestion des utilisateurs et matériels finaux

Administrer les comptes utilisateurs de l’entreprise dans le service d’annuaire (par exemple Active Directory) pour assurer la connexion de chaque poste utilisateur à l’infrastructure serveur

Configurer les stratégies de groupe (GPO) afin de fournir les ressources logicielles nécessaires aux utilisateurs et limiter l’accès aux fonctionnalités définies en conformité avec la PSSI (dont confidentialité, traçabilité, éthique, etc.) de l’entreprise

Affecter les groupes de sécurité aux utilisateurs en fonction des besoins du métier afin d’optimiser la gestion des accès aux ressources partagées (Dossiers partagés, imprimantes, etc.)

Configurer les limitations (volume, horaires, etc.) de l’utilisation des ressources pour être conforme avec la politique de l’entreprise

**MODALITÉS D'ÉVALUATION**

Application professionnelle réelle ou simulée sur la base d’une entreprise ayant un besoin de structuration et centralisation de son SI donnant lieu à la production d'un document écrit suivi d'une présentation orale

### RNCP42933BC03 — Déployer et maintenir le réseau informatique de l’entreprise

**LISTE DE COMPÉTENCES**

Schématiser le plan du réseau selon la topologie définie par la hiérarchie pour assurer la maintenance et la mise à jour et permettre les évolutions de l’infrastructure réseau

Réaliser les nouvelles connexions réseaux physiques au sein des baies de brassage et dans le respect des bonnes pratiques du « cable management » pour interconnecter les espaces au sein de l’entreprise

Effectuer les opérations de recettage pour référencer les prises réseaux en utilisant les outils de tests adaptés au câblage utilisé

Installer les bornes sans-fil en tenant compte de l’infrastructure existante et des besoins pour assurer l’activité nomade au sein de l’entreprise

Configurer les éléments actifs du réseau (commutateurs, points d’accès sans-fil, routeurs, etc.) en conformité avec le plan de l’infrastructure réseau afin d’assurer la communication des matériels entre eux, en interne et en externe à l’entreprise

Activer les interfaces de gestion des éléments actifs du réseau pour les administrer à distance en utilisant des protocoles de communication sécurisés (SSH, HTTPS, etc.)

Séparer les réseaux en utilisant des réseaux virtuels (VLAN) afin de cloisonner et de sécuriser les transmissions de données

Assurer la sécurité d’accès physique aux éléments actifs du réseau dans le respect de la PSSI de l’entreprise pour éviter les intrusions physiques dans son réseau

Identifier les causes des dysfonctionnements en suivant le modèle OSI pour dépanner les utilisateurs et restaurer la fluidité du réseau

**MODALITÉS D'ÉVALUATION**

Application professionnelle réelle ou simulée sur la base de la gestion d’un parc informatique donnant lieu à la production d'un document écrit

### RNCP42933BC04 — Maintenir en condition opérationnelle l’infrastructure informatique de l’entreprise

**LISTE DE COMPÉTENCES**

Suivre l’état et l’utilisation du parc informatique en activant la journalisation pour assurer la maintenance préventive et curative du matériel

Configurer la solution de supervision sélectionnée par sa hiérarchie pour automatiser les alertes liées au matériel informatique

Assurer l’état du stock de matériel de remplacement pour anticiper les interventions auprès de l’utilisateur

Configurer une solution de stockage sécurisée et redondée afin d’assurer la disponibilité, l’intégrité et la confidentialité des données dans le respect des règlements en vigueur (dont le RGPD) et des guides essentiels et préconisations diffusées par l’ANSSI

Configurer la solution de sauvegarde dans le respect de la PSSI et/ou des PCA et/ou PRA définis dans l’entreprise afin de pouvoir récupérer les données altérées, supprimées ou perdues

Restaurer des fichiers à partir de l'outil de sauvegarde en cas d’altération, de suppression ou de perte de données pour pouvoir garantir le fonctionnement des processus métier de l’entreprise

Réaliser les opérations d’extractions de données des boîtes de messagerie des utilisateurs pour assurer la migration des services de messagerie dans le respect de la législation en vigueur (dont RGPD)

Identifier les actions à mener, à partir des PCA et/ou PRA de l’entreprise, en cas de crise ou de sinistre ayant un impact sur le système d’information, pour permettre la continuité de service en mode dégradé

Restaurer la configuration des éléments actifs du système d’information (routeurs, commutateurs, serveurs, etc.) à partir des sauvegardes des configurations pour optimiser la reprise d’activité en cas de crise ou de sinistre

Assurer la redondance des éléments actifs du système d’information en cas de crise ou de sinistre (double alimentation, RAID, réplication de machines virtuelles, etc.) pour permettre la continuité de service en mode dégradé et la mise à jour documentaire

Installer une solution de pare-feu matériel en le connectant au réseau avec l’extérieur et anticiper la mise en place des règles de filtrage

Créer des règles de filtrage dans le respect de la PSSI de l’entreprise et en configurant des règles de pare-feu sans état (stateless) pour améliorer le niveau de sécurité des connexions

Configurer le proxy pour limiter l’accès aux sites externes non conformes avec la PSSI de l’entreprise

**MODALITÉS D'ÉVALUATION**

Application professionnelle réelle ou simulée sur la base d’une entreprise ayant un besoin de maintien en condition opérationnelle de son SI donnant lieu à la production d'un document écrit suivi d'une présentation orale

## Secteur d'activité et type d'emploi

### SECTEURS D'ACTIVITÉS

Le Technicien d'infrastructures informatiques sécurisées est présent dans les entreprises ou collectivités utilisatrices de l’informatique possédant à minima un réseau local et utilisant des services ou applications réseaux. Il exerce aussi bien dans des PME/PMI qu’au sein du service informatique ou de la DSI (Direction du Système d’Information) d’un grand groupe. Le Technicien d'infrastructures informatiques sécurisées exerce également dans les ESN pour des missions d’administration auprès de clients (mise à disposition) ou pour participer à des projets de mise en place de nouvelles solutions systèmes et réseaux. Il peut exercer aussi dans les entreprises offrant des services d’hébergement, de « cloud computing », etc. au sein desquels il administre et supervise les équipements du datacenter et résout les problématiques des clients.

### TYPE D'EMPLOIS ACCESSIBLES

Technicien systèmes et réseaux -Technicien systèmes et/ou Technicien réseaux - Technicien d’infrastructures informatiques - Technicien informatique et réseaux - Technicien d’exploitation réseaux

### RÉGLEMENTATIONS D'ACTIVITÉ

Le métier de Technicien d’infrastructures informatiques sécurisées s’exerce dans un cadre réglementaire très précis. En fonction de l’environnement dans lequel il évolue, il ne peut se soustraire :
Aux règlementations :
Le règlement général sur la protection des données (RGPD)
Aux directives :
La directive 2002/96/CE du 27 janvier 2003 relative aux déchets d’équipements électriques et électroniques
La directive Sécurité des réseaux et de l’information dite directive NIS et NIS2
Aux normes :
La norme internationale de sécurité des systèmes d'information (ISO/CEI 27000)
La norme internationale pour les systèmes de management de la continuité d’activité (SMCA/ISO 22301)
La certification Hébergeur de Données de Santé (HDS)
La norme de communication de tous les systèmes informatiques en réseau (Modèle OSI)
Aux référentiels :
Le référentiel général de sécurité (RGS)
Aux bonnes pratiques :
La bibliothèque pour l’infrastructure des technologies de l’information (ITIL : Information Technology Infrastructure Library),
L’Autorité Nationale en matière de Sécurité et de défense des Systèmes d'Information (ANSSI)
La méthode d’évaluation des risques en informatique EBIOS
La méthode de sécurisation de l’information MEHARI
Aux engagements pour un numérique responsable :
La Charte numérique responsable de l’INRO (Institut du Numérique Responsable) : https://charter.isit-europe.org/?lang=fr_FR
A différents protocoles :
dont les protocoles TCP, IP, VLAN, WLAN, etc.

## 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)<br>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)<br>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<br>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

Le candidat doit être titulaire d'une certification de niveau 4. 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, VAE

Le jury 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)

Cette certification ne figure pas au référentiel des niveaux de prise en charge (NPEC) en vigueur. En attendant que son niveau soit fixé, l'OPCO peut financer un contrat d'apprentissage sur la base d'une valeur d'amorçage (arrêté du 31 août 2022).

## Base légale

| | |
|---|---|
| **Date de décision** | 30/10/2026 |
| **Durée de l'enregistrement** | 5 ans |
| **Date d'échéance de l'enregistrement** | 30/10/2031 |
| **Date de dernière délivrance possible** | 30/10/2035 |

## Statistiques

| Année | Certifiés | Dont VAE | Insertion 6 mois | Métier 2 ans |
|---|---|---|---|---|
| 2024 | 54 | 0 | 60 % | — |
| 2023 | 62 | 0 | 90 % | 89 % |
| 2022 | 33 | 0 | 68 % | 82 % |
| 2021 | 30 | 0 | 84 % | 78 % |

## Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP36501

CORRESPONDANCES (PAR BLOCS)

RNCP36462, RNCP36501

## Pour plus d'informations

**Fiche officielle (France Compétences)**

https://www.francecompetences.fr/recherche/rncp/42933/