Ministère
de la Cybersécurité
et du Numérique
Québec
Secrétariat général

PAR COURRIEL

Québec, le 18 avril 2023

[redacted]

N/Réf. : 2223-DA-35

Objet : Votre demande en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1)

Madame,

Par la présente, nous donnons suite à votre demande, reçue le 22 mars 2023, visant à obtenir une copie du document « Programme de rehaussement de la cybersécurité (PRC) […] mentionné par la Fédération des cégeps dans son communiqué (Le gouvernement reconnaît le rôle de première importance des cégeps — Fédération des cégeps [fedecegeps.ca]».

Après vérification, nous vous invitons, conformément à l'article 13 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements (RLRQ, chapitre A-2.1, ci-après nommée « Loi sur l'accès »), à consulter le Plan annuel des investissements et dépenses en ressources informationnelles 2023-2024 du ministère de la Cybersécurité et du Numérique (MCN), la section Programme de rehaussement de cybersécurité (pp.20-21), qui fait l'objet d'une diffusion sur Internet et qui est disponible à l'adresse suivante :

https://www.tresor.gouv.qc.ca/fileadmin/PDF/budget_depenses/23-24/5_Plan_annuel_ressources_informationnelles.pdf

Également, nous vous transmettons ci-joint une copie du guide d'élaboration des plans d'action en lien avec le programme de rehaussement de la cybersécurité. Vous y trouverez notamment la description du programme (portée, objectif, financement) ainsi que les axes et objectifs.

…2

900, place D'Youville, 3e étage
Québec (Québec) G1R 3P7
Téléphone : 418 644-1030
acces@mcn.gouv.qc.ca

De plus, nous vous informons qu'un autre document détenu par le MCN relativement à votre demande n'est pas accessible et ne peut vous être transmis, et ce, en application des articles 14 et 34 alinéa 2 de la Loi sur l'accès.

Conformément à l'article 51 de la Loi sur l'accès, nous vous informons que vous pouvez demander la révision de cette décision auprès de la Commission d'accès à l'information dans les trente (30) jours suivant la date de la présente. À cet effet, vous trouverez ci-joint le texte des articles précités, ainsi qu'une note explicative concernant l'exercice de ce recours.

Nous vous prions d'agréer, Madame, nos salutations distinguées.

La responsable de l'accès aux documents
et de la protection des renseignements personnels,

Original signé

Renée Giguère

p. j. Articles de loi
Avis de recours
Document

Ministère
de la Cybersécurité
et du Numérique

Québec

Guide d'élaboration des plans d'action en lien avec le programme de rehaussement de la cybersécurité

Centre gouvernemental de cyberdéfense

Table des matières

Convention éditoriale

Acronyme	Définition
CDSI	Chef délégué de la sécurité de l'information
CGCD	Centre gouvernemental de cyberdéfense
COCD	Centre opérationnel de cyberdéfense
GMVI	Gestion des menaces, des vulnérabilités et des incidents
LGGRI	Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
MCN	Ministère de la Cybersécurité et du Numérique
OP	Organisme public
PQI-RI	Plan québécois des infrastructures en ressources informationnelles
PRC	Programme de rehaussement de la cybersécurité
Réseau	Réseau gouvernemental de cyberdéfense
ROCD	Responsable opérationnel de cyberdéfense
SIGRI	Système intégré de gestion des ressources informationnelles
VGQ	Vérificateur général du Québec

Préambule

Afin d'appuyer la transformation numérique gouvernementale, la sécurité de l'information et la cybersécurité sont primordiales pour maintenir la confiance des citoyens à l'égard des services numériques et faire face aux cybermenaces et aux cyberattaques.

À l'automne 2020, les organismes publics (OP) devaient préparer un plan d'action démontrant la prise en charge de quinze mesures de sécurité minimales identifiées par le Centre gouvernemental de cyberdéfense (CGCD). En 2021, un plan de redressement a également été exigé aux OP afin de mettre en œuvre certaines exigences découlant de la Directive sur la sécurité de l'information gouvernementale, remplacée en décembre 2021 par la Directive gouvernementale sur la sécurité de l'information.

Par ailleurs, dans son Rapport déposé à l'Assemblée nationale pour l'année 2021-2022, le Vérificateur général du Québec (VGQ) a présenté une étude portant sur la cybersécurité. Ses travaux ont mené à la formulation d'observations importantes qui pourraient permettre aux entités visées et au gouvernement du Québec d'améliorer leur posture en sécurité.

Le rehaussement de la cybersécurité dans les organismes publics par la mise en place d'un plan d'action consolidé par les centres opérationnels de cyberdéfense est incontournable. Les objectifs de la mise en place des plans d'action sont multiples, notamment :

- Effectuer un virage dans les approches liées à la cybersécurité en favorisant un suivi continu de l'état d'avancement en mode gestion de projets plutôt qu'en mode reddition de comptes;
- Déposer un plan d'action ambitieux, selon les capacités, dans lequel le chef délégué de la sécurité de l'information (CDSI) s'engage à respecter ses cibles de rehaussement de la cybersécurité;
- S'appuyer, s'il y a lieu, sur un levier financier pour inciter des obligations de résultats et accélérer le rehaussement de la cybersécurité.

Objectif

Le présent guide vise à soutenir les OP dans l'élaboration de leur plan d'actions et, le cas échéant, dans leur demande de financement en lien avec le Programme de rehaussement de la cybersécurité (PRC), annoncé lors du dépôt du budget 2022-2023.

Plan d'action

Un plan d'action consolidé annuel doit être soumis au MCN pour le rehaussement de la cybersécurité, qu'il y ait un besoin de financement ou non. Ce plan d'action est sous la responsabilité de chaque CDSI. Il doit ainsi s'assurer du suivi du plan et de sa réalisation. Ce plan consolide les initiatives identifiées par les OP de son portefeuille pour rehausser leurs postures de cybersécurité. Le plan d'action contient notamment les interventions et les actions à réaliser, un échéancier à respecter et doit être approuvé par chaque dirigeant d'organisme concerné.

Le MCN est responsable de recevoir et d'analyser les plans d'actions des CDSI et de recommander les actions à prioriser et à mettre en œuvre.

Cycle annuel

Le dépôt et le suivi formel de l'avancement des plans d'actions s'inscrit dans le cycle de collecte bisanuelle mis en place par le MCN. Ainsi, le plan d'action pour la période annuelle du 1er avril au 31 mars de chaque année devra être déposé au MCN au plus tard le 15 janvier de l'année du nouveau plan d'action, ainsi qu'une mise-à-jour du plan d'action déjà en réalisation. Par exemple, le nouveau plan d'action du 1er avril 2023 au 31 mars 2024 ainsi que la mise-à-jour devront être déposé au MCN au plus tard le 15 janvier 2023; une exception est prévue pour l'année 2022-2023 (voir la section suivante). Une mise à jour de l'état d'avancement du plan d'action devra être transmise lors de la deuxième collecte, soit au plus tard le 15 juin de chaque année.

Si le plan contient une demande de financement en lien avec le PRC, le CDSI recevra, par courriel, les initiatives autorisées et le pourcentage de financement accordé pour chacune d'entre elles dès la fin de l'analyse des plans d'action par le MCN.

> **N.B.** Les OP ayant obtenu du financement devront effectuer une mise à jour des dépenses dans SIGRI en amont de chaque mise à jour trimestrielle du plan d'action.

Un suivi informel sera assuré par le CGCD auprès des ROCD concernés. Ainsi, minimalement, une mise à jour du plan d'action devra être transmise au CGCD à l'adresse courriel cgcd@mcn.gouv.qc.ca au 30 septembre de chaque année, et devra être transmise au plus tard le 15 octobre de chaque année.

Ce suivi permettra de suivre l'avancement des plans à une fréquence régulière et d'évaluer si une réallocation des sommes non utilisées doit être envisagée en cas d'enjeux de réalisation.

Exception pour le plan d'action pour l'exercice 2022-2023

Pour la période annuelle 2022-2023, le plan d'action doit être transmis au MCN au plus tard le **15 juin 2022.**

Exceptionnellement, les CDSI souhaitant obtenir rapidement du financement de la part du PRC pour des initiatives dont le démarrage serait prévu à court terme, devront transmettre leur plan **au plus tard le 6 mai 2022** pour permettre un traitement avant la fin du mois de juin 2022.

Figure 1
Cycle annuel

Le programme de rehaussement de la cybersécurité

Afin d'appuyer les organismes publics dans leurs démarches de rehaussement de la sécurité de l'information et de la cybersécurité, le PRC a été mis en place, sous la responsabilité du ministère de la Cybersécurité et du Numérique (MCN). Le programme prend appui sur une provision de 100,0 M$ sur une durée de deux ans, soit 30,0 M$ pour l'année 2022-2023 et 70,0 M$ pour l'année 2023-2024.

Portée

Le PRC est accessible aux OP soumis à la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03).

Les OP ne disposant pas d'une enveloppe décennale au Plan québécois des infrastructures en ressources informationnelles (PQI-RI)[1] sont exclus du programme et ne peuvent recourir à la provision. Ils sont toutefois tenus de compléter un plan d'action consolidé.

Objectif

Dans le contexte actuel de rareté de main d'œuvre, particulièrement marquée dans le domaine des technologies de l'information, la mutualisation des ressources et des initiatives est essentielle pour poursuivre la prise en charge de la cybersécurité.

La mutualisation des actions et l'accroissement du financement deviennent nécessaires pour poursuivre la prise en charge de la cybersécurité et répondre aux exigences de protection des actifs informationnels du gouvernement du Québec. Ainsi, le PRC servira de levier pour accélérer la montée en maturité du Réseau gouvernemental de cyberdéfense (Réseau), dont des centres

[1] Société de l'assurance automobile du Québec (SAAQ); Commission des normes, de l'équité, de la santé et de la sécurité du travail (CNESST); Retraite Québec).

opérationnels de cyberdéfense (COCD), en facilitant la mise en œuvre d'actions concrètes génératrices de valeur pour l'ensemble du Réseau.

Financement

Les modalités d'octroi du financement sont établies selon un pourcentage fixé au démarrage de l'intervention et soumis à l'atteinte de jalons déterminés. La répartition des dépenses est assumée jusqu'à une hauteur de 75 % par le PRC; la balance des dépenses est assumée par les organismes publics concernés.

Axes et objectifs du programme de rehaussement en cybersécurité

Le PRC s'articule selon deux axes et quatre objectifs.

Axe 1 – Prévention

Objectif 1.1. Encadrement des risques et de la reddition des comptes

Veiller à ce que les activités de gouvernance permettent un meilleur encadrement de l'évaluation des risques et de la reddition de comptes, notamment en développant les capacités en gouvernance de l'écosystème du Réseau, en améliorant le niveau de maturité des COCD et des OP, constituant leur portefeuille, en favorisant le développement de solutions communes, en gérant les risques et en instaurant une culture de performance de la cybersécurité. Il s'agit de mesures permettant notamment de :

- Évaluer la maturité des organismes du portefeuille et prioriser les actions nécessaires selon le risque (ex. : démarche incluant des audits de sécurité).
- Permettre l'automatisation du suivi des mesures de cybersécurité et de la reddition de comptes pour le portefeuille (ex. : démarche incluant la mise en place de tableaux de bord)

Exemples : audit de sécurité et analyses externes, stratégie de mutualisation des services de cybersécurité, évaluation des menaces et gestion des risques.

Objectif 1.2. Protection contre les cyberattaques

Renforcer les mesures de cybersécurité afin de se protéger efficacement contre d'éventuelles cyberattaques notamment en développant les capacités proactives et préventives et en permettant de réduire les probabilités d'un événement de sécurité directement à la source. Il s'agit de mesures permettant notamment de :

- Adresser la désuétude des actifs du portefeuille en priorisant les infrastructures selon leur niveau de préjudice.
- Mettre en place la prévention de la perte de données (ex : identification, catégorisation et protection des données, gestion du cycle de vie).
- Instaurer un programme permanent de sensibilisation du personnel.

Exemples : rehaussement du seuil minimal de la cybersécurité, gestion de la désuétude, sensibilisation à la sécurité de l'information, gestion des identités et des accès, protection contre la fuite de données.

Axe 2 – Réaction

Objectif 2.1. Détection des cyberattaques

Améliorer les mesures de cybersécurité de façon à détecter efficacement les cyberattaques notamment en développant les capacités technologiques de cyberdéfense, lesquelles sont jugées primordiales et incontournables dans le contexte de l'augmentation des cyberattaques, de leur complexité, de leur ampleur et de la portée des actifs à protéger considérant les ressources spécialisées limitées en cybersécurité. Il s'agit de mesures permettant notamment de :

- Déployer une solution centralisée de surveillance et de détection de cyberattaque (ex : antivirus EDR, pare-feu, IPS, WAF, SIEM).
- Mettre en place un processus d'intégration de la sécurité dès la conception (ex. : DevSecOPS, plateforme de tests).

Exemples : journalisation des accès, automatisation de la réponse aux cyberattaques, surveillance et analyse des événements, tests d'intrusion, vérification des signalements de vulnérabilité, déploiement de solutions de sécurité.

Objectif 2.2. Réduction du temps de réponse et de récupération des données numériques

Améliorer les mesures de cybersécurité afin de réduire le temps de réponse et de récupération en cas de cyberattaque notamment en développant les capacités de réponse, en mettant en place différentes mesures visant l'atténuation des préjudices, la reprise rapide des activités suivant l'événement et la récupération des données numériques. Il s'agit de mesures permettant notamment de :

- Mettre en œuvre le processus de gestion des menaces, des vulnérabilités et des incidents (GMVI) au sein des organismes sous la responsabilité du CDSI.
- Pérenniser le cycle de vie du plan de reprise informatique (ex : évolution et essais annuels) et son arrimage avec le plan de continuité des affaires.

Exemples : mise en œuvre d'un processus de GMVI, élaboration de protocoles d'intervention, conception d'un plan de reprise informatique, simulation de crise.

Qualification des plans d'action par le MCN

Les plans comprenant une partie d'investissements doivent respecter les modalités relatives à l'élaboration de la programmation et des bilans des investissements et des dépenses en ressources informationnelles[2]. L'octroi du financement sera notamment priorisé selon l'évaluation des risques et des préjudices potentiels sur les données à protéger.

Critères de qualification

La qualification des plans d'action est conditionnelle[3] au respect des critères suivants :

Les plans doivent :

- Être détaillés afin de permettre une vue d'ensemble des activités ou des livrables nécessaires à la réalisation de chaque initiative identifiée;
- Être basés sur une planification annuelle, sans s'y limiter.

Les activités ou livrables consignés dans les plans doivent :

- Répondre à une exigence gouvernementale de cybersécurité, dont :
    - Le rehaussement du seuil de sécurité minimal (incluant les quinze mesures minimales de sécurité);
    - La mise en œuvre des plans de redressement en sécurité de l'information.

OU

- Contribuer à l'atténuation d'un risque gouvernemental ou organisationnel de niveau élevé ou très élevé.
    - Dans ce cas, un rapport d'audit décrivant les risques doit accompagner le plan.

Pour chaque activité ou livrable, les éléments suivants doivent être consignés :

- L'objectif visé;
- L'échéance, incluant le trimestre de début et le trimestre de fin;
- Un point de contrôle trimestriel (contrat, état d'avancement de l'application d'une mesure, appel d'offres, etc.);
- Des jalons trimestriels pour les activités ou les livrables échelonnés sur plus de trois mois. Par exemple :
    - Rapports intermédiaires;
    - Étape ou phase terminée à la fin du trimestre;
    - Nombre d'organismes, d'utilisateurs ou de postes couverts par l'initiative à la fin du trimestre;
    - Le numéro de SIGRI pour l'initiative.

[2] https://www.tresor.gouv.qc.ca/ressources-informationnelles/cadre-normatif-de-gestion-des-ressources-informationnelles/

[3] Les plans ne respectant pas ces critères se verront dépriorisés au profit de leur contrepartie.

Limitations

La qualification des plans est également assujettie aux limitations suivantes :

- ✓ Les activités ou les livrables doivent couvrir des mesures permanentes. Ils doivent s'inscrire dans le cadre de la mise en place d'un processus continu;
- ✓ Les activités ou les livrables constituant une innovation ou allant « au-delà » des exigences gouvernementales actuelles en matière de cybersécurité sont soumises à l'approbation du CGCD;
- ✓ Une solution existante ou déjà disponible de façon mutualisée ne sera pas financée;
- ✓ Lorsqu'une activité ou un livrable peut être réalisé par une solution mutualisée gouvernementale, le CGCD peut demander une révision du plan pour considérer cette dernière;
- ✓ Une activité ou un livrable débuté peut être financé à condition de comporter une bonification des fonctionnalités initialement prévues.

Facteurs de priorisation

En plus des critères de qualification, les facteurs suivants sont considérés pour prioriser l'octroi des ressources financières aux organismes publics porteurs des plans :

1. Les activités ou les livrables respectent les critères de qualification énoncés ci-haut;
2. Les activités ou les livrables atténuent un risque gouvernemental;
3. Les activités ou les livrables rehaussent la posture de cybersécurité d'un actif sensible ou d'un service essentiel;
4. Les activités ou les livrables optimisent, consolident ou mutualisent des ressources gouvernementales, incluant notamment la mise en commun de ressources humaines, informationnelles et matérielles.

Le ratio de financement des activités sera calculé en adéquation avec :

- ✓ L'atténuation des risques de sécurité gouvernementaux ou organisationnels;
- ✓ L'optimisation, la consolidation ou la mutualisation des ressources.

Points de contrôle dans les plans d'action

Afin d'assurer le respect des critères de qualification et de permettre le suivi de la réalisation des plans, il est essentiel de détailler les activités et les livrables pour chaque initiative identifiée. Voici quelques exemples pour permettre la réalisation de l'exercice conformément aux attentes.

Exemple détaillé et conforme aux attentes

Mise en place d'une solution technologique

#	Activité	Point de contrôle
1	Identifier les besoins d'affaires	Dossier d'affaires
2	Réaliser une preuve de concept	Résultats de la preuve de concept
3	Élaborer l'appel d'offres	Publication de l'appel d'offres
4	Sélectionner un fournisseur	Entente/engagement contractuel
5	Planifier l'implémentation de la solution	Stratégie de déploiement/feuille de route
6	Tester l'implémentation via un projet pilote	Résultats du projet pilote
7	Implémenter la solution	Nombre de poste déployé sur l'ensemble
8	Évaluer et améliorer la solution	• Documentation des changements • Indicateurs de performance

Exemple générique non-conforme aux attentes*

Mise en place d'un antivirus « EDR »

#	Activité	Point de contrôle
1	Mise en place d'un antivirus « EDR »	100% des systèmes avec un antivirus « EDR »

Note : sauf si cette activité peut être réalisée à l'intérieur de 3 mois

* L'absence de détail au niveau des activités ou des livrables dans le dernier exemple ne permet pas d'apprécier l'avancement de l'initiative et donc d'en assurer la réalisation à terme.

Informations figurant dans SIGRI

Toutes les initiatives doivent figurer dans le plan d'action avec leur numéro SIGRI. Avant de soumettre les plans d'actions, les OP doivent s'assurer que les initiatives pour lesquels une participation au financement du PRC est demandée figurent dans SIGRI. Pour une initiative donnée :

- Si l'initiative est entièrement budgétée à même les budgets alloués, elle doit figurer dans SIGRI en utilisant les comptes provisionnés (investissement SCT-1, dépense SCT-20);
- Si l'initiative dépasse le budget alloué et qu'un financement provenant du PRC est demandé, il faut indiquer :
    - Pour la partie investissement : l'OP doit utiliser le compte de demande de rehaussement (SCT-5);

- Pour la partie dépenses de fonctionnement : la programmation peut dépasser les dernières prévisions saisies en attendant l'approbation de l'allocation du budget demandé.

Par la suite, SIGRI devra refléter la réalité des allocations budgétaires en fonction du plan approuvé.

Pour plus de détails, se référer au guide d'élaboration d'une programmation et d'un bilan dans SIGRI[4].

Instructions concernant le gabarit Excel

Le gabarit est composé de trois onglets. Pour les initiatives demandant un financement, il est important que les intitulés des initiatives et des actions restent identiques d'une mise à jour à l'autre du fichier.

- **Instructions** : fournit les indications précises quant aux informations à fournir dans le plan d'action;
- **Identification** : indique le nom et les coordonnées de la personne qui peut être contactée en cas de questionnements sur le plan consolidé;
- **GAB_Plan d'action** : contient le plan d'action maintenu par le CDSI. Si dans le cadre de l'initiative, un rehaussement financier est souhaité, la section grise (Estimation des coûts pour l'exercice financier) doit être complétée, à l'exception de la colonne « Autorisation obtenue »).

[4] https://www.tresor.gouv.qc.ca/ressources-informationnelles/cadre-normatif-de-gestion-des-ressources-informationnelles/