Titre d’emploi: Conseiller senior gouvernance cybersécurité

OFFRE D'EMPLOI

Demande N°: 10850

Titre: Conseiller senior, Gouvernance cybersécurité
Supérieur: Directeur, Sécurité de l'information et transformation TI
Lieu de travail: Siège social
Statut: Indéterminé, temps plein
Groupe d'employés: assujeti à la convention collective des employés administratifs, professionnels et du soutien administratif
Échelle salariale: Classe 11
Date d'affichage du 7 mai 2024
Motif de l'affichage:

SOMMAIRE

Relevant du Directeur, sécurité de l’information et transformation TI, le Responsable gouvernance cybersécurité oriente, formalise et implante des éléments de gouvernance tels que les politiques, les directives, les processus de sécurité incluant la sensibilisation, la gestion du registre des risques cyber, le programme de conformité et d’audit interne et le suivi de la sécurité des tiers. Son périmètre couvre les Technologies de l’Information (TI) et les Technologies Opérationnelles (TO).

RÔLE ET RESPONSABILITÉS

- Contribuer à la définition et formalisation des politiques et directives de cybersécurité;
- Lancer les initiatives et projets nécessaires à l’implantation des politiques et directives de sécurité;
- Définir et mettre à jour le processus de gestion des risques cybersécurité, incluant les rôles et responsabilités, les activités et le workflow opérationnel;
- S’assurer que l’outillage de gestion des risques et de sensibilisation est aligné avec les politiques, directives et workflows et lancer les éventuelles initiatives et projets nécessaires;
- Agir à titre de principale personne-ressource et d’agent de liaison, ainsi qu’à titre d’expert pour les enjeux de gouvernance de cybersécurité;
- Assurer le pilotage de la gestion de risques : suivi de l’avancement des plans de traitement des risques, contribution aux décisions de traitement des risques, gestion des escalades décisionnelles, indicateurs et tableaux de bord, etc.;
- Définir et piloter le programme de sensibilisation des utilisateurs TI et TO au sens large : employés, partenaires, administrateurs, VIP. Le plan de sensibilisation inclut la formation, la communication et la simulation d’hameçonnage, les indicateurs et tableaux de bord;
- Gérer le programme de conformité cybersécurité d’ADM, incluant PCI DSS, Loi 25 pour les aspects cyber, future loi C26, etc;
- Planifier les différentes évaluations et audits internes de cybersécurité et suivre l’implantation des recommandations en découlant;
- Gérer le processus de sécurité des tiers (fournisseurs, partenaires, consultants, etc.);
- Définir les clauses de sécurité contractuelles, SLA cyber, niveaux de certifications nécessaires et suivre l’application de ces exigences dans le temps auprès des différents fournisseurs;
- Proposer des améliorations aux outils et processus de sécurité d’ADM afin d’accroitre la posture de sécurité;
- Collaborer avec le processus de gestion des risques corporatifs;
- Contribuer aux spécifications des attentes pour les évolutions de nos solutions de sécurité (DLP, VPN, pare-feu, etc.);
- Synthétiser les informations pertinentes relatives aux activités de cybersécurité pour communication aux Vice-Présidents, Président et au Conseil d’Administration;
- Contribuer à l’élaboration de la stratégie de cybersécurité et de la feuille de route;
- Apporter une contribution à d’autres chantiers, projets et processus relatifs à la cybersécurité;

- Peut être appelé à représenter ADM dans le cadre de différents forums;
- Effectue toutes autres tâches connexes à la fonction.

EXIGENCES

- Détenir un baccalauréat en technologies de l'information ou dans une discipline connexe;
- Posséder un minimum de dix (10) ans d'expérience dans le domaine de la cybersécurité. Une combinaison de formation et expérience pertinentes pourrait être considéré;
- Détenir une certification en matière de sécurité (ISO 2700X, CISSP, PCI DSS...);
- Expérience en sécurité des Technologies Opérationnelles pourrait être considéré comme un atout;
- Avoir une bonne aptitude aux travaux conceptuels : définition de processus, principes de gestion des risques, etc.;
- Avoir de bonnes aptitudes à l'apprentissage et à l'acquisition de nouveaux savoir-faire;
- Disposer de bonnes capacités de communication, de synthèse et de vulgarisation des concepts complexes;
- Expérience significative en gestion de risques;
- Excellentes capacités d'analyse/habiletés en résolutions de problèmes;
- Capacité à comprendre la réalité d'affaires des différentes entités d'ADM;
- Maîtrise du français (parlé et écrit);
- Bonnes aptitudes en anglais (parlé et écrit);
- Esprit d'équipe;
- Capacité de planification, d'organisation et de priorisation;
- Passer avec succès la cote d'enquête pour l'obtention du laisser-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.