Direction générale adjointe

CENTRE OPÉRATIONNEL DE CYBERDÉFENSE (DGACOCD)

CYBERSÉCURITÉ

Cadre provincial de gestion de la sécurité de l'information

MSSS-CDG01

2023-01-09

Votre gouvernement

Ministère de la Santé et des Services sociaux

Québec

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
CGRI	Comité de gouvernance en ressources informationnelles
CGSI	Chef gouvernemental de la sécurité de l'information
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
DO	Dirigeant de l'organisation
DPI	Dirigeant principal de l'information
É/O	Établissements et organismes
EIMSIG	Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale

Acronyme	Description
GMVI	Gestion des menaces, des vulnérabilités et des incidents
MCN	Ministère de la Cybersécurité et du Numérique
OP	Organismes publics
RAG	Réseau d'alerte gouvernemental
RAP	Réseau d'alerte provincial des COMSI
RGCD	Responsable gouvernemental de cyberdéfense
ROCD	Responsable organisationnel de cyberdéfense
SI	Sécurité de l'information
TCDSI	Table des chefs délégués de la sécurité de l'information

Table des matières

Acronymes 2

Préambule 6

Objectifs 6

Champ d'application et portée 6

Cadre légal et administratif 7

Définitions 8

Structure de gouvernance (schéma) 9

Comités (schéma) 10

Rôles et responsabilités 11

Coordination gouvernementale (MCN) 11

Chef gouvernemental de la sécurité de l'information (CGSI) 11

Responsable gouvernemental de cyberdéfense (RGCD) 12

Réseau gouvernemental de cyberdéfense (Réseau) 13

Centre gouvernemental de cyberdéfense (CGCD) 13

Équipe de réponse aux incidents de sécurité de l'administration québécoise (CERT/AQ) 14

Coordination provinciale 15

Chef délégué de la sécurité de l'information (CDSI) 15

Chef de la sécurité de l'information organisationnelle principal (CSIO principal) 17

Responsable opérationnel de cyberdéfense (ROCD) 18

Centre opérationnel de cyberdéfense (COCD) 20

Coordonnateur organisationnel des mesures de sécurité de l'information principal (COMSI principal) 21

Établissements et organismes (É/O) 22

Dirigeant de l'organisation (DO) 22

Chef de la sécurité de l'information organisationnelle (CSIO) 23

Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) 24

Détenteur de l'information 25

Gestionnaire 25

Personnel 25

Comités 26

Coordination gouvernementale (MCN) 26

Comité de gouvernance en ressources informationnelles (CGRI) 26

Table des chefs délégués de la sécurité de l'information (TCDSI) 26

Cellule gouvernementale de cyberdéfense (Cellule) 27

Réseau d'alerte gouvernemental (RAG) 27

Comité de crise gouvernemental en sécurité de l'information (CCGSI) 27

Coordination provinciale 28

Comité provincial de sécurité de l'information (CPSI) 28

Réseau d'alerte provincial des COMSI des É/O (RAP) 28

Établissements et organismes (É/O) 28

Comité chargé de la sécurité de l'information (CSI) 28

Entrée en vigueur et révision 29

Préambule

L'infonuagique, l'intelligence artificielle, la mobilité, l'Internet des objets ainsi que les nouvelles technologies de stockage et de transmission sont au cœur de l'utilisation quotidienne du numérique au ministère de la Santé et des Services sociaux (MSSS), ainsi que dans les établissements et les organismes du réseau de la Santé et des Services sociaux (RSSS).

La stratégie de transformation numérique du MSSS et du RSSS permettra à terme de bonifier la prestation de services aux citoyens. Elle constitue une opportunité, mais suscite également des préoccupations majeures à considérer en lien avec la protection de l'information sensible (médicale, psychosociale, etc.) détenue par ces entités.

C'est dans ce contexte que le présent cadre de gestion fixe les rôles et les responsabilités des intervenants imputables en matière de sécurité de l'information (SI), dans le respect des cinq principes directeurs préconisés par la Directive gouvernementale sur la sécurité de l'information : l'éthique, l'évolution, la responsabilité-imputabilité, la transparence et l'universalité.

Objectifs

Ce cadre de gestion vise :

- une définition claire des rôles et responsabilités des intervenants en matière de SI;
- le renforcement de leur imputabilité;
- la concertation et la collaboration afin de favoriser l'amélioration de la maturité en SI dans l'organisation;
- une gestion optimale des événements de sécurité par la mise en place d'une organisation fonctionnelle basée sur le principe de la chaine de commandement;
- l'adéquation face aux attentes et aux exigences gouvernementales.

Enfin, ce cadre de gestion complète les dispositions de la politique provinciale de la sécurité de l'information (PPSI).

Champ d'application et portée

Ce cadre de gestion s'applique aux entités suivantes :

- le MSSS;
- les organismes visés au paragraphe 5 de l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), ci-après appelés « établissement et organismes », ou É/O.

Il s'applique également à :

- toute information détenue par ces entités, peu importe sa nature, le support numérique sur lequel elle se trouve (enregistrement sonore ou vidéo, données électroniques ou numériques, etc.) ou sa localisation, et ce, durant tout son cycle de vie;
- la conservation de l'information assurée par un tiers.

Cadre légal et administratif

Le cadre légal et administratif applicable est celui défini dans la politique provinciale de sécurité de l'information (PPSI).

Ce cadre de gestion s'inscrit en conformité des exigences de :

- la Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LQ 2021, chapitre 22);
- la Directive gouvernementale sur la sécurité de l'information (2021);
- le Cadre gouvernemental de gestion de la sécurité de l'information.

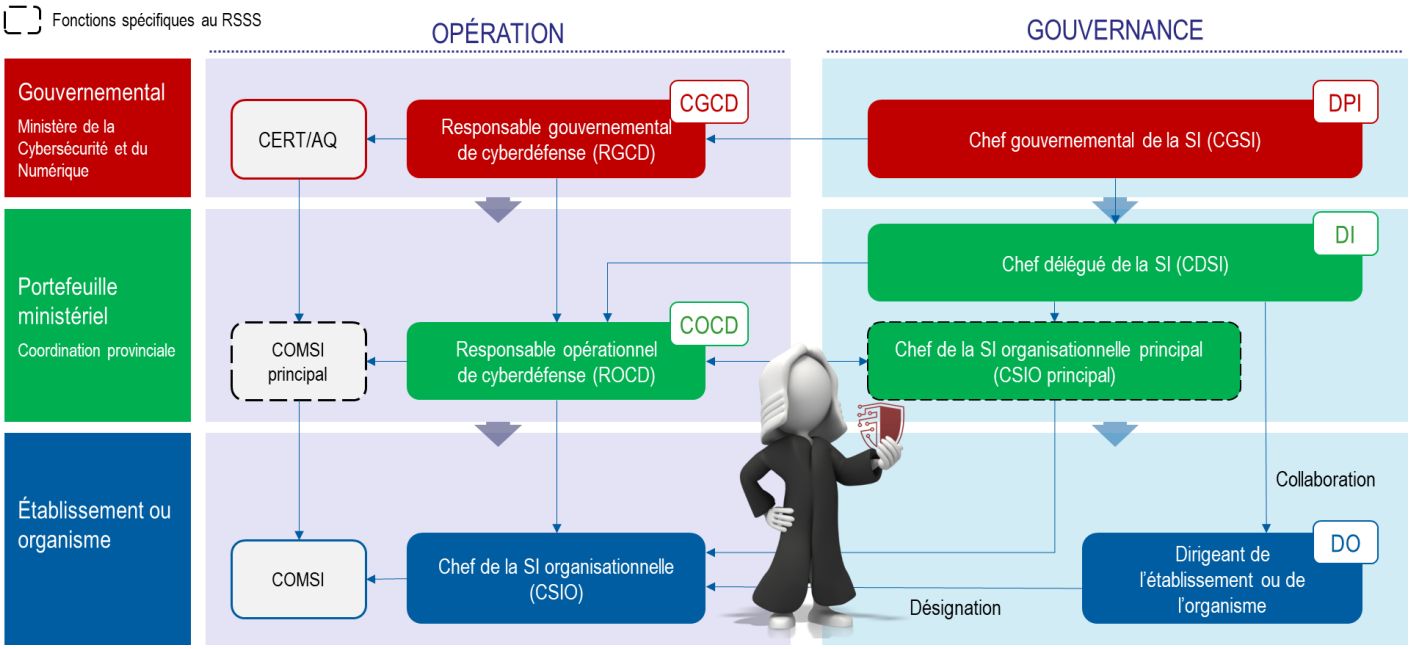
Définitions

Pour l'application du présent cadre de gestion, les termes suivants signifient :

Terme	Description
Actif informationnel	Actif au sens de la Loi sur le partage de certains renseignements de santé (LPCRS), soit, une banque d'information, 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.
Cycle de vie de l'information	L'ensemble des étapes que franchit l'information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisation.
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 de cette information ainsi que celle des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.
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.
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.
Risque lié à la sécurité de l'information	Probabilité non nulle que survienne un événement préjudiciable à la sécurité de l'information, plus ou moins prévisible, et qui peut affecter la réalisation des objectifs d'une organisation.
Utilisateur	Toute personne physique ou morale, groupe ou entité administrative, qui fait usage d'un ou de plusieurs actifs informationnels sous la responsabilité d'une organisation, dont notamment les stagiaires, les résidents, les externes, les chercheurs, les étudiants en recherche, les médecins, le personnel, les bénévoles, les usagers et les tiers.
Système d'information	Système constitué des ressources humaines, des ressources matérielles et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une organisation.

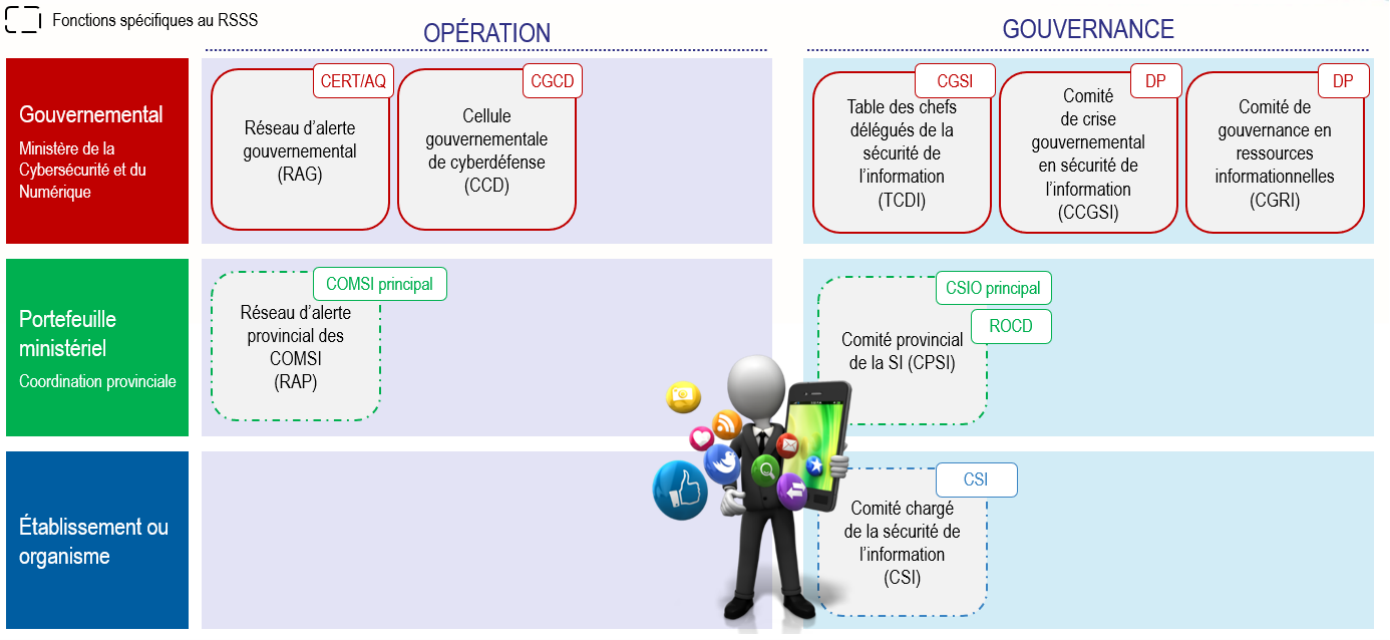
Structure de gouvernance (schéma)

La structure de gouvernance de la SI suivante présente l'organisation fonctionnelle mise en place afin de répondre aux exigences gouvernementales en matière de gestion de la SI, mais également pour prendre en compte les particularités liées au rôle des É/O du RSSS.



Comités (schéma)

Le schéma suivant illustre les comités et les groupes de travail qui sont intégrés à l'organisation de la SI et qui permettront la concertation et la communication entre les différents intervenants.



Rôles et responsabilités

La liste des responsabilités étant importante pour certains rôles, elle a été divisée par thèmes pour favoriser une meilleure compréhension du lecteur.

De plus, les trois niveaux de responsabilités ont été identifiés de la même façon que ceux du schéma illustrant la structure de gouvernance ainsi que celle des comités :

Rouge	Coordination gouvernementale
Vert	Coordination provinciale
Bleu	Établissements et organismes (É/O)

Coordination gouvernementale (MCN)

Cette section décrit les rôles et responsabilités des intervenants en matière de SI au niveau gouvernemental.

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

En vertu des obligations énoncées dans la Loi et la Directive, le 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 :

- 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;
- d'assurer la mise en œuvre des politiques et des stratégies établies en SI, en coordonner l'exécution et en surveiller l'application;
- d'élaborer, diffuser et maintenir à jour des cadres de gestion particuliers en SI, notamment au sujet des services communs;
- d'élaborer, diffuser et faire le suivi de la mise en œuvre de règles relatives à la SI applicable aux organismes publics (OP);
- d'élaborer, encadrer, mettre en place et maintenir à jour des processus gouvernementaux normalisés en gestion de la SI, et en assurer la coordination;
- de formuler, lorsque requis, des indications d'application en matière de SI;
- 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;
- 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);
- d'apporter un soutien continu aux OP dans le déploiement de pratiques exemplaires de SI;

- de développer et mettre à la disposition des OP des outils favorisant le développement des compétences en SI des employés de l'administration publique;
- d'établir les standards et les meilleures pratiques en SI pour l'ensemble du gouvernement.

Le CGSI exerce un lien fonctionnel sur les CDSI, les 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 CCGSI. À ce titre, il conseille le président du comité sur les enjeux de SI et de cybersécurité.

Responsable gouvernemental de cyberdéfense (RGCD)

Le 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 (ci-après « Réseau ») et de voir à son amélioration continue. Ses principales responsabilités sont :

- de mettre en place le CGCD, l'opérationnaliser et faire évoluer son offre de services;
- d'assurer le leadership du Réseau et de la communauté des responsables organisationnels de cyberdéfense (ROCD);
- d'animer la Cellule gouvernementale de cyberdéfense, et relayer les informations transmises par les ROCD au CGSI lorsqu'il le juge approprié;
- 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);
- de développer une vision gouvernementale des risques, des menaces et des vulnérabilités;
- 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;
- d'assurer la réalisation d'activités de surveillance en matière de sécurité de l'information;
- 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;
- de participer à l'élaboration des orientations gouvernementales en matière de cybersécurité;
- de consolider les relations avec les acteurs de l'écosystème de cybersécurité et favoriser l'innovation en la matière;
- d'assurer la mise en œuvre des attentes et des orientations du CGSI au sein du Réseau;
- 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.

Réseau gouvernemental de cyberdéfense (Réseau)

Le 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 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.

Centre gouvernemental de cyberdéfense (CGCD)

Le CGCD est le centre de commandement des opérations de cyberdéfenses 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 québécoise. Le CGCD intervient au niveau tactique et opérationnel afin de soutenir le Réseau dans ses activités de cyberdéfense. Il est responsable notamment :

- 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;
- 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;
- d'assurer, de façon constante, la réalisation d'activités de surveillance en matière de SI;
- 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;
- de mettre en place une surveillance normalisée et en continu des accès à l'information gouvernementale;
- 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;
- 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;
- de fournir des avis et des conseils aux COCD et aux OP;

- de développer des outils partageables au sein du Réseau;
- de développer ou d'assurer le développement et la mise en place de certains services de sécurité;
- d'assurer la mise en relation des intervenants de sécurité au sein de l'administration publique et avec tout autres partenaires jugés appropriés.

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

L'équipe du 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 :

- 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;
- de coordonner, au niveau tactique et opérationnel, la GMVI avec la collaboration du Réseau d'alerte gouvernemental (RAG) et de la Cellule de cyberdéfense;
- d'animer et coordonner le RAG et s'assurer d'une représentation adéquate des membres lors des rencontres de ce réseau.

Coordination provinciale

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[1] 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 :

Gouvernemental

- assurer la mise en œuvre, le respect, la coordination et le suivi des processus gouvernementaux normalisés, notamment de gestion des événements de sécurité;
- assurer et surveiller la mise en place des processus et des mesures de SI requis, conformément aux orientations gouvernementales;
- 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;
- formuler des indications d'application particulières, lorsque requis;
- fournir des conseils basés sur les orientations gouvernementales et les meilleures pratiques en SI.

Orientations stratégiques et priorités d'action

- déterminer les orientations stratégiques et les priorités d'action pour le MSSS et pour les É/O.

Encadrement, exigences, plans d'action

- s'assurer de la mise en œuvre d'un cadre de gouvernance qui régit la SI et l'approuver;
- 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;
- établir les attentes aux CSIO des É/O pour la mise en œuvre des mesures de cybersécurité, si applicable, et leur offrir du soutien.

[1] Un rapport entre deux personnes qui, selon le contexte, permet à l'une d'entre elles de formuler un ordre à l'autre, sans qu'il existe un lien hiérarchique entre ces personnes.

Organisation et opérationnalisation de la cybersécurité

- désigner, parmi le personnel d'encadrement sous sa direction, un ROCD qui voit au bon fonctionnement et à l'évolution de l'offre de service du COCD;
- coordonner et diriger, en collaboration avec son ROCD, les activités de son COCD;
- établir les attentes au CSIO principal pour la mise en œuvre des mesures de cybersécurité, si applicable;
- assurer la prise en charge des événements de sécurité afin de minimiser les préjudices potentiels.

Processus de gestion de la sécurité de l'information

- 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.

Événements de sécurité

- mettre en œuvre toute action requise pour la prise en charge d'un événement de sécurité;
- s'assurer de l'élaboration, du maintien à jour et de l'efficacité du processus ministériel GMVI applicable au MSSS et aux É/O;
- aviser sans délai le CGSI de tout événement de sécurité qui requiert son attention.

Le CDSI est de plus membre invité du CCGSI lorsqu'un incident touche un ou des organismes sous sa responsabilité. À ce titre, il collabore à la résolution de la crise, voit à l'application des recommandations et rend compte de l'avancement des actions au comité.

Comités et tables

- mettre en place, coordonner et animer les comités et groupes de travail requis à l'atteinte de la performance en matière de SI;
- mettre en place des mécanismes de concertation avec les CSIO;
- participer à la Table gouvernementale des CDSI.

Reddition de comptes

- assurer l'obtention de l'information nécessaire à la reddition de compte auprès du CGSI, ou de toute autre information demandée par ce dernier.

Compétences et sensibilisation

- favoriser le développement des compétences de son personnel en SI.

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

Le CDSI désigne un 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 :

Gouvernemental

- coordonner la mise en œuvre des processus gouvernementaux normalisés en SI;
- tenir informés les CSIO des É/O des attentes du gouvernement en matière de SI;
- 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;
- assurer la coordination et la cohérence des actions en SI, conformément aux exigences gouvernementales.

Orientations stratégiques et priorités d'action

- assister le CDSI dans la détermination et la mise en œuvre des orientations stratégiques et des priorités d'action.

Encadrement, exigences, plans d'action

- 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;
- coordonner la mise en œuvre des actions découlant du plan de sécurité élaboré par le CDSI;
- 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.
- 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;
- s'assurer du maintien à jour du registre d'autorité du MSSS, à titre de détenteur.

Organisation et opérationnalisation de la cybersécurité

- collaborer à l'application des mesures opérationnelles de SI recommandées par le ROCD.

Processus de gestion de la sécurité de l'information

- assurer la prise en compte de la SI dans les processus mis en place au sein du MSSS et des É/O.

Événements de sécurité

- collaborer avec le ROCD à l'implantation du processus gouvernemental GMVI au sein du MSSS et de chacun des É/O;
- mettre en œuvre toutes les mesures requises lors d'événements de sécurité afin de réduire au maximum les préjudices éventuels;
- aviser rapidement le CDSI de tout événement de sécurité qui risque de causer un préjudice sérieux;
- s'assurer que le ROCD tient un registre des événements de sécurité selon les modalités précisées par le CGSI.

Gestion des risques liés à la sécurité de l'information

- 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.

Reddition de comptes

- fournir les informations demandées par le CGSI, le CDSI ou le ROCD, ou toute autre information requise par les autorités;
- établir annuellement le portrait de la SI du MSSS et de chacun des É/O.

Comités et tables

- coordonner et animer les comités et groupes de travail requis pour le MSSS et les É/O;
- présider et coordonner le Comité provincial de sécurité de l'information (CPSI);
- mettre en place des mécanismes de concertation avec les CSIO des É/O.

Compétences et sensibilisation

- assurer le développement des compétences du personnel du MSSS en matière de SI;
- 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;
- 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.

Responsable opérationnel de cyberdéfense (ROCD)

Le ROCD dirige 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 :

Gouvernemental

- contribuer activement à rehausser la maturité du Réseau gouvernemental de cyberdéfense en participant à la définition de ses orientations, priorités d'action et pratiques;
- coordonner la mise en œuvre des processus gouvernementaux normalisés en matière de SI, particulièrement ceux relatifs à la cyberdéfense;
- représenter le MSSS et les É/O auprès du CGCD via la Cellule gouvernementale de cyberdéfense ; et y partager les préoccupations.

Orientations stratégiques et priorités d'action

- 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.

Organisation et opérationnalisation de la cybersécurité

- mettre en place le COCD, l'opérationnaliser et faire évoluer son offre de services;
- soutenir le CDSI dans la coordination et la direction de son COCD;
- 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;
- voir à déployer toute autre mesure de sécurité opérationnelle, notamment dans le cadre du processus ministériel GMVI;
- 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;
- s'assurer que chaque É/O se dote d'un Centre opérationnel de sécurité (COS)[2] 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;
- maintenir un registre de tous les représentants du RAG pour le MSSS et les É/O;
- 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 (GIA, infonuagique, etc.).

Événements de sécurité

- 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;
- 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;

[2] SOC *(Security operations center)* en anglais

- assurer le fonctionnement du réseau d'alerte provincial des COMSI des É/O (RAP).

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

Gestion des risques liés à la sécurité de l'information

- 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;
- développer une connaissance et une compréhension des risques liés à la SI;
- collaborer à la mise en œuvre et à l'évolution de la gestion intégrée des risques liés à la SI du MSSS.

Comités et tables

- assister aux rencontres de la Cellule gouvernementale de cyberdéfense;
- mettre en place et coordonner une instance de collaboration qui réunit tous les COMSI (MSSS et É/O) au moins quatre fois par année.

Reddition de comptes

- élaborer un bilan annuel de ses activités destiné au CDSI, ainsi que toute autre reddition de compte requise par ce dernier.

Compétences et sensibilisation

- assurer le développement des compétences du personnel du COCD en matière de cybersécurité;
- 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.

Centre opérationnel de cyberdéfense (COCD)

Le 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 :

- 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;
- 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;

- définir des mécanismes de suivi et de concertation afin de les accompagner dans la mise en place des mesures de sécurité;
- 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;
- maintenir une offre de services de cyberdéfense destinée au MSSS ainsi qu'aux É/O;
- fournir des avis et des conseils;
- dégager et déposer au ROCD des recommandations sur des pratiques ou indications d'application particulière qui permettraient de rehausser le niveau de sécurité;
- exercer toute autre activité de SI que lui attribue son CDSI.

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

Le 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 :

- déployer ce processus et en coordonner les actions, en collaboration étroite avec les intervenants impliqués;
- identifier les menaces, 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;
- s'assurer de l'élaboration, de la mise à jour et de l'application d'un plan interne de réponse aux MVI;
- collaborer étroitement avec son CSIO principal et son ROCD en leur fournissant le soutien technique nécessaire à l'exercice de leurs responsabilités;
- leur communiquer tout événement de sécurité d'intérêt ou nécessitant leur intervention;
- fournir aux COMSI des É/O l'information et le support nécessaires à l'exercice de leurs responsabilités;
- s'assurer de la réalisation d'analyses de risques de sécurité;
- 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;
- présider le RAI des COMSI et participer activement au RAG.

Établissements et organismes (É/O)

Dirigeant de l'organisation (DO)

En tant que premier responsable de la SI de son organisation, le DO 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 :

Gouvernemental

- s'assurer du respect des lois, des orientations et des règles de SI gouvernementales qui s'appliquent à son organisation.

Encadrement, exigences, plans d'action

- s'assurer de l'attribution appropriée des rôles et des responsabilités du présent cadre de gestion;
- approuver les bilans de SI et les plans d'action qui en découlent.

Processus de gestion de la sécurité de l'information

- s'assurer de la mise en œuvre des processus de gestion intégrée de la SI pour son organisation.

Événements de sécurité

- 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;
- demeurer alerte et se rendre disponible en cas d'incident afin de régler la situation promptement.

Comités et tables

- s'assurer de la mise en place d'un comité chargé de la SI (CSI) au sein de son organisation.

Compétences et sensibilisation

- sensibiliser et mobiliser ses gestionnaires quant aux règles et bonnes pratiques en SI;
- maintenir une vigilance en continu en matière de SI pour son organisation.

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

Le CSIO de chacun des É/O est le répondant en matière de SI pour son organisation. 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 :

Orientations stratégiques et priorités d'action

- coordonner la mise en œuvre des orientations stratégiques et des priorités d'action en SI provenant du CSIO principal ou de son organisation.

Encadrement, exigences, plans d'action

- 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;
- mettre en œuvre un plan d'action en SI qui favorise la performance de la gestion de la SI et en faire le suivi;
- 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;
- 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);
- 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;
- s'assurer de la mise en œuvre d'un registre d'autorité.

Processus de gestion de la sécurité de l'information

- s'assurer que son organisation participe aux processus provinciaux de gestion de la SI (ex. : GMVI).

Organisation et opérationnalisation de la cybersécurité

- s'assurer que des politiques internes ou des processus relatifs à la cybersécurité sont définis et mis en œuvre;
- collaborer étroitement avec le CSIO principal et le ROCD pour la mise en œuvre des mesures opérationnelles de SI recommandées par ce dernier;
- s'assurer de l'application effective de ces mesures à l'intérieur des délais impartis par le ROCD;
- s'assurer que son É/O 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.

Événements de sécurité

- s'assurer de la mise en œuvre et de l'amélioration continue du processus ministériel GMVI applicable à son organisation;

- 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;
- communiquer au CSIO principal toute situation à risque ou tout événement de sécurité majeur.

Gestion des risques liés à la sécurité de l'information

- voir à la mise en œuvre et à l'évolution d'un processus de gestion intégrée des risques liés à la SI;
- 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).

Reddition de comptes

- produire un bilan annuel et un plan d'action triennal en SI et les transmettre au CSIO principal.

Comités et tables

- participer activement aux rencontres du CPSI et y relayer les préoccupations de son organisation;
- mettre en œuvre, coordonner et animer le CSI requis pour son organisation.

Compétences et sensibilisation

- élaborer et mettre en œuvre un plan de sensibilisation en SI à l'intention de l'ensemble de son personnel.

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

Le COMSI apporte le support nécessaire à la gestion opérationnelle de la SI dans son organisation. Son rôle consiste notamment à :

- définir les mesures opérationnelles de SI à y mettre en place et faire le suivi de leur application;
- contribuer à l'élaboration du processus ministériel GMVI et à son amélioration continue;
- collaborer au déploiement de ce processus et en coordonner les actions à l'intérieur de son organisation, en collaboration étroite avec le COMSI principal;
- fournir l'expertise nécessaire à l'exercice des responsabilités de son CSIO et au support du COS (ou SOC) de son É/O;
- informer le ROCD et son CSIO de tout événement de sécurité d'intérêt ou nécessitant leur intervention;
- participer activement au RAI des COMSI ainsi qu'au RAG.

Détenteur de l'information

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

- s'assurer auprès de son CSIO que ces actifs sont classifiés adéquatement (catégorisation et analyse de préjudices), que cette classification est à jour et qu'ils sont consignés dans le registre d'autorité;
- collaborer avec le CSIO, le COMSI ou avec tout autre intervenant en SI, à l'élaboration et à l'application de l'ensemble des mesures de sécurité protégeant ces actifs;
- autoriser les accès à ces actifs ou leur retrait;
- s'assurer de la prise en charge des risques résiduels liés à tout projet ou à toute modification touchant ces actifs.

Gestionnaire

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

- informer adéquatement son personnel des exigences du présent cadre, 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;
- intégrer aux ententes de services 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;
- communiquer rapidement à son COMSI toute menace, vulnérabilité ou incident de SI dont il a connaissance, dans le respect du processus ministériel GMVI.

Personnel

Le personnel autorisé à accéder aux actifs informationnels du MSSS et des É/O joue un rôle prépondérant en matière de SI. À ce titre, il doit :

- 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;
- communiquer rapidement toute menace, vulnérabilité ou événement de sécurité dont il a connaissance, dans le respect du processus ministériel GMVI.
- Respecter et effectuer l'ensemble des actions de sensibilisation demandées par le CSIO.

Comités

Vous retrouvez dans cette section les comités appartenant à chacun des trois paliers.

Coordination gouvernementale (MCN)

Comité de gouvernance en ressources informationnelles (CGRI)

En vertu de la LGGRI, le CGRI a pour mandat :

- d'élaborer des orientations à proposer au Conseil des ministres;
- d'assurer la mise en œuvre concertée des orientations (stratégie, politique, etc.) déterminées par le ministre de la Cybersécurité et du Numérique ou le Conseil des ministres;
- d'identifier des opportunités d'optimisation, de partage et de mise en commun de services en ressources informationnelles et d'actifs informationnels, en favorisant leur interopérabilité;
- de recommander au Conseil des ministres les services pouvant être rendus par le ministère de la Cybersécurité et du Numérique.

Le CGRI peut également prendre en compte tout autre enjeu qui lui est formulé en matière de ressources informationnelles, notamment ceux étudiés en sous-comité. À ce titre, le Sous-comité Sécurité de l'information et données gouvernementales (SCSIDG) est un sous-comité permanent qui a pour mandat de conseiller le CGRI et le DPI sur les enjeux et risques associés à la SI et à la cybersécurité, ainsi que ceux liés à l'architecture d'entreprise gouvernementale (volet données gouvernementales). Le SCSIDG est présidé par l'un de ses membres qui est choisi par ses pairs et désigné par le CGRI. Il est composé de DI nommés par le CGRI et du DPI. Le SCSIDG a pour mission :

- de suivre et d'appuyer la mise en œuvre de la Politique gouvernementale de cybersécurité et du chantier sur la gestion des données numériques gouvernementales;
- de suivre et d'appuyer le déploiement du Réseau;
- d'examiner les sujets liés à la SI et aux données gouvernementales;
- de conseiller le DPI et le CGRI en ces matières.

Table des chefs délégués de la sécurité de l'information (TCDSI)

Cette table est présidée par le CGSI et regroupe l'ensemble des CDSI. La table peut également s'adjoindre d'autres spécialistes de l'Administration publique afin de lui assurer un soutien efficace dans l'exécution de ses travaux. Elle est convoquée par le CGSI à une fréquence qu'il détermine. Ses principaux mandats sont :

- d'assurer la concertation au regard de la mise en œuvre des orientations déterminées par le ministre de la Cybersécurité et du Numérique ou le Conseil des ministres, et des attentes ou indications d'application communiquées par le CGSI;
- d'identifier les opportunités d'optimisation, de partage et de mise en commun de services en SI;

- d'identifier les problématiques de SI rencontrées au sein de l'Administration gouvernementale et proposer des pistes de solutions;
- de contribuer à la définition, à la mise en œuvre et au suivi des projets gouvernementaux de SI.

Cellule gouvernementale de cyberdéfense (Cellule)

La Cellule regroupe le RGCD, qui anime la Cellule, et les ROCD. Elle favorise la prise de décision concertée et le partage d'information, et permet d'échanger régulièrement sur les enjeux de cyberdéfense et de statuer sur les actions et les solutions technologiques à mettre en œuvre au sein du Réseau. Les principaux objectifs de la Cellule sont :

- de partager, échanger et fédérer les actions en cyberdéfense;
- de recommander au RGCD des mesures de cyberdéfense à mettre en place au sein du Réseau;
- de mettre en œuvre des actions visant à rehausser le niveau de maturité global du Réseau;
- de coordonner, au niveau stratégique, le processus GMVI, selon les modalités établies.

Réseau d'alerte gouvernemental (RAG)

Coordonnée par le CERT/AQ, le RAG vise à améliorer la capacité opérationnelle du Réseau en matière de prévention et de réaction vis-à-vis des menaces, des vulnérabilités, des incidents et des cyberattaques. Il met en relation des intervenants opérationnels de cyberdéfense et leur fournit les moyens techniques nécessaires pour échanger efficacement l'information en situation de crise. La participation des représentants des OP à ces rencontres est obligatoire.

Comité de crise gouvernemental en sécurité de l'information (CCGSI)

Le CCGSI assure une gestion concertée des situations de crise en SI. Il est le centre de coordination de la gestion de crise et prend les décisions permettant de mettre en œuvre les mesures nécessaires pour contenir les effets négatifs de la crise et la résoudre dans les meilleurs délais.

Plusieurs OP siègent sur ce comité afin d'y apporter l'expertise spécifique à la mission de leur organisation et de conseiller quant aux actions et décisions à prendre en fonction de l'évolution de la crise. Les modalités entourant le fonctionnement du CCGSI sont encadrées par une charte et un plan gouvernemental de gestion de crise en sécurité de l'information arrimée au Plan national de sécurité civile. Présidé par le DPI ou son représentant, il a notamment pour mandat :

- d'évaluer les impacts de la situation de crise sur les activités gouvernementales;
- de prendre les décisions de nature stratégique afin de limiter les impacts et de résoudre les situations de crise;
- d'établir un plan d'intervention, ainsi qu'un plan de communication, et d'en assurer les suivis;
- de formuler des recommandations au dirigeant principal de l'information (DPI) ou au gouvernement;
- de mobiliser les ressources nécessaires à la mise en œuvre du plan d'intervention (ressources humaines, financières et matérielles);
- de superviser le rétablissement des activités en lien avec la sécurité de l'information;
- de clore la gestion de crise;
- de faire évoluer le processus en continu.

Coordination provinciale

Comité provincial de sécurité de l'information (CPSI)

Le CPSI est un comité stratégique de coordination provinciale pour la mise en œuvre de toute composante d'encadrement de la SI. Il est présidé par le CSIO principal.

Ce comité peut être consulté sur :

- les documents d'encadrement, les bilans, les plans d'action et toute proposition d'action ou état d'avancement de projets en lien avec la SI;
- les événements de sécurité ayant mis ou ayant pu mettre en péril la SI des É/O.

Il est constitué de membres permanents, temporaires et de participants sollicités en fonction des sujets.

Réseau d'alerte provincial des COMSI des É/O (RAP)

Ce réseau d'alerte demeure un canal majeur de partage d'expertise entre ses membres. Sous la responsabilité du ROCD et présidé par le COMSI principal, il est composé des COMSI des É/O. À ce titre, il :

- représente l'entité d'alerte centrale en matière de sécurité opérationnelle pour le MSSS et pour les É/O;
- soutient tous les COMSI dans l'exercice de leurs fonctions, notamment dans la prévention et la détection d'incidents de SI, leur prise en charge et leur suivi.

Établissements et organismes (É/O)

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

Le DO de chaque É/O s'assure de la mise en œuvre d'un CSI pour son organisation afin de favoriser la concertation et la collaboration entre les intervenants. Son CSIO met en œuvre ce comité, le coordonne et l'anime.

Entrée en vigueur et révision

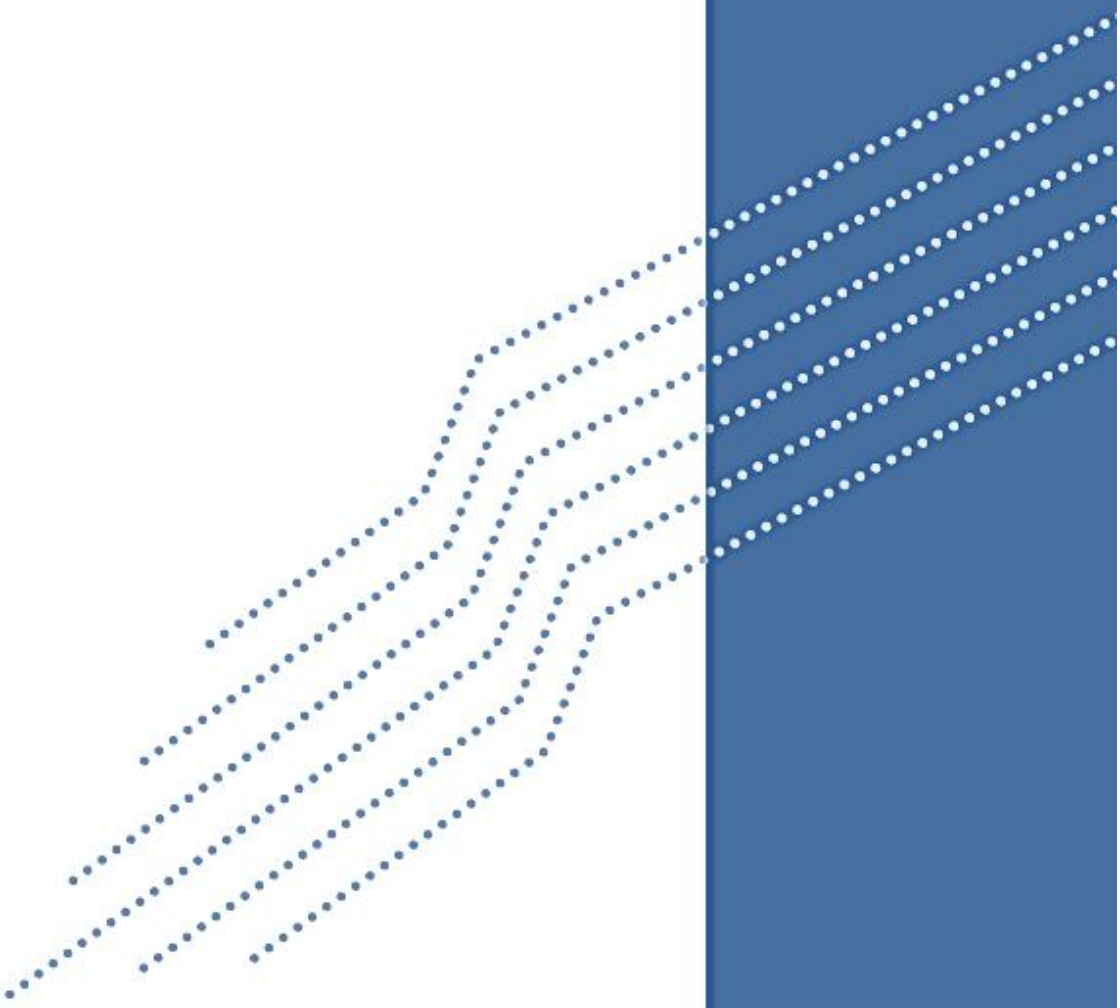
Ce cadre de gestion entre en vigueur à la date de son approbation. Il doit être révisé :

- tous les cinq ans;

ou

- lors de changements organisationnels ou de l'adoption de nouvelles orientations gouvernementales ou ministérielles.

Approuvé par le chef délégué de la sécurité de l'information (CDSI) :	Reno Bernier
Date d'approbation :	29 juin 2022



Santé
et Services sociaux
Québec