

> OFFRE D'EMPLOI

- Responsable de la Sécurité des Systèmes d'Information Mutualisé (H/F) - Responsable du pôle Cybersécurité

INFORMATIONS CLÉS

Réponse avant le :
16/02/2023

Référence :
17899

Direction :
Systèmes d'information

Cadre d'emploi :
Ingénieurs territoriaux

Lieu de Travail :
Centre Simone Signoret
38090 Villefontaine

Horaires :
Temps complet ouvrant droit à des
jours de RTT

Spécificités du poste :
Permis B obligatoire
Disponibilité horaire importante

Où adresser votre candidature :
Rappeler la référence **17899** sur
votre candidature
Par courrier : 17 avenue du
Bourg, 38081 L'Isle d'Abeau cedex
Par mail : recrutement@capi38.fr
Joindre obligatoirement : lettre de
motivation et curriculum vitae

CONTEXTE

La Communauté d'Agglomération Porte de l'Isère est une intercommunalité constituée de 22 communes, comptant 108 700 habitants. Elle occupe une situation géographique privilégiée (idéalement située à 20 minutes à l'est de Lyon) et dotée d'un excellent niveau d'accessibilité : aéroport, TGV et autoroutes. C'est un territoire singulier, à taille humaine, où patrimoine urbain, industriel et naturel vivent en parfaite harmonie. Engagée dans le développement durable, la transition énergétique et le respect de l'environnement, la CAPI est un territoire agréable à vivre, avec un tissu économique dynamique et innovant. Elle assure une large palette de compétences au quotidien : des missions de planification, aménagement et développement (habitat, économie, urbanisme, mobilités, éclairage public, voiries, transition énergétique), mais aussi une offre de services aux habitants : petite enfance, gestion d'équipements sportifs et culturels, lecture publique, eau et assainissement...

Au sein de la CAPI, est constituée en 2014 une **Direction des Systèmes d'Information** mutualisée sous la forme d'un service commun DSI. Ce dernier gère les systèmes d'information (SI) de la CAPI et des communes de Bourgoin-Jallieu et de la Verpillière, mais délivre aussi des prestations de services pour les autres communes du territoire. Le nécessaire développement de l'e-administration et des e-services aux usagers appelle le déploiement d'un Système d'information propre à répondre aux nouveaux enjeux et besoins des administrés et des services. Les collectivités membres du service commun DSI attendent de disposer d'un SI contributeur à l'efficacité des services par son apport en termes de qualité de service et de solutions techniques (démarche ITIL, sécurité, dématérialisation, relations utilisateurs, open data). Le souci de l'innovation, de la culture de la qualité du service rendu aux usagers, la fiabilité et régularité doivent guider le SI.

Ainsi, rattaché(e) au Responsable du Service des infrastructures Informatiques et de la Cybersécurité, **vous serez chargé(e) de collaborer à la définition de la politique de sécurité des Systèmes d'Information (PSSI) et la mettre en œuvre.**

Plus d'information sur www.capi-agglo.fr/la-capi/rh

Dans ce cadre, vos activités seront :

1. Définir la politique de sécurité des systèmes d'information
 - Evaluer les risques, les menaces et les conséquences notamment pour tout projet d'évolution du SI.
 - Définir les objectifs et les besoins liés à la sécurité des systèmes d'information, en collaboration avec les acteurs concernés (direction générale, direction des systèmes d'information, direction des ressources humaines, ...)
 - Définir et faire évoluer la politique de sécurité en cohérence avec les évolutions du SI
 - Mettre en place une organisation permettant d'assurer dans la durée, la gouvernance de la sécurité des SI.
 - Définir un plan d'action de réponse sur incident de sécurité
2. Préconiser des mesures de sécurité et un plan de mise en œuvre
 - Définir les normes et standards de sécurité à appliquer.
 - Etudier les moyens et procédures permettant d'assurer la sécurité des systèmes d'information et garantir leur bonne utilisation par les différents acteurs.
 - Assister les équipes dans la mise en œuvre des mesures de sécurité.
 - Proposer un plan de prévention des risques informatiques.
 - Piloter la définition des plans de reprise et de continuité d'activité (PRA / PCA). En assurer le suivi et l'évolution.
 - Etre force de proposition pour toutes les évolutions technologiques et les investissements liés à la sécurité
 - Etre force de proposition pour tout projet d'évolution (infrastructure ou applicatif) sur le volet sécuritaire (intégration dans les cahiers des charges des mentions relatives à la sécurité, analyse des offres sur cet aspect, ...).
3. Auditer et contrôler l'application des règles de la politique de sécurité
 - Contrôler et garantir que les équipes appliquent les principes et règles de sécurité du SI
 - Auditer (ou faire auditer par des prestataires) la vulnérabilité de briques du système d'information.
 - Organiser la réponse opérationnelle en cas de sinistre sécurité SI (solution de rétablissement après incident, actions correctives à mener, mise en œuvre du plan de reprise d'activité).
 - Analyser les causes d'incident et consolider les mesures de sécurité en conséquence.
 - Définir et contrôler de la gestion des habilitations
 - Elaborer et suivre les tableaux de bords des incidents de sécurité et assurer le reporting des problèmes et actions mises en œuvre.
4. Sensibiliser et former aux enjeux de la sécurité
 - Informer et sensibiliser la direction générale
 - Conduire des actions de sensibilisation et de formation auprès des utilisateurs sur les enjeux de la sécurité des systèmes d'information.
 - Elaborer la charte de sécurité et en assurer la promotion auprès des utilisateurs.
5. Réaliser une veille technologique et réglementaire
 - Appliquer les dispositions réglementaires en vigueur en matière de cybersécurité et de continuité d'activité.
 - Effectuer le suivi des évolutions réglementaires et techniques du domaine de la sécurité.
 - Assurer une veille sur les règlements et les standards liés aux évolutions législatives et réglementaires en se maintenant à jour des futures modifications afin d'anticiper les changements.
 - Assurer une veille réglementaire sur la protection des données personnelles dans une démarche de mise en conformité permanente vis-à-vis du RGPD et de maîtrise des enjeux majeurs (juridiques et financiers) liés à la protection des données personnelles.
 - Participer à des réseaux professionnels d'échanges de pratique.
6. Assurer le rôle d'encadrement des agents du pôles

Savoir et savoir-faire :

Le RSSI doit avoir une bonne connaissance des aspects juridiques et réglementaires de la sécurité SI, des normes et référentiels de sécurité. Il est impératif qu'il connaisse les logiciels, procédures et standards d'exploitation.

Compétences techniques requises :

- Connaissance des concepts techniques des applications informatiques, du système, des réseaux informatiques et des mécanismes de sécurité
- Maîtrise des fondamentaux dans les principaux domaines de la SSI
- Connaissance des standards de sécurité ISO2700x.
- Expérience dans le pilotage de projets organisationnels
- Connaissance juridique sur la sécurité des systèmes d'information
- Notions sur la réglementation et les procédures des marchés publics

1- Activités opérationnelles

- Assurer la conformité des paramétrages des équipements de sécurité
- Capacité à construire la stratégie cybersécurité de l'organisation
- Capacité à piloter et gérer des projets.
- Capacité à organiser et conduire le changement.
- Capacité de compréhension des menaces cybersécurité
- Capacité à gérer des situations de crise.
- Capacité à animer des groupes de travail, sessions de sensibilisation et formation.
- Gérer les incidents de cybersécurité en assurant les premières réactions et investiguer ces événements de cybersécurité

2- Activités de management

- Diriger, organiser, planifier et contrôler les activités du pôle cybersécurité, avec une attention particulière concernant la régulation du plan de charge
- Piloter les activités administratives (ex : budgets, achats, marchés publics, ...) avec l'appui de son adjoint et des assistantes rattachées au directeur
- Encadrer, coordonner et animer le personnel de son entité
- Assurer des activités de pilotage de projet, de conseil et de communication
- Maîtriser les fondamentaux du management et du management de projet

3- Autres activités :

- Piloter le schéma directeur d'évolution de la PSSI selon une logique de programmation pluriannuelle des investissements.
- Rendre compte à sa hiérarchie de son activité et collaborer avec les autres pôles de la DSI

Savoir être :

- Capacité d'adaptation
- Bon relationnel et esprit de synthèse
- Force de proposition et autonomie
- Pragmatisme et capacité de négociation
- Esprit d'analyse et de synthèse
- Réactivité
- Rigueur
- Capacité à manager et à planifier
- Disponible et sens du service

Votre rémunération :

- Rémunération statutaire + RIFSEEP + Prime de fin d'année.
- **Autres avantages :** Chèques déjeuners + Épargne chèques vacances + Comité des œuvres sociales + participation employeur mutuelle et prévoyance sous condition.

Plus d'information sur www.capi-agglo.fr/la-capi/rh