POLITIQUE GOUVERNEMENTALE EN CYBERSÉCURITÉ

MESURES CLÉS

SECRÉTARIAT
DU CONSEIL
DU TRÉSOR

Votre gouvernement

Québec

Cette publication a été réalisée par le Secrétariat du Conseil du trésor
en collaboration avec la Direction des communications.

Une version accessible de ce document est en ligne sur le site
Québec.ca/transformationnumerique.
Si vous éprouvez des difficultés techniques, veuillez communiquer
avec Gérald Nadeau au numéro (418) 643-0875 poste 5020.

Pour plus d'information :

Direction des communications
du ministère du Conseil exécutif
et du Secrétariat du Conseil du trésor
2e étage, secteur 800
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158
Télécopieur : 418 643-9226
Courriel : communication@sct.gouv.qc.ca

Dépôt légal – JUIN 2020
Bibliothèque et Archives nationales du Québec
ISBN 978-2-550-86838-5 (version électronique)

TABLE DES MATIÈRES

INTRODUCTION

En se dotant, pour la première fois, d'une Politique gouvernementale de cybersécurité, le gouvernement énonce une vision forte qui traduit la priorité et l'importance qu'il accorde à la cybersécurité. En appui à cette vision, la Politique énonce des principes et des objectifs dont la concrétisation est assurée par des mesures clés. Celles-ci sont porteuses de changement et visent à protéger les données des Québécoises et des Québécois.

Les cinq principes fondamentaux énoncés dans la Politique guideront la mise en œuvre des mesures clés tout au long de leur déploiement :

PRINCIPE 1 : Assurer l'application de mesures de protection proportionnelles à la valeur de l'information et aux risques encourus

PRINCIPE 2 : Favoriser et encourager l'adoption de comportements cybersécuritaires

PRINCIPE 3 : Miser sur le développement des compétences, l'attraction et la rétention des talents

PRINCIPE 4 : Encourager le partage et la mise en commun

PRINCIPE 5 : Intégrer la protection de l'information en amont.

AXE 1
LA CYBERSÉCURITÉ, UNE PRIORITÉ GOUVERNEMENTALE

Objectif 1 :
Gouverner la cybersécurité par une vision globale et concertée

1.1 Renforcer l'encadrement de la sécurité de l'information gouvernementale

La sécurité de l'information, au sein de l'administration publique, sera renforcée par la mise en place d'une gouvernance regroupant les différentes composantes que sont, notamment, les directives, les règles, les cadres de gestion, les matrices de responsabilité et les guides de bonnes pratiques. Ces composantes viseront à rehausser la maturité et la capacité des organismes publics en sécurité de l'information.

Ainsi, la Directive sur la sécurité de l'information gouvernementale, qui prescrit des obligations de sécurité de l'information aux organismes publics, sera révisée. Elle sera également appuyée par des règles précises qui viseront à standardiser et à harmoniser les pratiques de sécurité de l'information au sein de l'Administration gouvernementale.

1.2 Rehausser l'efficacité de la prise en charge des incidents et de la gestion de crise

Afin d'assurer une prise en charge rapide des incidents et d'en minimiser les répercussions, le processus gouvernemental de gestion des incidents et de gestion de crise sera rehaussé par la contribution active du Réseau gouvernemental de cyberdéfense, constitué du Centre gouvernemental de cyberdéfense et des centres opérationnels de cyberdéfense.

Ce processus fera l'objet de simulations périodiques qui viseront à en évaluer l'efficacité. Il prendra en compte les incidents classés selon leur niveau de sévérité ainsi que la gestion de crise et des communications afférentes.

1.3 Se doter de mécanismes de gestion de la performance en cybersécurité

Le gouvernement entend mesurer la progression vers l'atteinte des objectifs en matière de cybersécurité. Pour ce faire, il élaborera des indicateurs de gestion de la performance en cybersécurité.

Objectif 2 : Placer le personnel au cœur de la cybersécurité

2.1 Former le personnel de l'État afin qu'il assure une première barrière de sécurité quant aux cyberattaques

Le gouvernement renforcera les compétences en cybersécurité de son personnel, notamment grâce à son partenariat avec l'Académie de transformation numérique de l'Université Laval. Des formations en continu seront offertes au personnel de l'État de manière à permettre les apprentissages essentiels à l'adoption de comportements sécuritaires. De plus, ces formations seront adaptées aux différents rôles et responsabilités qu'exerce le personnel de l'État dans le cadre de ses activités professionnelles.

AXE 2
DES SERVICES PUBLICS SÉCURITAIRES

Objectif 3 : Assurer la protection et la résilience des services publics et des échanges électroniques gouvernementaux

3.1 Renforcer la résilience du gouvernement quant aux cyberincidents

Le gouvernement entend renforcer la résilience de ses systèmes d'information[1] par la mise en place de mesures d'atténuation des risques, notamment par le maintien de plans de reprise informatique qui respectent les objectifs de continuité des services. Il entend également, en cas d'incident, assister les organismes publics pour un rétablissement rapide et un retour coordonné à la situation normale.

3.2 Mettre en place une surveillance normalisée et en continu des accès

L'efficacité de la gestion des accès à l'information gouvernementale se traduit notamment par une surveillance normalisée et continue. Cette surveillance permet de détecter les accès non autorisés et d'analyser les comportements malicieux.

3.3 Établir la cartographie des actifs informationnels critiques

La cartographie des actifs informationnels critiques permet de prioriser les actions en matière de sécurité de l'information. Elle sera réalisée sur la base des travaux en cours qui portent sur la consolidation des centres de traitement de l'information et sur l'état de santé des actifs gouvernementaux.

Cette cartographie nécessite le recensement des actifs informationnels critiques[2] et leur catégorisation, qui constituent un préalable déterminant dans la sélection des mesures de protection à mettre en place. Celles-ci doivent être proportionnelles à la valeur établie de l'information en matière de disponibilité, d'intégrité et de confidentialité et aux préjudices encourus par un organisme public.

1. Système d'information : Système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'une organisation. [Source : Office québécois de la langue française]

2. Actif informationnel : Tout document défini au sens de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1). À titre de rappel, cette loi définit le document ainsi :
   « Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles. [...] est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite. »
   Actif informationnel critique : Actif informationnel nécessaire à la réalisation de la mission d'un organisme public.

3.4 Déployer une équipe pour tester les systèmes d'information gouvernementaux

Les vulnérabilités susceptibles de compromettre la sécurité de l'information des organismes publics seront détectées au moyen d'audits techniques. À cet égard, une équipe technique du Centre gouvernemental de cyberdéfense sera déployée pour évaluer la sécurité physique et logique de l'information gouvernementale. Celle-ci effectuera, notamment auprès des organismes publics, des tests d'intrusion et de vulnérabilité, des tests de piratage psychologique et des campagnes d'hameçonnage.

3.5 Accélérer la prise en charge des vulnérabilités au sein de l'appareil gouvernemental

Les vulnérabilités, dans les systèmes d'information gouvernementaux, peuvent découler de failles de sécurité existantes dans un produit acquis ou qui ne bénéficie plus du soutien technique de son fournisseur. Il peut aussi s'agir d'absence de mesures de sécurité de l'information lors du développement des systèmes d'information.

Ces vulnérabilités seront analysées et évaluées, au sein du réseau gouvernemental de cyberdéfense, afin d'élaborer des méthodes et des pratiques harmonisées de déploiement des solutions et des correctifs nécessaires.

3.6 Intégrer la sécurité en amont

Une proportion notable de cyberattaques vise directement les applications vulnérables. Pour faire face à cette menace, le gouvernement apportera aux organismes publics le soutien nécessaire à l'intégration de la sécurité de l'information et de la protection des renseignements personnels dès la conception des systèmes d'information ou lors de leur acquisition. Cette intégration en amont présente des bénéfices, notamment en matière de coût de développement et de répercussions sur le fonctionnement des systèmes d'information, contrairement à une intégration plus complexe en aval, particulièrement à la suite d'un cyberincident.

Objectif 4 : Être proactif à l'égard des menaces émergentes

4.1 Établir des partenariats durables de mise en commun du savoir et des ressources

Le gouvernement entend constituer un réseau québécois de vigie en cybersécurité, l'objectif premier étant de mettre en commun le savoir et les ressources requises pour faire face efficacement aux cybermenaces. Des liens de collaboration seront créés avec des partenaires de l'écosystème de différents milieux (ex. : entreprises de l'État, municipalités, établissements d'enseignement, entités de recherche et de développement, entreprises privées).

4.2 Créer les conditions d'utilisation sécuritaires des technologies de pointe

La forme sans cesse renouvelée des cybermenaces constitue un enjeu de taille, notamment celles qui sont inhérentes à l'utilisation des technologies de pointe comme l'infonuagique, les objets connectés, l'intelligence artificielle et la chaine de blocs.

Le Centre gouvernemental de cyberdéfense collaborera avec le Centre québécois d'excellence numérique dans l'analyse des risques associés à l'utilisation des technologies de pointe. Cette analyse contribuera à l'utilisation sécuritaire de ces technologies par les outils de prévention des cybermenaces, notamment ceux de détection des vulnérabilités et de surveillance des accès.

Objectif 5 : Miser sur les forces d'un réseau gouvernemental de cyberdéfense

5.1 Mettre en place le Centre gouvernemental de cyberdéfense

Les actions de prévention, de détection et de réaction aux cybermenaces ainsi que les bonnes pratiques en cybersécurité seront renforcées par la création du Centre gouvernemental de cyberdéfense, constitué d'équipes compétentes, mobilisées et performantes. Un cadre de gestion sera élaboré en vue de définir l'organisation fonctionnelle du Centre gouvernemental de cyberdéfense, ses rôles et ses responsabilités ainsi que les modalités et les processus de sa collaboration avec les organismes publics.

5.2 Opérationnaliser le Réseau gouvernemental de cyberdéfense par la mise en place de centres opérationnels de cyberdéfense

L'implication des organismes publics est essentielle pour assurer la protection de l'information gouvernementale. Pour ce faire, des centres opérationnels de cyberdéfense seront progressivement déployés et mis en œuvre pour assurer la couverture de l'ensemble des organismes publics. Ces centres agiront en synergie avec le Centre gouvernemental de cyberdéfense.

5.3 Mettre en place une centrale de surveillance des événements de sécurité

Le Centre gouvernemental de cyberdéfense mettra en place une centrale de surveillance (24 h/24, 7 j/7) pour colliger et analyser les événements de sécurité détectés par les organismes publics, qui touchent les actifs informationnels gouvernementaux. Le portrait centralisé de ces événements permettra de mieux prioriser les actions pour sécuriser ces actifs.

Objectif 6 : Tirer profit d'une expertise de pointe en cybersécurité

6.1 Mettre à contribution les établissements d'enseignement pour offrir des programmes de formation en cybersécurité

Le gouvernement entend doter le Québec d'un bassin plus grand de personnes qui détiennent des compétences en cybersécurité. Pour ce faire, des offres de formations intéressantes en cybersécurité devront être élaborées. À cet effet, la collaboration des établissements d'enseignement sera sollicitée.

AXE 3
DES CITOYENNES ET CITOYENS CONFIANTS ET AVERTIS

Objectif 7 : Préserver la confiance des citoyennes et citoyens à l'égard de la sécurité de leurs données

7.1 Créer une identité numérique pour chaque citoyenne et citoyen

Une identité numérique forte et sécuritaire est un élément clé de la transformation numérique gouvernementale. La mise en œuvre de la solution québécoise d'identité numérique assurera une accessibilité accrue aux services en ligne, une plus grande efficience dans la gestion des informations d'identité, d'adresse et de contact et la prise en compte des enjeux de sécurité et de risques de fraude afférents.

Objectif 8 : Faire des citoyennes et citoyens des utilisateurs numériques avertis

8.1 Lancer une campagne de sensibilisation auprès des citoyennes et citoyens

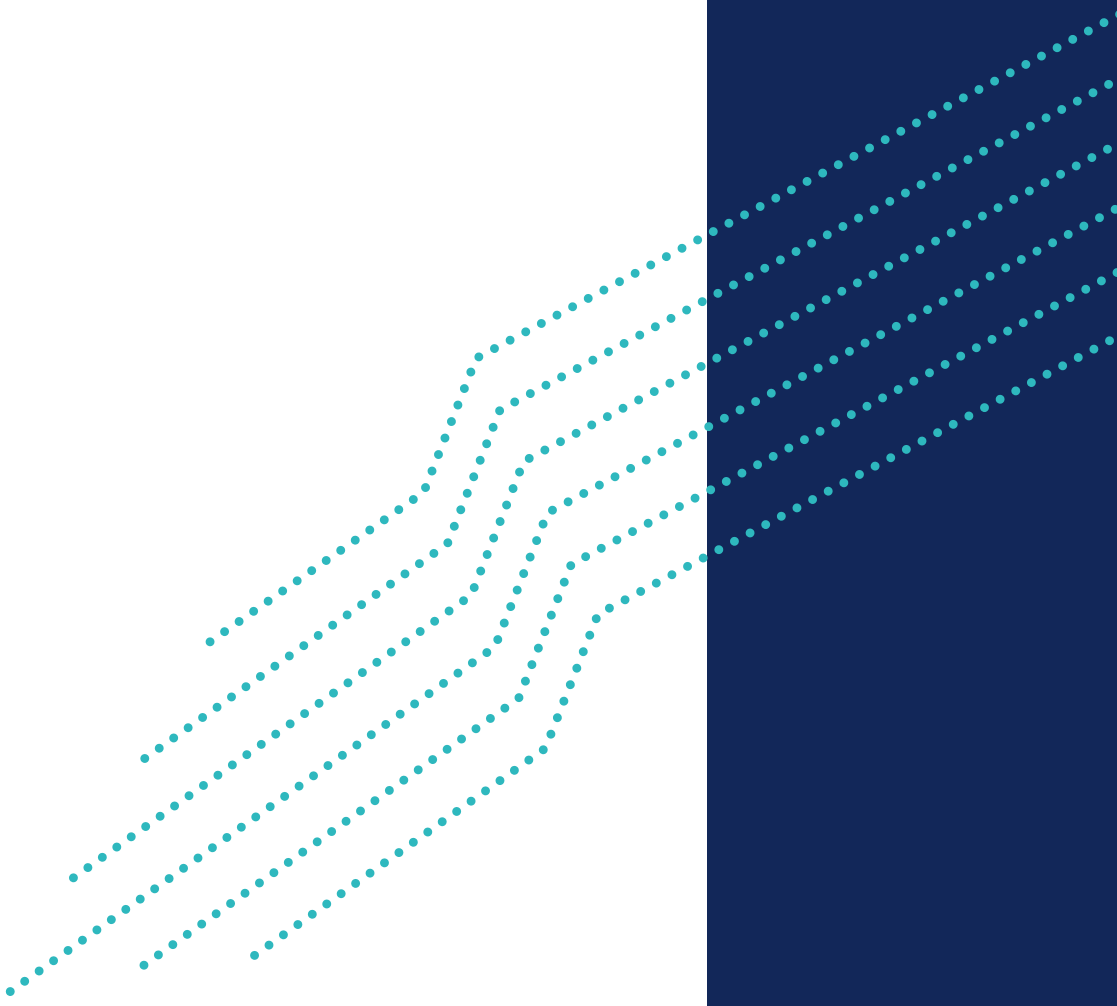
L'instauration d'une culture de cybersécurité passe par des actions de prévention et de promotion de la cyberhygiène. Une campagne de sensibilisation aux cyberrisques pour les citoyennes et citoyens ainsi que les entreprises sera lancée, de concert avec les institutions publiques et privées.

AXE 4
DES PARTENARIATS STRATÉGIQUES ET DURABLES

Objectif 9 : Tirer avantage des forces de l'écosystème

9.1 Engager des partenariats de collaboration en matière de recherche et d'innovation

Pour stimuler l'échange d'expertise et de connaissances, pour demeurer à l'affut des innovations qui ont un potentiel pour l'administration publique ainsi que pour maximiser les retombées qui découleront des sommes investies, le gouvernement entend tirer profit des forces de l'écosystème de cybersécurité et collaborer avec des organisations reconnues au plan national et international.



Québec