Responsable de la Sécurité des Systèmes d'Information F/H

Ingénieur.e territorial·e
Employeur : Rennes Métropole

Direction et Service :

Vous serez directement rattaché à la Direction Générale des Services
Vous travaillez en étroite collaboration avec la Direction des Services Numériques - notamment son référent SSI -, la mission DPO de nos collectivités ainsi que le Bureau PMO (Portfolio Management Office) qui recueille les demandes de nouveaux services numériques
L'équipe : Vous travaillerez avec un adjoint RSSI
Effectif Service : 2

Le sens de ce poste :

Au service des collectivités de Rennes Ville, son CCAS, la CEBR et Rennes Métropole vous pilotez la démarche d'amélioration continue de la sécurité de notre système d'information et de nos SI Industriels, selon les principes SSI: identifier, protéger, détecter, répondre, assurer la continuité/reconstruire et rendre compte.
Nos collectivités sont des écosystèmes complexes avec plus de 300 métiers, au service de 7000 agents, 240 000 citoyens de la ville de Rennes et 470 000 de Rennes Métropole.

Environnement et conditions de travail :

Horaires : classiques de bureau
Lieu de travail : Hotel de Rennes Métropole
Matériel(s) à disposition : Environnement numérique de travail DSN
Missions de suppléance : sans
Télétravail : Possible jusqu'à deux jours par semaine
Autres : Autres.

Éléments de statut:

Cadre d'emploi : Ingénieurs territoriaux
Parcours : P3.
Éléments complémentaires de rémunération : IFSE mensuelle brute de 935€ + prime annuelle brute de 1016.84€ + avantages

N° du poste : Création
Date de mise à jour de la fiche de poste : juin 2026

Vos 3 principales missions :

1-Organisation, stratégie et gouvernance SSI

Définition de la stratégie SSI : Élaborer la stratégie de cybersécurité alignée aux objectifs métiers, aux exigences réglementaires (RGPD, NIS2 …) et aux orientations de la collectivité, notamment les stratégies pour un numérique plus responsable.

Politique de sécurité du SI : Rédiger, diffuser et maintenir la Politique de Sécurité du SI (PGSSI / PSSI / PSSIO) et chartes adaptées au contexte de la collectivité.

Gouvernance : Animer les instances de pilotage (Comité de pilotage SSI, Comité opérationnel avec la DSN).

Processus de gestion de crise : Pilotage du processus d'organisation et de préparation à la gestion de crise.

Suivi & reporting : Produire des tableaux de bord de pilotage permettant d'identifier les risques avérés et d'apprécier l'efficacité des actions menées, rendre compte.

2-Pilotage gestion des risques et veille

Cartographie/Evaluation des risques : Identifier, classer et prioriser les risques (actifs, menaces, vulnérabilités) sur le périmètre.

Mesures & audit : Prescription, pilotage et suivi d'audits pour identifier des risques non couverts ou des failles de sécurité. Définition et mise en œuvre d'un plan de contrôle sur le SI permettant d'une part de vérifier l'autocontrôle effectué par les opérationnels (contrôle niveau 2), et d'autre part d'évaluer le niveau de sécurité SI effectivement mis en œuvre.

Veille : Assurer une veille technique et réglementaire (évolution des menaces, nouvelles normes).

3-Plan d'actions SSI et accompagnement sécurité

La réalisation de ces missions sera déléguée à l'adjointe RSSI selon un périmètre à discuter en fonction des compétences respectives de chacun.

Plans d'actions et programme SSI : Au travers d'un programme SSI, le RSSI décline la stratégie SSI en plan d'actions annuel/pluriannuel (mesures organisationnelles & techniques) en étroite collaboration avec la DSN qui pilote et met en œuvre les programmes opérationnels de sécurité suivant les exigences SSI.

Actions de réduction des risques SSI : Mise en œuvre d'actions non prévues dans le plan d'actions, pour réduire les risques SSI. Elles peuvent être mises en œuvre de manière réactive, par exemple suite à un incident ou lors de l'identification d'une nouvelle menace. Suivant la nature des actions, elles peuvent être mises en œuvre par la SSI, la DSN ou le métier.

Sensibilisation et formation à la sécurité : Définition du plan de sensibilisation et de formation incluant la définition des objectifs, l'identification des populations, les sujets SSI retenus par population, les choix de méthodologie de diffusion, les indicateurs et modalités de test. Mise en œuvre du plan (incluant production du contenu, validation du contenu, planification des sessions et déploiement. Évaluation du plan (incluant évaluation des connaissances, plan de test, alimentation des tableaux de bord SSI)

Conseil expertise SSI : Rôle de conseil SSI auprès des collaborateurs de la collectivité pour couvrir les besoins métiers, évaluer la sécurité de nouvelles technologies et approches métier, proposer des solutions de sécurité, dès le début de leurs réflexions

ISP: l'Intégration de la Sécurité dans les Projets (métiers et IT) s'effectue en différentes étapes : l'analyse de l'impact SSI d'une demande de projet par le bureau PMO, la définition de la démarche d'accompagnement du projet et la mise en œuvre de cet accompagnement qui peut prendre différentes formes (exigences CCTP, évaluation des réponses des candidats, accompagnement de la mise en œuvre SSI et élaboration d'un Plan d'Assurance Sécurité : contrôle de la sécurité sous la forme d'analyses de risques, d'audits, de tests d'intrusion, …)

Compétences

Les compétences relationnelles :

- Forte capacité d'écoute et d'adaptation à des interlocuteurs diversifiés (métiers, gouvernance, élus)
- Sens relationnel développé pour interagir avec les responsables de services d'équipes opérationnelles
- Capacité à supporter une pression entre acteurs pouvant être importante
- L'art du consensus pour fluidifier les processus et activités
- Appétence pour le travail en réseau

Les compétences nécessaires pour la prise de poste :

- Prise de hauteur pour prioriser les éléments d'un système complexe
- Esprit de synthèse / Qualité rédactionnelle
- Méthodologie et sens de l'organisation
- **Formation** : Bac + 5 / Master en cybersécurité, informatique ou équivalent (ex. : diplôme d'ingénieur, MSc Sécurité).
- **Expérience** : Minimum 5 ans d'expérience en cybersécurité, dont 2 ans à un poste de responsabilité (RSSI, CISO, CSIRT).
- **Certifications souhaitées** : certification de type SMSI (Système de management de la sécurité de l'information) telles que ISO 27001 Lead Implementer, ISO 27005 Risk Manager.

Les compétences pouvant être acquises une fois en poste :

- Connaissances de l'écosystème local, des partenaires et acteurs institutionnels.
- Connaissances détaillées des Responsabilités Numériques pour nos collectivités
- Connaissances des marchés publics