A.M., 2022

Arrêté numéro 2022-04 du ministre de la Cybersécurité et du Numérique en date du 26 juillet 2022

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03)

CONCERNANT le Cadre gouvernemental de gestion de la sécurité de l'information

LE MINISTRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE,

VU le deuxième alinéa de l'article 21 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03) suivant lequel le ministre de la Cybersécurité et du Numérique peut déterminer des orientations portant sur les principes ou les pratiques à appliquer en matière de gestion des ressources informationnelles, incluant les pratiques pour optimiser l'organisation du travail de même que la nécessité de considérer l'ensemble des technologies offrant un potentiel d'économies ou de bénéfices et des modèles de développement ou d'acquisition disponibles pour répondre aux besoins des organismes publics, dont les logiciels libres;

CONSIDÉRANT qu'il y a lieu, pour le ministre de la Cybersécurité et du Numérique, de déterminer des orientations en matière de sécurité de l'information, soient celles déterminées dans le Cadre gouvernemental de gestion de la sécurité de l'information, annexé au présent arrêté;

ARRÊTE CE QUI SUIT :

DÉTERMINE des orientations en matière de sécurité de l'information, soient celles déterminées dans le Cadre gouvernemental de gestion de la sécurité de l'information, annexé au présent arrêté.

Québec, le 26 juillet 2022

Le ministre de la Cybersécurité et du Numérique,
ÉRIC CAIRE

Cadre gouvernemental de gestion de la sécurité de l'information

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03, a. 21)

CHAPITRE I
DISPOSITIONS INTRODUCTIVES

1. Le présent cadre appuie la Directive gouvernementale sur la sécurité de l'information, approuvée par le décret numéro 1514-2021 du 8 décembre 2021 (2021, G.O. 2, 7694), et vise à établir une vision commune en matière de sécurité de l'information de même qu'à assurer la cohérence et la coordination des interventions en telle matière.

Il présente, dans le contexte de l'application de cette directive et de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), l'organisation fonctionnelle de la sécurité de l'information au sein de l'Administration publique.

Il précise la structure de gouvernance de la sécurité de l'information gouvernementale et énonce ou réaffirme les responsabilités des intervenants, comités, groupes de travail et autres entités en telle matière, en lien avec les responsabilités du ministre de la Cybersécurité et du Numérique et celles du sous-ministre de la Cybersécurité et du Numérique, également dirigeant principal l'information et chef gouvernemental de la sécurité de l'information.

2. Dans le présent cadre, on entend par :

1° « Cellule gouvernementale de cyberdéfense » : la Cellule de cyberdéfense visée à l'article 8 de la Directive;

2° « Centre gouvernemental de cyberdéfense (CGCD) » : l'unité administrative spécialisée en sécurité de l'information visée à l'article 12.5 de la Loi;

3° « Centre opérationnel de cyberdéfense (COCD) » : l'unité administrative spécialisée en sécurité de l'information visée à l'article 9 de la Directive;

4° « chef délégué de la sécurité de l'information (CDSI) » : le dirigeant de l'information qui agit à ce titre en vertu du paragraphe 9.1° du premier alinéa de l'article 10.1 de la Loi;

5° « chef gouvernemental de la sécurité de l'information (CGSI) » : le dirigeant principal de l'information qui agit à ce titre en vertu du paragraphe 1° du premier alinéa de l'article 7.1 de la Loi;

© Éditeur officiel du Québec, 2022

6° « chef de la sécurité de l'information organisationnelle (CSIO) » : un membre du personnel d'encadrement d'un organisme public désigné en vertu de l'article 10 de la Directive ou, selon le contexte, le chef délégué de la sécurité de l'information;

7° « comité de gouvernance en ressources informationnelles (CGRI) » : le comité visé à l'article 12.1 de la Loi;

8° « Directive » : la Directive gouvernementale sur la sécurité de l'information, approuvée par le décret numéro 1514-2021 du 8 décembre 2021 (2021, G.O. 2, 7694);

9° « événement de sécurité » : toute forme d'atteinte, présente ou appréhendée, telle 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'un organisme public ou d'une personne agissant pour ce dernier;

10° « indication d'application » : toute instruction au sens du deuxième alinéa de l'article 7 de la Loi;

11° « lien fonctionnel » : 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;

12° « Loi » : la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03);

13° « niveau gouvernemental » : un niveau de gestion qui, en matière de sécurité de l'information pour les organismes publics formant l'Administration publique, implique les intervenants, les comités, les groupes de travail et les autres entités visés au chapitre III;

14° « niveau de portefeuille » : un niveau de gestion qui, en matière de sécurité de l'information pour le ministère d'un ministre ainsi que les organismes publics qui sont rattachés à ce ministre, implique les intervenants et les entités visés au chapitre IV;

15° « niveau organisationnel » : un niveau de gestion qui, en matière de sécurité de l'information pour un organisme public, implique les intervenants visés au chapitre V;

16° « répondant en matière de sécurité de l'information » : la personne désignée en vertu de l'article 11 de la Directive;

17° « Réseau gouvernemental de cyberdéfense » : le réseau visé à l'article 7 de la Directive;

18° « responsable gouvernemental de cyberdéfense (RGCD) » : la personne désignée en vertu du paragraphe 4° du deuxième alinéa de l'article 5 de la Directive;

19° « responsable opérationnel de cyberdéfense (ROCD) » : la personne désignée en vertu du paragraphe 3° du deuxième alinéa de l'article 6 de la Directive.

3. Le présent cadre s'applique aux organismes publics visés à l'article 2 de la Loi, lesquels forment l'Administration publique aux fins de la Loi, de la Directive et du présent cadre.

CHAPITRE II
STRUCTURE DE GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION GOUVERNEMENTALE

4. L'organisation fonctionnelle de la sécurité de l'information au sein de l'Administration publique s'articule, dans le respect de la Loi et de la Directive, autour d'une structure de gouvernance qui repose sur ces trois niveaux de gestion :

1° un niveau gouvernemental;

2° un niveau de portefeuille;

3° un niveau organisationnel.

Une telle structure de gouvernance repose également sur la présence de liens fonctionnels entre les intervenants en matière de sécurité de l'information d'un niveau à l'autre, lesquels liens visent à favoriser une concertation agile et transparente pour répondre efficacement aux exigences de sécurité de l'information. Ces liens, énoncés dans la Directive et représentés par des pointillés à la Figure 1 ci-après, se résument notamment comme suit :

1° le chef gouvernemental de la sécurité de l'information (CGSI) avec les chefs délégués de la sécurité de l'information (CDSI), les chefs de la sécurité de l'information organisationnelle (CSIO) et les répondants en matière de sécurité de l'information;

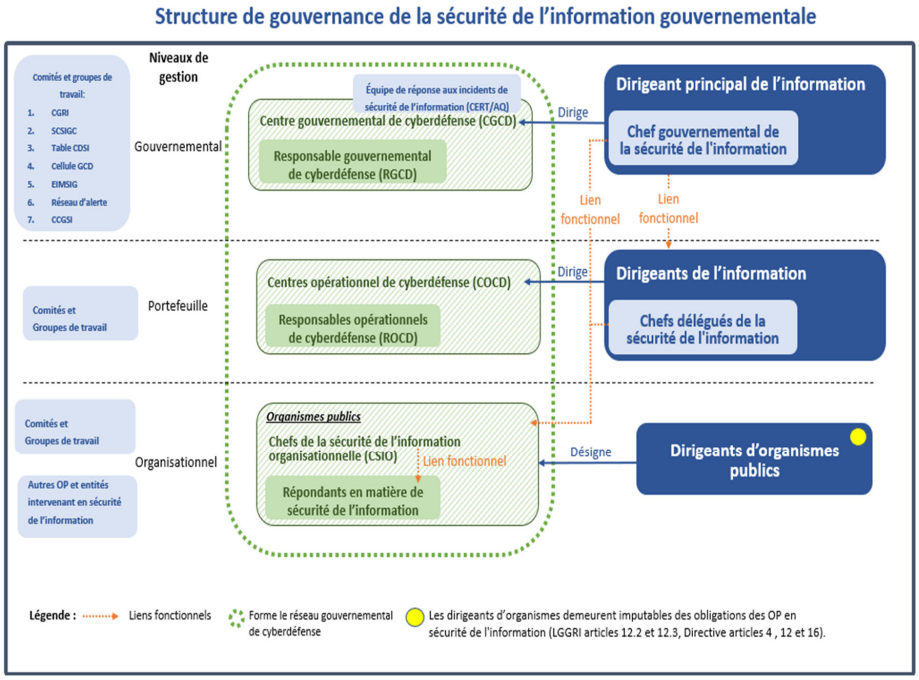
2° un chef délégué de la sécurité de l'information (CDSI) avec les chefs de la sécurité de l'information organisationnelle (CSIO) et les répondants en matière de sécurité de l'information, auxquels il se rattache;

3° un chef de la sécurité de l'information organisationnelle (CSIO) avec les répondants en matière de sécurité de l'information, auxquels il se rattache.

© Éditeur officiel du Québec, 2022

La structure de gouvernance visée au présent article est illustrée avec la Figure 1 :

Figure 1



CHAPITRE III
RESPONSABILITÉS AU NIVEAU GOUVERNEMENTAL

SECTION I
CHEF GOUVERNEMENTAL DE LA SÉCURITÉ DE L'INFORMATION (CGSI)

5. Le chef gouvernemental de la sécurité de l'information (CGSI) assure la coordination gouvernementale de la sécurité de l'information aux niveaux stratégique, tactique et opérationnel. Il assume les responsabilités prévues à l'article 12.6 de la Loi et à l'article 5 de la Directive.

SECTION II
RESPONSABLE GOUVERNEMENTAL DE CYBERDÉFENSE (RGCD)

6. Le responsable gouvernemental de cyberdéfense (RGCD) a pour rôle de voir au bon fonctionnement du Centre gouvernemental de cyberdéfense (CGCD) tel que le prévoit le paragraphe 4° du deuxième alinéa de l'article 5 de la Directive. Il assure également, en vertu du premier alinéa de l'article 7 de cette directive, le commandement et le leadership ainsi que la coordination et l'amélioration continue du Réseau gouvernemental de cyberdéfense.

Le responsable gouvernemental de cyberdéfense (RGCD) assume, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités suivantes :

1° collaborer avec le chef gouvernemental de la sécurité de l'information (CGSI) dans la direction, l'opérationnalisation et l'évolution de l'offre de service du Centre gouvernemental de cyberdéfense (CGCD);

2° contribuer à l'établissement d'une vision gouvernementale et à l'élaboration d'orientations afférentes en matière de cybersécurité;

3° assurer le déploiement, la coordination et le maintien de processus gouvernementaux normalisés de cybersécurité définis par le chef gouvernemental de la sécurité de l'information (CGSI), dont le processus de gestion des événements de sécurité;

© Éditeur officiel du Québec, 2022

4° animer la Cellule de cyberdéfense et, lorsqu'approprié, relayer au chef gouvernemental de la sécurité de l'information (CGSI) les informations qui lui sont communiquées par les responsables opérationnels de cyberdéfense (ROCD);

5° apporter aux centres opérationnels de cyberdéfense (COCD) le soutien et l'accompagnement nécessaires au respect par ces derniers des attentes du chef gouvernemental de la sécurité de l'information (CGSI), des bonnes pratiques de cybersécurité ainsi que des orientations, standards, stratégies, directives, règles et indications d'application pris en vertu de la Loi, et en assurer le suivi;

6° effectuer, dans le cadre de la lutte contre les cyberattaques et les cybermenaces au Québec, une veille dans le cyberespace en vue d'identifier et, le cas échéant, d'appliquer la prise en charge appropriée à l'égard des menaces pouvant compromettre la sécurité de l'information gouvernementale;

7° coordonner les activités de surveillance des réseaux informatiques gouvernementaux permettant de détecter les accès non autorisés et d'analyser les comportements malicieux;

8° conseiller le chef gouvernemental de la sécurité de l'information (CGSI) en matière de pratiques de cybersécurité lors de situations nécessitant une intervention particulière de ce dernier;

9° contribuer à la création de liens de collaboration durables avec les différents acteurs de la communauté des technologiques de l'information, spécialisés en sécurité de l'information, en vue de favoriser l'innovation en matière de cybersécurité et la mise en commun du savoir et des ressources requises pour faire face efficacement aux cyberattaques et aux cybermenaces;

10° effectuer, lorsque nécessaire, des vérifications de sécurité des systèmes gouvernementaux et en dégager les recommandations et les priorités d'action;

11° proposer au chef gouvernemental de la sécurité de l'information (CGSI) des mécanismes de suivi et de concertation et voir à leur mise en œuvre de manière à accompagner les centres opérationnels de cyberdéfense (COCD) dans la mise en place des mesures de sécurité;

12° s'assurer de la présence d'une offre de formation adéquate pour les employés du Centre gouvernemental de cyberdéfense (CGCD) et des centres opérationnels de cyberdéfense (COCD), dans l'objectif de développer et de maintenir une expertise de pointe en cybersécurité.

SECTION III
RÉSEAU GOUVERNEMENTAL
DE CYBERDÉFENSE

7. Le Réseau gouvernemental de cyberdéfense est, tel que le prévoit l'article 7 de la Directive, formé du Centre gouvernemental de cyberdéfense (CGCD), des centres opérationnels de cyberdéfense (COCD) et des organismes publics par l'intermédiaire de leurs chefs de la sécurité de l'information organisationnelle (CSIO). En plus de la mission prévue à cet article, le Réseau assume, dans l'organisation fonctionnelle de la sécurité de l'information, des responsabilités visant notamment à :

1° permettre la mutualisation des efforts et des ressources au sein de l'Administration publique;

2° favoriser l'échange et le partage des connaissances ainsi que le recours à des pratiques communes au sein de l'Administration publique.

SECTION IV
CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE (CGCD)

8. Le Centre gouvernemental de cyberdéfense (CGCD) assume, dans l'organisation fonctionnelle en matière de sécurité de l'information, la responsabilité d'apporter aux membres du Réseau gouvernemental de cyberdéfense le soutien nécessaire dans la prise en charge des exigences de cybersécurité en mettant à leur disposition des services centralisés, une expertise de pointe et des pratiques exemplaires en matière de cybersécurité.

SECTION V
ÉQUIPE DE RÉPONSE AUX INCIDENTS
DE SÉCURITÉ DE L'INFORMATION

9. Le Centre gouvernemental de cyberdéfense (CGCD) maintient, en son sein, une équipe appelée « Équipe de réponse aux incidents de sécurité de l'information ». Cette équipe intervient dans la coordination gouvernementale de gestion des événements de sécurité en collaboration avec la Cellule de cyberdéfense et le Réseau d'alerte gouvernemental. Elle est communément appelée « CERT/AQ » qui est un sigle combinant les expressions « computer emergency response team » et « administration québécoise ».

Le CERT/AQ assume, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités suivantes :

© Éditeur officiel du Québec, 2022

1° apporter aux membres du Réseau gouvernemental de cyberdéfense le soutien et l'accompagnement requis dans la gestion des événements de sécurité et dans l'amélioration de leurs capacités d'intervention en telle matière;

2° assurer l'animation et la coordination du Réseau d'alerte gouvernemental visé à l'article 17 et de l'Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale (EIMSIG) visée à l'article 14.

SECTION VI
COMITÉS ET GROUPES DE TRAVAIL

§1. Comité de gouvernance des ressources informationnelles (CGRI)

10. En matière de sécurité de l'information, le comité de gouvernance en ressources informationnelles (CGRI) a, en plus des mandats décrits à l'article 12.1 de la Loi, celui de formuler des recommandations au dirigeant principal de l'information sur les enjeux de sécurité de l'information qui lui sont présentés.

§2. Sous-comité Sécurité de l'information gouvernementale et cybersécurité (SCSIGC)

11. Le Sous-comité Sécurité de l'information gouvernementale et cybersécurité (SCSIGC), un sous-comité du comité de gouvernance en ressources informationnelles (CGRI), est composé de dirigeants de l'information choisis par le comité de gouvernance en ressources informationnelles (CGRI). Il est présidé par l'un de ses membres que désigne ce comité, sur recommandation de ses pairs. Il a pour mandat :

1° de suivre et d'appuyer la mise en œuvre de la Politique gouvernementale de cybersécurité;

2° de veiller à l'évolution du rôle de chef délégué de la sécurité de l'information (CDSI);

3° de suivre et d'appuyer le déploiement du Réseau gouvernemental de cyberdéfense;

4° d'examiner les sujets liés à la sécurité de l'information, y compris la cybersécurité;

5° d'examiner tout autre enjeu qui lui est délégué par le comité de gouvernance en ressources informationnelles (CGRI);

6° de conseiller le comité de gouvernance en ressources informationnelles (CGRI) et le dirigeant principal de l'information en matière de sécurité de l'information.

Les modalités de fonctionnement de ce sous-comité sont encadrées par une charte établie par le comité de gouvernance en ressources informationnelles (CGRI).

§3. Table des chefs délégués de la sécurité de l'information

12. La table des chefs délégués de la sécurité de l'information est présidée par le chef gouvernemental de la sécurité de l'information (CGSI) et elle regroupe l'ensemble des chefs délégués de la sécurité de l'information (CDSI). La table peut s'adjoindre d'autres spécialistes de l'Administration publique en mesure de lui assurer un soutien efficace dans l'exécution de ses travaux. La table a pour mandat :

1° de favoriser la concertation au regard de la mise en œuvre des orientations, standards, stratégies, directives, règles et indications d'application en matière de sécurité de l'information pris en vertu de la Loi;

2° de permettre aux membres d'exposer les travaux d'intérêt commun ainsi que les problématiques d'ensemble et de dégager les pistes de solutions correspondantes;

3° d'identifier les opportunités d'optimisation, de partage et de mise en commun de services;

4° de contribuer à l'élaboration, à la mise en œuvre et au suivi des projets à portée gouvernementale.

§4. La Cellule gouvernementale de cyberdéfense

13. La Cellule gouvernementale de cyberdéfense est formée des responsables opérationnels de cyberdéfense (ROCD) et du responsable gouvernemental de cyberdéfense (RGCD) qui en assure l'animation. Elle vise à mobiliser ses membres autour d'objectifs communs de cyberdéfense et leur permet :

1° d'échanger sur les enjeux de cyberdéfense;

2° de recommander au responsable gouvernemental de cyberdéfense (RGCD) les interventions, y compris les solutions technologiques afférentes, à mettre en œuvre;

3° de contribuer à la coordination de la gestion des événements de sécurité.

§5. Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale (EIMSIG)

14. L'Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale (EIMSIG) est une équipe gouvernementale multidisciplinaire d'échange de

© Éditeur officiel du Québec, 2022

connaissances sur les menaces et les incidents de sécurité de l'information, animée et coordonnée par l'Équipe de réponse aux incidents de sécurité de l'information (CERT/AQ).

15. Le noyau permanent de l'Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale (EIMSIG) est formé par l'Équipe de réponse aux incidents de sécurité de l'information (CERT/AQ), le ministère de la Sécurité publique, la Sûreté du Québec, le ministère de la Justice du Québec, le Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité le ministère du Conseil exécutif. Peut s'adjoindre à ce noyau tout autre organisme public à même de lui apporter l'expertise complémentaire nécessaire à la connaissance des menaces, des incidents ainsi que des préjudices qui peuvent en découler.

16. L'Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale (EIMSIG) assume, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités suivantes :

1° partager ses efforts de veille en matière de sécurité de l'information;

2° produire, à la demande du chef gouvernemental de la sécurité de l'information (CGSI) ou du responsable gouvernemental de cyberdéfense (RGCD), des avis et des conseils sur des enjeux particuliers en sécurité de l'information;

3° produire annuellement, à l'intention du chef gouvernemental de la sécurité de l'information (CGSI) et du responsable gouvernemental de cyberdéfense (RGCD), un rapport sur ses activités et sur l'analyse des menaces et des incidents de sécurité de l'information pertinents, incluant les recommandations d'améliorations afférentes;

4° participer, lorsque requis, au Réseau d'alerte gouvernemental visé à l'article 17.

§6. Réseau d'alerte gouvernemental

17. Le Réseau d'alerte gouvernemental est coordonné par l'Équipe de réponse aux incidents de sécurité de l'information (CERT/AQ). Il est formé de répondants en matière de sécurité de l'information visés à l'article 23. Il constitue, pour les organismes publics, un moyen d'échange dans le domaine de la cybersécurité. Il permet à ces organismes :

1° de contribuer à la gestion des événements de sécurité;

2° d'accéder à une information pertinente sur les menaces et les vulnérabilités en matière de sécurité de l'information;

3° de développer l'expertise en matière de sécurité de l'information et d'accroître leur capacité de réaction aux événements de sécurité;

4° d'échanger sur des solutions en sécurité de l'information.

§7. Comité de crise gouvernemental en sécurité de l'information

18. Le Comité de crise gouvernemental en sécurité de l'information (CCGSI) est le centre de coordination qui assure une gestion concertée des situations de crise en matière de sécurité de l'information et il prend, sur le plan administratif, les décisions à portée gouvernementale permettant de mettre en œuvre les mesures nécessaires pour contenir les effets négatifs d'une crise et de la résoudre dans les meilleurs délais.

Ce comité est présidé par le chef gouvernemental de la sécurité de l'information et il se compose de plusieurs organismes publics à même d'y apporter l'expertise spécifique à leur mission et de fournir des conseils quant aux actions et aux décisions à prendre en fonction de l'évolution d'une crise.

Les modalités de fonctionnement de ce comité sont encadrées par une charte et un plan gouvernemental de gestion de crise en sécurité de l'information, arrimés au Plan national de sécurité civile.

Ce comité assume, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités suivantes :

1° évaluer les impacts d'une situation de crise sur les activités gouvernementales;

2° prendre les décisions de nature stratégique afin de limiter les impacts et résoudre les situations de crise;

3° établir un plan d'intervention et un plan de communication, et en suivre la mise en œuvre;

4° formuler des recommandations d'amélioration de la gestion de crise au dirigeant principal de l'information ou au gouvernement;

5° mobiliser les ressources nécessaires à la mise en œuvre du plan d'intervention (ressources humaines, financières et matérielles);

© Éditeur officiel du Québec, 2022

6° superviser les activités de retour à la situation normale et, le cas échéant, le renforcement des mesures de sécurité de l'information;

7° clore la gestion de crise;

8° faire évoluer, en continu, le processus de gestion de crise gouvernemental en sécurité de l'information.

CHAPITRE IV
RESPONSABILITÉS AU NIVEAU DE PORTEFEUILLE

SECTION I
CHEFS DÉLÉGUÉS DE LA SÉCURITÉ DE L'INFORMATION (CDSI)

19. Un chef délégué de la sécurité de l'information (CDSI) assure la coordination de la sécurité de l'information aux niveaux stratégique, tactique et opérationnel pour les organismes publics auxquels il se rattache. Il assume les responsabilités énoncées à l'article 12.7 de la Loi et à l'article 6 de la Directive.

SECTION II
RESPONSABLES OPÉRATIONNELS DE CYBERDÉFENSE (ROCD)

20. Un responsable opérationnel de cyberdéfense (ROCD) assume, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités suivantes :

1° appuyer le chef délégué de la sécurité de l'information (CDSI) dans la direction, l'opérationnalisation et l'évolution de l'offre de service de son centre opérationnel de cyberdéfense (COCD);

2° conseiller le chef délégué de la sécurité de l'information (CDSI) notamment, sur les orientations, les priorités d'action, les pratiques communes de cybersécurité, les mécanismes de reddition de comptes et sur l'optimisation des ressources pour son organisation;

3° contribuer à la mise en œuvre des processus gouvernementaux normalisés en matière de cybersécurité;

4° assurer, une prise en charge rapide et concertée des événements de sécurité pour son organisation;

5° représenter son portefeuille ou son organisation auprès de la Cellule gouvernementale de cyberdéfense;

6° maintenir un registre des répondants en matière de sécurité de l'information visés à l'article 23 et qui lui sont rattachés, pour participer au Réseau d'alerte gouvernemental;

7° effectuer régulièrement les vérifications de sécurité des systèmes à l'égard des menaces et des vulnérabilités et, lorsque requis, recommander les correctifs nécessaires à l'organisme public concerné;

8° assurer le maintien d'un registre des événements de sécurité qui relèvent de son organisation;

9° assurer l'accompagnement nécessaire en sécurité opérationnelle aux organismes publics relevant de son organisation;

10° exercer toute autre activité de sécurité de l'information que lui attribue le chef délégué à la sécurité de l'information (CDSI).

SECTION III
CENTRES OPÉRATIONNELS DE CYBERDÉFENSE (COCD)

21. Un centre opérationnel de cyberdéfense (COCD) est un centre de commandement et de coordination des opérations de cyberdéfense. Il apporte aux organismes publics auxquels il se rattache le soutien nécessaire dans la prise en charge des exigences en matière de cybersécurité en rendant disponibles des services centralisés, une expertise de pointe et des pratiques exemplaires en telle matière.

CHAPITRE V
RESPONSABILITÉS AU NIVEAU ORGANISATIONNEL

SECTION I
CHEFS DE LA SÉCURITÉ DE L'INFORMATION ORGANISATIONNELLE (CSIO)

22. Un chef de la sécurité de l'information organisationnelle (CSIO) assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de son organisation. Il travaille en étroite collaboration avec les répondants en matière de sécurité de l'information pour assurer la prise en charge des exigences de sécurité de l'information.

Il assume, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités suivantes :

1° mettre en œuvre les décisions émanant du chef gouvernemental de la sécurité de l'information (CGSI) et du chef délégué de la sécurité de l'information (CDSI) auquel il se rattache, notamment les indications d'application et les indications d'application particulières, en coordonner l'exécution et veiller à leur application;

2° contribuer à la mise en œuvre du cadre de gouvernance qui régit la sécurité de l'information au sein de son organisation;

© Éditeur officiel du Québec, 2022

3° contribuer à la mise en œuvre des processus gouvernementaux normalisés en matière de gestion de la sécurité de l'information et des processus de sécurité de l'information élaborés par le chef délégué de la sécurité de l'information (CDSI);

4° s'assurer de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement, d'acquisition, d'évolution ou de remplacement d'un actif informationnel ou d'un service en ressources informationnelles;

5° aviser sans délai le chef délégué de la sécurité de l'information (CDSI) lorsqu'un événement de sécurité présente un risque qu'un préjudice sérieux soit causé;

6° mettre en œuvre les actions requises pour la prise en charge d'un événement de sécurité;

7° tenir un registre des événements de sécurité selon les exigences de la Directive et les modalités précisées par le chef délégué de la sécurité de l'information (CDSI);

8° fournir les informations demandées par le chef gouvernemental de la sécurité de l'information (CGSI) et le chef délégué de la sécurité de l'information (CDSI) auquel il se rattache relativement à la reddition de comptes, ou toute autre information requise par ces derniers;

9° mettre en place au sein de son organisation les comités et les groupes de travail appropriés de concertation en matière de sécurité de l'information et en assurer la coordination;

10° assurer le développement des compétences du personnel de son organisation en matière de sécurité de l'information.

SECTION II
RÉPONDANTS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

23. Les répondants en matière de sécurité de l'information, pour des domaines spécifiques en matière de sécurité de l'information, sont désignés par leur dirigeant d'organisme public respectif, à la demande du chef gouvernemental de la sécurité de l'information (CGSI) conformément à l'article 11 de la Directive. Ces répondants assument, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités qu'indique le chef gouvernemental de la sécurité de l'information (CGSI).

CHAPITRE VI
DISPOSITIONS DIVERSES ET FINALES

24. Lorsqu'un dirigeant d'organisme public au sens du troisième alinéa de l'article 8 de la Loi a son propre dirigeant de l'information désigné en application du deuxième alinéa de cet article, le dirigeant de l'information ainsi désigné est considéré intervenir, dans l'organisation fonctionnelle de la sécurité de l'information et avec les adaptations nécessaires, à la fois à titre de chef délégué à la sécurité de l'information à un niveau de portefeuille visé par le chapitre IV et à titre de chef de la sécurité de l'information organisationnelle à un niveau organisationnel visé au chapitre V, en vertu du paragraphe 9.1 du premier alinéa de l'article 10.1 de la Loi et du deuxième alinéa de l'article 10 de la Directive.

L'unité administrative spécialisée en sécurité de l'information qu'un tel dirigeant d'organisme public doit maintenir en vertu du deuxième alinéa de l'article 9 de la Directive est considérée intervenir quant à elle, dans l'organisation fonctionnelle de la sécurité de l'information, à un niveau de portefeuille visé par le chapitre IV.

25. Les dispositions du présent cadre ne doivent pas être interprétées comme ayant pour effet de modifier les obligations qu'ont les organismes publics à l'égard des ressources informationnelles et de l'information que ceux-ci détiennent ou utilisent, le tout conformément à la Loi, à la Directive et aux autres lois qui les régissent.

De plus, les dispositions du présent cadre doivent être interprétées comme référant de façon implicite à tous les autres organismes publics ou entités qui, en raison de leur mission ou de leur expertise, interviennent dans l'organisation fonctionnelle de la sécurité de l'information au sein de l'Administration publique, même si de tels organismes ou de telles entités ne sont pas mentionnés expressément dans l'une ou l'autre de ces dispositions. C'est le cas, à titre d'exemples, du Secrétariat du Conseil du trésor, de la Sûreté du Québec, du ministère de la Sécurité publique, du ministère de la Justice du Québec, du ministère du Conseil exécutif, de Bibliothèque et Archives nationales du Québec, du Contrôleur des finances et des organismes publics responsables de services communs.

26. Le Cadre de gestion de la sécurité de l'information du Conseil du trésor (2014) est abrogé.

27. Le présent cadre entre en vigueur à la date de sa publication à la *Gazette officielle du Québec*.

78127

© Éditeur officiel du Québec, 2022