Chambre de l'assurance

Conseiller(ère) principal(e), opérations TI et cybersécurité

Qui sommes-nous?

La Chambre de l'assurance a le mandat d'assurer un niveau élevé de protection du public en offrant un encadrement de qualité au secteur de l'assurance. Elle veille à la déontologie, à la discipline et à la formation continue de ses membres. La Chambre de l'assurance est née de la fusion de deux organismes à l'été 2025 : la Chambre de la sécurité financière (CSF) et la Chambre de l'assurance de dommages (ChAD).

À la hauteur du défi?

Relevant du Directeur Numérique, le conseiller principal, opérations TI et cybersécurité assure le bon fonctionnement, la fiabilité et la sécurité de l'architecture technologique de l'organisation. Il agit à la fois comme expert technique *hands-on* sur les systèmes, comme responsable de la livraison de projets d'architecture, et comme point d'ancrage interne de la surveillance cyber assurée en collaboration avec un SOC externe. Le conseiller agira à titre de pivot central à la gestion des opérations TI.

Ce rôle d'expert au sein d'une équipe d'une dizaine de personnes s'adresse à une personne autonome, capable de jongler entre les opérations courantes, l'avancement de projets et la vigilance en matière de sécurité informatique, et ayant de l'initiative.

Vos principales responsabilités

Opérations et administration des systèmes (volet principal)

En collaboration avec le responsable de l'infrastructure :

- Administrer, maintenir et optimiser les serveurs, le réseau, les environnements virtualisés et les services infonuagiques de l'organisation
- Assurer la disponibilité, la performance et la sauvegarde des systèmes critiques

Chambre de l'assurance

- Diagnostiquer et résoudre les incidents techniques de niveau avancé, incluant l'escalade et la coordination avec les fournisseurs
- Maintenir à jour la documentation technique, les configurations et les procédures opérationnelles
- Participer à la gestion des accès et du parc technologique

Cybersécurité et surveillance (en collaboration avec le SOC externe)

- Agir comme point de contact interne du SOC externe et coordonner le suivi des alertes, incidents et recommandations
- Participer à l'analyse et aux réponses aux incidents de sécurité, en lien avec l'équipe externe
- Mettre en œuvre et maintenir les contrôles de sécurité (gestion des correctifs, renforcement des systèmes, gestion des vulnérabilités, configuration des outils de protection)
- Contribuer à l'application des politiques de sécurité et à la conformité des normes applicables
- En collaboration avec la conseillère en gouvernance, assurer une veille sur les menaces et les bonnes pratiques en cybersécurité

Gestion de projets d'architecture

- En collaboration avec l'architecte de solution, planifier et livrer des projets d'amélioration ou de modernisation de l'infrastructure (migrations, mises à niveau, déploiement de nouvelles solutions)
- Évaluer les besoins technologiques, recommander des solutions et estimer les efforts requis
- Coordonner les intervenants internes et les fournisseurs externes tout au long des projets

Votre formation

- Diplôme en informatique, en génie informatique ou dans un domaine connexe (ou expérience équivalente)
- Une ou plusieurs certifications, tel que Microsoft, VMware, ainsi que des certifications en sécurité comme CompTIA Security+ — un atout

Votre expérience

- Minimum de huit ans d'expérience pertinente en administration de systèmes et en infrastructure TI
- Expérience concrète en cybersécurité, idéalement en collaboration avec un SOC ou un fournisseur de services de sécurité gérés

Vos compétences et aptitudes

- Maîtrise approfondie des environnements serveurs (Windows, Linux), de la réseautique et de la virtualisation
- Bonne connaissance des plateformes infonuagiques, tel qu'Azure et M365
- Connaissance des principes et outils de cybersécurité (pare-feu, EDR/XDR, SIEM, gestion des identités, gestion des vulnérabilités)

- Compréhension des cadres de référence en sécurité (ISO 27001) — un atout
- Capacité à gérer plusieurs priorités simultanément
- Rigueur, sens de l'organisation et souci de la documentation
- Habileté à communiquer avec des intervenants techniques et non techniques
- Esprit d'analyse et approche structurée de résolution de problèmes
- Aptitude à collaborer efficacement avec des fournisseurs et partenaires externes

Nous offrons

- Poste permanent 35 h (lundi au vendredi) par semaine, horaire flexible et mode de travail hybride
- Rémunération alignée sur le marché : échelle salariale entre 92 968 $ et 139 452 $
- Large gamme d'avantages sociaux compétitifs : REER comprenant une généreuse cotisation de l'employeur, assurances collectives dont la prime est majoritairement payée par l'employeur, minimum de 3 semaines de vacances, congés personnels, 13 jours fériés
- Équipe conviviale et des initiatives de groupe favorisant la collaboration
- Environnement de travail sain et des activités de bien-être au travail
- Bureau au cœur du centre-ville, connecté au réseau souterrain et facilement accessible en transports en commun ou en transport actif

Important : Le poste requière occasionnellement de travailler en dehors des heures régulières, pour des interventions critiques ou la coordination d'incidents de sécurité.

Prêt à relever le défi?

Vous êtes passionné par les infrastructures TI, les projets technologiques et la cybersécurité? Vous souhaitez jouer un rôle de pivot au sein d'une équipe collaborative, où votre expertise contribuera autant au maintien des opérations critiques qu'à la réalisation d'initiatives stratégiques de modernisation? Ce défi est pour vous.

Merci de faire parvenir votre candidature à recrutement@chambresf.com avec un court courriel expliquant votre motivation pour le poste. Les candidatures sont acceptées jusqu'au vendredi 24 juillet 2026. Les candidatures retenues seront contactées dans la semaine du 27 juillet 2026.