

CONCOURS ITRF – SESSION 2024
Fiche de poste

Administrateur-trice réseau et sécurité

Corps : Ingénieur-e d'études de recherche et de formation

Nature du concours : externe

Branche d'activités professionnelles (B.A.P.) : BAP E « Informatique, Statistiques et Calcul scientifique »

Emploi-type : Administrateur-trice systèmes et réseaux

Localisation du poste : Université de Montpellier – Direction du Système d'Information et du Numérique (DSIN)

Nombre de poste : 1

Descriptif des activités de la structure :

La Direction du Système d'Information et du Numérique (DSIN) est composée d'une centaine d'agents répartis sur 5 services. Elle met en œuvre la politique des systèmes d'information et des technologies de l'information et de la communication définie par l'Université de Montpellier dans les domaines de l'enseignement, de la recherche, de la documentation et de la gestion et, d'une manière plus générale, à tout ce qui a une relation avec le traitement informatisé ou numérique de l'information.

Mission principale :

Au sein du « Service Infrastructure et Cloud - SIC » dans le bureau « Réseau, sécurité et TOIP » l'administrateur-trice des systèmes, réseaux et télécommunications a en charge la mise en place et l'exploitation des moyens informatiques, matériels, logiciels et de sécurité sur tous les sites gérés de l'Université de Montpellier (périmètre : 7000 points de connexion dans 250 locaux techniques, sites géographiques répartis sur la région, 40 km de fibre noire sur les villes de Montpellier et Nîmes). Sa mission s'inscrit dans un contexte d'évolution des pratiques vers plus d'agilité.

Activités :

L'administrateur-trice réseau et sécurité assure l'exploitation des équipements pour le maintien en conditions opérationnelles et de sécurité des infrastructures. Pour atteindre cet objectif il-elle réalise les activités suivantes :

- Étudier, concevoir et mettre en place des architectures réseaux sécurisées (réseaux fédérateurs, réseaux de campus, réseaux locaux, gardes-barrières)
- Mettre en place les outils de mesure de performance du réseau, établir les procédures d'analyse des résultats
- Administrer, superviser et faire évoluer le réseau, la téléphonie IP et les services associés (DNS, haute-disponibilité, répartiteur de charge, ...)
- Installer, administrer et faire évoluer les équipements de sécurité et les services associés (garde-barrières, IPS, certificats)
- Gérer le fonctionnement du PRA/PCA pour les applications/services critiques
- Mettre en place les accès distants sécurisés (VPN utilisateurs, VPN site à site, ...)
- Gérer l'interconnexion de l'entité avec les réseaux extérieurs (HdMon, THDoc, RENATER)
- Gérer la mobilité des usagers avec l'exploitation du réseau WiFi (1200 bornes), la sécurité associée et les serveurs d'authentification unifiés
- Établir les politiques de sécurité et appliquer les règles correspondantes sur les équipements
- Assurer la distribution du courriel et identifier les messages indésirables (anti spam, phishing,...).
- Assurer la veille technologique et pratiquer des audits
- Prendre en charge la responsabilité de projets
- Négocier avec les fournisseurs et les prestataires de services

- Assister et conseiller les utilisateurs en matière de sécurité (résolution ou remontée des incidents et optimisation des performances)
- Participer aux actions de formation et d'accompagnement des utilisateurs sur les aspects réseaux et sécurité
- Anticiper les contraintes environnementales et techniques
- Rédiger des comptes rendus d'intervention, des notices utilisateurs, des procédures

Compétences

- **Connaissances**

- Maîtrise des technologies, protocoles et outils des systèmes de communication et de télécommunication
- Maîtrise des concepts et techniques d'architecture des systèmes, des réseaux et de la téléphonie
- Maîtrise des mécanismes de mise en œuvre des processus autour de la sécurité informatique
- Avoir une connaissance approfondie des normes et activités liées à la gestion des moyens informatiques
- Avoir une connaissance approfondie des systèmes d'exploitation Linux
- Connaître un outil de virtualisation système
- Connaître des langages de script
- Connaître les pratiques et outils DevOps

- **Compétences opérationnelles :**

- Savoir piloter des opérations ou des projets techniques complexes
- Savoir adapter les nouvelles technologies aux besoins et prendre en compte l'impact de leur introduction
- Savoir analyser et résoudre des problèmes complexes sur les infrastructures ;
- Savoir gérer les situations d'urgence et les priorités
- Savoir rédiger des documents d'analyse et de synthèse
- Appliquer les normes et standards de sécurité
- Maîtriser les outils de bureautique et de présentation
- Maîtriser l'anglais technique du domaine

- **Compétences comportementales :**

- Savoir travailler en équipe et partager son expérience
- Savoir dialoguer avec les utilisateurs en s'adaptant à leurs attentes
- Savoir être organisé, rigoureux et méthodique
- Savoir rendre compte de son travail
- Savoir respecter la confidentialité
- Savoir être force de proposition et innovant
- Être capable de gérer des situations d'urgence et hiérarchiser les priorités.

Domaine de formation souhaité : filière informatique

Contraintes du poste :

- Horaires décalés suivant nécessité de service
- Disponibilité et réactivité en cas d'incidents de sécurité concernant le système d'information

Conditions particulières d'exercice :

- Déplacements fréquents, port de charges lourdes
- Contrainte forte de continuité de service (services réseaux, examens numériques,)
- Contraintes horaires en fonction des pics d'activité