

CPSRS

CHEF DE PROJET SYSTEMES, RESEAUX ET SECURITE

Formation menant à la certification Chef de projet systèmes, réseaux et sécurité, RNCP39115 Titre de niveau 6 reconnu par l'Etat, enregistré au Répertoire National des Certifications Professionnelles par décision du directeur général de France compétences en date du 31/05/2024 délivré sous l'autorité Sciences-U Lyon (accessible par la VAE).

OBJECTIFS

La croissance numérique et le métier de Chef de Projets Systèmes, réseaux et sécurité sont indissociables. Le Chef de Projets Systèmes, réseaux et sécurité est la clé de voûte entre les piliers opérationnels et les piliers stratégiques de la DSI. Il coordonne sous la responsabilité du manager de la DSI, les projets agiles de conception systèmes-réseaux et sécurité informatique, et est en mesure d'accompagner ses équipes dans l'aspect technique de la création des infrastructures systèmes et réseaux et leur sécurisation.

COMPÉTENCES DÉVELOPPÉES

- Concevoir une solution réseau - système d'information durable et sécurisée
- Réaliser, administrer et assurer l'évolutivité d'un système-réseau informatique sécurisé
- Conduire un projet informatique responsable
- Sécuriser des infrastructures systèmes et réseaux informatiques

DÉBOUCHÉS PROFESSIONNELS

- Administrateur(trice) système/ réseaux / infrastructure
- Superviseur(euse) réseaux/ Ingénieur (e) Système et réseaux
- Technicien(ienne) réseau et télécom
- Développeur(euse) Infrastructure réseaux
- Analyste d'exploitation informatique
- Chef(fe) de produit cybersécurité
- Technicien(ienne) parc, systèmes et réseaux / Technicien(ienne) système et réseaux
- Opérateur(trice) d'équipe support technicien
- Technicien(ienne) de maintenance système informatique
- Chef(fe) de projet IT

POURSUITE D'ÉTUDES/PASSERELLES ET INSERTION

- Formation de niveau 7 en Sécurité informatique (CFA de La Salle)
- Formation Ingénieur Informatique

68 % des certifiés poursuivent vers une certification de niveau 7 dans le secteur. 32% intègrent le monde professionnel dont 16% dans l'emploi visé.

PUBLICS ET PRÉREQUIS

Niveau requis :

Être titulaire d'une certification professionnelle de niveau 5 et/ou avoir validé 2 premières années d'enseignement supérieur (120 ECTS) dans le domaine visé par la certification professionnelle (administration logiciel et réseau/ de l'informatique avec par exemple : BTS SIO / CIEL, L2 info, BUT2 info réseaux télécom...)

Qualités attendues : Esprit logique et rigoureux, grande faculté d'adaptation, aptitude à tenir à jour ses connaissances et à suivre les évolutions technologiques, aptitude à la relation humaine et à la communication interpersonnelle.

ACCESSIBILITÉ

Pour l'accès à la formation, une rencontre avec le référent handicap permettra d'évaluer les possibilités d'adaptation : prise de contact alternance@groupe-saintjean.fr. Les locaux sont accessibles aux personnes à mobilité réduite.

MODALITES D'ACCES ET PROCÉDURE D'ADMISSION

L'admission ne peut être valide qu'à la signature du contrat d'apprentissage ou de professionnalisation avec l'entreprise d'accueil. Elle se déroule en 2 temps :

- 1- Candidater en ligne sur notre site
- 2- Après une session de tests, un entretien de motivation avec un membre de l'équipe pédagogique vous sera proposé.

Les candidatures sont ouvertes de début décembre à mi-juillet dans la limite des places disponibles.

VALIDATION

La validation de la certification prévoit le passage d'épreuves certifiantes, selon les modalités d'évaluation inscrites au référentiel.

Chaque bloc de formation fait l'objet d'une validation. La validation de l'ensemble des blocs de compétences permet la délivrance de la certification. Enfin, la validation est soumise à une période d'activité en entreprise minimale de 90 jours.

En cas de validation partielle, l'obtention de chaque bloc de compétences fait l'objet de la délivrance d'une attestation de compétences.

Les certifications TOEIC (anglais) et Voltaire (français) sont également proposées. La formation octroie un niveau 6 (Bac+3).

RÉSULTATS ET TAUX DE SATISFACTION

Résultats : Lors de la session 2025, le taux d'obtention de ce titre au CFA de La Salle a été de 100 %.

Taux de satisfaction : Nous nous engageons à évaluer le taux de satisfaction de nos alternants à la fin de chaque cycle. 100% des alternants de la promotion 2024-2025 sont satisfaits ou très satisfaits de la formation.

DURÉE ET RYTHME

Cette formation est dispensée sous contrat d'apprentissage ou de professionnalisation.

Durée : Le contrat est d'environ 12 mois. Les cours sont répartis sur 10 mois, d'août N à fin juin / début juillet N+1, soit 595 heures.

Rythme : Le rythme de l'alternance est de 1 à 2 semaines en centre de formation, 2 à 3 semaines en entreprise.

COÛT

Le coût de la formation est pris en charge par l'OPCO et l'entreprise, l'alternant n'avance aucun frais.

MODALITÉS

- 90 % des cours sont assurés par des professionnels de la cybersécurité
- Les cours sont dispensés en petits groupes
- Un accompagnement individualisé et personnalisé est assuré
- La formation se tient en présentiel

Moyens pédagogiques

- Cours
- Mini-projets
- Projet annuel
- E-learning

Moyens techniques

- Accès wifi dans tout l'établissement
- Laboratoires réseaux (équipement Cisco)
- CyberRange Airbus - Simulateur Cyberdéfense
- Centre de ressources documentaires...

PROGRAMME

Concevoir une solution réseau - système d'information durable et sécurisée

- Conception et sécurité des bases de données
- Réseau Informatique & CISCO
- Supervision du Système d'Information
- Linux avancé
- Scripting Shell

Réaliser, administrer et assurer l'évolutivité d'un système-réseau informatique sécurisé

- Algo et Python
- Langage C
- Scripting Shell
- Linux avancé
- Supervision du Système d'Information
- Réseau Informatique
- Hacking éthique

Conduire un projet informatique responsable

- Planification de projets SI
- Communication & Anglais professionnel

Sécuriser des infrastructures systèmes et réseaux informatiques

- Linux avancé
- Supervision du Système d'Information
- Assembleur x86
- Cryptologie
- Détection et analyse de vulnérabilités
- Analyse de risques et intrusion physique
- Sécurité wifi
- Hardening des OS
- Forensic
- Réseau Informatique
- Hacking éthique
- OSINT et Ingénierie sociale