POLITIQUE GOUVERNEMENTALE DE CYBERSÉCURITÉ

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 – MARS 2020
Bibliothèque et Archives nationales du Québec
ISBN 978-2-550-86364-9 (version électronique)

MESSAGE DU MINISTRE RESPONSABLE DE L'ADMINISTRATION GOUVERNEMENTALE ET PRÉSIDENT DU CONSEIL DU TRÉSOR

La Politique gouvernementale de cybersécurité constitue le premier jalon des interventions mises de l'avant pour doter l'administration publique de véritables moyens de sensibilisation, de collaboration et d'innovation en cybersécurité. Assurer la transformation numérique de l'État ne peut se faire sans prendre en compte ni prévoir, entre autres, les risques inhérents à la recrudescence des cyberattaques.

À ce titre, le déploiement de cette toute première politique nous permettra, de concert avec l'ensemble des forces de l'écosystème, de mieux soutenir les organismes publics dans cette nécessaire mobilisation. Ainsi, le gouvernement fait de la cybersécurité une réelle priorité.

Je vous invite à prendre connaissance de cette nouvelle politique et, puisque nous sommes, toutes et tous, concernés par ces enjeux, à promouvoir et à adopter des habitudes et des comportements plus sécuritaires.

Christian Dubé

MOT DU MINISTRE DÉLÉGUÉ À LA TRANSFORMATION NUMÉRIQUE GOUVERNEMENTALE

L'importance cruciale et stratégique pour un État d'assurer sa cybersécurité dans un monde numérique en perpétuelle évolution est un constat partagé par l'ensemble des acteurs de la scène nationale et internationale.

Considérant l'augmentation exponentielle des flux de données personnelles et professionnelles, nous nous devons d'offrir à tous les Québécois et Québécoises des services numériques sécurisés.

Votre gouvernement ne fait aucun compromis avec la protection de vos données.

Votre gouvernement fait de la cybersécurité une priorité.

Votre gouvernement s'appuiera sur le savoir et l'expertise québécois qui font notre fierté.

Ensemble, faisons du Québec un leader mondial en cybersécurité et relevons les défis que dicte notre époque pour la protection de notre souveraineté numérique.

J'ai le privilège et l'honneur, à titre de ministre délégué à la Transformation numérique gouvernementale, de vous présenter votre première Politique gouvernementale de cybersécurité.

Éric Caire

TABLE DES MATIÈRES

CONTEXTE

L'accroissement rapide des interactions numériques, l'importance des informations échangées, la multiplication de ces échanges et les nombreux usages dorénavant possibles confèrent à celles-ci une valeur indéniable. Quotidiennement, que ce soit pour assurer des transactions ou de simples échanges sociaux, les technologies numériques sont omniprésentes.

Les évolutions comme l'intelligence artificielle, l'Internet des objets et les nouvelles technologies de stockage et de transmission multiplient les possibilités. Les appareils offrent une plus grande performance de traitement de l'information et leur usage est facilité par des capacités de stockage et de connexion jamais atteintes. L'émergence d'outils technologiques aussi puissants transforme les milieux de travail et l'économie dans leur ensemble. La prestation des services gouvernementaux à la population et aux entreprises n'y fait pas exception; elle se transforme.

Certes, cette transformation amène des possibilités, mais elle s'accompagne également d'enjeux qui se multiplient en matière de protection de l'information gouvernementale ainsi que des systèmes informatiques et des infrastructures qui assurent les services à la population. Le personnel de l'État est aussi confronté à l'usage du numérique dans son quotidien et a parfois accès à des données qui ont dorénavant une grande valeur aux yeux de certaines personnes malveillantes. Devant ces enjeux de cybersécurité internes et externes, des moyens s'imposent notamment pour :

- mobiliser l'ensemble des acteurs de l'écosystème de cybersécurité;
- innover dans la prise en charge des risques de cybersécurité, et ce, dans un processus d'amélioration continue;
- intervenir de façon proactive en anticipant les menaces et en adaptant constamment les moyens de s'en protéger;
- favoriser et encourager les actions de sensibilisation qui visent à promouvoir l'adoption de comportements sécuritaires auprès de la population et du personnel de l'État.

C'est en conformité avec la transformation numérique gouvernementale et sur la base des acquis et des réalisations de l'Administration gouvernementale en matière de cybersécurité que s'inscrit la présente Politique. Elle s'adresse tant aux organisations publiques et à leur personnel qu'à la population en plus de préciser les objectifs de l'État en ce qui concerne la cybersécurité.

OBJECTIF

La Politique gouvernementale de cybersécurité vise à instituer une Administration gouvernementale résiliente et cyberprotégée qui offre des services numériques centrés sur la personne. Sa mise en œuvre se traduira par des mesures clés assorties de plans d'action adaptés aux enjeux et aux possibilités en matière de cybersécurité.

PORTÉE

La Politique s'applique à l'ensemble des organismes publics assujettis à la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (L.R.Q.,c. G-1.03). Elle concerne les relations de ces organisations avec les usagers des services publics et avec leurs partenaires.

DÉFINITIONS

Cyberattaque : Ensemble coordonné d'actions malveillantes conduites par l'intermédiaire du cyberespace, qui visent à endommager, à forcer ou à détourner un réseau ou un système informatique afin de commettre un acte préjudiciable[1].

Cyberespace : Espace virtuel constitué par l'interconnexion mondiale des systèmes informatiques, des réseaux de télécommunication et des infrastructures de technologies de l'information, qui permet l'échange d'informations entre utilisateurs individuels ou collectifs[1].

Cyberhygiène : Ensemble des règles à observer et des pratiques récurrentes qui sont associées à la sécurité d'un système d'information[1].

Cyberprotection : Ensemble des moyens, techniques ou juridiques, qui contribuent à assurer la cybersécurité[1].

Cyberrisque : Ensemble de risques liés à l'utilisation des technologies de l'information[1]. Dans le présent document, le terme s'applique plus particulièrement au cyberespace.

Cybersécurité : Capacité, pour un système en réseau, de se protéger et de résister à des événements issus du cyberespace et susceptibles de porter atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information qu'il contient.

Cyberdéfense : Ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité[1]. Dans le présent document, la notion d'importance vitale fait référence à la valeur de l'information établie selon la confidentialité, l'intégrité et la disponibilité requises et tient compte notamment d'exigences légales, réglementaires et contractuelles.

Résilience : Capacité des systèmes à résister ou à se relever en cas d'incident.

1. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. *Grand dictionnaire terminologique.*

STRUCTURE DE LA POLITIQUE

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

OBJECTIF 2
Placer le personnel au cœur de la cybersécurité

Axe 2 — Des services publics sécuritaires

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

OBJECTIF 4
Être proactif à l'égard des menaces émergentes

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

OBJECTIF 6
Tirer profit d'une expertise de pointe en cybersécurité

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

OBJECTIF 8
Faire des citoyennes et citoyens des utilisateurs numériques avertis

Axe 4 — Des partenariats stratégiques et durables

OBJECTIF 9
Tirer avantage des forces de l'écosystème

PRINCIPES

La Politique gouvernementale de cybersécurité repose sur cinq principes fondamentaux.

1 PRINCIPE

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

2 PRINCIPE

Favoriser et encourager l'adoption de comportements cybersécuritaires

3 PRINCIPE

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

4 PRINCIPE

Encourager le partage et la mise en commun

5 PRINCIPE

Intégrer la protection de l'information en amont

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

Les mesures de protection à mettre en place doivent être proportionnelles à la valeur établie de l'information et aux risques encourus. Cette valeur est évaluée selon la confidentialité, l'intégrité et la disponibilité requises et tient compte notamment d'exigences légales, réglementaires et contractuelles.

PRINCIPE 2
Favoriser et encourager l'adoption de comportements cybersécuritaires

La responsabilité, en matière de cybersécurité, est partagée entre les acteurs de l'Administration gouvernementale. Les tentatives de cyberattaques sont une réalité quotidienne pour le personnel de l'État et la population, qui en sont la cible principale. Un tel enjeu impose de favoriser et d'encourager des actions d'éducation et de sensibilisation qui visent à promouvoir l'adoption de comportements sécuritaires quant aux cybermenaces.

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

L'attraction et la rétention des talents en cybersécurité sont des enjeux et des défis d'importance. De tels enjeux nécessitent des efforts soutenus pour mettre à niveau les compétences existantes, développer celles de demain et augmenter l'attractivité et la fidélisation des expertises, particulièrement dans un contexte des plus concurrentiels.

PRINCIPE 4
Encourager le partage et la mise en commun

La cybersécurité est une composante majeure des systèmes ouverts sur le cyberespace, voire une nécessité. Son renforcement, dans une perspective de protection de l'information et de résilience des systèmes gouvernementaux, implique d'aller au-delà des réalisations en silo et de prôner une ouverture sur le partage et la mise en commun des connaissances, de l'expertise et des bonnes pratiques en cybersécurité. La concrétisation de cette ouverture requiert des alliances stratégiques avec les acteurs de l'écosystème et permet d'élaborer les mesures préventives à l'égard des cyberrisques.

PRINCIPE 5
Intégrer la protection de l'information en amont

La protection de l'information en amont permet de sécuriser les systèmes en intégrant les mesures nécessaires dès leur conception ou leur acquisition. Ces mesures assurent autant la protection de l'information, tout au long de son cycle de vie, que la résilience des systèmes gouvernementaux et des infrastructures critiques.

AXES D'INTERVENTION ET OBJECTIFS

AXE 1
LA CYBERSÉCURITÉ, UNE PRIORITÉ GOUVERNEMENTALE

Au gouvernement du Québec, la cybersécurité constitue un objectif stratégique en soutien à la réalisation de la mission de l'État et de ses cibles de transformation numérique. Elle repose sur un leadership gouvernemental, l'instauration d'une gouvernance forte et intégrée de la cybersécurité et l'amélioration des comportements cybersécuritaires du personnel de l'État.

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

Adopter une gouvernance qui s'appuie sur une vision globale et concertée simplifie la gestion des risques encourus et assure une meilleure protection de l'information. Une telle approche nécessite une cohésion d'ensemble et une forte concertation entre les acteurs de l'écosystème gouvernemental de cybersécurité. 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.

Cet objectif implique notamment :

- d'adapter le cadre législatif et réglementaire qui régit la sécurité de l'information et la protection des renseignements personnels et de veiller à son application. Les textes qui en découleront devront cibler autant la protection de l'information que la résilience des systèmes à l'ère du numérique;
- de réviser le cadre de gestion de la sécurité de l'information en mettant notamment l'accent sur la définition d'une structure gouvernementale de coordination et de collaboration, le partage des rôles et des responsabilités, le suivi des réalisations et la mesure des bénéfices afférents, ainsi que sur la détermination d'indicateurs de performance viables et appropriés. Afin d'accroître les réflexes de cybersécurité, la gestion gouvernementale des risques, des incidents de sécurité et des situations de crise sera soutenue par des pratiques standardisées;
- de soutenir et d'accompagner les organisations publiques dans la prise en charge des incidents et des exigences de cybersécurité.

Objectif 2.
Placer le personnel au cœur de la cybersécurité

L'Administration gouvernementale entend faire du personnel de l'État un acteur averti quant aux comportements et aux pratiques exemplaires à adopter devant les cybermenaces. Elle mise ainsi sur le développement de ses compétences et sa sensibilisation à l'égard des cyberrisques et vise à ancrer la cybersécurité dans la culture des organisations publiques afin que cette priorité gouvernementale devienne l'affaire de tous. De telles initiatives permettront au personnel de participer à la résilience globale de son organisation, voire à celle de l'écosystème gouvernemental.

Cet objectif implique notamment que :

- l'ensemble du personnel de l'État devienne le maillon fort de la cybersécurité par des comportements proactifs et adéquats à l'égard de l'information, des risques et des cybermenaces;
- des actions de prévention et de promotion de la cyberhygiène soient mises en œuvre dans les milieux de travail.

Ces actions sont appuyées par des programmes de formation et de sensibilisation en continu et sont renforcées par des pratiques de vérification des connaissances en cybersécurité et par l'application des comportements exemplaires en la matière.

AXE 2
DES SERVICES PUBLICS SÉCURITAIRES

L'apparition de nouveaux risques de sécurité de l'information à l'ère du numérique représente un défi d'importance. La protection de l'information et la résilience des services publics étant au cœur des préoccupations de l'Administration gouvernementale, les risques doivent être identifiés, traités et leurs impacts potentiels réduits à un niveau acceptable. À cet égard, l'Administration gouvernementale doit se doter de mesures pour se prémunir et faire face à tout type d'attaques et à d'éventuels sinistres.

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

La protection de l'information gouvernementale, des systèmes, des infrastructures et des moyens de communication qui permettent d'offrir les services publics est un impératif absolu que le gouvernement entend assurer. Devant les enjeux de cybersécurité, des mesures à l'égard des risques et des menaces internes et externes s'imposent. Il en est de même de la résilience des services publics et des communications gouvernementales en cas de cyberattaque ou de sinistre.

Cet objectif implique notamment :

- un processus rigoureux de gestion des cyberrisques, basé sur une bonne connaissance des menaces et des mesures possibles en matière de cybersécurité, sur la détermination des actifs critiques et de leur emplacement ainsi que sur la catégorisation de l'information;
- la mise en place de mesures d'atténuation des risques (comme les mécanismes d'habilitation sécuritaire, le cloisonnement des réseaux informatiques, la détection des incidents et la réponse automatique à ceux-ci, la sauvegarde régulière de l'information, les plans de reprise informatique et la vérification de leur déploiement effectif, les tests d'intrusion et les exercices de simulation d'attaque), menées en partenariat avec les acteurs de l'écosystème de cybersécurité québécois, canadien et international;
- que tous les échanges d'information entre les ministères, les organisations et les acteurs de l'écosystème soient réalisés par l'entremise de réseaux de télécommunication reconnus qui assurent une protection adéquate;
- une gestion de l'identité et des accès qui prend appui sur une identité numérique conviviale, interopérable et hautement sécuritaire ainsi que sur l'application normalisée de la surveillance des accès;
- que la protection de l'information et la résilience des systèmes, des infrastructures et des moyens de communication, qui permettent d'offrir les services publics, soient intégrées dès leur conception ou qu'elles soient prévues dans les contrats d'acquisition et de soutien, et ce, pour tout le cycle de vie.

Le gouvernement entend stimuler la collaboration des organisations publiques dans l'implantation de moyens technologiques innovants pour la protection adéquate de l'information, en demeurant responsable à chacune des étapes du cycle de vie de celle-ci. Il en est de même pour la protection des échanges et des communications entre les organisations publiques et avec les partenaires.

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

La forme sans cesse renouvelée des cybermenaces constitue un enjeu de taille pour l'Administration gouvernementale. La protection à l'égard des cybermenaces émergentes, souvent inconnues, est de plus en plus complexe. Devant celles-ci, le gouvernement entend augmenter les capacités institutionnelles d'analyse des risques émergents et de prospective et mettre en place les mesures préventives appropriées de protection et de renforcement de la résilience de ses systèmes.

Cet objectif implique notamment :

- d'établir des liens avec certains partenaires de confiance afin de constituer un réseau d'alerte;
- de fédérer des initiatives de recherche et de veille en matière de cybersécurité.

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

Le renforcement des dispositifs de prévention et de réaction à l'égard des cybermenaces, requiert la mise en place d'un réseau gouvernemental de cyberdéfense, sous le leadership d'une structure gouvernementale de commandement. Cette structure jouera, au sein du réseau, le rôle d'entité de confiance qui coordonnera la prise en charge des incidents de sécurité et des communications opérationnelles.

Cet objectif implique notamment :

- de coordonner les efforts en cybersécurité des organisations publiques et des unités opérationnelles de cyberdéfense, comme le partage et la mise en commun des connaissances et de l'expertise ainsi que le recours à des pratiques standardisées;
- de jouer un rôle collaboratif dans l'écosystème de cybersécurité québécois, national et international, tout en tenant compte des impératifs de souveraineté numérique pour une autonomie accrue du public sur ses données et une capacité pleine et entière de l'État pour en assurer la protection;
- de mettre en place un processus de communication aux autorités concernées.

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

Pour réussir la transformation numérique gouvernementale, il est nécessaire d'avoir une main d'œuvre hautement qualifiée en sécurité de l'information. Cette expertise doit évoluer en continu, au rythme des changements technologiques.

Cet objectif implique notamment :

- de cibler les champs de compétences requis en cybersécurité adaptés à la nouvelle réalité;
- de diversifier les profils et les domaines de compétences du personnel qui travaille en cybersécurité;
- d'offrir des programmes de formation selon les champs de compétences déterminés, en mettant à contribution les forces vives du Québec dans le domaine des pratiques sécuritaires en technologies de l'information, particulièrement de la cybersécurité;
- de déterminer le parcours de personnes susceptibles de renforcer le bassin gouvernemental de ressources en cybersécurité, mais non formées dans le domaine, et de leur offrir la possibilité de réorienter leur carrière par des formations spécialisées en la matière;
- d'évaluer en continu les moyens de formation offerts et les compétences acquises en sécurité de l'information, et ce, en réponse aux défis.

Pour favoriser cette main-d'œuvre qualifiée, le gouvernement entend fédérer les efforts et coordonner une démarche collective auprès de l'ensemble des acteurs de l'écosystème québécois de cybersécurité. Par ailleurs, il mettra à contribution les établissements d'enseignement du Québec, en misant sur l'attractivité et la diversité.

AXE 3

Des citoyennes et citoyens confiants et avertis

L'utilisation des services publics repose non seulement sur le niveau de confiance des citoyennes et citoyens quant à la robustesse des systèmes gouvernementaux, mais également sur leur habileté ainsi que sur leur capacité d'en faire usage de façon sécuritaire afin de préserver la confidentialité de leurs données personnelles et le respect de leur vie privée.

Objectif 7.

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

Le gouvernement entend préserver la confiance des citoyennes et citoyens à l'égard de la sécurité de leurs données par son engagement de transparence en faveur d'une utilisation éthique et par l'intégration de pratiques exemplaires pour en assurer la protection.

Cet objectif implique notamment :

- de fournir à toute personne une identité numérique qui lui permet de s'identifier et de s'authentifier de façon sécuritaire;
- de faciliter, selon les lois applicables, l'accès par toute personne aux données qui la concernent;
- de permettre à toute personne, selon les lois applicables, de mettre à jour les données que le gouvernement détient à son égard.

Objectif 8.

Faire des citoyennes et citoyens des utilisateurs numériques avertis

Le gouvernement entend mener des actions de sensibilisation à l'égard du public afin que celui-ci acquière des habitudes et des comportements sécuritaires qui contribuent à accroître sa confiance dans ses relations numériques avec l'État.

Cet objectif implique notamment :

- de rendre des contenus informatifs accessibles au public, en mettant à profit l'ensemble de l'écosystème;
- de stimuler l'acquisition des compétences du public, par l'entremise des établissements d'enseignement;
- d'assurer que les interactions numériques entre l'Administration gouvernementale et le public soient connues, standardisées et sécuritaires, et ce, afin d'éviter les bris de confidentialité.

AXE 4

Des partenariats stratégiques et durables

Le gouvernement vise à tirer avantage de l'ensemble des ressources disponibles, incluant des solutions et des services offerts par des tiers. Un partenariat durable en matière de conseil, d'expertise, de collaboration et de soutien constitue une valeur ajoutée dans un écosystème où les échanges entre les parties prenantes jouent un rôle déterminant. De plus, le gouvernement du Québec verra à convenir, avec les parties, de retombées tangibles pour l'Administration gouvernementale.

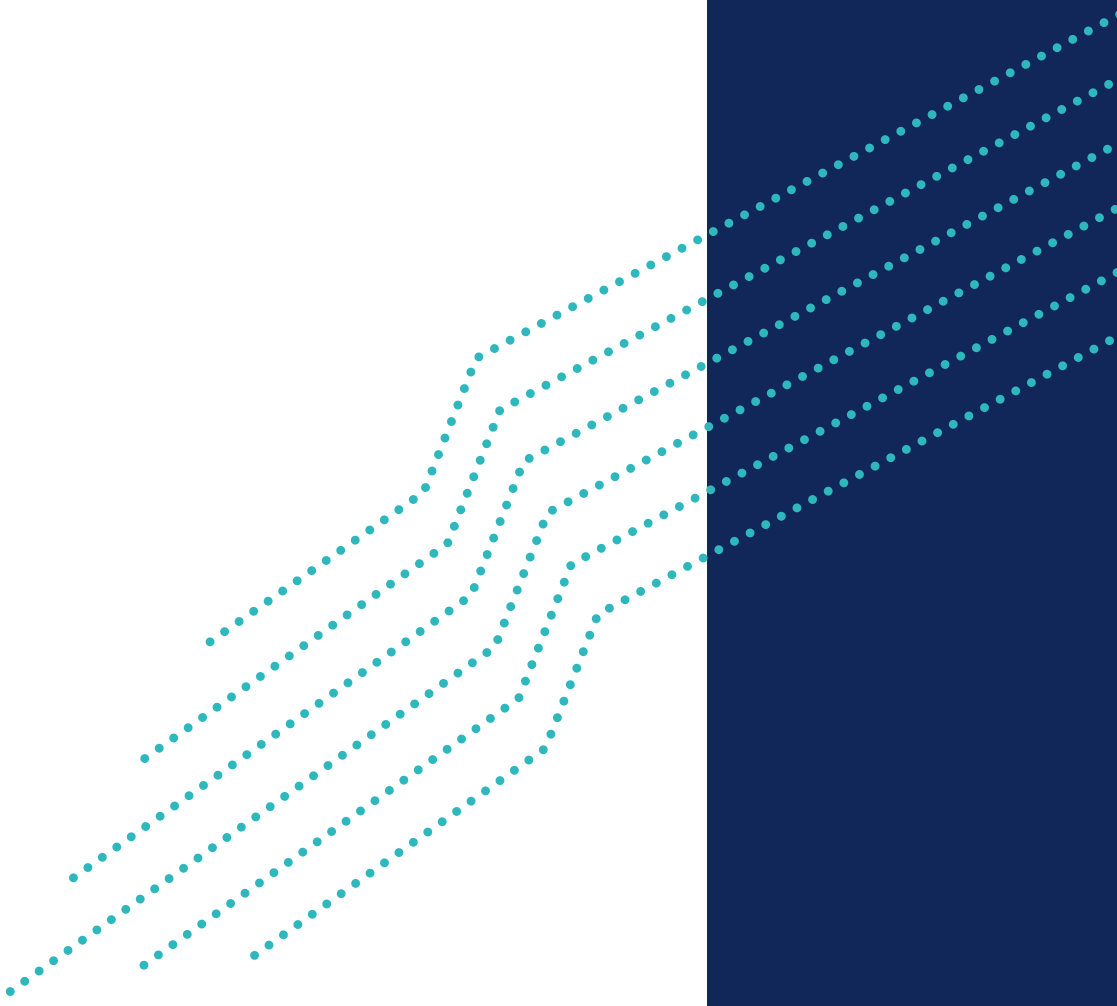
Objectif 9.
Tirer avantage des forces de l'écosystème

Tout en préservant la souveraineté sur ses données, le gouvernement entend tirer avantage des forces de l'écosystème en tissant des alliances stratégiques afin de faire du Québec un espace de conception de solutions innovantes en cybersécurité. À cet égard, il favorisera la recherche, l'innovation, et la mise en place de programmes avec différents partenaires gouvernementaux pour stimuler l'échange d'expertise et le partage de bonnes pratiques.

Cet objectif implique notamment :

- de faire en sorte que le gouvernement du Québec assure une synergie pour l'atteinte de buts communs avec les partenaires de l'écosystème;
- de rallier les organisations dans la détermination de pistes de solution sur des thèmes particuliers en lien avec la cybersécurité, en stimulant la recherche et l'innovation;
- de maximiser les retombées, au sein de l'Administration gouvernementale, qui découlent des sommes investies en provenance de fonds publics.

Ce faisant, le gouvernement contribuera à faire du Québec un pôle reconnu en cybersécurité, lequel concourra au développement économique et à l'attraction des talents en cette matière.



Québec