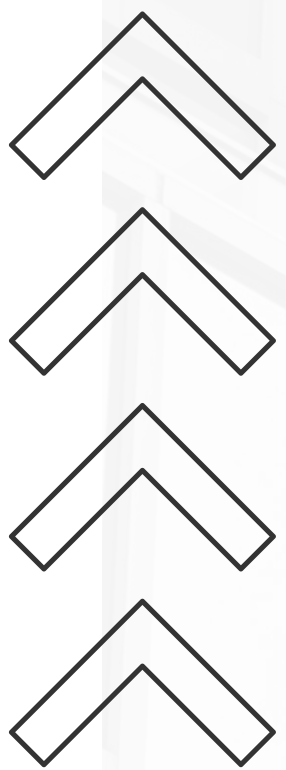


# PROGRAMME DE FORMATION

**Développer et sécuriser des  
infrastructures réseaux IP et  
WiFi en environnement  
professionnel**



+33 7 61 71 00 54

[skillup.conseil@gmail.com](mailto:skillup.conseil@gmail.com)



**Modalités d'admission et de déroulement :**

Pour toutes nos formations, merci de vous inscrire par courrier, par mail, ou par téléphone. Votre demande d'inscription sera traitée dans un délai de deux jours ouvrés. Toute commande de formation doit faire l'objet d'une confirmation écrite et suppose que le client accepte le contenu du stage et les prérequis, dont il s'engage à avoir eu connaissance. La formation ne pourra débuter qu'au moins après les 10 jours calendaires suivant la réception du bon de commande.

**Lieu de la formation**

La formation se déroule en présentiel en région parisienne

**Accessibilité pour les personnes en situation de handicap :**

Cette formation est accessible aux personnes en situation de handicap. Le référent en la matière se tient à votre écoute pour évaluer puis préciser votre projet de formation et anticiper les éventuels aménagements à réaliser pour vous accueillir.

Contact : 07 61 71 00 56 / [skillup.conseil@gmail.com](mailto:skillup.conseil@gmail.com)

**Délai et modalités d'accès**

Le délai d'accès à la formation est de 10 à 20 jours suite à l'inscription auprès du référent pédagogique.

**Prérequis d'accès à la formation**

- Maîtriser les bases de l'utilisation d'un ordinateur et d'un environnement numérique
- Connaître les principes fondamentaux des réseaux informatiques
- Disposer de notions élémentaires sur l'adressage IP et les équipements réseaux
- Être amené à intervenir sur des infrastructures réseau ou WiFi en environnement professionnel

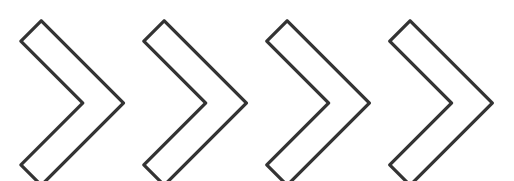
**Public concerné**

- Techniciens réseaux
- Administrateurs systèmes et réseaux
- Responsables informatiques
- Techniciens support
- Toute personne souhaitant développer des compétences en déploiement et sécurisation des infrastructures IP et WiFi

**Objectifs et compétences visées**

À l'issue de la formation, les participants seront capables de :

- Identifier les composants et le fonctionnement d'une infrastructure réseau IP et WiFi professionnelle
- Configurer et déployer des équipements réseaux filaires et sans fil en environnement professionnel
- Structurer et sécuriser un réseau à l'aide des mécanismes de segmentation, de contrôle d'accès et des protocoles WiFi sécurisés
- Diagnostiquer les incidents réseaux et appliquer des procédures de résolution adaptées
- Superviser les performances d'une infrastructure réseau et appliquer les bonnes pratiques de cybersécurité



### Méthodes pédagogiques mobilisées

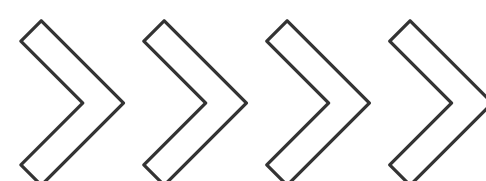
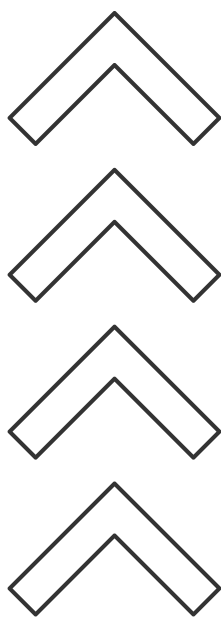
- Présentiel interactif : formation en salle avec aménagement favorisant les échanges et les travaux collaboratifs
- Supports multimédia : démonstrations techniques, vidéos pédagogiques et outils de supervision réseau
- Documentation personnalisée : remise d'un support pédagogique complet et de fiches pratiques
- Études de cas : analyses d'architectures réseaux réelles en environnement professionnel
- Travaux pratiques : configuration d'équipements réseau, paramétrage WiFi et tests de sécurité
- Accompagnement individualisé : assistance technique durant les ateliers pratiques
- Évaluations formatives : quiz techniques, exercices de validation et mises en situation professionnelles

### Durée

14 heures

### Tarif

600 €



## Planning de formation

### Jour 1 : Cartographier les activités de l'entreprise et identifier les leviers digitaux

08h00 - 08h30 : Introduction et recueil des attentes

- Présenter les objectifs de la formation
- Identifier les attentes spécifiques des participants
- Expliquer le déroulé pédagogique et les méthodes utilisées

08h30 - 10h00 : Comprendre les processus métier et les points de friction

- Cartographier les processus clés d'une entreprise
- Repérer les activités à forte valeur ajoutée ou génératrices de coûts
- Identifier les dysfonctionnements, lenteurs ou doublons

10h00 - 10h15 : Pause

10h15 - 12h00 : Panorama des leviers digitaux disponibles

- Présenter les grandes familles d'outils : Cloud, SaaS, automatisation, data, collaboration
- Identifier les usages transverses (CRM, ERP, GED, outils collaboratifs)
- Étudier des cas concrets de digitalisation réussie

12h00 - 13h30 : Pause déjeuner

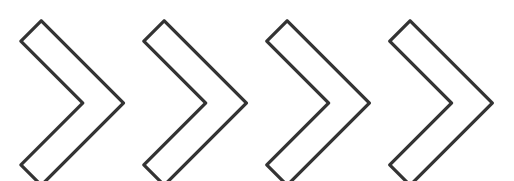
13h30 - 15h00 : Méthodologie de repérage des opportunités digitales

- Élaborer une grille d'analyse des besoins métiers
- Faire le lien entre problème opérationnel et solution digitale
- Structurer une démarche d'identification des priorités

15h00 - 15h15 : Pause

15h15 - 17h00 : Atelier – Diagnostic d'un processus métier

- Appliquer la méthodologie sur un cas réel ou simulé
- Cartographier le processus et repérer les points d'amélioration
- Présenter les premiers leviers digitaux envisagés



## Jour 2 : Sécuriser et superviser les infrastructures réseaux IP et WiFi

08h00 – 08h30 : Réactivation des acquis et analyse des pratiques

- Réviser les notions essentielles abordées lors de la première journée
- Identifier les difficultés rencontrées lors des ateliers pratiques
- Structurer les bonnes pratiques de gestion d'infrastructures réseaux

08h30 – 10h00 : Sécurisation des infrastructures IP

- Identifier les principales menaces réseaux en environnement professionnel
- Configurer les mécanismes de filtrage et de contrôle d'accès
- Mettre en œuvre les bonnes pratiques de sécurisation des équipements réseau

10h00 – 10h15 : Pause

10h15 – 12h00 : Sécurisation des réseaux WiFi professionnels

- Configurer les protocoles de sécurité WPA2 et WPA3
- Mettre en œuvre une authentification sécurisée des utilisateurs
- Analyser les risques liés aux accès sans fil non sécurisés

12h00 – 13h30 : Pause déjeuner

13h30 – 15h00 : Supervision et diagnostic des infrastructures réseaux

- Utiliser des outils de supervision et d'analyse réseau
- Interpréter les indicateurs de performance et de disponibilité
- Diagnostiquer les incidents et appliquer des procédures correctives

15h00 – 15h15 : Pause

15h15 – 17h00 : Mise en situation professionnelle et évaluation finale

- Réaliser une configuration complète d'une infrastructure réseau sécurisée
- Appliquer les procédures de sécurisation et de contrôle des accès
- Présenter les solutions mises en œuvre et argumenter les choix techniques réalisés

### Méthode d'évaluation

Évaluation finale sous forme de mise en situation technique complète durant laquelle chaque participant devra configurer, sécuriser et tester une infrastructure réseau IP et WiFi professionnelle, suivie d'un débriefing individualisé avec le formateur.

