

Titre d'emploi: Conseiller, Gestion des identités et des accès



OFFRE D'EMPLOI

Demande N°: 12090

Titre: Conseiller, Gestion des identités et des accès
Supérieur: Chef, Opération cyber sécurité
Lieu de travail: Siège social
Statut: Indéterminé, temps plein
Groupe d'employés: non assujetti
Échelle salariale: Classe E
Date d'affichage du 2 octobre 2026
Motif de l'affichage: Création de poste

SOMMAIRE

Le ou la titulaire du poste est responsable de la définition, de l'évolution, de l'opérationnalisation et de la gouvernance des capacités de gestion des identités, des permissions et des accès à privilèges de l'organisation. Dans un environnement aéroportuaire critique et fortement réglementé, la personne assure que les mécanismes d'accès aux systèmes, aux applications et aux infrastructures d'ADM sont sécuritaires, maîtrisés, conformes et alignés avec les besoins opérationnels, tout au long du cycle de vie des identités. Elle agit comme référence organisationnelle pour les sujets de gestion des accès et contribue directement à la réduction du risque cyber.

RÔLE ET RESPONSABILITÉS

- Définir la vision et les orientations des capacités de gestion des identités et des accès, en cohérence avec la stratégie de cybersécurité d'ADM.
- Élaborer et maintenir la feuille de route des capacités de gestion des identités et des accès et d'accès à privilèges.
- Assurer l'alignement avec les exigences réglementaires, les obligations de conformité et les priorités organisationnelles.
- Encadrer la gestion du cycle de vie des identités (employés, contractuels, fournisseurs, comptes techniques).
- Définir et faire évoluer les modèles d'attribution des droits d'accès (rôles, attributs, séparation des tâches).
- Veiller à l'application des principes de moindre privilège et de contrôle rigoureux des accès.
- Piloter les mécanismes de contrôle des accès à privilèges pour les environnements technologiques et opérationnels.
- Encadrer la gestion sécurisée des comptes à privilèges et des comptes techniques.
- Assurer la traçabilité, la journalisation et la supervision des accès sensibles.
- Prioriser les besoins en fonction des risques, des impacts opérationnels et des exigences de sécurité.
- Assurer la cohérence entre la conception, la mise en œuvre et l'exploitation des solutions.
- Assurer la coordination, l'encadrement et la supervision des fournisseurs technologiques et des fournisseurs de services de sécurité gérés (MSSP), en collaboration avec les équipes internes, afin de garantir la qualité, la conformité et l'atteinte des objectifs collectifs dans ce domaine.
- Conseiller les équipes d'affaires et techniques sur les bonnes pratiques en matière de gestion des accès.
- Participer à la sensibilisation et à l'adoption des contrôles de sécurité liés aux accès.
- Agir comme point de référence interne pour les sujets de gestion des identités et des accès et accès à privilèges.

EXIGENCES

- Diplôme universitaire de premier cycle en informatique, cybersécurité ou domaine connexe toute combinaison équivalente de formation et d'expérience pourra être considérée.
- Minimum de dix (10) années d'expérience en cybersécurité, gestion des identités, gestion des accès ou gouvernance de la sécurité.
- Expérience en rôle de coordination, de gouvernance ou de pilotage transversal.
- Expérience en environnements technologiques hybrides (sur site et infonuagiques).

- Maîtrise de la suite bureautique de MS Office.
- Souci du détail et bonne gestion des priorités, avoir le sens de l'organisation.
- Posséder de l'initiative et un bon jugement.
- Avoir une bonne capacité d'adaptation aux changements.
- Excellente maîtrise du français et de l'anglais (parlé et écrit), pour assurer les échanges avec les partenaires et intervenants externes et la communauté aéroportuaire.
- Passer avec succès la cote d'enquête pour l'obtention du laissez-passer pour zones réglementées.

Ce concours est ouvert simultanément à l'interne et à l'externe; cependant, les candidatures provenant de l'interne seront traitées en priorité.

Nous vous remercions de l'intérêt porté envers ADM. Seules les candidatures sélectionnées seront contactées.