INTERNE/EXTERNE

La Direction des Systèmes d'Information
***R*echerche un Responsable Sécurité des Systèmes d'Information** (H/F) - **(Réf. 5191)**
Dans le cadre d'emplois des Ingénieurs territoriaux

MISSIONS

Sous la responsabilité du Directeur des Systèmes d'Information, vous assurez le pilotage de la démarche de cybersécurité sur un périmètre organisationnel et/ou géographique au sein de la collectivité. Vous définissez et déclinez, la politique de sécurité des systèmes d'information (prévention, protection, détection, résilience, remédiation) et veillez à son application. Vous assurez un rôle de conseil, d'assistance, d'information, de formation et d'alerte, en particulier auprès de la Direction Générale. Vous vous assurez de la mise en place des solutions et des processus opérationnels pour garantir la protection des données et le niveau de sécurité des SI. Vous jouez un rôle opérationnel dans la mise en œuvre de la politique de sécurité des SI. A ce titre, vos principales missions sont les suivantes :

IDENTIFIER :

- Décliner les axes et les objectifs stratégiques en matière de cybersécurité pour la Collectivité et les faire valider par la Direction
- Identifier les enjeux et les risques de sécurité majeurs sur votre périmètre
- Décliner et maintenir la politique de sécurité des SI en collaboration avec les parties prenantes
- Définir un plan d'actions annuel ou pluriannuel sur votre périmètre
- Définir une politique d'investissement au regard des objectifs de sécurité
- Contribuer à définir l'organisation de la cybersécurité au sein de la Collectivité et l'animer
- Suivre les évolutions réglementaires et techniques de votre domaine ; assurer les relations avec les acteurs du secteur public autour de la cybersécurité

PROTEGER :

- Organiser les structures de pilotage des plans d'actions de sécurité au sein des entités
- Définir les mesures organisationnelles et techniques à mettre en œuvre pour atteindre les objectifs de sécurité
- Assurer un support à la mise en œuvre en fournissant une assistance technique et méthodologique ainsi que des outils et services de sécurité, éventuellement à travers un catalogue de services
- Diffuser une culture SSI à destination des utilisateurs et décideurs
- Assurer la promotion des chartes de sécurité informatique sur votre périmètre
- Évaluer le niveau de sécurité au sein de votre périmètre, notamment à travers la réalisation d'audits périodiques et de contrôles permanents
- Contrôler que les politiques et règles de sécurité des SI sont appliquées sur votre périmètre et vis-à-vis des tiers et sous-traitants
- Contribuer à répondre aux sollicitations des prospects et des clients de l'organisation sur les aspects sécurité (dans le cadre d'appels d'offres)

DETECTER :

- Prendre les mesures techniques et organisationnelles permettant la surveillance des événements de sécurité, l'appréciation des incidents de sécurité et la réaction face aux attaques, assurer la mise en place d'un SOC (Security Operation Center)

REPONDRE :

- Veiller à ce que le dispositif de gestion de crise de sécurité soit opérationnel
- Contribuer au pilotage de la gestion des incidents et des crises de sécurité, le cas échéant en lien avec le CSIRT (Computer Security Incident Response Team)

ASSURER LA CONTINUITE ET RECONSTRUIRE :

- Préparer et mettre en œuvre un plan de continuité informatique, dans le cadre du plan de continuité des activités (PCA)
- Préparer et mettre en œuvre un plan de reprise informatique, dans le cadre du plan de reprise des activités (PRA)
- Proposer la stratégie de cyber-résilience

RENDRE COMPTE :

- Rapporter régulièrement auprès de votre hiérarchie sur le niveau de couverture courant des risques de sécurité SI
- Assurer un rôle de conseil auprès de votre hiérarchie et des métiers de votre périmètre
- Représenter l'organisation dans les relations avec les autorités de régulation

Participation à l'astreinte informatique (2 à 3 fois par an).

PROFIL ATTENDU

Titulaire d'un t**itre d'ingénieur ou d'un MASTER spécialisé dans le domaine de la stratégie ou de la conception des systèmes d'information**), vous pouvez faire valoir une **expérience dans des fonctions similaires**, idéalement en collectivité territoriale ainsi qu'une maîtrise du **cadre réglementaire** (RGPD notamment). Une bonne connaissance des procédures des marchés publics.

Recrutement par voie statutaire (titulaires, lauréats de concours) ou à défaut par voie contractuelle

Pour tous renseignements, vous pouvez contacter le Chargé de Développement R.H. référent du dossier à l'adresse mail suivante : l.mantilaro@amiens-metropole.com. Pour postuler, veuillez compléter votre dossier de candidature (en rappelant la référence **5191**) sur le site www.amiens.fr (Rubrique Vivre à Amiens → Emploi → Nos offres d'emplois), **avant le 25/04/2025. Lien d'accès direct pour postuler** : https://demarches.amiens.fr/emploi-et-developpement-economique/depot-candidature-rh/?reference=5191&gestionnaire=LM