FICHE 4

Modèle de fiche de poste de responsable de la sécurité des systèmes d'information (RSSI) de GHT

La mise en œuvre, dans le cadre d'un GHT, d'un projet commun de convergence des systèmes d'information vers un système d'information unique et homogène entraîne une réflexion incontournable sur la gestion de la sécurité des systèmes d'information. C'est dans ce nouveau contexte que l'exercice de la fonction de responsable de la sécurité des systèmes d'information (RSSI) doit désormais être envisagé.

L'exercice du métier de RSSI au sein d'un GHT n'est pas fondamentalement différent de celui d'un RSSI en établissement, mais il se voit complexifié par la multiplicité des acteurs, des enjeux et des contraintes. Il en ressort une nécessité encore plus grande de définir avec précision son cadre d'exercice et les missions qui lui sont confiées.

Présentation de la fiche

Cette fiche pratique a pour objectifs de présenter les fonctions relevant du RSSI, ainsi que les compétences techniques et personnelles requises pour les accomplir. Cette fiche a pour modèle la fiche de poste de RSSI présentée dans la boîte à outils pour l'atteinte des prérequis du programme Hôpital numérique et a été adaptée au contexte des GHT.

Le RSSI de GHT est obligatoirement mutualisé entre plusieurs structures.

La fiche de poste du RSSI élaborée par l'établissement de santé support du GHT précise *a minima* les informations suivantes:

- la présentation du GHT, de l'établissement de santé support et du service de rattachement du RSSI ;
- le contexte d'intervention du RSSI ;
- la description des missions et des activités du RSSI ;
- le profil et les compétences attendues pour occuper cette fonction ;
- les moyens mis à disposition du RSSI par l'établissement de santé.

Pour accompagner les établissements de santé dans l'élaboration d'une fiche de poste du RSSI (à partir de la présente fiche pratique) adaptée à leurs besoins, sont distinguées ci-après dans le document:

- en violet les explications sur l'objet et le contenu d'une section, ainsi que les informations ayant vocation à accompagner l'établissement dans l'élaboration de la fiche de poste du RSSI. Ces indications devront être supprimées de la fiche avant sa diffusion au sein de l'établissement;
- en noir les listes *a maxima* des missions/activités pouvant être exercées par le RSSI d'un établissement et les compétences attendues à ce poste. Parmi ces listes, chaque structure sélectionne celles qu'elle conserve *in fine* dans la fiche de poste du RSSI au regard de ses besoins propres.

Identification du poste RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION DU GHT

Présentation de l'établissement de santé/du service de rattachement duRSSI

Cette section vise à décrire les caractéristiques du GHT, des établissements de santé qui en font partie et du service au sein duquel le RSSI exerce ses missions.

Les informations suivantes sont notamment décrites :

- les missions, l'organisation et la composition de l'établissement et du service auquel est rattaché le RSSI;
- la place du RSSI dans l'organigramme, son positionnement hiérarchique et les liens fonctionnels le rattachant aux autres acteurs de l'établissement de santé support et des établissements parties au GHT

Contexte d'intervention

Cette section a pour objectif de dire s'il s'agit d'une création de poste ou d'un remplacement. Dans ce dernier cas, il convient de décrire les niveaux de maturité des établissements en matière de sécurité de leur système d'information et les actions déjà entreprises dans ce domaine.

Par exemple, peuvent être indiquées les informations suivantes :

- l'existence d'une politique de sécurité des systèmes d'information, d'un plan de continuité d'activité…;
- l'historique des analyses de risques et des audits de sécurité des systèmes d'information réalisées;
- les actions de sensibilisation des acteurs de l'établissement à la sécurité des systèmes d'information menées.

Chaque établissement partie au GHT peut ajouter toute autre information sur le contexte d'intervention qu'il juge pertinent de porter à la connaissance du RSSI.

Est également précisée la façon dont le poste est partagé entre les différents établissements parties au GHT.

Description des missions et des activités

La présente section vise à décrire les missions et les activités placées sous la respon- sabilité du RSSI. La liste proposée ci-dessous recense ainsi *a maxima* ces missions et activités. L'établissement de santé ne conservera que celles qu'il souhaite confier au RSSI en fonction de ses propres besoins.

Le RSSI est chargé de réaliser les missions et les activités suivantes.

- Définition et mise en œuvre de la politique de sécurité des systèmes d'information
  - Définit les objectifs et les besoins liés à la sécurité des systèmes d'information de l'établissement, en collaboration avec les acteurs concernés (direction générale,

direction des systèmes d'information, direction des ressources humaines, direction qualité, représentants du personnel médical et soignant).

- Rédige la politique de sécurité des systèmes d'information du GHT et les procédures de sécurité associées en collaboration avec les acteurs concernés (*voir ci-dessus*).
- Met en œuvre la politique de sécurité des systèmes d'information au sein des établissements parties au GHT, en assure les évolutions et les mises à jour.
- Met en place une organisation permettant d'assurer, dans la durée, la gouvernance de la sécurité du système d'information des établissements.

O Diagnostic et analyse des risques de la sécurité des systèmes d'information

- Choisit une méthode d'analyse de risques adaptée à la taille et à l'activité du GHT.
- Évalue les risques sur la sécurité des systèmes d'information.

O Choix des mesures de sécurité et plan de mise en œuvre

- Étudie les moyens permettant d'assurer la sécurité des systèmes d'information et leur bonne utilisation par les acteurs du GHT.
- Propose aux instances du GHT, pour arbitrage, une liste de mesures de sécurité à mettre en œuvre, assure dans la durée, le suivi et l'évolution de ce plan d'actions.
- Assure la maîtrise d'ouvrage de la mise en œuvre des mesures de sécurité (cette mission, selon le type de mesure technique ou organisationnelle, peut être éventuellement partagée avec un responsable métier ou le responsable du système d'information).

O Sensibilisation, formation et conseil sur les enjeux de la sécurité des systèmes d'information

- Informe régulièrement et sensibilise les directions des établissements sur les enjeux et les risques de la sécurité des systèmes d'information.
- Conduit des actions de sensibilisation et de formation auprès des utilisateurs sur les enjeux de la sécurité des systèmes d'information.
- Participe à la réalisation de la charte de sécurité des systèmes d'information du GHT et en assure la promotion auprès de l'ensemble des utilisateurs.

O Audit et contrôle de l'application des règles de la politique de sécurité des systèmes d'information

- Conduit régulièrement des audits de sécurité des systèmes d'information afin de vérifier la bonne application de la politique de sécurité par les acteurs de l'établissement.
- Surveille et gère les incidents de sécurité survenus au sein des établissements.
- Vérifie l'intégration de la sécurité des systèmes d'information dans l'ensemble des projets des établissements parties au GHT.

O Veille technologique et prospective

- Suivi des évolutions réglementaires et techniques afin de garantir l'adéquation de la politique de sécurité des systèmes d'information avec ces évolutions.

Profil et compétences requises

Cette section vise à décrire le profil requis et les compétences techniques et personnelles nécessaires

pour occuper le poste du RSSI. Une liste de compétences *a maxima* est proposée ci-dessous.

O Niveau de formation et d'expérience

- Formation de niveau licence (ou master 2) avec une spécialisation complémentaire en sécurité des systèmes d'information.
- Cadre technique ayant une expérience avérée dans la conduite de projets en milieu hospitalier.

O Compétences techniques

- Connaissance des concepts techniques des applications informatiques hospitalières, des réseaux informatiques et des mécanismes de sécurité.
- Connaissance des standards de sécurité ISO 2700x.
- Expérience dans le pilotage de projets organisationnels dans le milieu hospitalier.
- Connaissance juridique sur la sécurité des systèmes d'information, et particulièrement des textes régulant la santé.
- Notions sur la réglementation et les procédures des marchés publics (pour les établissements publics).

O Compétences personnelles

- Capacité à piloter et gérer des projets.
- Capacité à organiser et conduire le changement.
- Capacité à gérer des situations de crise.
- Capacité à animer des groupes de travail, sessions de sensibilisation et formation.
- Bon relationnel et esprit de synthèse.

Moyens mis à disposition

Cette section précise les moyens humains, matériels et financiers qui seront mis à la disposition du RSSI pour mener à bien les missions et les activités décrites précédemment (ex: poste de travail, équipe dédiée, budget alloué…).