

La cybersécurité au gouvernement du Québec

Une gouvernance en évolution

Présentation au PSCIOC

27 octobre 2021

Ordre du jour

CYBERDÉFENSE



- Présentation de la **Politique gouvernementale de cybersécurité**
- Présentation du **Projet de loi n° 95 (2021)**
- Présentation du **Réseau gouvernemental de cyberdéfense**
- Réalisations du **Centre gouvernemental de cyberdéfense**

Contexte



« Les **lois** et les règlements devront continuer d'**évoluer** afin de pouvoir utiliser le **plein potentiel** du **numérique** et d'atteindre les **cibles de transformation** que se fixe le gouvernement. »

– Stratégie de transformation numérique gouvernementale 2019-2023

CYBERDÉFENSE



« Sa mise en œuvre impose une gouvernance forte et intégrée qui repose sur un **cadre légal**, administratif et normatif **adapté à l'ère du numérique**. »

– Politique gouvernementale de cybersécurité



Politique gouvernementale de cybersécurité

Adoptée en mars 2020

- Prend appui sur la Stratégie de transformation numérique gouvernementale
- Élaborée à l'aide d'un **comité d'experts** en cybersécurité
- Vise l'Administration publique, les citoyens et les partenaires de l'écosystème de la cybersécurité
- Se traduit par des **mesures clés** assorties de plans d'action adaptés aux enjeux et aux possibilités en matière de cybersécurité

Consulter la Politique et les mesures clés

[Politique gouvernementale de cybersécurité | Gouvernement du Québec \(quebec.ca\)](#)

[Mesures clés | Gouvernement du Québec \(quebec.ca\)](#)

CYBERDÉFENSE





Politique gouvernementale de cybersécurité

Des objectifs répartis sur quatre axes

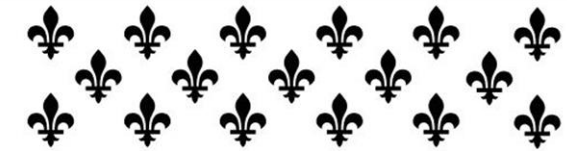
1. La cybersécurité, une priorité gouvernementale
2. Des services publics sécuritaires
3. Des citoyennes et citoyens confiants et avertis
4. Des partenariats stratégiques et durables

CYBERDÉFENSE



Projet de loi n° 95

- Projet de loi n° 95, Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives - Assemblée nationale du Québec (assnat.qc.ca)



ASSEMBLÉE NATIONALE DU QUÉBEC

PREMIÈRE SESSION

QUARANTE-DEUXIÈME LÉGISLATURE

Projet de loi n° 95
(2021, chapitre 22)

**Loi modifiant la Loi sur
la gouvernance et la gestion des
ressources informationnelles des
organismes publics et des entreprises
du gouvernement et d'autres
dispositions législatives**

Présenté le 5 mai 2021
Principe adopté le 1^{er} juin 2021
Adopté le 9 juin 2021
Sanctionné le 10 juin 2021

Éditeur officiel du Québec
2021

Objectif

Instaurer un cadre de gouvernance et de gestion en matière de ressources informationnelles applicable aux organismes publics et aux entreprises du gouvernement, lequel vise particulièrement à :

Offrir aux citoyens et aux entreprises **des services simplifiés, intégrés et de qualité**

Protéger adéquatement les RI des organismes publics

Instaurer une gouvernance et une gestion optimales des **données numériques gouvernementales**

Coordonner les **initiatives de transformation numérique** des organismes publics

Consulter le Projet de loi n° 95 (2021) :

[Projet de loi 95](#)

Principaux changements

CYBERDÉFENSE

Les principaux changements abordés concernent les chapitres suivants :



Dirigeant principal de l'information et dirigeant de l'information

LGGRI, chapitre II



Transformation numérique

LGGRI, chapitre II.3



Sécurité de l'information

LGGRI, chapitre II.4



Planification et gestion pour les organismes publics

LGGRI, chapitre III



Données numériques gouvernementales

LGGRI, chapitre II.2



Autres dispositions

LCCJTI, chapitre V



Dirigeant principal de l'information

Nouvelles fonctions

CYBERDÉFENSE

9



Dirigeant principal de l'information (DPI)*

Nouvelles fonctions

LGGRI, article 7.1

Chef gouvernemental de la sécurité de l'information

Gestionnaire des données numériques gouvernementales

Chef gouvernemental de la transformation numérique

*Il peut déléguer par écrit à une personne relevant de sa direction l'exercice de l'une ou l'autre des responsabilités qu'il assume.



Dirigeant principal de l'information

Nouvelles fonctions

CYBERDÉFENSE

10

Vision globale

Développer et soumettre une vision globale en matière de RI, incluant en ce qui concerne la **transformation numérique de l'Administration publique**, et de proposer les moyens pour la mettre en œuvre

Indication d'application

Toute instruction donnée par écrit, portant sur

- l'exécution d'activités,
- l'acquittement de responsabilités
- l'application de mesures en matière de RI

Les organismes publics doivent s'y conformer

Développement d'une expertise en matière de RI

Offrir aux organismes publics des services, des conseils ou du soutien et à renforcer le savoir-faire de l'État, notamment en :

Sécurité de l'information

Transformation numérique

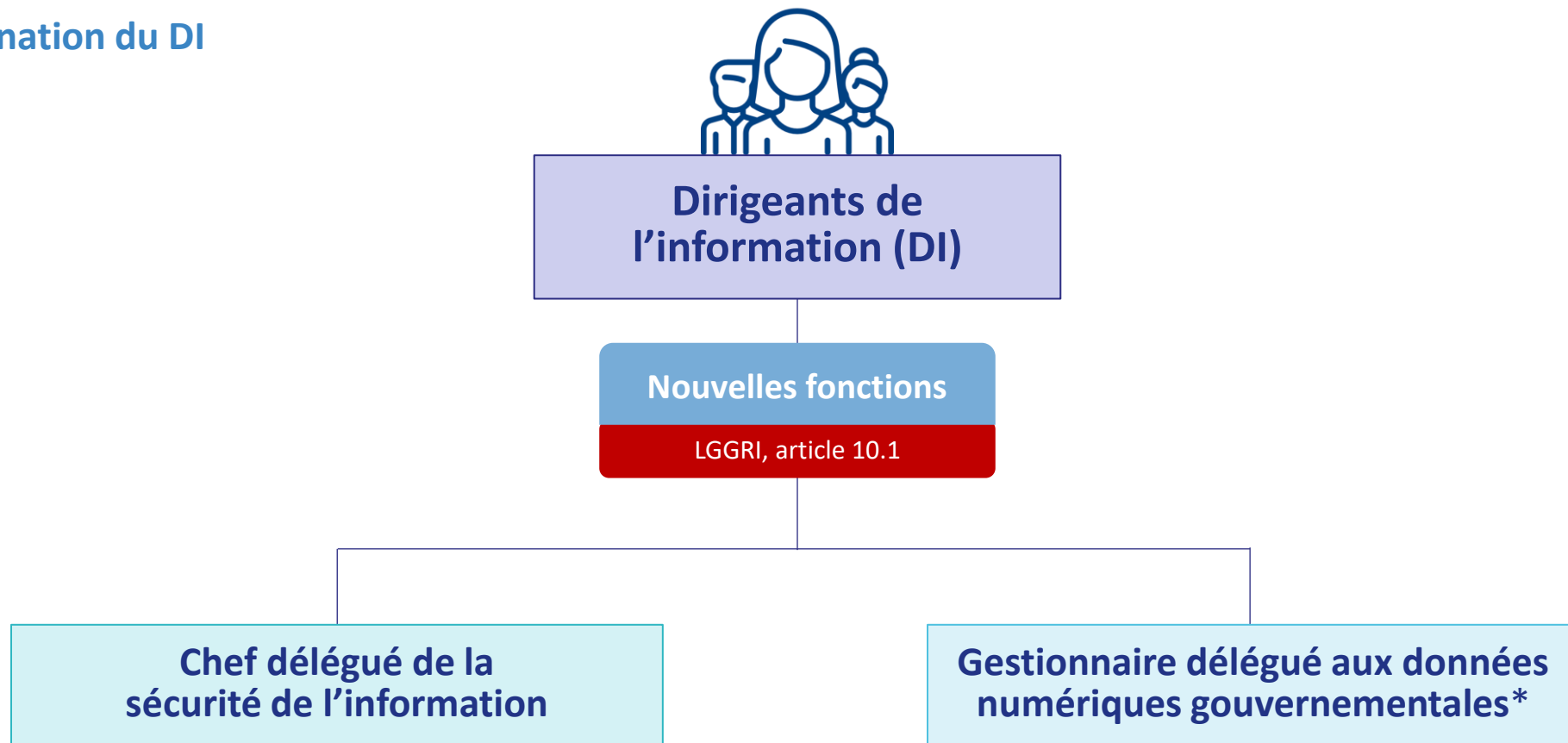
Technologies de l'information

LGGRI, chapitre 7



Dirigeant de l'information

Nouvelles fonctions et modalités de désignation du DI





Sécurité de l'information

Résumé des principaux changements

CYBERDÉFENSE

12

Objectif

Établir une **gouvernance globale et concertée** en matière de sécurité de l'information et en **surveiller** la mise en œuvre des exigences dans les organismes publics

LGGRI, chapitre II.2

- Créer les fonctions **de chef gouvernemental de la sécurité de l'information** et de **chef délégué de la sécurité de l'information**.
- Permettre le partage rapide de certaines informations lors d'une atteinte à la confidentialité, à la disponibilité ou à l'intégrité d'une RI ou d'une information.
- Permettre au DPI, au chef gouvernemental de la sécurité de l'information et aux DI de formuler des **indications d'application** en matière de sécurité de l'information.
- Maintenir au sein du SCT une unité administrative spécialisée en sécurité de l'information.



Chef gouvernemental de la sécurité de l'information

(fonction attribuée au DPI et pouvant être déléguée)

Responsabilités :

- Diriger l'action gouvernementale en matière de sécurité de l'information;
- Recommander au Conseil du trésor des règles pour assurer la sécurité de l'information, incluant celles relatives à l'authentification et à l'identification, ainsi que recommander au président du Conseil du trésor des cibles de performance applicables aux organismes publics en matière de sécurité de l'information;
- Établir le modèle de classification de sécurité des données numériques gouvernementales en fonction de leur nature, de leurs caractéristiques, de leur utilisation et des règles qui les régissent, et le faire approuver par le Conseil du trésor;
- Signifier aux organismes publics des attentes en matière de sécurité de l'information et leur formuler des indications d'application;
- Surveiller la mise en œuvre par les organismes publics des obligations en matière de sécurité de l'information découlant de l'application de la présente loi, veiller à leur respect et évaluer les mesures prises par les organismes publics en telle matière;
- Rendre compte au président du Conseil du trésor, selon les conditions et modalités déterminées par ce dernier, des résultats liés aux cibles de performance ainsi que du respect des obligations et lui formuler toute recommandation nécessaire;
- Exercer toute autre fonction que lui attribue le président du Conseil du trésor ou le gouvernement.



Chef délégué de la sécurité de l'information

(fonction attribuée aux DI sous l'autorité fonctionnelle du chef gouvernemental de la sécurité de l'information)

Responsabilités :

- Appuyer le chef gouvernemental de la sécurité de l'information dans la prise en charge de l'action gouvernementale en matière de sécurité de l'information;
- Appliquer, sous la direction du chef gouvernemental de la sécurité de l'information, les standards, les directives, les règles ou les indications d'application relatifs à la sécurité de l'information pris en vertu de la présente loi;
- Assurer la protection des ressources informationnelles et de l'information, notamment par la gestion des risques et des vulnérabilités, ainsi que par la mise en œuvre de mesures visant à les protéger de toute forme d'atteinte, telles des menaces ou des cyberattaques;
- Prendre toute action requise en cas d'atteinte à la protection des ressources informationnelles et de l'information;
- Formuler, en matière de sécurité de l'information, des indications d'application particulières pour ces organismes;
- Surveiller la mise en œuvre des obligations en matière de sécurité de l'information découlant de l'application de la présente loi, veiller à leur respect et évaluer les mesures prises par ces organismes en telle matière;
- Rendre compte de sa gestion au chef gouvernemental de la sécurité de l'information et lui transmettre tout renseignement demandé, selon les modalités que détermine le président du Conseil du trésor.



Sécurité de l'information

Partage rapide de certaines informations*

Règlement
d'application
à venir

LGGRI, articles 12.2, 12.3 et 12.4

- Mesures qu'un organisme public doit prendre lorsqu'il constate qu'une RI ou une information sous sa responsabilité est ou a été l'objet d'une atteinte à sa confidentialité, à sa disponibilité ou à son intégrité
- Mesures que l'organisme peut prendre pour prévenir ou réduire ces risques d'atteintes;

Indications d'application en sécurité de l'information

À venir

LGGRI, articles 12.6 et 12.7

Indication d'application émise par le chef gouvernemental ou indication d'application particulière par le chef délégué à l'intention des organismes publics auxquels il est rattaché

Unité administrative spécialisée en sécurité de l'information

LGGRI, article 12.5

- Obligation de maintenir au sein du Secrétariat du Conseil du trésor
- Sous la direction du chef gouvernemental de la sécurité de l'information
- Actuellement le Centre gouvernemental de cyberdéfense

CYBERDÉFENSE

15

*Dispositions dont l'entrée en vigueur se fera à la date de l'entrée en vigueur du premier règlement pris en vertu du nouvel article 22.1.1. prévue pour l'automne 2021

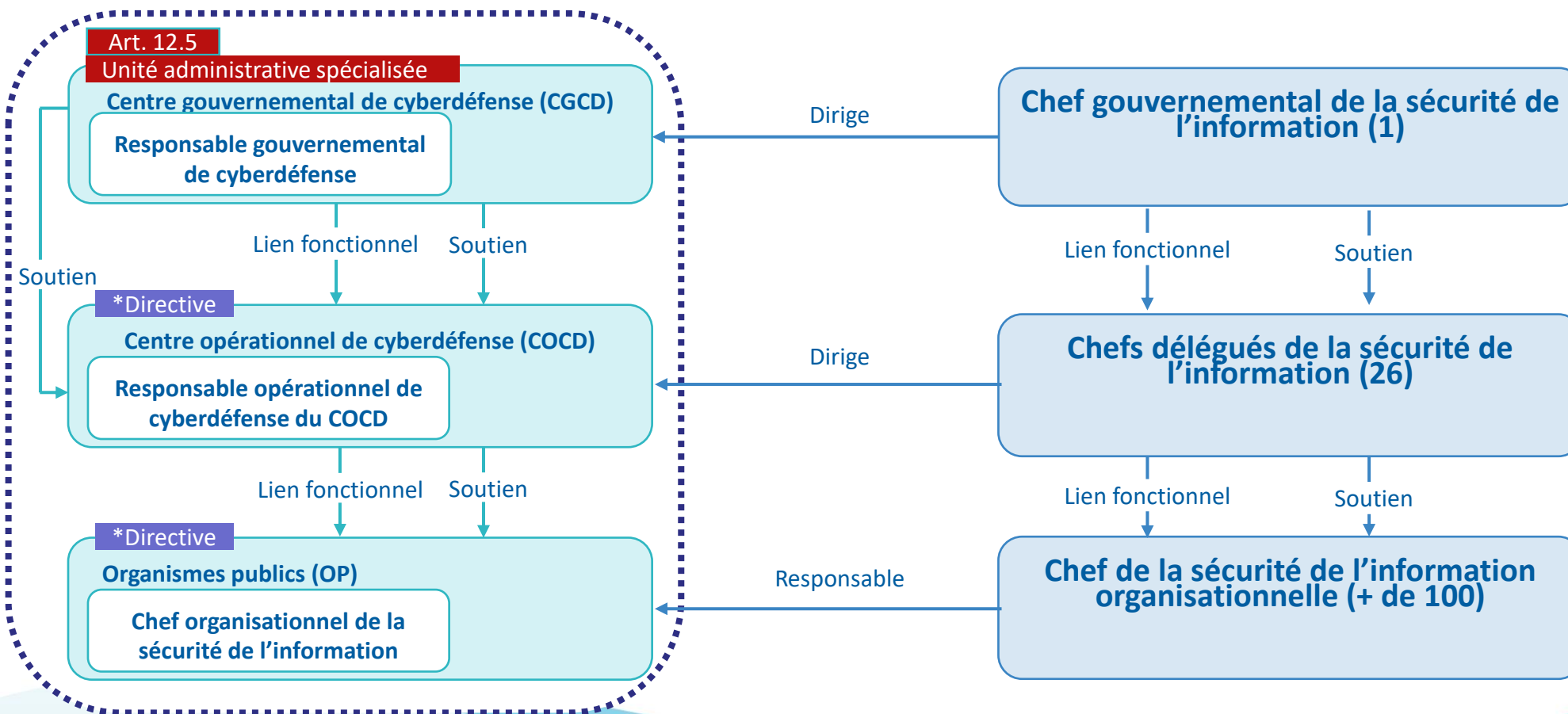


Réseau gouvernemental de cyberdéfense

Structure

CYBERDÉFENSE

16





Réseau gouvernemental de cyberdéfense (suite)

CYBERDÉFENSE

17

Proactivité, collaboration, partage, échanges et enseignement

Mission

Renforcer les dispositifs de **prévention** et de **réaction** à l'égard des cybermenaces

*Directive gouvernementale
sur la sécurité de l'information

*La Directive gouvernementale sur la sécurité de l'information n'est pas encore adoptée par le Conseil des ministres; dispositions sujettes à changement

- Assurer une prise en charge commune des incidents de cybersécurité
- Assurer une surveillance constante des cybermenaces
- Permettre aux autorités gouvernementales d'intervenir rapidement et de manière coordonnée face aux cybermenaces
- Veiller à instaurer les meilleures pratiques de cyberdéfense dans l'administration publique
- Être le point de contact pour les organismes publics afin d'obtenir des avis et des conseils en matière de cybersécurité
- Contribuer à améliorer les compétences en matière de cybersécurité auprès des organismes publics



Centre gouvernemental de cybersécurité

Un chef de file en cybersécurité

CYBERDÉFENSE

18

Mission

Protéger les ressources informationnelles
du gouvernement du Québec contre les
cyberattaques

- Offrir des services de sécurité centralisés
- Développer les capacités du Réseau gouvernemental de cybersécurité
- Développer et diffuser des technologies et des outils de cybersécurité spécialisés qui permettent de renforcer la cybersécurité
- Agir comme centre de coordination lors de la gestion des incidents de sécurité
- Conseiller les autorités en matière de position à prendre en matière de gestion des cyberrisques



Centre gouvernemental de cyberdéfence (suite)

Plusieurs réalisations

CYBERDÉFENSE

19

Structure du CGCD

Direction de la prévention et de la gestion
des incidents

Direction des pratiques et du
développement des compétences en
cyberdéfense

Direction du développement du Réseau
gouvernemental de cyberdéfense

- Déploiement de quinze mesures minimales de sécurité à l'échelle gouvernementale
- Réalisation d'une campagne d'hameçonnage à l'échelle gouvernementale
- Réalisation de plus de 75 tests d'intrusions sur des services numériques gouvernementaux
- Service de balayage des actifs gouvernementaux et surveillance constante du *Darkweb*
- Mise en place d'une offre de formations destinée aux intervenants en sécurité de l'information