

Responsable Sécurité des Systèmes d'Information (RSSI)

CADRE D'EMPLOI :

Filière Technique - Catégorie A
Cadre d'emplois des ingénieurs

SERVICE D'AFFECTATION :

Systèmes, Réseaux et Utilisateurs
Sous la responsabilité du responsable de service.

ACTIVITES

Organisation et mise en œuvre de la sécurité des SI de la collectivité

- Conduire une analyse des besoins de la collectivité en matière de sécurité informatique
- Définir les normes, outils, procédures et règles de sécurité pour la collectivité
- Négocier, avec la ligne hiérarchique, les moyens de la mise en œuvre des évolutions de la sécurité
- Élaborer des préconisations d'optimisation technique et financière
- Vérifier la conformité réglementaire des systèmes et réseaux

Garantir l'intégrité, l'accessibilité et la disponibilité des SI

- Établir un plan de prévention
- Organiser des tests et simulations sécurité
- Évaluer les différents facteurs de risques (techniques, juridiques, etc.) pour la collectivité
- Formuler des propositions pour éviter les incidents
- Superviser des systèmes de sécurité SI
- Organiser les dispositifs de sécurité physique des services et équipements
- Intégrer des plans de continuité et de reprise d'activité

Sensibilisation des utilisateurs aux enjeux de sécurité

- Informer et sensibiliser aux enjeux de la sécurité
- Alerter et conseiller les utilisateurs en cas de risques
- Accompagner les utilisateurs dans leur apprentissage du cadre réglementaire et des procédures sécurité Animer des formations sur la sécurité informatique

MISSIONS DETAILLEES :

Missions communes :

Vous effectuerez des missions communes (référencées dans un document « Socle commun ») au niveau de l'administration des équipements de sécurité dans les domaines suivants, et **en relation avec les administrateurs du pôle** (réseau, serveurs, firewall externe, firewall interne, firewall applicatif, AD, Reverse Proxy, Radius, Antivirus, EDR, Bastion...).

Vous **participerez activement au processus de mutualisation informatique** avec les Communes et les EHPAD de l'Agglomération en ce qui concerne l'application de la politique de sécurité, et le déploiement des outils de sécurité.

Missions spécifiques affectées à l'agent :

- Politique de Sécurité des Systèmes d'Information : mise à jour et extension du document existant, définissant la politique de sécurité de la collectivité,
- Feuille de route cybersécurité : suivi et mise en œuvre des actions du plan de sécurisation 2023-2026,
- ANSSI : analyse et suivi des audits réalisés avec le suivi de l'ANSSI concernant les vulnérabilités extérieures et de l'AD,
- Plan de Continuité d'Activité : analyse des besoins de continuité, mise à jour des processus avec les services utilisateurs.
- Plan de Reprise d'Activité : définition des actions à engager, mise en place des processus.
- Opérationnel : Suivi des tickets d'incidents liés à la cybersécurité, analyse et traitement des remontées utilisateurs,
- Gestion de projet : le RSSI sera associé à l'ensemble des grands projets applicatifs et techniques, afin d'évaluer les risques et réaliser les préconisations techniques,
- Relation intégrateur : le RSSI sera associé aux projets et suivi de maintenance des intégrateurs en charge des équipements de cybersécurité.
- Monitoring des outils de sécurité : surveillance et contrôle des outils de monitoring de sécurité, en relation avec le pôle des administrateurs.
- Mises à jour : suivi des mises à jour des outils de sécurité, suivi des failles CVE et des alertes CRT.
- Veille technologique : suivi des nouveaux outils disponibles sur le marché, réalisation de rapports et de propositions d'améliorations techniques.
- Gestion de crise : participation active à la cellule de crise en cas de cyberattaque, en relation avec le CRT mandaté par l'assureur de la collectivité.

RELATIONS FONCTIONNELLES :

- Au sein d'un pôle des administrateurs composé de six agents avec le RSSI, et en relation étroite avec le pôle « support technique » et le service « études et suivi des logiciels métiers » de la Direction des Systèmes d'Information.
- En relation directe avec les services et certains services cibles en fonction des projets.
- Après filtrage du service support, relation directe avec les utilisateurs des services municipaux, des services de l'Agglomération, des services des Communes mutualisées de l'Agglomération et avec certaines associations.
- Relations avec les principaux fournisseurs et opérateurs avec qui la collectivité a contractualisé.
- Relations occasionnelles avec les élus.

EXPERIENCE

Minimum BAC + 5 dans le domaine de l'informatique,
5 années d'expérience en matière de gestion et suivi de la cybersécurité,

SAVOIR-FAIRE

- Maîtrise des outils techniques
- Architectures et fonctionnalités du système d'information et des réseaux de la collectivité
- Orientations stratégiques de la sécurité
- Démarche d'assurance qualité
- Connaissance des aspects réglementaires liés à la cybersécurité, des institutions et acteurs (CNIL, ANSSI,...)
- Aisance rédactionnelle pour la mise en place de procédures et la mise à jour de la PSSI.

SAVOIRS ETRE :

Confidentialité
Sens du service public,
Maîtrise de soi.

CONTRAINTE ET DIFFICULTES DU POSTE :

Horaires déterminés avec l'équipe en fonction de l'amplitude horaire nécessaire pour le bon fonctionnement de la collectivité.

Travail d'équipe.

Astreinte téléphonique en journée un samedi tous les deux mois

Interventions ponctuelles en dehors des heures de fonctionnement des services.

AVANTAGES LIÉS AU POSTE :

- Régime indemnitaire
- Prime annuelle
- Prise en charge employeur prévoyance et participation pour le contrat de mutuelle labellisé
- Adhésions CNAS / COSEL
- Titres restaurants.