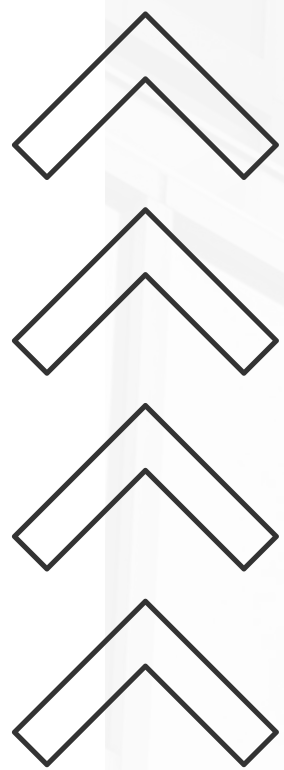


PROGRAMME DE FORMATION

**Optimiser la gestion des
services numériques et des
infrastructures sécurisées**



+33 7 61 71 00 54

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

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

- Posséder des connaissances de base en environnement informatique et réseaux
- Utiliser régulièrement des outils numériques en contexte professionnel

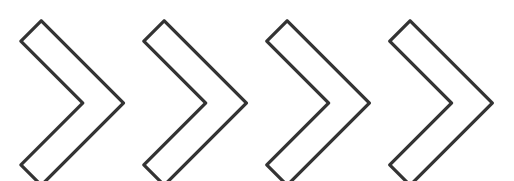
Public concerné

- Responsables informatiques
- Administrateurs systèmes et réseaux
- Techniciens infrastructures
- Responsables sécurité informatique
- Chefs de projets numériques
- Toute personne souhaitant renforcer ses compétences en gestion des services numériques sécurisés

Objectifs et compétences visées

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

- Identifier les enjeux stratégiques liés à la gestion des services numériques et à la sécurisation des infrastructures informatiques
- Analyser les vulnérabilités, risques et incidents susceptibles d'impacter les systèmes d'information
- Mettre en œuvre des mesures de protection, de supervision et de contrôle des accès adaptées aux environnements numériques
- Structurer des procédures de continuité, de maintenance et d'amélioration continue des services numériques sécurisés
- Appliquer les bonnes pratiques de gouvernance, de conformité réglementaire et de cybersécurité dans un contexte professionnel



Méthodes pédagogiques mobilisées

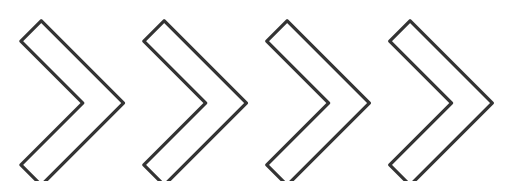
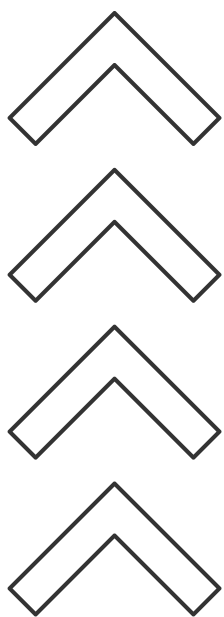
- Présentiel interactif : Formation en salle avec aménagement favorisant les interactions et travaux de groupe
- Supports multimédia : Utilisation de vidéos, présentations dynamiques et outils digitaux pour illustrer les concepts
- Documentation personnalisée : Remise d'un livret pédagogique complet et d'outils pratiques adaptés au contexte des participants
- Accompagnement individualisé : Temps dédiés au coaching individuel et à la personnalisation des apprentissages
- Évaluations formatives : Exercices d'auto-évaluation et quiz permettant de mesurer la progression des acquis tout au long de la formation.

Durée

14 heures

Tarif

600 €



Planning de formation

Jour 1 : Gouvernance des services numériques et sécurisation des infrastructures

08h00 – 08h30 : Accueil des participants et cadrage de la formation

- Présenter les objectifs pédagogiques et le déroulement de la formation
- Identifier les attentes et besoins des participants
- Introduire les enjeux actuels des services numériques sécurisés

08h30 – 10h00 : Fondamentaux des infrastructures numériques sécurisées

- Identifier les composants d'une infrastructure informatique moderne
- Analyser les risques liés aux réseaux, serveurs et services cloud
- Comprendre les principes fondamentaux de cybersécurité et de disponibilité des services

10h00 – 10h15 : Pause

10h15 – 12h00 : Organisation et gestion des services numériques

- Structurer les processus de gestion des services informatiques
- Définir les rôles et responsabilités dans une organisation numérique
- Mettre en œuvre des procédures de supervision et de maintenance

12h00 – 13h30 : Pause déjeuner

13h30 – 15h00 : Sécurisation des accès et protection des données

- Identifier les mécanismes d'authentification et de contrôle d'accès
- Appliquer les bonnes pratiques de gestion des mots de passe et habilitations
- Mettre en œuvre des stratégies de sauvegarde et de protection des données sensibles

15h00 – 15h15 : Pause

15h15 – 17h00 : Gestion des vulnérabilités et prévention des cybermenaces

- Détecter les principales vulnérabilités des systèmes et réseaux
- Analyser les typologies d'attaques informatiques courantes
- Élaborer des mesures préventives adaptées aux infrastructures numériques



Jour 2 : Supervision, continuité des services et amélioration continue

08h00 – 08h30 : Réactivation des acquis et revue des notions clés

- Consolider les connaissances acquises lors de la première journée
- Répondre aux questions techniques des participants
- Préparer les activités pratiques de la journée

08h30 – 10h00 : Supervision et surveillance des infrastructures

- Utiliser des outils de monitoring et de supervision des services numériques
- Identifier les indicateurs de performance et de sécurité
- Configurer des alertes et mécanismes de détection d'incidents

10h00 – 10h15 : Pause

10h15 – 12h00 : Gestion des incidents et continuité d'activité

- Mettre en œuvre une procédure de gestion des incidents informatiques
- Élaborer un plan de continuité et de reprise d'activité
- Organiser la communication et la coordination en situation de crise numérique

12h00 – 13h30 : Pause déjeuner

13h30 – 15h00 : Gouvernance numérique et conformité réglementaire

- Identifier les obligations réglementaires liées à la sécurité numérique
- Appliquer les principes de gouvernance des systèmes d'information
- Structurer une démarche d'amélioration continue de la sécurité informatique

15h00 – 15h15 : Pause

15h15 – 17h00 : Atelier pratique et évaluation finale

- Réaliser une analyse de cas d'infrastructure numérique sécurisée
- Construire un plan d'optimisation des services numériques
- Présenter les solutions proposées et argumenter les choix techniques

Méthode d'évaluation

Évaluation finale sous forme de mise en situation professionnelle portant sur l'analyse, la sécurisation et l'optimisation d'une infrastructure numérique. Chaque participant devra démontrer sa capacité à identifier les risques, proposer des solutions adaptées et structurer un plan d'amélioration opérationnel, suivi d'un débriefing personnalisé avec le formateur.

