



# TITRE PRO

NIVEAU BAC +3

## ADMINISTRATEUR D'INFRASTRUCTURES SÉCURISÉES

Codes Rome

M 1801-M1802-M1810

DURÉE : 14 MOIS

Une opération soutenue par l'État dans le cadre de l'AMI "Compétences et Métiers d'Avenir" du programme France 2030 opéré par la Caisse des dépôts.  
Financements possibles avec le FIAF pour les publics salariés.

## APPRENDRE UN MÉTIER

L'administrateur d'infrastructures sécurisées **veille à la mise en place, l'administration et la protection des réseaux et serveurs** d'une entreprise, sur site comme dans le cloud. Il assure la **supervision, la maintenance et la continuité de service** afin de garantir la performance et la sécurité des systèmes.

Face aux menaces, il **analyse les risques, applique des mesures de cybersécurité et intervient en cas d'incident**. Il conçoit également des solutions techniques pour **anticiper les évolutions**, qu'il teste puis intègre en production. Pédagogue et vigilant, il **sensibilise les utilisateurs** aux bonnes pratiques, tout en collaborant avec les techniciens, responsables informatiques et prestataires.

Son rôle combine **expertise technique et sens des responsabilités** pour maintenir des infrastructures fiables et sécurisées.

## ACTIVITÉS

### Administrer et sécuriser les infrastructures

- Appliquer les bonnes pratiques dans l'administration des infrastructures
- Administrer et sécuriser les infrastructures réseaux
- Administrer et sécuriser les infrastructures systèmes
- Administrer et sécuriser les infrastructures virtualisées

### Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

- Concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure
- Mettre en production des évolutions de l'infrastructure
- Mettre en œuvre et optimiser la supervision des infrastructures

### Participer à la gestion de la cybersécurité

- Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure
- Participer à l'élaboration et à la mise en œuvre de la politique de sécurité
- Participer à la détection et au traitement des incidents de sécurité

## PROFIL MÉTIER REQUIS

- Compétences en systèmes, réseaux, cloud et cybersécurité
- Capacité à diagnostiquer et résoudre des incidents
- Rigueur, organisation et sens des responsabilités
- Analyse, veille technologique et réactivité
- Bon relationnel et pédagogie auprès des utilisateurs
- Anglais technique

## EMPLOIS VISÉS

- Administrateur systèmes et réseaux
- Administrateur systèmes (et sécurité)
- Administrateur réseaux (et sécurité)
- Administrateur infrastructures
- Administrateur d'infrastructures et cloud
- Administrateur cybersécurité
- Responsable infrastructure systèmes et réseaux

## CONTENU DE LA FORMATION

La formation est validée par un **TITRE PROFESSIONNEL de niveau 6, délivré par le Ministère du Travail, de l'emploi et de l'insertion, équivalent à un BAC+3**. Elle est enregistrée au Répertoire National des Certifications Professionnelles sous le numéro de fiche **RNCP37680**.

**Pour obtenir le titre professionnel, les compétences des candidats seront évaluées au vu :**

- D'une mise en situation professionnelle, suivie d'un entretien technique avec le jury.
- D'un questionnaire professionnel en anglais.
- Du dossier Professionnel (DP).

Dans ce DP, les candidats décrivent par activité et à partir d'exemples concrets, les pratiques professionnelles en rapport direct et étroit avec le titre professionnel visé.

- Des résultats des ECF, évaluations réalisées pendant le parcours de formation.
- D'un entretien final avec le jury destiné à vérifier le niveau de maîtrise par le candidat des compétences requises pour l'exercice des activités auxquelles conduit le titre.

## RYTHME DE L'ALTERNANCE

La formation est dispensée à la CCI formation alternance située au centre ville de Nouméa par une équipe pédagogique et en entreprise (privée ou publique) par un tuteur.

**Durée : 14 mois.**

**70%**

Temps de formation  
en entreprise

**30%**

Temps de  
formation  
en école

**96%**  
des entreprises  
partenaires  
recommandent  
les écoles CCI

## CONDITIONS D'ADMISSION DES CANDIDATS

**Être titulaire d'un diplôme de niveau 5 (BAC+2)** à dominante systèmes/réseaux/cybersécurité (ex : BTS SIO, BTS CIEL, TP TSSR ou équivalent inscrit au RNCP). À défaut, avoir son **BAC et une expérience professionnelle d'au moins 3 ans** dans le domaine informatique. Disposer d'un ordinateur et d'une connexion internet à domicile. L'admission est conditionnée à la validation des différentes étapes du processus de recrutement.

La formation est également accessible **aux salariés en poste, avec au minimum 6 mois d'ancienneté** dans l'entreprise. Dans ce contexte, le FIAF peut étudier la prise en charge du **parcours diplômant**. Contactez le **FIAF** afin d'étudier les **possibilités de financement**.

### RECHERCHE D'ENTREPRISE



Dépôt de  
dossier

[www.pointa.nc](http://www.pointa.nc)  
[dossier@pointa.nc](mailto:dossier@pointa.nc)  
24 69 49

**2**

Questionnaire  
connaissances  
techniques

**3**

Entretien de  
motivation

**4**

Job dating

**5**

Signature du  
contrat

(Possibilité de le signer 2  
mois avant le début de la  
formation)

**6**

Début de la  
formation