Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale Québec	**POLITIQUE**
	Code : PO-24
	Direction responsable : Direction des ressources informationnelles (DRI)
	Adoptée au comité de direction le : 20 juin 2017 Révisions approuvées le : 9 janvier 2024
	Adoptée au conseil d'administration le : 6 février 2024
	Résolution no. : CA-CIUSSS-2024-02[PO-24]-06 Entrée en vigueur le : 20 juin 2017
	Champ d'application : Toute personne physique ou morale qui utilise ou peut avoir accès à un ou plusieurs actifs informationnels
TITRE : Cadre de gestion de la sécurité de l'information	

CONSULTATIONS	
☐ Conseil des infirmières et infirmiers :	☐ Cadres :
☐ Conseil multidisciplinaire :	☐ Autres :
☐ Conseil des médecins, dentistes et pharmaciens :	

Table des matières

Historique des modifications

Version	Détail	Auteur	Date
0,1	Version initiale du document	Denis Bouchard	15 mars 2017
0,4	Version pour comité de sécurité de l'information	Denis Bouchard	8 mai 2017
1.0	Version approuvée par le comité de sécurité	Denis Bouchard	15 mai 2017
1.1	Version approuvée par le comité de direction	Denis Bouchard	20 juin 2017
1.2	Mise à jour au regard du nouveau cadre provincial de gestion de la sécurité de l'information	Zidane Toffa	16 janvier 2023
2.0	Nouvelle version	Barbara Marier	30 octobre 2023

1. Acronymes

Acronyme	Description
CCGSI	Comité de crise gouvernemental en sécurité de l'information
CDSI	Chef délégué de la sécurité de l'information
CERT/AQ	Équipe de réponse aux incidents de sécurité de l'administration québécoise
CGCD	Centre gouvernemental de cyberdéfense
CGSI	Chef gouvernemental de la sécurité de l'information
CGSI	Cadre de gestion de la sécurité de l'information
CIUSSS	Centre intégré universitaire de santé et de services sociaux
COCD	Centre opérationnel de cyberdéfense
COMSI	Coordonnateur organisationnel des mesures de sécurité de l'information
COS	Centre opérationnel de sécurité En anglais : « Security operations center » (SOC)
CPSI	Comité provincial de sécurité de l'information
CSI	Comité chargé de la sécurité de l'information
CSIO	Chef de la sécurité de l'information organisationnelle
DGTI	Direction générale des technologies de l'information
DL	Direction de la logistique
DO	Dirigeant de l'organisation
DRHC	Direction des ressources humaines et des communications
DRI	Direction des ressources informationnelles
DSP	Direction des services professionnels
É/O	Établissements et organismes
GIA	Gestion des identités et des accès
GMVI	Gestion des menaces, des vulnérabilités et des incidents
MCN	Ministère de la Cybersécurité et du Numérique
MSSS	Ministère de la Santé et des Services sociaux
MVI	Menaces, vulnérabilités et incidents
OP	Organismes publics
PPSI	Politique provinciale de sécurité de l'information
RAG	Réseau d'alerte gouvernemental
RAI	Réseau d'alerte interne des COMSI
RGCD	Responsable gouvernemental de cyberdéfense
ROCD	Responsable organisationnel de cyberdéfense
RSSS	Réseau de la santé et des services sociaux
SI	Sécurité de l'information
TCDSI	Table des chefs délégués de la sécurité de l'information

2. Préambule

Le présent cadre de gestion de la sécurité de l'information découle de la nécessité de faire évoluer l'encadrement de la sécurité de l'information au sein du Centre intégré universitaire de santé et de services sociaux (CIUSSS) de la Capitale-Nationale, organisme relevant du dirigeant réseau de l'information (DRI)[1] pour prendre en compte les nouveaux besoins d'encadrement et les nouvelles exigences gouvernementales découlant de la loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement du Québec (LGGRI) et de la Directive gouvernementale sur la sécurité de l'information gouvernementale (décret numéro 1514-2021).

Le nouveau cadre provincial de gestion de la sécurité de l'information (MSSS-CDG01) établi par le ministère de la Santé et des Services sociaux (MSSS) confère aux intervenants en matière de sécurité de l'information de nouvelles responsabilités. Le CIUSSS de la Capitale-Nationale est assujetti aux dispositions de ce nouveau cadre provincial et doit mettre en place un cadre de gestion conforme aux exigences requises.

3. Champ d'application

Le présent cadre de gestion s'applique à toute personne physique ou morale qui utilise ou peut avoir accès à un ou plusieurs actifs informationnels, peu importe l'endroit où elle se trouve, la localisation de l'actif ou le support sur lequel se retrouve l'actif informationnel.

Les actifs informationnels visés par le présent cadre de gestion sont ceux que le CIUSSS de la Capitale-Nationale détient dans l'exercice de sa mission, que sa conservation soit assurée par lui-même ou par un tiers.

4. Définitions

Pour l'application du présent cadre de gestion, les termes et expressions suivantes signifient :

1° **Actif informationnel**
Actif au sens de la Loi sur le partage de certains renseignements de santé (LPCRS), soit une banque d'informations, un système d'information, un réseau de télécommunication, une infrastructure technologique ou un ensemble de ces éléments ainsi qu'une composante informatique d'un équipement médical spécialisé ou ultraspécialisé.

Est également considéré comme un actif informationnel, tout support papier contenant de l'information.

[1] Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI) article 2, paragraphe 5.

2° **Architecture de sécurité**
Stratégies d'affaires, modèles, processus, services et orientations en matière de sécurité de l'information. Il s'agit de la base sur laquelle reposent toutes les décisions relatives aux exigences et aux mesures de contrôle de l'architecture technologique de sécurité.

3° **Détenteur de l'information**
Un employé désigné par son organisation, appartenant à la classe d'emploi de niveau-cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité entourant cette information ainsi que celle des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.

4° **Événement de sécurité**
Toute forme d'atteinte, présente ou appréhendée, telles une cyberattaque ou une menace à la confidentialité, à l'intégrité et à la disponibilité d'une information ou d'une ressource informationnelle sous la responsabilité d'une organisation ou d'une personne agissant pour cette dernière.

5° **Gestion intégrée des risques liés à la sécurité de l'information**
Approche de gestion des risques qui repose sur une gestion globale, proactive et continue des risques liés à la sécurité de l'information à tous les niveaux hiérarchiques de l'organisation.

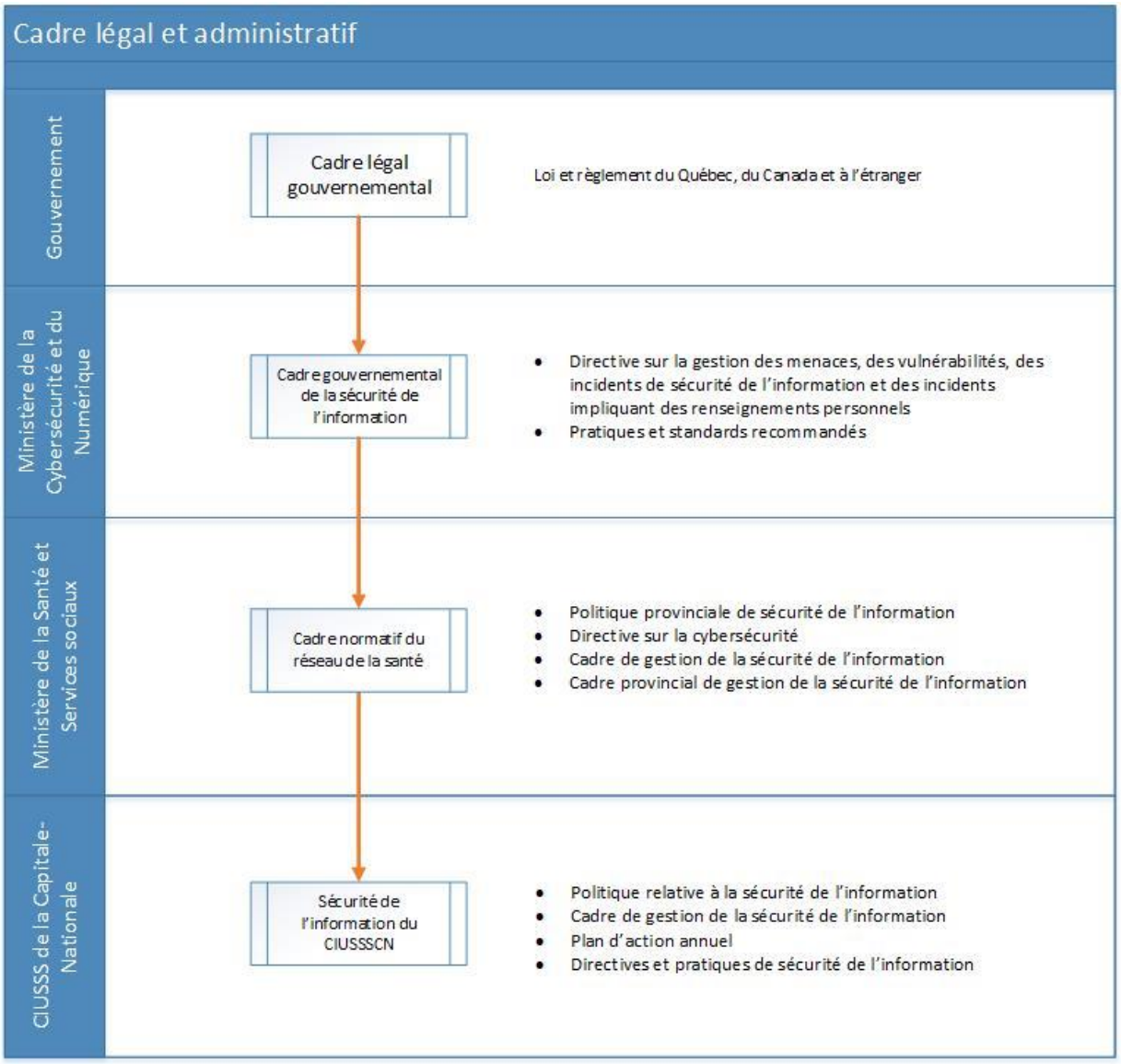
6° **Registre d'autorité**
Recueil où sont notamment consignés les noms des détenteurs de l'information, les systèmes d'information qui leur sont assignés ainsi que les noms des principaux intervenants en matière de sécurité de l'information.

7° **Réseau**
Ensemble des organismes qui relèvent du dirigeant réseau de l'information (DRI) de la santé et des services sociaux en vertu de l'article 2, paragraphe 5 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI).

8° **Système d'information**
Système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une organisation.

5. Cadre légal et administratif

Le cadre de gestion de la sécurité de l'information du CIUSSS de la Capitale-Nationale vient positionner comment s'inscrit la gestion de la sécurité de l'information par rapport aux lois et règlements en vigueur. S'ajoutent les exigences du ministère de la Cybersécurité et du Numérique (MCN), des règles particulières émises par le DRI et des directives, cadres normatifs et de gestion, règles du réseau de la santé. Le schéma suivant présente le cadre légal et administratif des différents paliers.



6. Objectifs

Le cadre de gestion de la sécurité de l'information complète les dispositions de la politique relative à la sécurité de l'information et renforce la gouvernance de la sécurité de l'information de l'établissement, par la mise en place d'une structure fonctionnelle de la sécurité de l'information et par la définition de rôles et responsabilités en la matière.

Les rôles et responsabilités définis dans le cadre de gestion de la sécurité de l'information concernent l'approbation, la mise en place, la coordination, le développement, le suivi et l'évaluation de la sécurité de l'information dans l'établissement, en tenant compte des exigences du cadre légal et administratif applicable au Réseau et des principes généraux de la politique provinciale de sécurité de l'information du Réseau et de celle de l'établissement.

Le cadre de gestion de la sécurité de l'information s'inscrit dans le cadre normatif du Réseau, tout en s'appuyant sur le cadre légal et le cadre normatif gouvernemental, tel qu'illustré ci-dessous.

7. Structure fonctionnelle de la sécurité de l'information

Le cadre de gestion de la sécurité de l'information met en œuvre la structure fonctionnelle requise pour assurer une gouvernance forte et intégrée, pour favoriser la concertation entre les services, pour profiter de la complémentarité de leurs ressources et pour optimiser l'efficacité de leurs actions.

Le schéma ci-dessous illustre la structure fonctionnelle de la sécurité de l'information au sein de l'établissement :

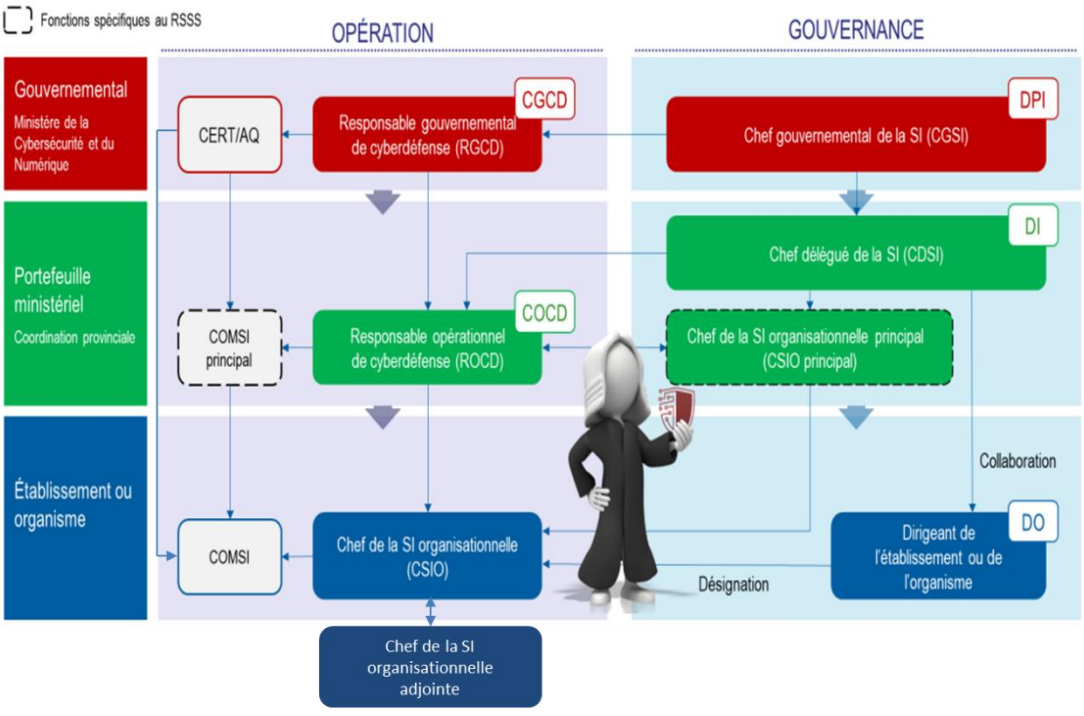


Figure 2: Structure fonctionnelle de la sécurité de l'information du RSSS

Le schéma ci-dessous illustre la structure fonctionnelle de la sécurité de l'information au sein du CIUSSS de la Capitale-Nationale :

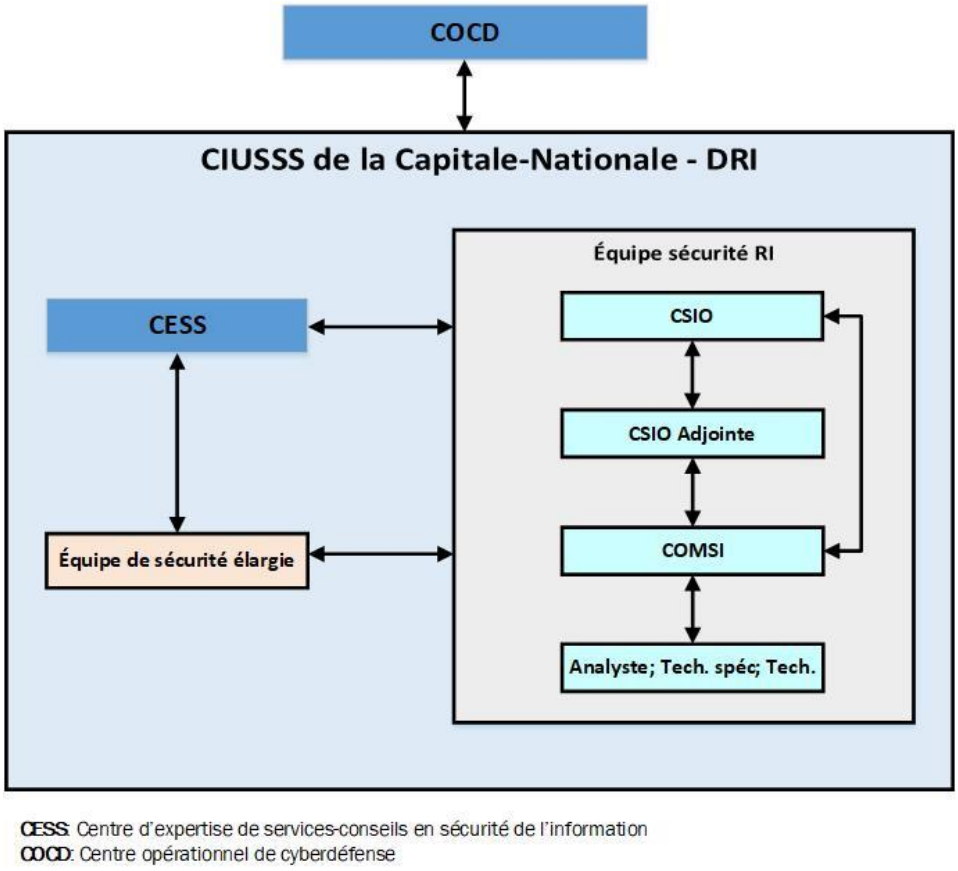


Figure 3: Structure fonctionnelle de la sécurité de l'information du CIUSSS de la Capitale-Nationale

8. Rôles et responsabilités

8.1 Coordination gouvernementale (MCN)

8.1.1 Chef gouvernemental de la sécurité de l'information (CGSI)

En vertu des obligations énoncées dans la Loi et la Directive, le chef gouvernemental de la sécurité de l'information (CGSI) a pour responsabilité d'assurer la coordination gouvernementale de la SI au niveau stratégique, tactique et opérationnel. En plus de celles-ci, il a pour autres responsabilités :

1. D'assurer la mise en œuvre d'une structure de gouvernance de la SI visant à instaurer un climat d'échange et de collaboration entre l'ensemble des intervenants;
2. D'assurer la mise en œuvre des politiques et des stratégies établies en SI, en coordonner l'exécution et en surveiller l'application;
3. D'élaborer, diffuser et maintenir à jour des cadres de gestion particuliers en SI, notamment au sujet des services communs;
4. D'élaborer, diffuser et faire le suivi de la mise en œuvre de règles relatives à la SI applicable aux organismes publics (OP);
5. D'élaborer, encadrer, mettre en place et maintenir à jour des processus gouvernementaux normalisés en gestion de la SI, et en assurer la coordination;
6. De formuler, lorsque requis, des indications d'application en matière de SI;
7. De mettre en place des mécanismes de reddition de comptes permettant l'obtention des informations nécessaires à l'évaluation de la performance des organismes publics (OP) en SI;
8. D'animer et de coordonner les comités et groupes de travail dont il est responsable, dont la table des chefs délégués de la sécurité de l'information (TCDSI);
9. D'apporter un soutien continu aux OP dans le déploiement de pratiques exemplaires de SI;
10. De développer et mettre à la disposition des OP des outils favorisant le développement des compétences en SI des employés de l'administration publique;
11. D'établir les standards et les meilleures pratiques en SI pour l'ensemble du gouvernement.

Le CGSI exerce un lien fonctionnel sur le chef délégué de la sécurité de l'information (CDSI), le chef de la sécurité de l'information organisationnelle (CSIO) et les répondants en SI pour des domaines spécifiques en matière de SI au sein des OP. Il est de plus membre permanent du Comité de crise gouvernemental en sécurité de l'information (CCGSI). À ce titre, il conseille le président du comité sur les enjeux de SI et de cybersécurité.

8.1.2 Responsable gouvernemental de cyberdéfense (RGCD)

Le responsable gouvernemental de cyberdéfense (RGCD) est désigné par le CGSI. Il est chargé de la gestion et de l'opérationnalisation du CGCD, ainsi que de diriger le Réseau gouvernemental de cyberdéfense. Ses principales responsabilités sont :

1. De mettre en place le CGCD, l'opérationnaliser et faire évoluer son offre de services;
2. D'assurer le leadership du Réseau et de la communauté des responsables organisationnels de cyberdéfense (ROCD);
3. D'animer la cellule gouvernementale de cyberdéfense, et relayer les informations transmises par les ROCD au CGSI lorsqu'il le juge approprié;
4. De proposer, définir, coordonner et maintenir les processus gouvernementaux normalisés en matière de SI, particulièrement ceux relatifs à la cyberdéfense, dont celui de gestion des menaces, des vulnérabilités et des incidents (GMVI);
5. De développer une vision gouvernementale des risques, des menaces et des vulnérabilités;
6. De contribuer à rehausser la maturité du Réseau, notamment en coordonnant la gestion et la cohésion des actions des COCD, ainsi qu'en les accompagnant dans la mise en œuvre de leurs attentes et la prise en charge de leurs responsabilités;
7. D'assurer la réalisation d'activités de surveillance en matière de sécurité de l'information;
8. De dégager et déposer au CGSI des recommandations sur des pratiques ou indications d'application qui permettraient de rehausser le niveau de sécurité des OP;
9. De participer à l'élaboration des orientations gouvernementales en matière de cybersécurité;
10. De consolider les relations avec les acteurs de l'écosystème de cybersécurité et favoriser l'innovation en la matière;
11. D'assurer la mise en œuvre des attentes et des orientations du CGSI au sein du Réseau;
12. D'identifier les opportunités d'optimisation des ressources informationnelles en matière de SI à l'échelle gouvernementale.

Le RGCD exerce un lien fonctionnel sur les ROCD afin de faciliter, si la situation le requiert, la transmission d'instructions obligatoires à ces derniers. La transmission de telles instructions pourrait survenir, par exemple, afin de prévenir ou gérer une menace, une vulnérabilité ou un incident. Le RGCD pourrait alors ordonner l'application de mesures extraordinaires ou exiger de rendre compte sur des questions particulières.

Le RGCG est membre permanent du CCGSI. À ce titre, il conseille le comité et lui procure un soutien sur toute question opérationnelle de cyberdéfense. Également, il coordonne les actions du CGCD et du Réseau gouvernemental de cyberdéfense en lien avec les actions à prendre concernant la menace, la vulnérabilité ou l'incident visé.

8.1.3 Réseau gouvernemental de cyberdéfense (Réseau)

Le réseau gouvernemental de cyberdéfense (Réseau) est formé du CGCD par l'intermédiaire du responsable gouvernemental de cyberdéfense (RGCD), des centres opérationnels de cyberdéfense par l'intermédiaire des responsables opérationnels de cyberdéfense, et des OP par l'intermédiaire des CSIO et des répondants en matière de SI. Il est dirigé par le CGCD, qui joue au sein du Réseau le rôle d'entité de confiance et de coordonnateur de la prise en charge des événements de sécurité et des communications opérationnelles.

Le Réseau a pour mission de renforcer les dispositifs de prévention et de réaction à l'égard des cybermenaces. Il permet de mutualiser les efforts en cybersécurité en favorisant le partage et la mise en commun des connaissances et de l'expertise, ainsi que le recours à des pratiques communes.

8.1.4 Centre gouvernemental de cyberdéfense (CGCD)

Le centre gouvernemental de cyberdéfense (CGCD) est le centre de commandement des opérations de cyberdéfense ainsi que le centre de coordination et de soutien aux membres du Réseau. Il voit à l'amélioration continue du Réseau par le développement des pratiques et des expertises. Il a comme mandat d'offrir des services centralisés en SI, d'assurer une surveillance constante des cybermenaces et de coordonner des interventions rapides en cas d'événement de sécurité pouvant porter atteinte à la confidentialité, l'intégrité ou la disponibilité des données numériques gouvernementales québécoises. Le CGCD intervient au niveau tactique et opérationnel afin de soutenir le Réseau dans ses activités de cyberdéfense. Il est responsable notamment :

1. D'assurer, avec la collaboration du Réseau, une prise en charge rapide et concertée des menaces, des vulnérabilités et des incidents, ainsi qu'un échange en temps réel des informations relatives à toute situation qui pourrait affecter la SI gouvernementale;
2. d'offrir des services centralisés en SI qui optimisent l'utilisation des ressources et maximisent la capacité à analyser les risques en SI à l'échelle gouvernementale;
3. D'assurer, de façon constante, la réalisation d'activités de surveillance en matière de SI;
4. D'effectuer les vérifications de sécurité des systèmes gouvernementaux à l'égard des menaces et des vulnérabilités de façon régulière et continue, et de recommander les correctifs nécessaires de sécurité physique ou logique aux COCD ou aux OP concernés;
5. De mettre en place une surveillance normalisée et en continu des accès à l'information gouvernementale;
6. De définir des mécanismes de suivi et de concertation afin d'accompagner les COCD et les OP dans la mise en place des mesures de sécurité;
7. D'assurer le développement et le maintien d'une expertise de pointe en cybersécurité pour les employés du CGCD et des COCD. À cet effet, définir les besoins, identifier les expertises prioritaires à développer ou à

maintenir, identifier les cours ou les parcours de développement requis et en faciliter l'accès;
8. De fournir des avis et des conseils aux COCD et aux OP;
9. De développer des outils partageables au sein du Réseau;
10. De développer ou d'assurer le développement et la mise en place de certains services de sécurité;
11. D'assurer la mise en relation des intervenants de sécurité au sein de l'administration publique et avec tout autre partenaire jugé approprié.

8.1.5 Équipe de réponse aux incidents de sécurité de l'administration québécoise (CERT/AQ)

L'équipe de réponse aux incidents de sécurité de l'administration québécoise (CERT/AQ) fait partie du CGCD. Elle intervient dans la coordination gouvernementale de la GMVI à un niveau tactique et opérationnel. Elle a pour mission d'assister le Réseau dans sa capacité à prévenir et à gérer les incidents et les cyberattaques, et de contribuer à améliorer cette capacité. Son offre de services est intégrée à celle du CGCD, et est regroupée en trois catégories, soit la prévention, la réaction et l'amélioration. Le CERT/AQ a notamment pour responsabilité :

1. D'assister et de soutenir les COCD et les OP dans l'atténuation des risques de SI, la prévention des menaces, la correction des vulnérabilités et des incidents de sécurité, et la réaction à ceux-ci;
2. De coordonner, au niveau tactique et opérationnel, la GMVI avec la collaboration du réseau d'alerte gouvernemental (RAG) et de la Cellule de cyberdéfense;
3. D'animer et coordonner le RAG et s'assurer d'une représentation adéquate des membres lors des rencontres de ce réseau.

8.2 Coordination provinciale

8.2.1 Chef délégué de la sécurité de l'information (CDSI)

Le sous-ministre associé de la direction générale des technologies de l'information (DGTI) détient ce rôle. À ce titre, il agit sous le lien fonctionnel du CGSI, et exerce un lien fonctionnel sur le ROCD ainsi que sur le CSIO principal. Il offre également du soutien à ses CSIO. Le CDSI est responsable d'assurer la coordination de la SI au niveau stratégique, tactique et opérationnel pour le MSSS et pour les É/O. Il détient également les responsabilités suivantes :

1. Assurer la mise en œuvre, le respect, la coordination et le suivi des processus gouvernementaux normalisés, notamment de gestion des événements de sécurité;
2. Assurer et surveiller la mise en place des processus et des mesures de SI requis, conformément aux orientations gouvernementales;

3. Mettre en œuvre les décisions et les orientations émises par le CGSI, notamment les indications d'application, en surveiller l'application et en coordonner l'exécution;
4. Formuler des indications d'application particulières, lorsque requis;
5. Fournir des conseils basés sur les orientations gouvernementales et les meilleures pratiques en SI;
6. Déterminer les orientations stratégiques et les priorités d'action pour le MSSS et pour les É/O;
7. S'assurer de la mise en œuvre d'un cadre de gouvernance qui régit la SI et l'approuver;
8. Élaborer et assurer la mise en place et le suivi d'un plan d'action qui favorise la performance de la gestion de la SI quant aux résultats atteints et aux ressources utilisées;
9. Établir les attentes aux CSIO des É/O pour la mise en œuvre des mesures de cybersécurité, si applicable, et leur offrir du soutien;
10. Désigner, parmi le personnel d'encadrement sous sa direction, un ROCD qui voit au bon fonctionnement et à l'évolution de l'offre de services du COCD;
11. Coordonner et diriger, en collaboration avec son ROCD, les activités de son COCD;
12. Établir les attentes au CSIO principal pour la mise en œuvre des mesures de cybersécurité, si applicable;
13. Assurer la prise en charge des événements de sécurité afin de minimiser les préjudices potentiels;
14. S'assurer de l'élaboration des processus de gestion de la SI, du déploiement des mesures afférentes et du suivi de leur mise en œuvre;
15. Mettre en œuvre toute action requise pour la prise en charge d'un événement de sécurité;
16. S'assurer de l'élaboration, du maintien à jour et de l'efficacité du processus ministériel GMVI applicable au MSSS et aux É/O;
17. Aviser sans délai le CGSI de tout événement de sécurité qui requiert son attention;
18. Mettre en place, coordonner et animer les comités et groupes de travail requis à l'atteinte de la performance en matière de SI;
19. Mettre en place des mécanismes de concertation avec les CSIO;
20. Participer à la table gouvernementale des CDSI;
21. Assurer l'obtention de l'information nécessaire à la reddition de comptes auprès du CGSI, ou de toute autre information demandée par ce dernier;
22. Favoriser le développement des compétences de son personnel en SI.

8.2.2 Chef de la sécurité de l'information organisationnelle principal (CSIO principal)

Le CDSI désigne un chef de la sécurité de l'information organisationnelle principal (CSIO Principal) afin de le soutenir dans ses responsabilités en matière de SI. Le CSIO principal a pour responsabilité d'assurer la coordination de la SI au niveau stratégique, tactique et opérationnel pour le MSSS et pour les É/O. Il travaille en étroite collaboration avec le ROCD et les CSIO des É/O afin de mettre en œuvre les attentes du gouvernement en matière de SI. À ce titre, il doit :

1. Coordonner la mise en œuvre des processus gouvernementaux normalisés en SI;
2. Tenir informés les CSIO des É/O des attentes du gouvernement en matière de SI;
3. Mettre en œuvre les décisions émanant du CGSI, du CDSI et du ROCD, notamment les indications d'application et les indications d'application particulières, en coordonner l'exécution et en assurer le respect;
4. Assurer la coordination et la cohérence des actions en SI, conformément aux exigences gouvernementales;
5. Assister le CDSI dans la détermination et la mise en œuvre des orientations stratégiques et des priorités d'action;
6. Élaborer, faire approuver par le CDSI, mettre en œuvre et veiller au respect du présent cadre de gestion par le MSSS et par les É/O;
7. Coordonner la mise en œuvre des actions découlant du plan de sécurité élaboré par le CDSI;
8. S'assurer de l'intégration des exigences de SI lors de la réalisation de projets de développement, de l'acquisition de systèmes d'information ou d'impartition de services (ex. : infonuagique) pour le MSSS et pour les É/O;
9. S'assurer que le MSSS et les É/O intègrent, aux ententes de service et aux contrats sous leur responsabilité, des clauses contractuelles garantissant la SI des actifs informationnels;
10. S'assurer du maintien à jour du registre d'autorité du MSSS, à titre de détenteur;
11. Collaborer à l'application des mesures opérationnelles de SI recommandées par le ROCD;
12. Assurer la prise en compte de la SI dans les processus mis en place au sein du MSSS et des É/O;
13. Collaborer avec le ROCD à l'implantation du processus gouvernemental GMVI au sein du MSSS et de chacun des É/O;
14. Mettre en œuvre toutes les mesures requises lors d'événements de sécurité afin de réduire au maximum les préjudices éventuels;
15. Aviser rapidement le CDSI de tout événement de sécurité qui risque de causer un préjudice sérieux;
16. S'assurer que le ROCD tient un registre des événements de sécurité selon les modalités précisées par le CGSI;

17. S'assurer de la mise en œuvre et de l'évolution d'un processus intégré de gestion des risques liés à la SI au MSSS et dans les É/O;
18. Fournir les informations demandées par le CGSI, le CDSI ou le ROCD, ou toute autre information requise par les autorités;
19. Établir annuellement le portrait de la SI du MSSS et de chacun des É/O;
20. Coordonner et animer les comités et groupes de travail requis pour le MSSS et les É/O;
21. Présider et coordonner le Comité provincial de sécurité de l'information (CPSI);
22. Mettre en place des mécanismes de concertation avec les CSIO des É/O;
23. Assurer le développement des compétences du personnel du MSSS en matière de SI;
24. S'assurer de l'élaboration et de la mise en œuvre d'un plan de sensibilisation à la SI de tout le personnel du MSSS;
25. S'assurer que les CSIO des É/O élaborent et mettent en œuvre un tel plan à l'intention de l'ensemble de leur personnel.

8.2.3 Responsable opérationnel de cyberdéfense (ROCD)

Le responsable opérationnel de cyberdéfense (ROCD) dirige le COCD du MSSS et agit sous le lien fonctionnel du RGCD. Il en assure le commandement, la coordination, l'amélioration continue et le leadership en matière de cybersécurité au sein du MSSS et des É/O. Il doit être membre du personnel d'encadrement. Désigné par le CDSI, il représente officiellement ce dernier dans la prise en charge des mesures opérationnelles de SI, en étroite collaboration avec le CSIO principal. À ce titre, il doit :

1. Contribuer activement à rehausser la maturité du Réseau gouvernemental de cyberdéfense en participant à la définition de ses orientations, priorités d'action et pratiques;
2. Coordonner la mise en œuvre des processus gouvernementaux normalisés en matière de SI, particulièrement ceux relatifs à la cyberdéfense;
3. Représenter le MSSS et les É/O auprès du CGCD via la cellule gouvernementale de cyberdéfense ; et y partager les préoccupations;
4. Conseiller le CDSI sur des orientations, des priorités d'action et des pratiques communes afin d'optimiser les ressources, de concert avec le CSIO principal;
5. Mettre en place le COCD, l'opérationnaliser et faire évoluer son offre de services;
6. Soutenir le CDSI dans la coordination et la direction de son COCD;
7. Consulter le CSIO principal sur les mesures opérationnelles de SI à mettre en place afin de prévenir ou de gérer une menace, une vulnérabilité ou un incident, s'assurer de leur mise en place effective et préciser les délais de réalisation impartis en fonction du niveau de risque encouru;
8. Voir à déployer toute autre mesure de sécurité opérationnelle, notamment dans le cadre du processus ministériel GMVI;

9. S'assurer que le COCD réalise, au besoin ou de façon régulière, des balayages de vulnérabilité sur les actifs informationnels des É/O, de concert avec chaque CSIO concerné;
10. S'assurer que chaque É/O se dote d'un Centre opérationnel de sécurité (COS) (ou SOC) et que son COCD leur apporte le soutien nécessaire, notamment sur les paramètres de mise en place et d'exploitation des services de sécurité déterminés par le ROCD;
11. Maintenir un registre de tous les représentants du RAG pour le MSSS et les É/O;
12. S'assurer que le COCD collabore à la mise en place et à l'amélioration de l'architecture de sécurité du MSSS et des É/O (Gestion des identités et des accès (GIA), infonuagique, etc.);
13. Prendre en charge l'implantation du processus gouvernemental GMVI, veiller à sa mise en place et à son opérationnalisation au MSSS et dans les É/O, en étroite collaboration avec le CSIO principal;
14. Assurer et coordonner la prise en charge rapide et concertée des événements de sécurité, dont les menaces, les vulnérabilités et les incidents, ainsi qu'un échange en temps réel de l'information relative à toute situation pouvant affecter la SI;
15. Assurer le fonctionnement du réseau d'alerte interne (RAI) des COMSI;
16. S'assurer d'une veille continue du COCD sur les menaces et sur l'identification des mesures d'atténuation des risques liés à la SI;
17. Développer une connaissance et une compréhension des risques liés à la SI;
18. Collaborer à la mise en œuvre et à l'évolution de la gestion intégrée des risques liés à la SI du MSSS;
19. Assister aux rencontres de la cellule gouvernementale de cyberdéfense;
20. Mettre en place et coordonner une instance de collaboration qui réunit tous les COMSI (MSSS et É/O) au moins quatre fois par année;
21. Élaborer un bilan annuel de ses activités destiné au CDSI, ainsi que toute autre reddition de comptes requise par ce dernier;
22. Assurer le développement des compétences du personnel du COCD en matière de cybersécurité;
23. Apporter un support pour le contenu des activités de sensibilisation à la SI, lorsque requis.

Enfin, le ROCD doit exercer toute autre activité de SI que lui attribue le CDSI.

8.2.4 Centre opérationnel de cyberdéfense (COCD)

Le Centre opérationnel de cyberdéfense (COCD) est une entité sous la direction et la coordination du CDSI, qui désigne un ROCD pour le soutenir à cet égard. Il a comme mandat d'assurer le commandement, la coordination, l'amélioration continue et le leadership en matière de cybersécurité pour le MSSS et les É/O. Le COCD intervient au niveau tactique et opérationnel.

À ce titre, il doit :

1. Assurer, avec la collaboration des répondants identifiés, une prise en charge rapide et concertée des événements de sécurité, dont les menaces, les vulnérabilités et les incidents, ainsi qu'un échange en temps réel des informations relatives à toute situation qui pourrait affecter la SI gouvernementale;
2. Effectuer les vérifications de sécurité des systèmes à l'égard des menaces et des vulnérabilités de façon régulière et continue, et de recommander les correctifs nécessaires de sécurité physique ou logique aux É/O concernés;
3. Définir des mécanismes de suivi et de concertation afin de les accompagner dans la mise en place des mesures de sécurité;
4. Leur apporter le soutien nécessaire à la mise en place et à l'évolution d'un COS (ou SOC), dans le respect des paramètres de mise en place et d'exploitation des services de sécurité déterminés par le ROCD;
5. Maintenir une offre de services de cyberdéfense destinée au MSSS ainsi qu'aux É/O;
6. Fournir des avis et des conseils;
7. Dégager et déposer au ROCD des recommandations sur des pratiques ou indications d'application particulière qui permettraient de rehausser le niveau de sécurité;
8. Exercer toute autre activité de SI que lui attribue son CDSI.

8.2.5 Coordonnateur organisationnel des mesures de sécurité de l'information principal (COMSI principal)

Le coordonnateur organisationnel des mesures de sécurité de l'information principal (COMSI principal) œuvre au COCD et supporte le ROCD dans l'exercice de ses responsabilités en matière de gestion opérationnelle de la SI. Il est responsable de l'application et de l'amélioration continue du processus GMVI au MSSS et dans les É/O, en soutien à son CSIO.

À ce titre, il doit :

1. Déployer ce processus et en coordonner les actions, en collaboration étroite avec les intervenants impliqués;
2. Identifier les menaces, les vulnérabilités et les incidents (MVI) touchant le MSSS et les É/O, en tenir informé son CSIO et les escalader selon les conditions définies par le processus GMVI lorsque requis;
3. S'assurer de l'élaboration, de la mise à jour et de l'application d'un plan interne de réponse aux MVI;
4. Collaborer étroitement avec son CSIO principal et son ROCD en leur fournissant le soutien technique nécessaire à l'exercice de leurs responsabilités;
5. Leur communiquer tout événement de sécurité d'intérêt ou nécessitant leur intervention;

6. Fournir aux COMSI des É/O l'information et le support nécessaires à l'exercice de leurs responsabilités;
7. S'assurer de la réalisation d'analyses de risques de sécurité;
8. Définir les mesures opérationnelles de SI à mettre en place au sein du MSSS et des É/O et faire le suivi de leur application;
9. Présider le RAI des COMSI et participer activement au RAG.

8.3 Le CIUSSS de la Capitale-Nationale

8.3.1 Conseil d'administration

Le conseil d'administration doit :

1. Adopter la politique et le plan d'action établi par l'établissement en matière de sécurité de l'information, lesquels sont conformes à la Politique provinciale de sécurité de l'information et au cadre provincial de gestion de la sécurité de l'information, et suit leur application dans l'établissement;
2. Recevoir et entériner annuellement, ou au besoin, le bilan de la sécurité de l'information de l'organisme.

8.3.2 Dirigeant de l'organisation (DO)

En tant que premier responsable de la sécurité de l'information de son organisation, le dirigeant de l'organisation (DO), soit le président-directeur général du CIUSSS de la Capitale-Nationale, doit désigner un CSIO qui appartient à la classe d'emploi de niveau cadre pour son organisation et lui octroyer les ressources nécessaires à la réalisation de ses responsabilités.

Le DO doit :

1. S'assurer du respect des lois, des orientations et des règles de SI gouvernementales qui s'appliquent à son organisation;
2. Approuver le cadre de gestion de la DI adapté à l'établissement;
3. S'assurer de l'attribution appropriée des rôles et des responsabilités du présent cadre de gestion;
4. S'assurer de la mise en œuvre des processus de gestion intégrée de la SI pour son organisation;
5. Établir avec son CSIO une forte relation de collaboration lui permettant d'être mis au fait de toute situation à risque ou de tout événement de sécurité majeur;
6. Demeurer alerte et se rendre disponible en cas d'incident afin de régler la situation promptement;

7. S'assurer de la mise en place d'un comité chargé de la SI (CSI) au sein de son organisation afin de favoriser la concertation et la collaboration entre les intervenants;
8. Sensibiliser et mobiliser ses gestionnaires quant aux règles et bonnes pratiques en SI;
9. Maintenir une vigilance en continu en matière de SI pour son organisation.

8.3.3 Chef de la sécurité de l'information organisationnelle (CSIO)

Le chef de la sécurité de l'information organisationnelle (CSIO) est le répondant en matière de SI. Il est de niveau d'emploi-cadre, nommé par le DO et détient un lien fonctionnel important avec le CSIO principal du MSSS et le ROCD. Le CSIO doit de plus :

1. Coordonner la mise en œuvre des orientations stratégiques et des priorités d'action en SI provenant du CSIO principal ou de son organisation;
2. Veiller au respect du présent cadre de gestion, ainsi que de tout autre document d'encadrement de la SI en vigueur et applicable à son organisation;
3. Mettre en œuvre un plan d'action en SI qui favorise la performance de la gestion de la SI et en faire le suivi;
4. Voir à l'élaboration et à l'application de l'ensemble des mesures liées à la protection des actifs informationnels, en collaboration avec les détenteurs et son COMSI;
5. S'assurer de la prise en charge des exigences de SI lors de la réalisation de projets de développement, de l'acquisition de systèmes d'information ou de l'impartition de services pour le MSSS et les É/O (ex. : infonuagique);
6. S'assurer de l'intégration, aux ententes de service et des contrats sous la responsabilité de son organisation, des clauses contractuelles garantissant la SI des actifs informationnels;
7. S'assurer de la mise en œuvre d'un registre d'autorité;
8. S'assurer que son organisation participe aux processus provinciaux de gestion de la SI (ex. : GMVI);
9. S'assurer que des politiques internes ou des processus relatifs à la cybersécurité sont définis et mis en œuvre;
10. Collaborer étroitement avec le CSIO principal et le ROCD pour la mise en œuvre des mesures opérationnelles de SI recommandées par ce dernier;
11. S'assurer de l'application effective de ces mesures à l'intérieur des délais impartis par le ROCD;
12. S'assurer que son organisme se dote d'un COS (ou SOC), dans le respect des paramètres de mise en place et d'exploitation des services de sécurité déterminés par le ROCD;
13. S'assurer de la mise en œuvre et de l'amélioration continue du processus ministériel GMVI applicable à son organisation;
14. S'assurer de la mise en œuvre et du maintien à jour d'un registre des événements de sécurité pour son organisation, conformément au processus ministériel GMVI ainsi qu'aux modalités précisées par le CGSI;

15. Communiquer au CSIO principal toute situation à risque ou tout événement de sécurité majeur;
16. Voir à la mise en œuvre et à l'évolution d'un processus de gestion intégrée des risques liés à la SI;
17. S'assurer que les détenteurs de l'information soient rapidement informés de tout risque résiduel identifié lors de la réalisation de projets de développement, de l'acquisition de systèmes d'information ou de l'impartition de services pour le MSSS et les É/O (ex. : infonuagique);
18. Produire un bilan annuel et un plan d'action triennal en SI et les transmettre au CSIO principal;
19. Participer activement aux rencontres du CPSI et y relayer les préoccupations de son organisation;
20. Voir à mettre en place, coordonner et animer un groupe de travail requis pour son organisation;
21. Élaborer et mettre en œuvre un plan de sensibilisation en SI à l'intention de l'ensemble de son personnel.

8.3.4 Chef adjoint de la sécurité de l'information organisationnelle (CSIO adjoint)

Le chef adjoint de la sécurité de l'information organisationnelle (CSIO adjoint) apporte son soutien au CSIO de son organisme, notamment en ce qui concerne l'encadrement de la sécurité de l'information, le choix des moyens pour répondre aux exigences des règles particulières adoptées par la DRI et la planification des actions en sécurité. À cet égard, il doit :

1. Accompagner le CSIO dans la définition des orientations stratégiques, des directives et des plans d'action en matière de sécurité de l'information;
2. Participer à la rédaction des documents d'encadrement de la sécurité de l'information de son organisme, notamment la politique et le cadre de gestion de sécurité de l'information;
3. Accompagner le CSIO dans la mise en œuvre des orientations internes découlant des directives ministérielles et celles de la direction des ressources informationnelles (DRI), des politiques internes et des pratiques généralement admises à cet égard;
4. Participer à la définition et accompagner le CSIO dans la mise en œuvre de processus formels de gestion de la sécurité de l'information;
5. Accompagner les directions partenaires en matière de sécurité de l'information et participer à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information dans les ententes de service et les contrats;
6. Assister les détenteurs de l'information dans la catégorisation de l'information relevant de leur responsabilité, dans l'identification et l'évaluation des situations de risques ainsi que dans la définition de plans

d'action visant à réduire les risques de sécurité de l'information à un niveau acceptable pour l'organisme et pour le MSSS;
7. Identifier et prendre en charge les exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information;
8. Élaborer et mettre en œuvre le programme de formation et de sensibilisation en matière de sécurité de l'information;
9. Tenir à jour le registre d'autorité de la sécurité de l'information;
10. Assurer la coordination et la réalisation de projets de sécurité de l'information;
11. Produire les bilans et les plans d'action de sécurité de l'information de son organisme.

8.3.5 Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Le coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) apporte le support nécessaire à la gestion opérationnelle de la SI dans son organisation. Son rôle consiste notamment à :

1. Définir les mesures opérationnelles de SI à mettre en place et faire le suivi de leur application;
2. Contribuer à l'élaboration du processus ministériel GMVI et à son amélioration continue;
3. Collaborer au déploiement de ce processus et en coordonner les actions à l'intérieur de son organisation, en collaboration étroite avec le COMSI principal;
4. Fournir l'expertise nécessaire à l'exercice des responsabilités de son CSIO et au support du COS (ou SOC) de son organisme;
5. Informer le ROCD et son CSIO de tout événement de sécurité d'intérêt ou nécessitant leur intervention;
6. Participer activement au RAI des COMSI ainsi qu'au RAG.

8.3.6 Équipe de sécurité élargie

Le rôle de chaque membre de l'équipe de Sécurité élargie est de :

1. Soutenir les activités de l'équipe de Sécurité RI COS (ou SOC) en coordonnant et en opérationnalisant l'ensemble des activités opérationnelles en matière de SI dans son équipe d'expertise;
2. Représenter son équipe en identifiant, soulevant et proposant des solutions concernant les enjeux et les problématiques de sécurité présents dans son secteur d'expertise;
3. Veiller à la mise en place et au respect des orientations, politiques, directives et bonnes pratiques en matière de sécurité de l'information;
4. S'assurer que l'information communiquée par l'équipe de Sécurité RI COS (ou SOC) est partagée adéquatement avec les membres de son équipe d'expertise.

8.3.7 Comité chargé de la sécurité de l'information (CSI)

Le comité de sécurité de l'information est l'instance de concertation en matière de sécurité de l'information. Il est présidé par le CSIO, à titre de représentant du dirigeant de l'organisme, du CSIO adjoint, des détenteurs de l'information ainsi que des unités administratives responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels ainsi que, sur invitation, de toute personne jugée pertinente.

Plus particulièrement, il doit :

1. Examiner et formuler des recommandations concernant les orientations, les politiques, les directives, les cadres de gestion, les plans d'action et les bilans de l'organisme, ainsi que toute proposition d'action ou état d'avancement de projet en sécurité de l'information;

2. S'assurer de la prise en charge des risques, des situations vulnérables ou des incidents identifiés;

3. Analyser et formuler des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'établissement;

4. S'arrimer avec le comité de gestion des risques, le comité sur l'accès et la protection des renseignements personnels et le comité de vérification pour traiter les dossiers communs le plus efficacement possible;

5. Collabore étroitement avec le comité de gestion des risques afin de documenter et de résoudre les incidents reliés à la sécurité de l'information et en assurer le suivi;

6. S'assurer que les besoins d'affaires de l'établissement soient répondus de façon sécuritaire;

7. S'assurer que les exigences de sécurité de l'information qui sont requises soient mises en place tout en considérant « l'expérience client ».

8.3.8 Centre d'opération de sécurité COS (ou SOC)

Le rôle de l'équipe de Sécurité RI COS (ou SOC) est de coordonner, d'actualiser et d'opérationnaliser l'ensemble des activités en matière de SI en cohérence avec les orientations stratégiques et les exigences tactiques et opérationnelles sous la gouverne du CSIO, du CSIO adjoint et du COMSI.

Les rôles de l'équipe COS (ou SOC) sont regroupés sous deux volets.

Volet Gouvernance et architecture

Pour le volet gouvernance et architecture, le rôle de l'équipe est de :

Contribuer proactivement à la gestion de la sécurité de l'information par une intégration systématique de ses façons de faire dès la conception de l'application, l'acquisition de système d'information, et ce, tout au long de son existence caractérisée par les activités d'exploitation, de maintenance, de support, et ce, durant tout le cycle de vie de l'actif informationnel pour bien maintenir un standard de qualité vérifiable et une sécurité mesurable sur le plan de la conformité, des coûts, d'efficacité et de robustesse.

Volet opérationnel

Pour le volet opérationnel, le rôle de l'équipe vise principalement à :

1. Détecter, investiguer, de répondre et de prévenir de façon proactive les cybermenaces;
2. S'assurer de la correction des vulnérabilités dans les délais prescrits selon le GMVI;
3. Surveiller proactivement les résultats du balayage périodique des vulnérabilités externes et internes;
4. Prendre en charge les avis de vulnérabilité émis par le MCN (CERT/AQ);
5. S'assurer de l'implantation des 15 mesures minimales de sécurité;
6. S'assurer de l'implantation d'une architecture de sécurité basée sur les recommandations du COCD;
   - Isoler les équipements non gérés (BioMed);
   - Implanter des éléments de sécurité internes (IDS/IPS, FW de segmentation, etc.);
7. Effectuer des rencontres internes mensuelles.

8.3.9 Détenteur de l'information

Le détenteur de l'information s'assure de la protection adéquate des actifs informationnels qui lui sont confiés par le DO de son organisation. À ce titre, il doit :

1. S'impliquer dans l'ensemble des activités relatives à la sécurité, entre autres, la catégorisation en termes de disponibilité, d'intégrité et de confidentialité, l'évaluation des risques, la détermination du niveau de protection visé, l'élaboration des contrôles non technologiques et, finalement, la prise en charge des risques résiduels;
2. S'assurer de connaître et évaluer les risques et vulnérabilités de leurs actifs informationnels, prioriser les actions correctives appropriées et gérer leurs applications selon le plan d'action déterminé;
3. S'assurer que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement;

4. S'assurer que leur nom et les actifs informationnels dont ils assument la responsabilité sont consignés et mis à jour dans le registre d'autorité;
5. Identifier le ou les pilotes de systèmes;
6. Sensibiliser les utilisateurs à la sécurité de l'information dans leurs domaines d'affaires;
7. Définir et assurer la mise en place d'un plan de continuité des affaires pour leurs processus critique en cas d'indisponibilité de leur actif informationnel.
8. Définir les profils d'accès supportés par les applications relevant de leurs autorités et s'assurer de la conformité des mécanismes d'accès aux exigences de sécurité;
9. Réviser les accès attribués périodiquement en s'assurant de maintenir de façon restrictive les accès privilégiés afin de tendre vers le moindre privilège;
10. Ajuster, dans les délais recommandés, tout écart constaté entre les habilitations, les profils d'accès à l'information et les autorisations d'accès octroyées;
11. S'assurer que les trajectoires encadrant l'utilisation et le support de leur système d'information respectent les exigences légales de protection des renseignements personnels.

8.3.10 Les pilotes de systèmes

Identifiés par les détenteurs de l'information, les pilotes de systèmes doivent :

1. S'occuper de la création, destruction et réactivation des codes d'accès à l'application, et octroyer les privilèges selon les profils d'accès appropriés aux fonctions;
2. Informer les utilisateurs, lors de l'attribution des accès, de leurs obligations face à l'utilisation des systèmes d'information dont ils sont responsables;
3. Appliquer les contrôles de qualité et d'intégrité sur les actifs informationnels dont ils ont la responsabilité;
4. Identifier les personnes autorisées à agir en relève en leur nom et assurer la disponibilité de celles-ci;
5. Participer à la rédaction du plan de continuité des affaires et connaître le processus d'affaires supporté par l'application dont il est le pilote;
6. Participer à la mise en place, la gestion et la diffusion de moyens de relève adéquats en cas de panne ou d'interruption;
7. Réaliser ou coordonner les tests requis avant la mise en production de tout changement ou mise à jour en lien avec l'application;
8. S'assurer du fonctionnement sécuritaire d'un actif informationnel dès le début du projet et lors de sa mise en exploitation en respectant les règles de sécurité établies;
9. Être apte à faire le lien entre divers systèmes d'information qui supportent une activité;
10. Soutenir le service de première ligne aux utilisateurs en cas d'un mauvais fonctionnement du système;

11. Collaborer avec le fournisseur pour la résolution des problèmes et lui communiquer les besoins de changements souhaités;
12. S'assurer des transferts de connaissance adéquats;
13. S'assurer du contrôle de la qualité des données du système.

8.3.11 Gestionnaire

Le gestionnaire joue un rôle actif et mobilisateur en SI. À ce titre, il doit :

1. Informer adéquatement son personnel des exigences du présent cadre de gestion, ainsi que de tout autre document d'encadrement de la SI en vigueur et applicable à son organisation lorsqu'il utilise les actifs informationnels mis à sa disposition;
2. Intégrer aux ententes de service et aux contrats attribués par son unité administrative des clauses contractuelles garantissant la SI des actifs informationnels et s'assurer que tout consultant, partenaire ou fournisseur s'engage formellement à les respecter;
3. Communiquer rapidement à son COMSI toute menace, toute vulnérabilité ou tout incident de SI dont il a connaissance, dans le respect du processus ministériel GMVI.

8.3.12 Personnel

Le personnel autorisé à accéder aux actifs informationnels du MSSS et du CIUSSS de la Capitale-Nationale joue un rôle prépondérant en matière de SI. À ce titre, il doit :

1. Utiliser ces actifs avec discernement et aux seules fins permises par son lien d'emploi, dans le respect des documents d'encadrement de la SI en vigueur;
2. Communiquer rapidement toute menace, vulnérabilité ou tout événement de sécurité dont il a connaissance, dans le respect du processus ministériel GMVI.
3. Respecter et effectuer l'ensemble des actions de sensibilisation demandées par le CSIO.

8.3.13 La Direction des ressources informationnelles (DRI)

La Direction des ressources informationnelles (DRI) agit en tant que partenaire de services. Elle fournit et maintient en état les moyens techniques de sécurité et s'assure de leur conformité aux besoins de sécurité (Disponibilité-Intégrité-Confidentialité) déterminés par les détenteurs de l'information lors de la catégorisation de l'information. En outre, la DRI soutient les détenteurs de l'information dans l'élaboration et la mise en œuvre des mesures qu'ils déterminent, lors des analyses de risques de sécurité, pour gérer les risques identifiés et assurer la sécurité de leurs actifs informationnels.

8.3.14 La Direction des ressources humaines

La Direction des ressources humaines est responsable d'informer tout employé de ses obligations découlant de la politique de sécurité ainsi que de participer à la production et à la dispensation des programmes de formation.

8.3.15 La Direction de la logistique (DL)

La Direction de la logistique (DL) est responsable du volet ententes et contrats avec les fournisseurs et autres partenaires de l'établissement. Elle doit s'assurer de l'application de la politique de sécurité de l'information dans les contrats et ententes avec les fournisseurs, consultants et partenaires.

8.3.16 La Direction des services professionnels (DSP)

La Direction des services professionnels (DSP) s'assure que tout médecin, résident, dentiste ou pharmacien connaisse ses obligations découlant de la politique de sécurité de l'information ainsi que des normes, directives, procédures en vigueur en matière de sécurité de l'information.

9. Dispositions finales

Le présent cadre de gestion entre en vigueur à la date de son adoption par le conseil d'administration.

Le cadre de gestion doit être réévalué à chaque modification de la Politique relative à la sécurité de l'information et à l'occasion de changements organisationnels ou de nouvelles orientations ministérielles.

10. Références

1- La loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, L.R.Q, c.G-1.03.

2- Directive gouvernementale sur la sécurité de l'information, décembre 2021 (décret numéro 1514-2021).

3- Politique provinciale de gestion de la sécurité de l'information, Ministère de la Santé et des Services sociaux, septembre 2022.

4- Cadre provincial de gestion de la sécurité de l'information, Ministère de la Santé et des Services sociaux, juillet 2022.