Responsable Sécurité des Systèmes d'Information - Multisite (H/F/X)

LA SOCIÉTÉ

Plus grand groupe hospitalier de Wallonie (Belgique), **HELORA**, par la diversité des métiers qu'il réunit, comprend près de 7.000 collaborateurs.

Multi-sites, **HELORA** couvre 4 bassins de soins situés dans le Hainaut et le Brabant Wallon.

L'approche universitaire, les projets d'infrastructures, les investissements médicaux ambitieux et le professionnalisme de ses collaborateurs permettent à **HELORA** d'offrir aux patients des soins en constante évolution, sécuritaires et de la plus haute qualité.

Vous souhaitez proposer vos talents et vos compétences auprès d'un hôpital en plein essor, venez vivre la **#HELORA** Expérience sur l'un de nos 7 sites.

FONCTION

MISSION

De manière à contribuer à la santé globale de nos patients de manière fiable, appréciée, et efficiente dans le respect des normes d'hygiène, de sécurité et des valeurs institutionnelles, le Responsable Sécurité des Systèmes d'Information (RSSI) a pour mission de garantir la sécurité, la confidentialité, l'intégrité et la disponibilité des systèmes d'information et des données au sein des CHU HELORA, en alignement avec les enjeux stratégiques de l'établissement et les exigences réglementaires

Le RSSI est le gardien de la résilience des CHU Helora et joue un rôle de véritable partenaire métier.

- Définir et mettre en oeuvre les politiques de sécurité pour protéger les systèmes d'information
- Evaluer la vulnérabilité des systèmes, afin de protégrer les infrastructures IT et les données
- Gérer les risques et les incidents de sécurité de l'information
- Analyser les demandes d'utilisation de nouveaux dispositifs connectés et remettre un avis
- Gérer la mise en conformité des fournisseurs avec les exigences réglementaires
- Piloter le Comité de sécurité de l'information (COSI)
- Sensibiliser les collaborateurs à la sécurité des systèmes d'information
- Accompagner la transformation numérique des CHU Helora

1. Définition et mise en œuvre de la politique de sécurité (PSSI)

Établir un cadre de sécurité cohérent et conforme aux exigences légales et opérationnelles.

- Rédiger et actualiser la Politique de Sécurité des Systèmes d'Information (PSSI) en collaboration avec la Direction Générale et la Direction Informatique.
- Adapter la PSSI aux spécificités des 7 hôpitaux et des centres associés (polycliniques, centres de prélèvements).
- Veiller à la conformité avec les réglementations : RGPD, certification HDS, NIS2, ISO 27001, et normes sectorielles.
- Définir des indicateurs de performance (KPI) pour mesurer l'efficacité de la PSSI et rendre compte à la direction.

2. Sécurisation des infrastructures et des données

Protéger les systèmes et les données contre les cybermenaces et les accès non autorisés.

- Superviser la sécurisation des réseaux, serveurs, postes de travail, et dispositifs médicaux connectés (IoMT).
- Gérer les accès et les identités (IAM)
- Chiffrer les données sensibles (dossiers patients, résultats d'analyses, imagerie médicale) en transit et au repos.
- Sécuriser les échanges entre les sites (ex : partage de dossiers patients, télémédecine) et avec les partenaires externes.
- Contrôler les accès physiques aux salles serveurs et aux équipements critiques.

3. Gestion des risques et des incidents

Identifier, évaluer et atténuer les risques, et réagir efficacement en cas d'incident.

- Réaliser des analyses de risques régulières pour identifier les vulnérabilités (ex : audits, tests d'intrusion).

- Élaborer des plans d'atténuation pour les risques identifiés (ex : mise à jour des systèmes, formation des équipes).
- Piloter la réponse aux incidents (cyberattaques, fuites de données, indisponibilités) en coordination avec les équipes IT et la direction.
- Mettre en place des procédures de détection précoce (SIEM, monitoring 24/7).
- Participer à l'élaboration des PCA/PRA pour garantir la continuité des soins en cas de crise (ex : ransomware, panne majeure).

4. Conformité et audits

Assurer le respect des obligations légales et des bonnes pratiques.

- Participer a l'organisation des audits internes et externes pour vérifier la conformité aux normes (ISO 27001, HDS, NIS2,…)
- Collaborer avec les autorités de contrôle (CCB, auditeurs certifiés) lors des inspections.
- Documenter les preuves de conformité (registres, rapports, procédures).
- Veiller à la traçabilité des accès aux données de santé pour répondre aux exigences légales (ex : secret médical, RGPD …).

5. Sensibilisation et formation

Impliquer l'ensemble du personnel dans la culture de la cybersécurité.

- Organiser des campagnes de sensibilisation pour tous les collaborateurs (médicaux, administratifs, techniques).
- Former les équipes aux bonnes pratiques (ex : reconnaissance des phishing, gestion des mots de passe).
- Adapter les formations aux spécificités des métiers (ex : médecins, infirmiers, personnel IT).
- Promouvoir une culture de vigilance via des newsletters, des simulations d'attaques, et des retours d'expérience.

6. Collaboration et coordination

Travailler en transversalité pour intégrer la sécurité dans tous les projets.

- Collaborer avec la Direction Informatique et les équipes techniques pour sécuriser les projets IT.
- Travailler avec les directions des soins et médicales pour sécuriser les outils métiers (DPI, PACS, télémédecine).
- Coordonner avec les prestataires externes (hébergeurs, fournisseurs de solutions) pour garantir leur conformité aux exigences de sécurité

7. Veille et innovation

Anticiper les évolutions technologiques et réglementaires.

- Assurer une veille active sur les cybermenaces émergentes et les évolutions légales.
- Évaluer l'impact des nouvelles technologies (IA, IoMT, cloud) sur la sécurité des systèmes.
- Proposer des solutions innovantes pour renforcer la sécurité (ex : authentification forte, analyse comportementale).
- Représenter les CHU HELORA dans les réseaux professionnels et les instances dédiées à la cybersécurité en santé.

8. Participation aux projets stratégiques

Intégrer la sécurité dès la conception des nouveaux projets.

- Contribuer à la sécurisation des nouvelles infrastructures hospitalières prévues dans les prochaines années.
- Accompagner la digitalisation des soins (ex : télémédecine, dossiers patients partagés).
- Sécuriser les projets de transformation numérique (ex : migration vers le cloud, déploiement de l'IA).

9. Reporting et communication

Informer la direction et les parties prenantes sur l'état de la sécurité.

- Rendre compte régulièrement à la Direction Générale et au Comité de Direction
- Communiquer sur les incidents majeurs et les actions correctives mises en place.
- Présenter des tableaux de bord synthétiques sur l'état de la sécurité (KPI, niveaux de risque, conformité).

10. Gestion des relations avec les autorités et les partenaires

Représenter les CHU HELORA auprès des acteurs externes.

- Être l'interlocuteur privilégié pour les autorités (CCB, auditeurs).
- Collaborer avec les autres établissements de santé pour partager les bonnes pratiques et les retours d'expérience.
- Négocier avec les assureurs pour couvrir les risques cybernétiques.

PROFIL

Formation

- Posséder un Master en informatique orienté cybersecurité ou une expérience équivalente probante
- Certication ISO27001 LI est un plus
- Maitrise d'une méthode de gestion des risques SSI (EbiosRM, ISO27005…)

Expérience requise:

- Connaissances avancées en gestion des risques ;
- Connaissances en continuité et reprise d'activités ;
- Avoir une connaissance ou une expérience d'une méthodologie de gestion de projets comme Prince2 ou équivalente ;
- Une expérience de minimum 5 années dans une fonction similaire ;
- Une expérience en sécurité de l'information probante
- Bonnes capacités de négociation
- Leadership probant
- Orienté partenariat métiers
- Expérience du milieu hospitalier est un atout
- Bon pédagogue et garant de solutions pragmatiques

Qualités personnelles :

- Structuré, organisé, pro-actif, autonome;
- Facilitateur entre tous les intervenants du projet;
- Bonnes capacités de communication;
- Savoir fédérer et embarquer l'ensemble des collaborateurs dans cette dynamique de transformation.

OFFRE

Nous offrons un **contrat à durée indéterminée** à temps plein (38h/semaine), ainsi qu'un package relatif à la fonction.

Présence sur sites attendue (à temps plein dans un premier temps) - Belgique

Postulez Maintenant