PROPULSER L'ADMINISTRATION PUBLIQUE NUMÉRIQUE DE DEMAIN

STRATÉGIE GOUVERNEMENTALE DE CYBERSÉCURITÉ ET DU NUMÉRIQUE 2024–2028

Votre gouvernement

Québec

PROPULSER L'ADMINISTRATION PUBLIQUE NUMÉRIQUE DE DEMAIN

STRATÉGIE GOUVERNEMENTALE
DE CYBERSÉCURITÉ ET DU NUMÉRIQUE
2024–2028

RÉDACTION
La Direction des politiques et de la performance numérique
du Sous-ministériat adjoint à la gouvernance des ressources informationnelles
du ministère de la Cybersécurité et du Numérique

ÉDITION
La Direction des communications du ministère de la Cybersécurité et du Numérique

Le présent document est disponible en version électronique,
à l'adresse quebec.ca/gouvernement/ministere/cybersecurite-numerique,
dans la section Publications.

Si vous éprouvez des difficultés techniques ou si vous souhaitez
obtenir une version adaptée du document, veuillez communiquer
avec la Direction des communications :

Direction des communications
Ministère de la Cybersécurité et du Numérique
900, place D'Youville, 2e étage
Québec (Québec) G1R 3P7
Courriel : information@mcn.gouv.qc.ca

Dépôt légal – Juillet 2024
Bibliothèque et Archives nationales du Québec
ISBN : 978-2-550-97215-0 (version imprimée)
ISBN : 978-2-550-97216-7 (version électronique)

MOT DU PREMIER MINISTRE

En seulement quelques années, la cybersécurité et la transformation numérique de l'État se sont imposées au Québec et partout à travers le monde. Elles ont modifié la manière de concevoir le travail ainsi que les relations avec la population.

Il devient alors nécessaire pour les administrations de revoir les façons de faire, d'optimiser leurs processus et d'améliorer leur performance dans le but d'offrir des services sécuritaires de qualité aux citoyennes et aux citoyens.

Grâce à sa créativité et à son esprit d'innovation, le Québec s'est positionné, au fil du temps, comme un pionnier dans la conception et le développement de nouvelles technologies, dont celles liées à l'intelligence artificielle. Notre nation est reconnue comme un pôle d'innovation dans ce secteur de pointe : c'est pourquoi nous devons bâtir à partir de cette fierté pour que notre État soit plus efficace.

Le Québec a entrepris de grands chantiers pour moderniser son offre de prestations numériques et des changements importants sont déjà en branle. Il est maintenant temps d'accélérer la transformation numérique de l'État afin que l'ensemble des citoyennes et des citoyens du Québec puisse bénéficier de services numériques accessibles, complets, conviviaux et sécuritaires.

Par cette *Stratégie gouvernementale de cybersécurité et du numérique 2024–2028*, le Québec se donne les moyens d'offrir à sa population une expérience citoyenne simple et accessible, où elle se sentira en confiance et protégée.

François Legault
Premier ministre du Québec

Québec, juillet 2024

MOT DU MINISTRE

La création du ministère de la Cybersécurité et du Numérique, le 1er janvier 2022, est un geste fort et concret qui démontre l'engagement et l'importance que notre gouvernement accorde à la transformation numérique gouvernementale. C'est avec fierté que je vous présente la *Stratégie gouvernementale de cybersécurité et du numérique 2024–2028*, laquelle poursuit le travail entamé par la *Stratégie de transformation numérique gouvernementale 2019–2023*.

Maintenant que l'ensemble des ministères et organismes sont en mouvement vers une seule transformation numérique gouvernementale, la *Stratégie 2024–2028* propose des actions significatives pour propulser encore plus loin l'administration publique. Ainsi, nous définissons notre vision d'une utilisation transparente, innovante et performante du numérique, avec comme objectifs en tête d'améliorer l'expérience et la confiance des citoyennes et des citoyens à l'égard des services numériques de l'État et de travailler en collaboration avec l'écosystème numérique québécois.

Parmi les conditions nécessaires à l'atteinte de ces objectifs figurent l'adoption d'une réelle culture numérique au sein de l'administration publique ainsi que le démantèlement du travail en silo. À cet égard, je tiens à saluer l'engagement et l'expertise du personnel du Ministère, qui saura accompagner les organismes publics dans la mise en œuvre de la Stratégie.

Bien sûr, la cybersécurité demeure au cœur de nos préoccupations. Le gouvernement fait de la sécurité des données qui lui sont confiées sa priorité afin d'être à la hauteur de la confiance que lui accordent les citoyennes, les citoyens et les entreprises.

Ces derniers ont, avec raison, de grandes attentes envers la transformation numérique gouvernementale. Nous devons leur fournir des services plus accessibles, plus rapides et plus sécuritaires. Nous avons également le devoir de les accompagner dans le développement de leurs compétences numériques et de nous assurer de continuer à offrir des services de qualité à ceux qui sont moins à l'aise d'interagir dans l'univers numérique.

Compte tenu de la progression constante de l'utilisation du numérique dans toutes les sphères d'activité de la société, la Stratégie nous permet d'être à l'écoute de la population et de répondre aux attentes et aux besoins qu'elle manifeste.

Éric Caire
Ministre de la Cybersécurité et du Numérique

Québec, juillet 2024

MOT DU SOUS–MINISTRE

La transformation numérique et le renforcement de la cybersécurité sont des défis auxquels l'administration publique québécoise doit impérativement répondre. Partout à travers le monde, les administrations publiques des États sont à l'œuvre pour moderniser leurs façons de faire. Pour y arriver, elles misent sur les dernières innovations technologiques et le Québec ne fait pas exception.

Depuis l'élaboration de la *Stratégie de transformation numérique gouvernementale 2019–2023*, l'administration publique québécoise a pu compter sur plusieurs autres réalisations comme la *Stratégie d'intégration de l'intelligence artificielle dans l'administration publique 2021–2026* et la *Politique gouvernementale de cybersécurité*, en vigueur depuis 2020.

Ces dernières ont déjà permis à plus de 300 organismes publics du Québec d'accomplir des progrès significatifs en ces matières. Elles ont également mené au déploiement graduel du Service d'authentification gouvernementale, à la création du Centre québécois d'excellence numérique ainsi que du Réseau gouvernemental de cyberdéfense et à la mise en place de plusieurs initiatives comme la plateforme de signalement de vulnérabilité.

La nouvelle *Stratégie gouvernementale de cybersécurité et du numérique 2024–2028* est une occasion de plus pour l'administration publique d'exceller et de se propulser encore plus loin en matière de transformation numérique.

Stéphane Le Bouyonnec
Sous-ministre de la Cybersécurité et du Numérique
et dirigeant principal de l'information

Québec, juillet 2024

TABLE DES MATIÈRES

AXE II – ACCÉLÉRER LA TRANSFORMATION NUMÉRIQUE DE L'ADMINISTRATION PUBLIQUE 27

INTRODUCTION

Le numérique et les enjeux de cybersécurité occupent une place centrale dans la vie d'une grande majorité de Québécoises et de Québécois. La première révolution industrielle a transformé le monde de l'agriculture, de l'économie et la société dans son ensemble. Déjà bien amorcée, la quatrième révolution, fondée sur le potentiel du numérique et des données, nous conduit assurément vers une cinquième révolution avec l'intelligence artificielle (IA), l'automatisation et la robotisation comme principales locomotives. Conséquemment, ces développements représentent une opportunité sans précédent d'accélérer la transformation des services publics favorisant la performance de l'État au bénéfice des citoyennes et des citoyens. La présente *Stratégie gouvernementale de cybersécurité et du numérique 2024–2028* s'inscrit en phase avec les progrès réalisés à ce jour par les organismes publics tout en misant sur un usage responsable, transparent et éthique des données. Bien ancré dans les habitudes de vie des Québécoises et des Québécois, l'usage des appareils technologiques ou numériques atteint de nouveaux sommets puisque selon les données de 2022[1], 95 % des adultes au Québec possèdent l'un de ces appareils. Cette proportion passe à 100 % pour les 25 à 44 ans et est de 79 % pour les 75 ans et plus. De plus, ce sont 84 % des citoyennes et des citoyens du Québec qui sont propriétaires d'un téléphone intelligent, alors que ce taux était de 77 % en 2019.

Cette omniprésence du numérique, de même que la multiplication des plateformes technologiques de haute qualité offertes par un nombre croissant d'organisations du secteur privé, fait en sorte que les citoyennes et les citoyens[2] s'attendent désormais aux plus hauts standards en matière de services numériques de la part de l'administration publique[3].

Dans ce contexte en grande évolution, le gouvernement du Québec est déjà en action. Dès 2019, il a adopté la *Stratégie de transformation numérique gouvernementale 2019–2023* (ci–après « *Stratégie 2019–2023* ») dans le but de fournir à l'administration publique une vision commune et cohérente en vue de réaliser la transformation de l'État par le numérique.

Cette vision était claire :
des services publics plus rapides et intuitifs,
propulsés par le numérique.

1. ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE. (2022). *Portrait numérique des foyers québécois. Édition 2022*, [En ligne], [https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/portrait-numerique-des-foyers-quebecois-2022/], (Consulté en avril 2023).
2. Dans le cadre de la présente stratégie, le terme « citoyen » inclut les entreprises (citoyens corporatifs) lorsque cela est applicable.
3. Dans le cadre de la présente stratégie, le terme « administration publique » englobe 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* (chapitre G–1.03).

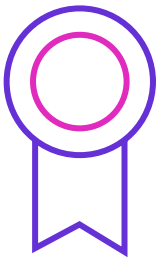
La *Stratégie 2019–2023* a eu pour effet d'engager l'administration publique sur la voie de la transformation numérique, notamment en fournissant des structures de gouvernance en ressources informationnelles solides, permettant une action concertée et structurante entre les organismes publics.

À ce chapitre, la création du ministère de la Cybersécurité et du Numérique (MCN), le 1er janvier 2022, témoigne de l'importance capitale d'assurer la protection des données publiques, de tirer profit du numérique pour améliorer la performance de l'administration publique et pour transformer les services publics afin que ces derniers soient modernes, sécuritaires, intuitifs et accessibles en tout temps. Le Québec a fait preuve d'avant–gardisme en devenant le premier État en Amérique du Nord à réunir la cybersécurité et le numérique au sein d'une même entité, en faisant du même souffle une mission de l'État à part entière.

Forte de la maturité acquise et des avancées réalisées dans les dernières années, l'administration publique doit maintenant accélérer la cadence et redoubler d'efforts pour réaliser la transformation par le numérique et rapidement offrir des services publics plus intuitifs et faciles d'utilisation pour les citoyennes et les citoyens ainsi qu'améliorer l'efficience de l'État.

LES PRINCIPAUX ACCOMPLISSEMENTS EN MATIÈRE DE CYBERSÉCURITÉ ET DE NUMÉRIQUE

Avec la *Stratégie 2019–2023* et l'ensemble de son action en matière de cybersécurité et de numérique, l'administration publique québécoise a posé les bases de sa transformation par le numérique et s'est donné l'impulsion nécessaire vers une vision commune de cette transformation. Le gouvernement du Québec se démarque depuis 2019 par ses réalisations. En voici quelques–unes :



CRÉATION DU CENTRE QUÉBÉCOIS D'EXCELLENCE NUMÉRIQUE

Le Centre québécois d'excellence numérique (CQEN), une entité consacrée exclusivement à la transformation numérique gouvernementale, a été créé en juin 2019 avec une mission claire : accélérer et faciliter la transformation numérique en favorisant le partage et la collaboration. Il poursuivra son action par la mise en œuvre d'initiatives numériques visant l'usage d'automatisation ou d'intelligence artificielle pour améliorer les services publics à portée gouvernementale.

DÉPLOIEMENT DU RÉSEAU GOUVERNEMENTAL DE CYBERDÉFENSE

Créé en 2020, le Centre gouvernemental de cyberdéfense (CGCD) est un rouage essentiel de la protection des infrastructures numériques au Québec. Le CGCD a pour mission de :

- surveiller et contrer les risques et les menaces pouvant peser sur les organismes publics et les ministères ;
- prendre en charge les vulnérabilités détectées au niveau gouvernemental afin de prévenir les incidents ;
- déployer les mesures nécessaires afin de protéger les données gouvernementales.

Le CGCD coordonne le Réseau gouvernemental de cyberdéfense, constitué de près d'une trentaine de centres opérationnels de cyberdéfense (COCD), ce qui lui permet de desservir l'ensemble des organismes publics en matière de cybersécurité. Le CGCD a mis en place plusieurs services permettant d'améliorer la protection des services numériques et des données citoyennes.

ADOPTION DE LA POLITIQUE GOUVERNEMENTALE DE CYBERSÉCURITÉ

En vigueur depuis 2020, la Politique gouvernementale de cybersécurité vise à répondre aux défis de cybersécurité dans un contexte de transformation numérique. Son but est d'améliorer la protection contre les cybermenaces au sein de l'administration gouvernementale, contribuant ainsi à accroître le niveau de maturité des organismes publics en matière de cybersécurité. Sa mise en œuvre est assurée par des mesures clés assorties de plans d'action.

RESTRUCTURATION DU COMITÉ DE GOUVERNANCE EN RESSOURCES INFORMATIONNELLES

Depuis 2020, le Comité de gouvernance en ressources informationnelles est rigoureusement structuré, s'alignant sur les meilleures pratiques observées au sein des conseils d'administration. Réunissant le dirigeant principal de l'information, qui le préside, et les dirigeants de l'information, le Comité de gouvernance en ressources informationnelles favorise la concertation entre les organismes publics et soutient l'évolution des pratiques en gestion des ressources informationnelles au sein de l'administration publique.

ADOPTION DE LA *STRATÉGIE D'INTÉGRATION DE L'INTELLIGENCE ARTIFICIELLE DANS L'ADMINISTRATION PUBLIQUE 2021–2026*

Adoptée en juin 2021, la *Stratégie d'intégration de l'intelligence artificielle dans l'administration publique 2021–2026* vise à positionner l'administration publique comme acteur exemplaire de l'IA et représente à la fois un moteur de transformation des processus d'affaires et l'une des réponses à la rareté de la main–d'œuvre. Le Québec a fait une entrée remarquée au 7e rang mondial des écosystèmes d'IA[4], entre autres grâce à des investissements de plus de 750 M$ en appui au développement de l'écosystème d'IA depuis 2016 et par la qualité de la stratégie d'intégration de l'IA dans l'administration publique. En plus de notre action gouvernementale en IA, les investissements du gouvernement du Québec ont permis au Québec de se démarquer, notamment dans la recherche en apprentissage profond, à travers l'attraction de chercheurs de renommée mondiale ou, de grandes entreprises leaders en IA et le développement croissant d'entreprises en démarrage spécialisées ainsi qu'en matière d'adoption de l'IA par les PME de tous les secteurs. À l'hiver 2024, le ministre de la Cybersécurité et du Numérique a pris un arrêté ministériel afin de déterminer les exigences en matière de ressources informationnelles au regard de l'utilisation de l'IA par les organismes publics[5]. Les prochaines années seront résolument marquées par l'omniprésence de l'IA dans les transformations de l'État, et celui–ci veillera à son usage éthique et responsable.

LANCEMENT DE LA PLATEFORME DE SIGNALEMENT DE VULNÉRABILITÉ

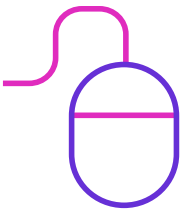
Lancée en octobre 2021, la Plateforme de signalement de vulnérabilité permet aux chercheuses et aux chercheurs en sécurité de l'information ainsi qu'au grand public de rapporter des vulnérabilités concernant des services numériques gouvernementaux exposés sur Internet.

4. LA PRESSE. *Intelligence artificielle : Le Québec se classe 7e au monde*, [En ligne], 2022, [Intelligence artificielle | Le Québec se classe 7e au monde | La Presse] (Consulté en mai 2024).

5. Arrêté numéro 2024–01 du ministre de la Cybersécurité et du Numérique en date du 28 février 2024.

LANCEMENT DU PROGRAMME DE PRIME AUX BOGUES

En septembre 2023, le Programme de prime aux bogues est lancé[6]. Le Programme encourage les chercheuses et les chercheurs en sécurité de l'information à signaler de manière éthique les vulnérabilités découvertes sur des actifs informationnels de l'administration publique.



MISE EN LIGNE DU SERVICE D'AUTHENTIFICATION GOUVERNEMENTALE

Le Service d'authentification gouvernementale, en déploiement graduel depuis décembre 2022, permet aux citoyennes et aux citoyens d'accéder aux prestations électroniques de services du gouvernement du Québec et à leurs dossiers en ligne en toute sécurité.

MODIFICATIONS AU CADRE LÉGISLATIF EN MATIÈRE DE RESSOURCES INFORMATIONNELLES DANS L'ADMINISTRATION PUBLIQUE

Sanctionnée le 10 juin 2021, la *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* (LQ 2021, chapitre 22) renforce la gouvernance des ressources informationnelles. Elle a notamment permis la création de trois nouvelles fonctions assumées par le dirigeant principal de l'information, soit celles de chef gouvernemental de la sécurité de l'information, de gestionnaire des données numériques gouvernementales et de chef gouvernemental de la transformation numérique.

La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* a été modifiée de nouveau, le 6 décembre 2023[7], et a permis à l'État de se doter d'outils pour assurer une gouvernance forte et cohérente au regard des projets jugés prioritaires. Également, d'autres modifications visaient à renforcer la sécurité des actifs informationnels pour une action unifiée en cyberdéfense.

6. Arrêté numéro 2023–01 du ministre de la Cybersécurité et du Numérique en date du 8 septembre 2023.

7. *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* (LQ 2023, chapitre 28).

VISION

1 AMÉLIORER L'EXPÉRIENCE DES CITOYENNES ET DES CITOYENS PAR LE BIAIS DES SERVICES NUMÉRIQUES OFFERTS PAR L'ADMINISTRATION PUBLIQUE

La transformation numérique gouvernementale vise l'atteinte d'objectifs clairs : une expérience client améliorée qui s'exprime par des services accessibles, complets, conviviaux, sécuritaires et de qualité.

En ce sens, les organismes qui composent l'administration publique doivent travailler de concert pour offrir aux citoyennes et aux citoyens une expérience unifiée. Peu importe le service gouvernemental utilisé, les Québécoises et les Québécois doivent vivre une expérience transparente, continue, de qualité équivalente, le tout en s'adressant à un seul gouvernement.

Dans ce contexte, il importe que la conception des services se fasse en atténuant la fracture numérique. Pour ce faire, les politiques publiques et les initiatives doivent viser à faciliter l'accès aux technologies de l'information pour tous, à améliorer les compétences numériques des personnes en situation d'exclusion et à promouvoir l'utilisation des outils et services en ligne inclusifs et équitables.

2 INSPIRER LA CONFIANCE DES CITOYENNES ET DES CITOYENS PAR UN ÉCOSYSTÈME CYBERSÉCURITAIRE

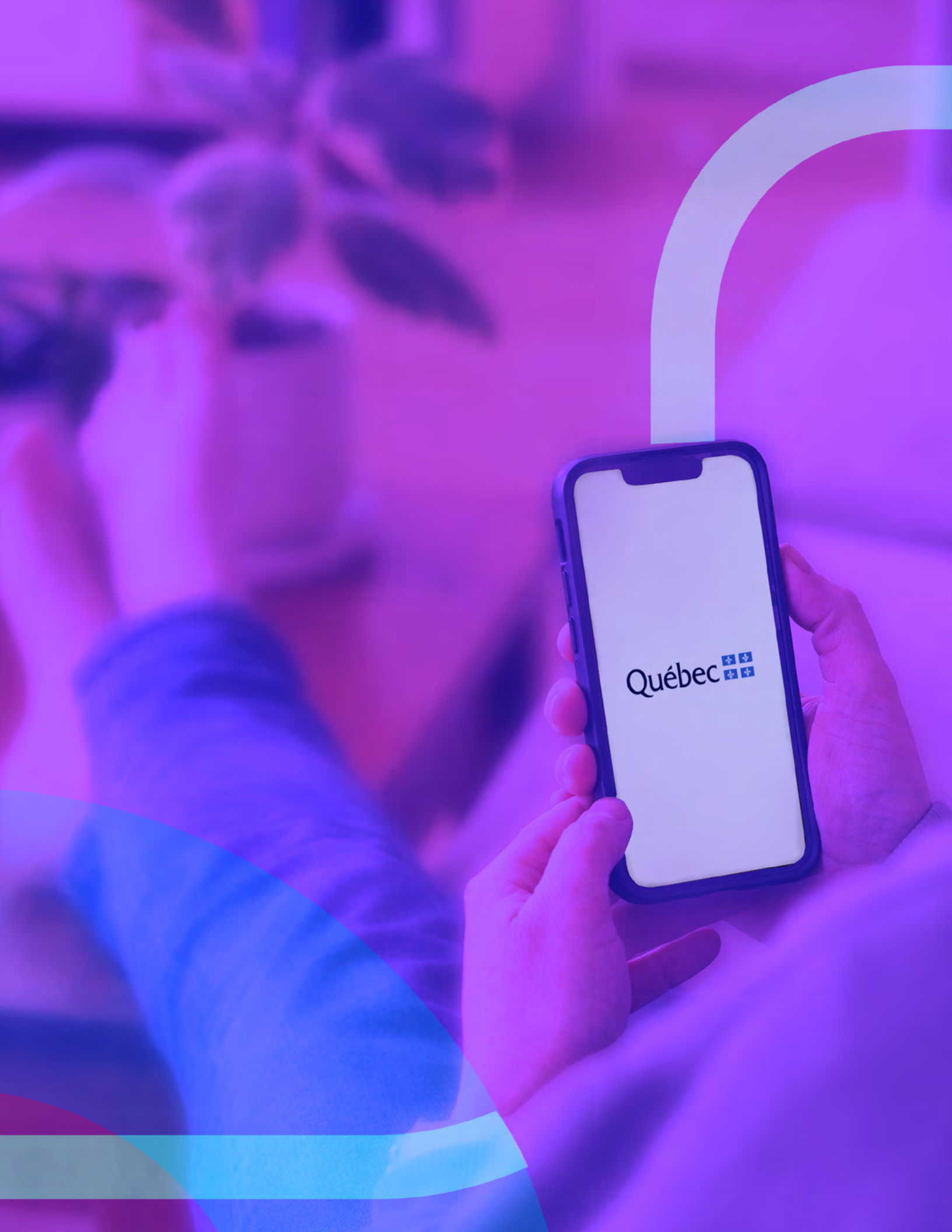
L'administration publique doit inspirer la confiance en démontrant sa capacité à réaliser une telle transformation de façon exemplaire et sécuritaire.

Le succès de la réalisation de cette transformation repose notamment sur le maintien d'une posture forte en cybersécurité permettant à l'administration publique de paver la voie à des services publics durables, résilients et résolument tournés vers l'avenir pour les générations futures.

3 AU COEUR DE LA PERFORMANCE DE L'ÉTAT : L'ÉCOSYSTÈME NUMÉRIQUE QUÉBÉCOIS

Le Québec bénéficie d'un écosystème numérique riche et diversifié, composé de nombreuses entreprises spécialisées, d'instituts de recherche, d'organismes à but non lucratif et de spécialistes œuvrant dans l'industrie de la cybersécurité et du numérique.

L'administration publique ne peut pas réaliser sa transformation par le numérique et croître en maturité en matière de cybersécurité en faisant cavalier seul. Elle doit s'appuyer sur l'expérience, l'expertise de pointe et la forte capacité d'innovation des partenaires de l'écosystème numérique québécois, qui peuvent grandement contribuer à l'atteinte de ses objectifs.


Québec

UNE NOUVELLE STRATÉGIE POUR UNE ADMINISTRATION PUBLIQUE CYBERSÉCURITAIRE ET NUMÉRIQUE

L'évolution des conditions du monde numérique, et plus largement, de la société, amène l'administration publique à proposer des services adaptés. À ce chapitre, pensons notamment aux éléments suivants qui façonnent invariablement l'offre numérique de l'administration publique :

- L'accélération sans précédent des développements technologiques, notamment ceux résultants de l'utilisation de l'intelligence artificielle ;
- Le nombre croissant des cyberattaques dans le monde et au Québec, menaçant les citoyennes et les citoyens, les entreprises et les administrations publiques ;
- Le recours accru à l'infonuagique, qui a un impact important sur les organisations quant au développement et à la gestion de leurs services numériques ;
- La rareté de main–d'œuvre, incluant celle spécialisée en ressources informationnelles, qui menace la capacité de maintien et d'évolution des services publics ;
- La croissance rapide de l'utilisation du numérique et de l'appétit pour les services numériques au sein de la population, de même que le télétravail ;
- Le caractère de plus en plus crucial que représentent les données pour les organisations : la protection et la valorisation de ces dernières s'imposant maintenant comme un levier essentiel de compétitivité.

Ainsi, il devient indispensable pour le gouvernement du Québec d'adapter sa stratégie en matière de cybersécurité et du numérique, afin qu'elle soit en adéquation avec cet environnement en perpétuelle évolution.

La *Stratégie gouvernementale de cybersécurité et du numérique 2024–2028* (ci–après « *Stratégie 2024–2028* ») vise à propulser l'administration publique vers une vision commune renouvelée de l'action de l'État. Elle a aussi pour objectif d'inspirer la confiance des citoyennes et des citoyens dans la capacité de l'administration publique québécoise à réaliser des projets porteurs de transformation par le numérique qui contribueront significativement à améliorer la qualité des services et à simplifier leur vie quotidienne.

La *Stratégie 2024–2028* s'inspire des meilleures pratiques adoptées par d'autres administrations publiques à travers le monde dans le domaine. Elle prend aussi appui sur l'ensemble des apprentissages réalisés par l'administration publique québécoise au fil des projets de transformation numérique qu'elle a mis en œuvre jusqu'à présent.

PORTÉE ET STRUCTURE DE LA *STRATÉGIE 2024–2028*

La *Stratégie 2024–2028* 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*, ce qui représente plus de 300 organismes publics, dont ceux des réseaux de la santé et des services sociaux, de l'éducation et de l'enseignement supérieur.

Elle est un document de vision à portée globale, qui pourra être complété par des stratégies et des plans d'actions spécifiques à des domaines d'affaires précis. À ce titre, la *Politique gouvernementale de cybersécurité*, en vigueur depuis 2020, et la *Stratégie d'intégration de l'intelligence artificielle dans l'administration publique 2021–2026* y seront maintenant associées.

La *Stratégie 2024–2028* s'articule en trois axes, lesquels regroupent dix objectifs. Pour chacun de ces objectifs, des priorités stratégiques sont indiquées pour guider les prochaines actions de l'administration publique, et des cibles à portée gouvernementale sont fixées afin de mesurer la progression générale de la mise en œuvre de cette dernière dans les domaines de la cybersécurité et du numérique. Certaines priorités stratégiques ne font pas l'objet de cibles, mais toutes constituent des éléments à respecter pour une action cohérente de l'administration publique.

MISE EN ŒUVRE ET SUIVI

La mise en œuvre de la *Stratégie 2024–2028* et l'atteinte des cibles gouvernementales reposent sur le leadership qui sera exercé par le ministère de la Cybersécurité et du Numérique ainsi que sur l'action structurée et concertée des organismes publics. L'implication de l'ensemble du personnel de l'administration publique, ce qui comprend les employés, les gestionnaires et les hauts dirigeants, sera un facteur de succès.

COORDINATION À L'ÉCHELLE GOUVERNEMENTALE

Un suivi régulier de l'avancement de la *Stratégie 2024–2028* sera effectué par le Comité de gouvernance en ressources informationnelles, présidé par le dirigeant principal de l'information et composé des dirigeants de l'information désignés en vertu de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*.

CONTRIBUTION DES ORGANISMES PUBLICS

Depuis 2021, la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* prévoit que les organismes publics ont l'obligation d'établir un plan de transformation numérique qui se veut un vecteur d'innovation pour l'amélioration des services gouvernementaux.

Lors de leur révision annuelle, les plans de transformation numérique des organismes publics devront être alignés avec la *Stratégie 2024–2028* et préciser comment l'organisme prévoit contribuer à l'atteinte des cibles gouvernementales qui les concernent. Les plans de transformation numérique permettront ainsi de structurer l'action des organismes publics en vue de concrétiser la vision gouvernementale en matière de cybersécurité et du numérique.

SUIVI ET REDDITION DE COMPTES

Mis en ligne en 2020, le Baromètre numériQc (ci–après « le Baromètre ») est un outil simple et visuel qui permet de partager publiquement les avancées de la transformation numérique de l'administration publique.

Dans la première année de mise en œuvre de la présente Stratégie, le Baromètre évoluera pour incorporer les nouvelles cibles gouvernementales en matière de cybersécurité et du numérique.

Les résultats relatifs à l'atteinte des cibles seront publiés annuellement sur le Baromètre.

TABLEAU SYNOPTIQUE

AXE I

Accroître la cybersécurité de l'administration publique

OBJECTIF 1

Renforcer la sécurité de l'information des services publics

Priorité stratégique

1.1 Accroître les capacités gouvernementales de surveillance des menaces, vulnérabilités et incidents relatifs à la cybersécurité

1.2 Renforcer la posture de sécurité de l'information gouvernementale

1.3 Mutualiser les initiatives et les expertises au sein du Réseau gouvernemental de cyberdéfense

OBJECTIF 2

Protéger les données des citoyennes et des citoyens, des entreprises et de l'administration publique

Priorité stratégique

2.1 Classifier et sécuriser les données numériques gouvernementales

2.2 Développer les compétences et l'expertise en cybersécurité au sein de l'administration publique

AXE II

Accélérer la transformation numérique de l'administration publique

OBJECTIF 3

Instaurer une offre unifiée de services numériques gouvernementaux

Priorité stratégique

3.1 Adopter une vision gouvernementale unifiée

3.2 Atténuer la fracture numérique et favoriser la littératie numérique

3.3 Déployer la prestation de service numérique gouvernementale autour d'une plateforme commune

3.4 Offrir une identité numérique aux citoyennes et aux citoyens

3.5 Soutenir l'adoption du Service d'authentification gouvernementale par les organismes publics

OBJECTIF 4

Accroître la mobilité et la valorisation des données numériques gouvernementales

Priorité stratégique

4.1 Instaurer une culture des données au sein de l'administration publique

4.2 Déployer des sources officielles de données numériques gouvernementales

4.3 Faire des données ouvertes un levier pour une administration publique plus transparente et performante

OBJECTIF 5

Accroître la performance de l'administration publique grâce à l'intelligence artificielle responsable

Priorité stratégique

5.1 Assurer une gouvernance et une utilisation éthique de l'intelligence artificielle dans l'administration publique

5.2 Favoriser l'émergence de projets en intelligence artificielle

5.3 Automatiser les processus d'affaires gouvernementaux

OBJECTIF 6

Maximiser les retombées des projets en ressources informationnelles et en assurer le succès

Priorité stratégique

6.1 Prioriser les projets à l'échelle gouvernementale

6.2 Prioriser les investissements en ressources informationnelles en fonction des bénéfices financiers et de la valeur publique générés

6.3 Développer et maintenir l'expertise de l'administration publique dans les domaines liés aux ressources informationnelles

OBJECTIF 7

Favoriser la mutualisation et la mise en œuvre de fondations numériques gouvernementales

Priorité stratégique

7.1 Établir et assurer la gouvernance de la mutualisation, notamment des fondations numériques

7.2 Mutualiser l'expertise et les connaissances entre les organismes publics

AXE III

Développer des infrastructures technologiques pérennes et sécuritaires

OBJECTIF 8

Consolider les actifs technologiques

Priorité stratégique

8.1 Consolider l'offre infonuagique gouvernementale

8.2 Consolider les centres de traitement informatique

OBJECTIF 9

Résorber la désuétude des actifs informationnels de l'administration publique

Priorité stratégique

9.1 Assurer une gestion responsable de la désuétude des actifs informationnels de l'administration publique

OBJECTIF 10

Soutenir le déploiement des infrastructures de télécommunication

Priorité stratégique

10.1 Développer et pérenniser le Réseau gouvernemental de télécommunication

AXE I

AXE I

ACCROÎTRE LA CYBERSÉCURITÉ DE L'ADMINISTRATION PUBLIQUE

La transformation numérique de l'administration publique nécessite que la gestion des risques en sécurité de l'information soit prise en compte dès qu'elle est planifiée afin d'éviter la perturbation ou l'arrêt des services essentiels à la population, ou encore le vol de données. Ces défis mettent en lumière la nécessité d'assurer la protection des données des citoyennes et des citoyens ainsi que celles des organisations à l'égard des cybermenaces ainsi que la résilience des services publics et des infrastructures critiques. Ainsi, la cybersécurité s'impose comme un pilier essentiel de l'évolution de la société à l'ère du numérique.

Dans ce contexte, il incombe à l'État de jouer un rôle de leader en veillant à ce que sa propre transformation numérique soit réalisée dans un environnement cybersécuritaire. L'exemplarité de l'administration publique en cette matière revêt une importance particulière, car elle constitue un facteur clé pour développer et maintenir la confiance des citoyennes et des citoyens à l'égard de sa capacité à prévenir les incidents de sécurité, à assurer la résilience de ses services offerts à la population et à conduire une transformation numérique réussie. L'État entend ainsi renforcer la sécurité des services publics notamment en augmentant sa capacité à cibler les menaces, les vulnérabilités et à prévenir les incidents de cybersécurité.

Pour ce faire, l'administration publique se donne les deux objectifs suivants :

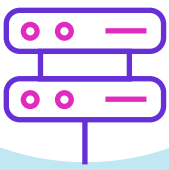
OBJECTIFS DE L'AXE I

OBJECTIF 1

Renforcer la sécurité de l'information des services publics

OBJECTIF 2

Protéger les données des citoyennes et des citoyens, des entreprises et de l'administration publique



OBJECTIF 1

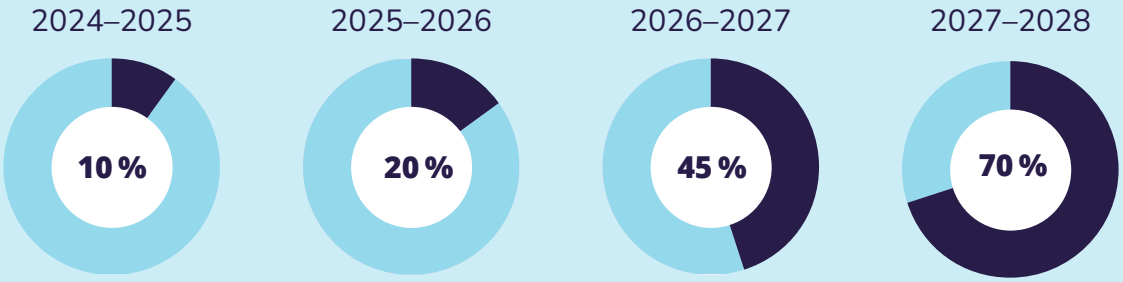
RENFORCER LA SÉCURITÉ DE L'INFORMATION DES SERVICES PUBLICS

L'administration publique a une importante responsabilité envers la sécurité et la résilience des services publics. Elle doit notamment assurer la confidentialité, l'intégrité et la disponibilité de l'information générée par les services qu'elle offre à la population.

Pour bien protéger l'information, la posture de sécurité des organismes publics doit évoluer et s'adapter continuellement aux nouvelles technologies ainsi qu'aux nouvelles techniques d'attaques des acteurs malveillants. L'administration publique mise sur la force du Réseau gouvernemental de cyberdéfense (Réseau) pour mettre en place les mesures de cybersécurité et pour mutualiser les services ainsi que les expertises nécessaires au renforcement de la sécurité des services publics.

En complément, afin de détecter et de contrer les cyberattaques tentant de contourner les mécanismes de protection, une détection et une surveillance accrue seront déployées. En se dotant d'une vue d'ensemble des tentatives d'atteintes à la sécurité de l'information, l'administration publique pourra réagir plus rapidement et réduire les préjudices.

CIBLES



Indicateur Pourcentage de centres opérationnels de cyberdéfense intégrés dans le service de détection et de surveillance des événements de sécurité offerts par le Centre gouvernemental de cyberdéfense

Sous le leadership du Centre gouvernemental de cyberdéfense, le Réseau est constitué de 26 centres opérationnels de cyberdéfense soutenant 306 organismes publics. Il a pour mission de renforcer les dispositifs de prévention et de réaction à l'égard des cybermenaces afin de contrer les risques de cybersécurité auxquels l'administration publique est confrontée quotidiennement.

1.1 ACCROÎTRE LES CAPACITÉS GOUVERNEMENTALES DE SURVEILLANCE DES MENACES, VULNÉRABILITÉS ET INCIDENTS RELATIFS À LA CYBERSÉCURITÉ

La transformation numérique de l'État représente une opportunité pour l'administration publique d'améliorer la performance et la convivialité des services offerts aux citoyennes et aux citoyens. Une augmentation du nombre de services numériques implique toutefois des opportunités additionnelles d'exploitation par des acteurs malveillants. Qu'ils aient pour objectif le vol ou la corruption de données, l'extorsion ou l'atteinte à la disponibilité d'un service, les acteurs malveillants ciblent l'administration publique en raison de l'importance de ses services à la population, de son accès aux données citoyennes et de sa visibilité médiatique. L'identification actuelle des menaces et des vulnérabilités ainsi que la surveillance des événements de sécurité sont des éléments essentiels à la protection des services publics. Une meilleure surveillance permet de détecter rapidement les tentatives d'attaques et les incidents de sécurité pour en informer les organismes publics concernés. Une intervention immédiate élimine ou minimise les préjudices afférents.

La bonification des capacités gouvernementales est essentielle afin de découvrir davantage et plus rapidement les brèches de données et tout autre type d'incident pour diminuer les préjudices pouvant y être associés. L'automatisation des pratiques et l'utilisation de technologies émergentes, telles que l'intelligence artificielle et ses capacités d'analyse prédictive, seront considérées pour décupler la capacité d'analyse gouvernementale et améliorer la performance des processus. Ainsi, le temps de détection et de réaction aux cybermenaces et aux cyberattaques pourra être réduit.

1.2 RENFORCER LA POSTURE DE SÉCURITÉ DE L'INFORMATION GOUVERNEMENTALE

Assurer la cybersécurité et la résilience des services publics contre des cybermenaces et des cyberattaques en constante mouvance requiert une posture de sécurité évolutive.

D'une part, l'adoption d'un référentiel gouvernemental permettant de déterminer les mesures de sécurité devant être mises en place par les organismes publics est essentielle à l'amélioration de la maturité gouvernementale en matière de cybersécurité.

D'autre part, l'encadrement stratégique, tactique et opérationnel de l'action gouvernementale quant aux mesures devant être mises en place est requis pour assurer des niveaux de sécurité cohérents et adéquats au sein des organismes publics de l'administration publique.

Par ailleurs, la standardisation des pratiques gouvernementales, par l'adoption et le maintien à jour de processus gouvernementaux normalisés, ainsi que la centralisation de services clés contribuent également au renforcement de la posture de sécurité en permettant une action gouvernementale rapide et concertée.

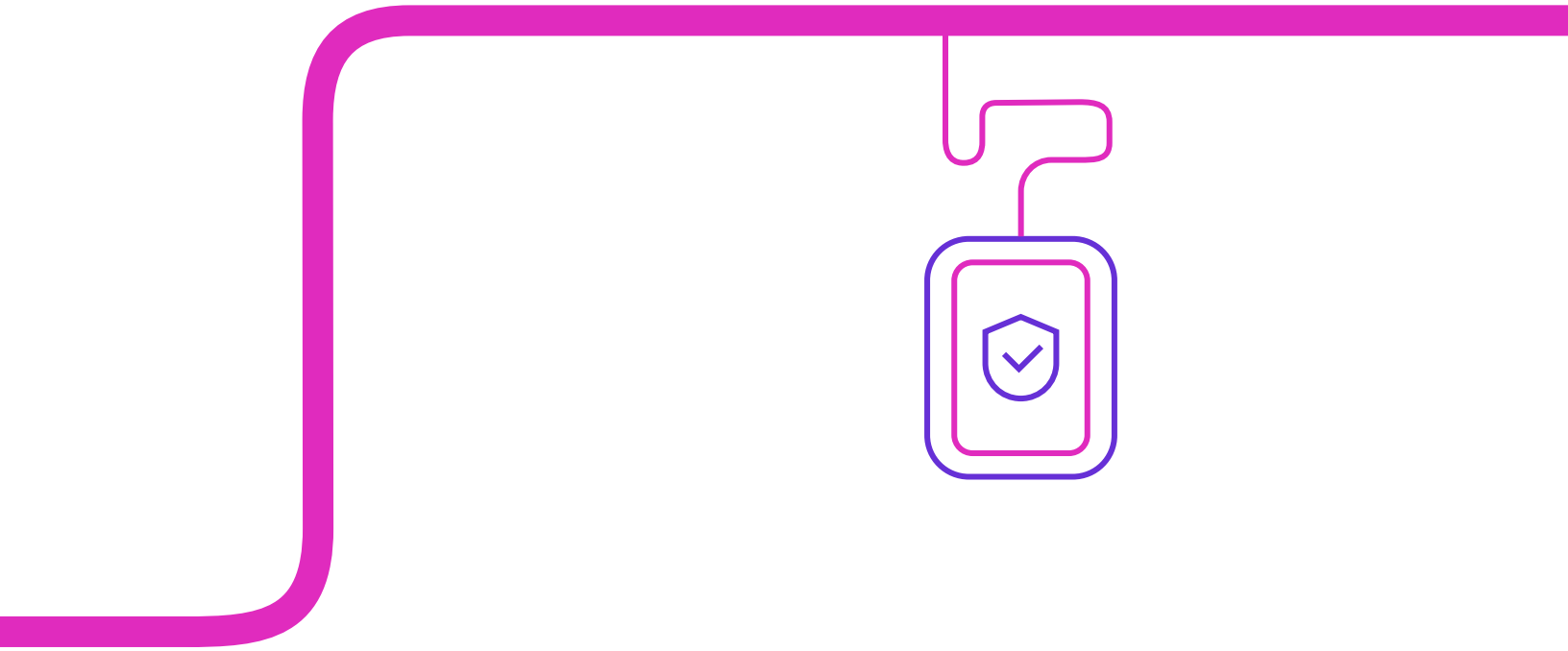
Finalement, la poursuite du développement d'une offre de services à l'intention des organismes publics, centralisée au MCN, est également indispensable pour répondre aux besoins opérationnels du Réseau gouvernemental de cyberdéfense. Pour ce faire, le Centre gouvernemental de cyberdéfense élargira la portée des services actuels, mettra en place une équipe d'intervention spécialisée en réponse aux incidents et offrira de nouveaux outils et services, tel que le service de protection lors de la navigation Web.

En somme, la mise en place de ces processus et mesures de contrôle contribuera à l'établissement des fondations nécessaires à l'atteinte de cette posture en sécurité de l'information.

1.3 MUTUALISER LES INITIATIVES ET LES EXPERTISES AU SEIN DU RÉSEAU GOUVERNEMENTAL DE CYBERDÉFENSE

L'encadrement opérationnel de la sécurité de l'information et la centralisation des services de cybersécurité requérant peu de connaissances sectorielles sont réalisés au Centre gouvernemental de cyberdéfense. Les centres opérationnels de cyberdéfense, quant à eux, soutiennent les organismes publics dans l'application des exigences, dans la prise en charge des menaces, vulnérabilités et incidents détectés par les services centralisés.

Ils complètent également l'offre du Réseau en concentrant leurs efforts sur les actions nécessitant une connaissance des particularités et des technologies propres aux organismes publics qui leur sont rattachés afin de mutualiser les pratiques et les services adaptés à leur secteur d'activité.



OBJECTIF 2

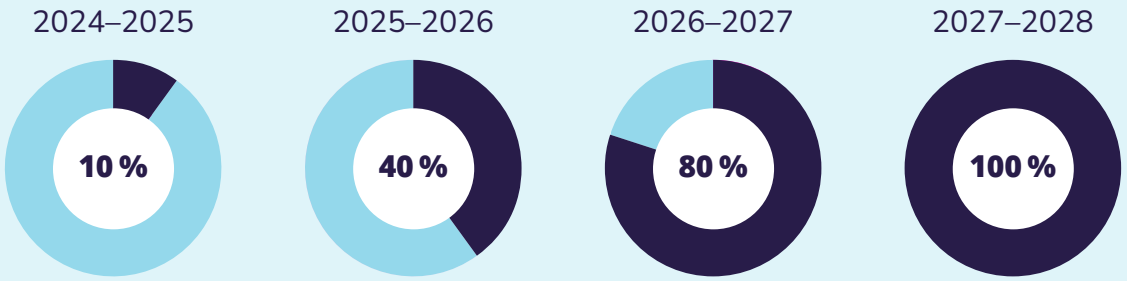
PROTÉGER LES DONNÉES DES CITOYENNES ET DES CITOYENS, DES ENTREPRISES ET DE L'ADMINISTRATION PUBLIQUE

L'administration publique détient et traite une masse critique de renseignements personnels et confidentiels. La confiance du public envers l'État est importante à préserver et dépend, entre autres, de sa capacité à protéger de tels renseignements d'une utilisation malveillante des données telle que l'usurpation d'identité.

Le contexte de mobilité et de valorisation des données numériques gouvernementales rehausse l'importance de la sécurité de l'information. Au sein de l'administration publique, cela passe notamment par une classification de sécurité des données uniforme et applicable à l'ensemble des organismes publics.

Par ailleurs, il importe que l'ensemble du personnel de l'administration publique dispose des connaissances, des compétences et des réflexes appropriés en matière de cybersécurité pour être en mesure d'utiliser les outils numériques et de réaliser son travail quotidien sans compromettre la sécurité des données détenues par l'administration publique.

CIBLES



Indicateur Pourcentage des organismes publics ayant commencé l'application du marquage des données non structurées prévu au modèle de classification de sécurité des données numériques gouvernementales

2.1 CLASSIFIER ET SÉCURISER LES DONNÉES NUMÉRIQUES GOUVERNEMENTALES

La classification de sécurité est à la base de la sécurisation des données numériques gouvernementales et donc, des renseignements personnels et confidentiels des citoyennes et des citoyens, des entreprises et de l'État. Les organismes publics ont la responsabilité de classifier les données qu'ils détiennent selon leur sensibilité et de leur accorder un niveau de sécurité propre à leur contexte organisationnel. Dans une optique de cohérence gouvernementale, un nouveau modèle de classification de sécurité sera déployé dans les organismes publics. Celui–ci prendra appui sur les meilleures pratiques de classification des données numériques et tiendra compte de leur nature, de leurs caractéristiques, de leur utilisation, de même que des règles qui les régissent.

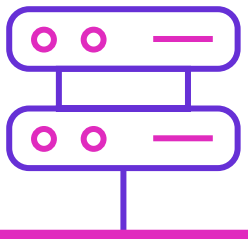
Le modèle permettra aux organismes publics de réduire les risques d'une atteinte à la confidentialité, à l'intégrité ou à la disponibilité des données. Il assurera également une classification plus cohérente entre les organismes publics et facilitera une interopérabilité avec d'autres acteurs de l'écosystème de la sécurité de l'information.

2.2 DÉVELOPPER LES COMPÉTENCES ET L'EXPERTISE EN CYBERSÉCURITÉ AU SEIN DE L'ADMINISTRATION PUBLIQUE

La première ligne de défense contre les cyberattaques repose sur l'humain. Le personnel de l'État doit donc être informé des bonnes pratiques à intégrer au quotidien, ainsi que des tendances et menaces émergentes en matière de cybersécurité. Ces connaissances et le développement des compétences de l'ensemble du personnel de l'administration publique sont nécessaires pour adopter les bons réflexes et réduire les cyberrisques. Chaque décision ou action d'une personne doit être effectuée en pleine conscience des éventuelles répercussions sur la sécurité de l'information.

À cet effet, il est essentiel de promouvoir une culture de la cybersécurité à l'échelle gouvernementale. Cela contribuera à minimiser les erreurs humaines en favorisant un apprentissage continu adapté aux nouvelles menaces, fournissant ainsi au personnel de l'État les compétences nécessaires pour se protéger efficacement contre les attaques et assurer la sécurité des données, des systèmes et des infrastructures numériques.

Il faut également mentionner que les rôles et responsabilités des intervenants du Réseau gouvernemental de cyberdéfense et des autres contributeurs à la sécurité de l'information, œuvrant dans la prévention, la détection et la réaction en cette matière, revêtent une importance capitale. Leur expertise doit être maintenue à jour en continu. Ils doivent pouvoir s'adapter à un environnement en perpétuel changement. Ainsi, une offre de formations spécialisées en cybersécurité et de formations pratiques dans un environnement simulé doit être disponible.



AXE II

AXE II

ACCÉLÉRER LA TRANSFORMATION NUMÉRIQUE DE L'ADMINISTRATION PUBLIQUE

Afin de poursuivre la démarche entamée par la *Stratégie 2019–2023*, l'administration publique entend accélérer sa transformation numérique, ce qui lui permettra d'améliorer l'efficacité et la performance des services qu'elle dispense et donc, par le fait même, de mieux répondre aux besoins des Québécoises et des Québécois tout en améliorant leur expérience client.

UNE COMPRÉHENSION COMMUNE DE LA TRANSFORMATION NUMÉRIQUE ET CE QU'ELLE IMPLIQUE POUR LES ORGANISMES PUBLICS

La transformation numérique est « une démarche visant le changement en profondeur d'une organisation par l'intégration de technologies numériques à l'ensemble de ses processus administratifs, de ses communications et de ses activités, par la refonte de son modèle d'entreprise et par l'adaptation de sa culture organisationnelle aux nouvelles réalités du numérique[8] ».

La transformation numérique constitue ainsi un changement culturel, organisationnel et opérationnel, intégrant des compétences numériques, des processus numériques et des technologies numériques et s'opérant à tous les niveaux et à toutes les fonctions de l'organisation de manière continue. Ce changement permet à un organisme public de mieux répondre aux besoins évolutifs de sa clientèle, d'améliorer l'expérience client et l'expérience employé, en plus de rehausser la transparence, la performance et son efficacité.

8. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE. *Vitrine linguistique*, [En ligne], [https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26558201/transformation-numerique], (Consulté en février 2024).

La transformation numérique d'un organisme public passe par la réalisation de nombreuses initiatives qui vont bien au–delà des ressources informationnelles. En effet, une telle transformation implique d'abord et avant tout les secteurs d'affaires de l'organisme. Ce sont eux qui doivent la piloter puisqu'elle peut viser la transformation des processus d'affaires, la restructuration organisationnelle, la formation et le développement des compétences, ainsi qu'un profond changement de culture organisationnelle. Les secteurs responsables des ressources informationnelles, quant à eux, ont la responsabilité de soutenir cette transformation, notamment en fournissant une expertise ainsi que des systèmes et des solutions répondant aux besoins.

Par ailleurs, il importe qu'une réelle culture numérique soit promue et intégrée à tous les niveaux des organismes publics. Une telle culture se caractérise avant tout par l'innovation, mais aussi par une approche centrée sur la personne, les décisions appuyées par les données probantes et la collaboration de l'ensemble des parties prenantes. Cela comprend le travail en réseau, une plus grande tolérance au risque ainsi que l'ouverture, l'agilité et la flexibilité.

Transformation numérique durable et éthique

Bien que les technologies de l'information puissent apporter de grands bénéfices en matière de protection de l'environnement et du climat, les conséquences environnementales négatives de ces dernières soulèvent de plus en plus de préoccupations auprès des spécialistes et de la société civile. Alors que l'usage et le cycle de vie complet des appareils électroniques génèrent une quantité importante de gaz à effet de serre et de déchets, la consommation d'énergie imputable aux technologies de l'information ne cesse d'augmenter[9].

En cohérence avec ses objectifs de développement durable, il importe que l'administration publique considère ces enjeux stratégiques et contribue à l'effort collectif afin de réduire l'empreinte environnementale du numérique dans ses actions. À ce chapitre, les organismes publics auront un rôle important à jouer pour mettre la transformation numérique au service de la transition écologique et énergétique. Au niveau gouvernemental, le développement éthique et durable sera au cœur de la gouvernance des ressources informationnelles, notamment en accordant une importance particulière à la mutualisation et à la réutilisation des infrastructures technologiques existantes ou en développement. Les initiatives de déploiement de nouveaux services numériques devront également tenir compte de la fracture numérique afin de déployer des services accessibles à l'ensemble de la population.

9. HYDRO–QUÉBEC. *Diminuer la pollution numérique, c'est possible*, [En ligne], [https://www.hydroquebec.com/a/decarboner.html] (consulté en février 2024).

Pour parvenir à accélérer cette transformation, l'administration publique se donne cinq objectifs :

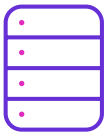
OBJECTIFS DE L'AXE II

OBJECTIF 3

Instaurer une offre unifiée de services numériques gouvernementaux

OBJECTIF 4

Accroître la mobilité et la valorisation des données numériques gouvernementales



OBJECTIF 5

Accroître la performance de l'administration publique grâce à l'intelligence artificielle responsable

OBJECTIF 6

Maximiser les retombées des projets en ressources informationnelles et en assurer le succès

OBJECTIF 7

Favoriser la mutualisation et la mutualisation et la mise en œuvre de fondations numériques gouvernementales

OBJECTIF 3

INSTAURER UNE OFFRE UNIFIÉE DE SERVICES NUMÉRIQUES GOUVERNEMENTAUX

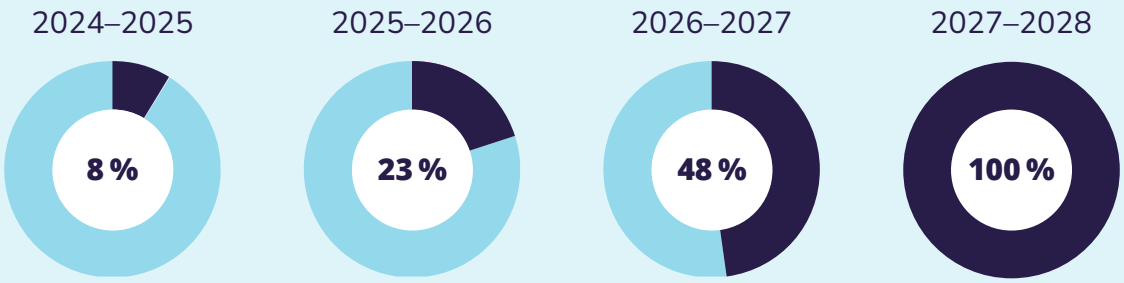
L'omniprésence du numérique dans la société contribue à hausser significativement les attentes des citoyennes et des citoyens envers l'accès à des services en ligne. Influencés par les expériences vécues avec le secteur privé dont la qualité et la convivialité des services numériques ne cessent de s'améliorer, ceux–ci s'attendent désormais à ce que l'administration publique s'adapte à ces nouveaux standards. Ils s'attendent à des expériences plus simples, rapides, personnalisées et requérant moins d'interactions pour réaliser des démarches liées aux événements de vie auprès de l'État. Les services publics doivent donc s'adapter pour répondre à ces nouvelles attentes. En ce sens, l'administration publique entend se positionner à l'avant–garde des meilleures pratiques mondiales en matière de services numériques. Elle doit également veiller à l'accessibilité et l'inclusivité assurant que les services sont disponibles pour tous, indépendamment des capacités physiques ou cognitives ou de leur maîtrise de la technologie.

Parallèlement, la transparence et la responsabilité sont des éléments clés pour établir la confiance des citoyennes et des citoyens dans les services numériques gouvernementaux. Ceux–ci doivent être informés de la manière dont leurs données sont collectées, utilisées et protégées, ainsi que des décisions prises par le gouvernement. La transparence renforce la confiance des citoyennes et des citoyens dans leurs institutions publiques et favorise une relation de collaboration.

En complément à la nécessité d'une expérience citoyenne centrée sur l'utilisateur, une offre unifiée et personnalisée de services numériques est essentielle pour répondre de manière holistique aux besoins de la population. Plutôt que de disperser les services à travers de multiples plateformes et applications, une approche unifiée offre une expérience cohérente et transparente, simplifiant ainsi l'accès aux différents services gouvernementaux.

L'administration publique peut également tirer parti des technologies émergentes telles que l'intelligence artificielle et l'analyse des données. Cela permet de mieux anticiper les besoins des citoyennes et des citoyens et d'offrir des solutions proactives qui améliorent leur expérience globale avec les services numériques gouvernementaux.

CIBLES



Indicateur Pourcentage des prestations électroniques de services (PES) des organismes publics, s'adressant aux citoyennes et aux citoyens, arrimées au Service d'authentification gouvernementale

3.1 ADOPTER UNE VISION GOUVERNEMENTALE UNIFIÉE

À l'heure actuelle, chaque organisme public développe sa propre vision de son offre de services en fonction de sa mission. Un même citoyen doit donc comprendre et s'adapter au mode de prestation de chacun de ces organismes publics.

La vision gouvernementale unifiée vise à présenter une approche fédératrice de l'administration publique face aux citoyennes et aux citoyens. Elle permettra à chaque organisme public de déployer ses services en faisant en sorte que le citoyen perçoive les services reçus comme provenant d'une seule et même entité gouvernementale.

3.2 ATTÉNUER LA FRACTURE NUMÉRIQUE ET FAVORISER LA LITTÉRATIE NUMÉRIQUE

La fracture numérique réfère aux inégalités d'accès aux technologies, notamment par manque de ressource ou de compétence. Concept influençant la fracture numérique, la littératie numérique fait référence, quant à elle, à la capacité d'une personne à utiliser et comprendre les technologies ou à communiquer avec celles–ci.

La fracture numérique, entre autres causée par le manque de littératie numérique, peut entraîner des conséquences négatives pour les communautés et les individus touchés, en particulier pour ceux qui ont des besoins spécifiques tels que les personnes âgées, les personnes en situation de pauvreté, les personnes vivant dans des zones rurales ou isolées, les personnes ayant des handicaps, les minorités ethniques ou linguistiques, etc. Ces personnes peuvent se retrouver exclues de la société numérique et des opportunités qu'elle offre, comme l'accès à l'emploi, à l'éducation ou à des services en ligne.

Le ministre de la Cybersécurité et du Numérique a la responsabilité de favoriser l'accès aux services publics pour l'ensemble des citoyennes et des citoyens afin qu'ils puissent bénéficier des avantages de leur utilisation dans un mode numérique.

En ce sens, les organismes publics doivent fournir des services numériques de qualité à toute la population, sans égard à l'origine, au genre, à l'âge, à la situation géographique ou à toutes autres conditions socio–économiques. Ils doivent aussi favoriser le développement en compétences numériques de la population et répondre aux besoins spécifiques des citoyennes et des citoyens en situation de fracture numérique, tout en conservant la possibilité d'accéder aux prestations de services par les canaux traditionnels.

Les organismes publics devront porter une attention particulière à cet enjeu dans le développement de tous nouveaux services numériques. Par ailleurs, à l'initiative du ministère de la Cybersécurité et du Numérique, une réflexion, menée à l'échelle gouvernementale, est en cours dans le but de dégager les meilleures pistes d'actions pour atténuer les effets de la fracture numérique.

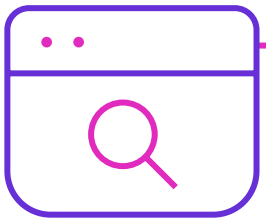
3.3 DÉPLOYER LA PRESTATION DE SERVICE NUMÉRIQUE GOUVERNEMENTALE AUTOUR D'UNE PLATEFORME COMMUNE

Un gouvernement numérique doit offrir un point de contact commun permettant aux citoyennes et aux citoyens de transiger directement avec une seule entité unifiée, garantissant une expérience sans interruption en utilisant le mode de communication de leur choix pour y accéder (appareil mobile, ordinateur, point de service physique, etc.) et en obtenant l'accompagnement dont ils ont besoin.

En ce sens, la prestation de service gouvernementale unifiée sera construite autour d'une plateforme commune arrimée à Québec.ca et intégrant l'ensemble des services numériques offerts par les organismes publics. Ultimement, il sera notamment possible pour la citoyenne et le citoyen :

- de visualiser à un seul et même endroit l'ensemble de ses informations personnelles en lien avec les services gouvernementaux ;
- de s'authentifier avec un seul compte gouvernemental afin d'accéder aux services numériques des différents organismes publics ;
- de visualiser facilement l'état de ses demandes de prestations de services ;
- de recevoir des correspondances sécurisées concernant ses différentes interactions avec les organismes publics (correspondances écrites officielles, notifications, rappels, alertes, etc.) ;
- de rétroagir sur les services reçus.

Pour y parvenir, l'administration publique, appuyée par le leadership du ministère de la Cybersécurité et du Numérique, devra concevoir et mettre en œuvre une architecture de services unifiée entre les organismes publics et travailler à assurer davantage d'interopérabilité entre leurs systèmes de mission respectifs.



3.4 OFFRIR UNE IDENTITÉ NUMÉRIQUE AUX CITOYENNES ET AUX CITOYENS

Lorsqu'une personne cherche à s'identifier pour obtenir un service, que ce soit auprès du gouvernement ou d'une entreprise, elle doit présenter un document avec photo comme la carte d'assurance maladie ou le permis de conduire. Cette action implique le partage d'une quantité importante de renseignements personnels qui ne sont pas nécessaires à la prestation du service souhaité. L'exposition fréquente de ces renseignements à de multiples intervenants contribue à augmenter les risques liés à l'usurpation d'identité.

Pour réduire significativement ces risques et pour améliorer l'expérience citoyenne au quotidien, l'État québécois créera un portefeuille numérique qui permettra à son détenteur d'avoir à portée de main ses renseignements personnels et certaines attestations dans un environnement numérique sécuritaire lui permettant d'en contrôler l'accès.

Cela impliquera :

- un accès simple et sécuritaire aux services gouvernementaux en mettant à la disposition des citoyennes et des citoyens une application mobile qui leur permettra de faire la preuve de leur identité ;
- la simplification des formalités d'identification pour les citoyennes et les citoyens dans l'exercice de leurs droits civils et une plus grande sécurité des transactions ;
- une meilleure gestion des renseignements personnels et l'utilisation de technologies hautement sécuritaires afin de réduire les risques de vols de renseignements personnels et d'usurpation d'identité ;
- un niveau de confiance accru des citoyennes et des citoyens au moment d'effectuer différents types d'échanges et de transactions.

3.5 SOUTENIR L'ADOPTION DU SERVICE D'AUTHENTIFICATION GOUVERNEMENTALE PAR LES ORGANISMES PUBLICS

Le Service d'authentification gouvernementale est une solution innovante qui offre aux citoyennes et aux citoyens[10] l'accès aux services gouvernementaux grâce à un moyen unique et simple de se connecter aux plateformes d'échanges sécurisées du gouvernement. Ce faisant, le Service d'authentification gouvernementale contribue à réduire les risques liés à la protection des renseignements personnels et à l'usurpation d'identité.

Le déploiement du Service d'authentification gouvernementale a commencé en décembre 2022 et se poursuivra afin de s'étendre à l'ensemble des entités et services de l'administration publique. À terme, l'adoption du Service d'authentification gouvernementale par l'ensemble des organismes publics pour les services numériques nécessitant une authentification améliorera grandement l'expérience des citoyennes et des citoyens dans leurs interactions avec l'administration publique.

10. À terme, il est envisagé que les entreprises québécoises soient également incluses.

OBJECTIF 4

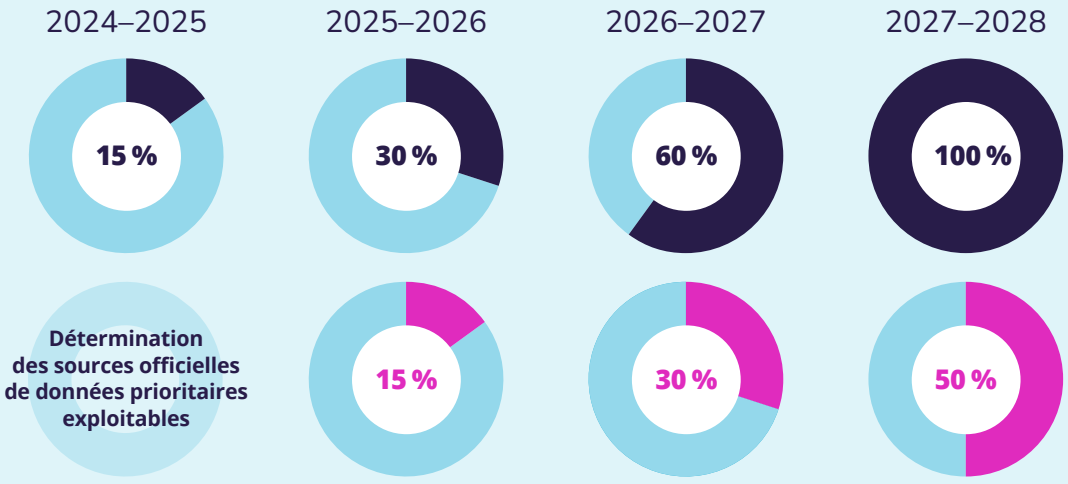
ACCROÎTRE LA MOBILITÉ ET LA VALORISATION DES DONNÉES NUMÉRIQUES GOUVERNEMENTALES

L'administration publique détient une quantité importante de données qui présentent un potentiel d'utilisation à ce jour inestimé. Utilisées de manière éthique et responsable, elles offrent une opportunité pour améliorer la prestation de services à la population. En mettant en valeur ces données et en rendant disponibles de façon simple et sécuritaire des sources de données de qualité, le gouvernement peut créer des solutions innovantes pour répondre aux besoins de la population.

Sécuritaires et destinées à améliorer la communication de données entre organismes publics, les plateformes numériques sont conçues pour conserver les informations des citoyennes et des citoyens. Autrement dit, ces derniers n'auront pas besoin de fournir ces mêmes informations à plusieurs reprises, car elles sont déjà en possession de l'administration publique.

Pour mettre davantage ces données en valeur, le gouvernement doit cependant adopter une approche collaborative et axée sur les données. En démocratisant l'accès et les usages aux données gouvernementales et en encourageant l'innovation dans la prestation de services, l'État peut contribuer à renforcer la confiance du public, à stimuler la croissance économique et à améliorer la qualité de vie des citoyennes et des citoyens.

CIBLES



Indicateurs

- Pourcentage d'organismes publics ayant commencé la démarche de cartographie et d'inventaire des données numériques gouvernementales
- Pourcentage de sources officielles de données identifiées et exploitables

4.1 INSTAURER UNE CULTURE DES DONNÉES AU SEIN DE L'ADMINISTRATION PUBLIQUE

Pour assurer que tous les organismes publics disposent des capacités requises afin de mettre pleinement en valeur les données qu'ils détiennent, l'administration publique doit développer une vision cohérente et unifiée des données numériques.

Cette vision des données numériques contribuera à accroître la valeur des données au service de la mission, de l'efficacité des services et de l'intérêt public, dans une optique de « gouvernement unifié ». Les orientations qui en découleront permettront aux organismes publics d'accélérer et de faciliter leur transformation numérique en améliorant et en développant de nouveaux services à partir des données.

Pour y parvenir, un cadre normatif et des pratiques seront établis afin que les organismes publics prennent en compte l'aspect primordial d'une utilisation éclairée, éthique et pertinente des données tout en favorisant la promotion de la mobilité des données entre organismes publics. Il importera également de faciliter l'accès aux données à l'échelle gouvernementale.

En ce sens, une gestion efficace et cohérente des données numériques en découlera et permettra l'adoption de normes et de règles claires pour assurer que les données sont sécurisées, fiables, complètes et à jour. De plus, l'amélioration de la qualité des données constituera une condition essentielle pour exploiter pleinement le potentiel de cet actif collectif afin de faciliter le déploiement de services proactifs et de processus automatisés, notamment grâce à l'intelligence artificielle.

4.2 DÉPLOYER DES SOURCES OFFICIELLES DE DONNÉES NUMÉRIQUES GOUVERNEMENTALES

Dans leurs interactions avec l'État, les citoyennes et les citoyens sont souvent confrontés à devoir fournir les mêmes informations ou documents à plusieurs reprises. Ainsi, la mise en place des sources officielles de données s'inscrit dans une perspective globale de renforcer les capacités du gouvernement à fournir aux citoyennes et aux citoyens des services intégrés de manière efficace et efficiente.

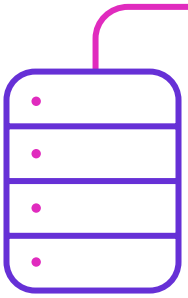
Dans cette optique, le gouvernement accorde une priorité particulière à la mutualisation, au partage et à la réutilisation des données afin d'éviter que les citoyennes et les citoyens aient à soumettre la même information plusieurs fois. L'identification et la désignation des données de référence provenant de sources reconnues garantissent l'unicité et l'exactitude de l'information, simplifiant ainsi sa gestion et renforçant sa protection. À cet égard, il est impératif de normaliser et de structurer rigoureusement les données pour favoriser l'interopérabilité entre les systèmes, constituant ainsi un levier essentiel dans une approche d'un gouvernement centré sur les citoyennes et les citoyens.

4.3 FAIRE DES DONNÉES OUVERTES UN LEVIER POUR UNE ADMINISTRATION PUBLIQUE PLUS TRANSPARENTE ET PERFORMANTE

À l'ère du numérique, le gouvernement ouvert est une approche qui place la transparence, l'innovation, la collaboration et la participation citoyenne au cœur de l'action publique. En faisant preuve d'ouverture et en plaçant les citoyennes et les citoyens comme partie prenante dans ses décisions, le gouvernement est à même de développer des programmes et des services plus adéquats et plus efficaces pour servir la population.

Le gouvernement du Québec est membre du Partenariat pour un gouvernement ouvert, une démarche internationale regroupant plus de 104 partenaires gouvernementaux et 75 gouvernements nationaux[11].

À l'échelle locale, l'administration publique contribue à un écosystème riche et dynamique composé de nombreux partenaires de la société civile[12]. Maintenant, elle est prête à faire un pas supplémentaire afin de se doter d'orientations gouvernementales en la matière dans le but de guider les organismes publics dans leur participation au gouvernement ouvert, mais aussi pour favoriser l'accès à de l'information fiable pour les citoyennes et les citoyens. Plus particulièrement, ces orientations veilleront à accroître la quantité de données ouvertes mises à la disposition de la population par les organismes publics.



11. *OPEN GOVERNMENT PARTNERSHIP*. [En ligne], [https://www.opengovpartnership.org/fr/about/] (consulté en février 2024).

12. Plus de 100 organisations publient des données ouvertes sur le site Web donneesquebec.ca.

OBJECTIF 5

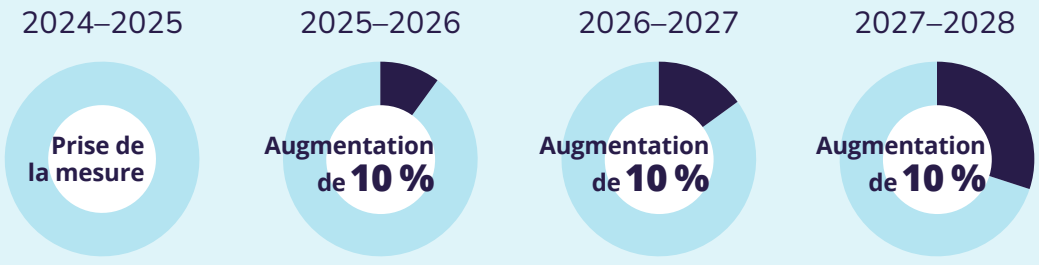
ACCROÎTRE LA PERFORMANCE DE L'ADMINISTRATION PUBLIQUE GRÂCE À L'INTELLIGENCE ARTIFICIELLE RESPONSABLE

Le domaine de l'intelligence artificielle (IA) a fait l'objet de développements significatifs au cours des dernières années, façonnant l'ensemble des secteurs d'activités et s'imposant désormais comme un sujet incontournable.

À ce chapitre, les outils basés sur l'IA générative, qui étaient généralement inconnus du grand public avant la fin de l'année 2022, se sont imposés rapidement dans les diverses facettes de notre société durant les derniers mois, venant bouleverser les habitudes et ouvrant la porte à de nombreuses possibilités. Le contexte réglementaire mondial entourant l'IA a lui aussi évolué récemment pour répondre aux préoccupations croissantes en matière de sécurité, d'éthique et de confidentialité.

La montée en puissance de l'IA générative démontre l'importance pour le Québec d'avoir lancé la *Stratégie d'intégration de l'intelligence artificielle dans l'administration publique 2021–2026*. Toutefois, l'évolution rapide de l'IA et les nouveaux défis qui en résultent poussent l'administration publique québécoise à s'adapter rapidement. La mise en œuvre de cette stratégie repose sur des mesures clés établissant les actions concrètes à mettre de l'avant. Ces mesures clés continueront d'être bonifiées afin de refléter le contexte stratégique lié à l'IA, d'assurer une action cohérente responsable et de soutenir les projets transformateurs de services publics par l'usage de l'IA.

CIBLES



Indicateur Augmentation du nombre d'initiatives en intelligence artificielle dans l'administration publique

5.1 ASSURER UNE GOUVERNANCE ET UNE UTILISATION ÉTHIQUE DE L'INTELLIGENCE ARTIFICIELLE DANS L'ADMINISTRATION PUBLIQUE

Plus qu'une simple technologie numérique, l'IA nécessite une approche concertée afin d'en retirer les bienfaits tout en limitant les biais et les dérives potentielles. Au sein de l'administration publique québécoise, cela se traduira par des processus de gouvernance et d'imputabilité et répondant aux différents enjeux qu'implique l'intégration responsable de l'IA. Ainsi, l'éthique de l'IA et son opérationnalisation demeureront un axe central pour tout projet en IA dans les organismes publics.

Bien que l'usage de l'IA demeure un vecteur puissant pour répondre à des enjeux de performance ou de capacité, il ne pourra se faire au détriment des droits des citoyennes et des citoyens. L'État veillera à maintenir un cadre réglementaire adapté aux bouleversements induits par l'IA. À l'instar d'autres administrations à l'international, le Québec s'assurera de collaborer avec ses partenaires nationaux et internationaux pour fournir une réponse adéquate aux défis engendrés par cette technologie adaptée au secteur public.

5.2 FAVORISER L'ÉMERGENCE DE PROJETS EN INTELLIGENCE ARTIFICIELLE

L'IA présente un potentiel important pour accroître la performance et l'excellence opérationnelle de l'administration publique ainsi que la qualité, l'efficience et l'équité des services publics offerts aux citoyennes et aux citoyens. L'IA peut, entre autres, être utilisée pour optimiser les processus et soutenir la prise de décision.

Le succès des projets d'IA requiert toutefois des conditions particulières, dont une expertise de pointe, l'accès aux données et des infrastructures technologiques adéquates et sécurisées. Ces projets doivent également faire l'objet d'un arrimage gouvernemental afin de cibler les cas les plus prometteurs, promouvoir l'adoption des meilleures pratiques et miser sur le potentiel de mutualisation des expertises et des technologies.

Pour ce faire, le soutien des projets à toutes les étapes de la chaîne de valeur (de la conception de systèmes d'IA jusqu'à leur mise en production) permettra d'assurer leur alignement avec les objectifs gouvernementaux en matière de transformation numérique et d'accélérer la mise en production de systèmes robustes et éthiques.

5.3 AUTOMATISER LES PROCESSUS D'AFFAIRES GOUVERNEMENTAUX

Face aux importants défis de main–d'œuvre et dans le contexte où l'administration publique doit optimiser la gestion de ses ressources, l'automatisation des processus s'avère essentielle pour continuer à répondre aux attentes de la population en matière de prestation de services. Dans ce contexte, l'utilisation de l'IA offre une opportunité sans précédent.

En automatisant les tâches répétitives, l'administration publique peut libérer le personnel de l'État pour se concentrer sur des tâches plus stimulantes et à plus forte valeur ajoutée. En ce sens, les organismes publics devront accorder une importance particulière à l'automatisation des processus, notamment à l'aide de l'intelligence artificielle, dans le cadre de l'élaboration de leur plan de transformation numérique.

OBJECTIF 6

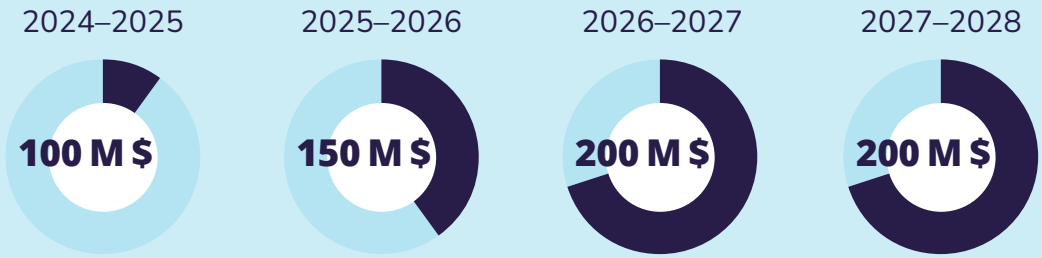
MAXIMISER LES RETOMBÉES DES PROJETS EN RESSOURCES INFORMATIONNELLES ET EN ASSURER LE SUCCÈS

L'État québécois consacre plus de cinq milliards de dollars par année aux projets et aux activités en ressources informationnelles menés par les organismes publics. En février 2024, 2 120 projets en ressources informationnelles étaient considérés comme actifs au sein de l'administration publique.

Le contexte de rareté des ressources fait en sorte que ces initiatives ne peuvent pas toutes être réalisées dans les délais souhaités, ce qui peut ralentir la transformation numérique de l'État.

L'administration publique doit disposer des conditions gagnantes qui lui permettront de livrer des projets technologiques selon les délais impartis et en fonction des ressources prévues. Cet impératif de livraison doit s'accomplir par une révision des processus entourant la priorisation des projets et des investissements en ressources informationnelles.

CIBLES



Indicateur Somme des bénéfices quantifiables et récurrents identifiés dans les plans de matérialisation des bénéfices des projets qualifiés des organismes publics ainsi que des économies récurrentes générées dans le cadre de l'offre de service du ministère de la Cybersécurité et du Numérique

6.1 PRIORISER LES PROJETS À L'ÉCHELLE GOUVERNEMENTALE

Puisque le démarrage de nouvelles initiatives en ressources informationnelles est décentralisé dans chacun des organismes publics, les besoins auxquels elles répondent sont souvent davantage sectoriels ou ministériels que liés aux priorités gouvernementales.

Ainsi, dans le but d'éviter la dispersion des efforts et des ressources des organismes publics dans un trop grand nombre d'initiatives, un portefeuille de projets prioritaires en ressources informationnelles sera élaboré afin d'établir les priorités gouvernementales au regard des initiatives en transformation numérique et s'assurer que les actions comportant le plus de bénéfices pour les citoyennes et les citoyens et les entreprises seront priorisées.

6.2 PRIORISER LES INVESTISSEMENTS EN RESSOURCES INFORMATIONNELLES EN FONCTION DES BÉNÉFICES FINANCIERS ET DE LA VALEUR PUBLIQUE GÉNÉRÉS

Les sommes importantes et le nombre de ressources humaines consacrées aux projets en ressources informationnelles rendent nécessaires de suivre et de mesurer les bénéfices générés par ceux–ci. Il importe que chaque dollar investi profite aux citoyennes et aux citoyens, que ce soit grâce aux gains en efficacité pour l'administration publique ou par l'amélioration directe des services reçus. À terme, une meilleure gestion des bénéfices dans les projets en ressources informationnelles permettra de générer davantage de valeur pour l'ensemble du Québec.

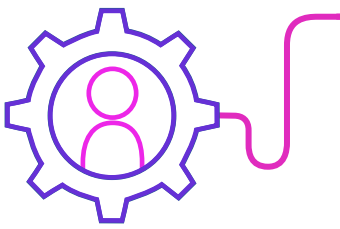
C'est pour cette raison que la poursuite de la mise en application du Cadre gouvernemental de gestion des bénéfices des projets en ressources informationnelles[13] par les organismes publics est centrale à la réalisation de la *Stratégie 2024–2028*. Les projets des organismes publics devront être priorisés en fonction des bénéfices financiers estimés et de la valeur publique escomptée.

6.3 DÉVELOPPER ET MAINTENIR L'EXPERTISE DE L'ADMINISTRATION PUBLIQUE DANS LES DOMAINES LIÉS AUX RESSOURCES INFORMATIONNELLES

La vitesse d'évolution des technologies de l'information exige de l'administration publique qu'elle reste à l'affût de la progression constante des compétences et des expertises qui lui permettront de se positionner à l'avant–garde des opportunités offertes par le numérique et des impératifs de la cybersécurité. Les nombreux projets à la base des ambitions gouvernementales en matière du numérique et de la cybersécurité ne pourront être réalisés que si l'administration publique dispose de la main–d'œuvre et de l'expertise nécessaires. Par ailleurs, l'administration publique doit s'assurer de développer son expertise interne dans les domaines critiques du numérique, notamment en matière de cybersécurité et d'IA.

En réponse à ces nombreux défis et en cohérence avec la *Stratégie de gestion des ressources humaines de la fonction publique 2023–2028*, l'administration publique devra innover en matière d'expérience employé, notamment pour les domaines du numérique et de la cybersécurité. C'est en faisant preuve de créativité, d'audace et de flexibilité que l'État pourra se positionner comme un employeur de choix dans ces domaines. Ainsi, lorsqu'un expert du domaine des ressources informationnelles se cherchera un emploi, il devra sentir que son expérience, en tant qu'employé de l'administration publique, sera valorisante, enrichissante et qu'elle lui permettra de répondre à ses besoins de développement personnel et professionnel.

Au–delà du recrutement, les organismes publics doivent faire en sorte de développer et de maintenir l'expertise détenue par leur personnel en ressources informationnelles en leur offrant les moyens et le temps de se former de façon continue.



13. Arrêté numéro 2022–01 du ministre de la Cybersécurité et du Numérique en date du 27 mai 2022.

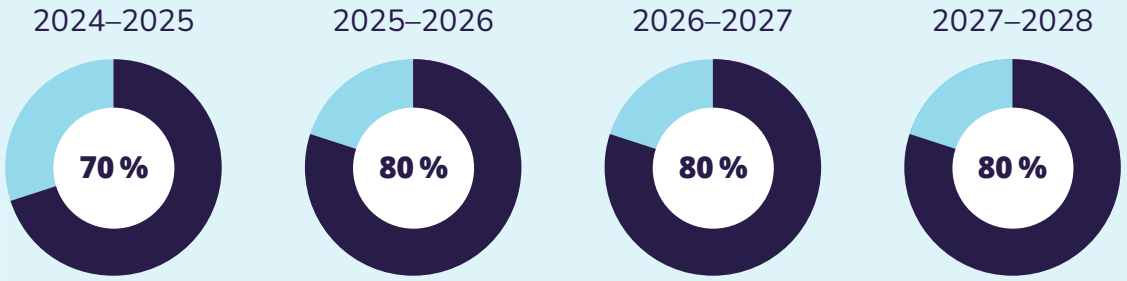
OBJECTIF 7

FAVORISER LA MUTUALISATION ET LA MISE EN ŒUVRE DE FONDATIONS NUMÉRIQUES GOUVERNEMENTALES

La mutualisation fait partie des objectifs du cadre de gouvernance et de gestion des ressources informationnelles placés sous la responsabilité du dirigeant principal de l'information. Dans un contexte marqué par la rareté de main–d'œuvre et les capacités limitées dans plusieurs organismes publics, la mutualisation des services, des infrastructures, de l'expertise et des ressources s'avère indispensable pour appuyer la cadence de la transformation numérique gouvernementale tout en favorisant une synergie accrue entre les différentes entités.

Dans ce contexte, les initiatives de mutualisation telles que la mise en œuvre de fondations numériques gouvernementales ainsi que diverses autres initiatives tireront directement profit de cette démarche collaborative. En consolidant ses efforts et en partageant efficacement les ressources, l'administration publique québécoise renforcera sa capacité à relever les défis liés à la transformation numérique et, par le fait même, son autonomie numérique.

CIBLES



Indicateur Pourcentage des nouveaux projets qualifiés en ressources informationnelles ayant fait l'objet d'une analyse sur la possibilité de mutualiser ou de réutiliser des solutions existantes entre les organismes publics au cours de la phase de planification

7.1 ÉTABLIR ET ASSURER LA GOUVERNANCE DE LA MUTUALISATION, NOTAMMENT DES FONDATIONS NUMÉRIQUES

Pour générer les bénéfices escomptés, la mutualisation entre les organismes publics doit faire l'objet d'orientations claires, ainsi que d'une gouvernance établissant les rôles et responsabilités des acteurs impliqués.

La mise en place d'une telle gouvernance permettra notamment d'outiller et de guider les organismes publics en vue de l'adoption de ces nouvelles pratiques.

La mutualisation est une approche stratégique visant à favoriser la mise en commun de ressources, d'expertises, de services, d'infrastructures ou d'activités en maximisant les avantages de la collaboration et de la coopération des organismes publics comme la réutilisation des infrastructures technologiques existantes ou en développement.

Les fondations numériques gouvernementales constituent une forme de mutualisation dont l'administration publique doit tirer profit. Elles permettent d'accélérer la transformation numérique de l'État et de mettre en commun des services d'intérêt gouvernemental au bénéfice des citoyennes et des citoyens, des entreprises et du personnel de l'État. De plus, ces fondations permettent d'assurer une uniformité dans la prestation de services numériques offerte par les organismes publics en fournissant des services cohérents.

L'établissement d'un cadre cohérent des fondations numériques gouvernementales permettra le développement de ces dernières de façon concertée et en mettant les organismes publics à contribution.

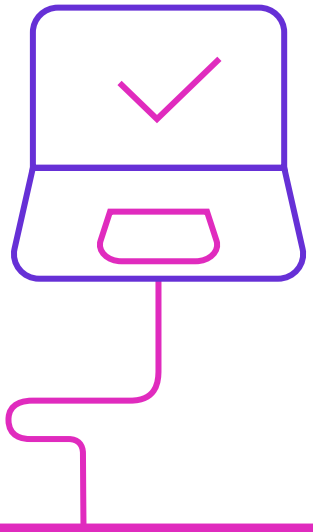
Les fondations numériques gouvernementales sont des plateformes ou des composants communs pouvant être utilisés et intégrés à même les prestations de services de l'ensemble des organismes publics. Concrètement, il s'agit d'initiatives numériques à haut potentiel de réutilisation entre les organismes publics, qui seront mises en place pour éviter les dédoublements dans les actifs informationnels au sein de l'administration publique. À titre d'exemple, on peut citer :

- un service commun de rétroaction permettant aux organismes publics d'interagir de façons plus uniforme et coordonnée auprès des citoyennes et des citoyens ;
- une plateforme commune de développement d'applications permettant aux différents organismes publics de bénéficier et de récupérer des développements ou encore des parties de code déjà développées par d'autres organismes ;
- une modernisation de la plateforme bureautique gouvernementale permettant une collaboration dynamique entre différents partenaires et favorisant la mutualisation des expertises et des connaissances.

7.2 MUTUALISER L'EXPERTISE ET LES CONNAISSANCES ENTRE LES ORGANISMES PUBLICS

L'administration publique est composée de ressources compétentes, mais en nombre insuffisant. Il s'agit là d'un frein à la transformation numérique de l'État.

La mutualisation de l'expertise et des connaissances est essentielle pour que le gouvernement puisse atteindre ses objectifs et mieux répondre aux besoins des citoyennes, des citoyens et des entreprises. La mise en commun de l'expertise et des connaissances doit se réaliser de façon concertée pour ne pas nuire à la continuité des services tout en permettant une transformation numérique réussie.



AXE III

AXE III

DÉVELOPPER DES INFRASTRUCTURES TECHNOLOGIQUES PÉRENNES ET SÉCURITAIRES

Les actifs informationnels et les infrastructures technologiques jouent un rôle essentiel dans le déploiement de la transformation numérique de l'État, mais également pour la cybersécurité. Ce sont eux qui rendent possible cette transformation.

Les actifs informationnels de l'administration publique sont les fondations qui permettent à ses programmes et services de fonctionner. Il importe de s'assurer que ceux–ci continuent de répondre aux besoins et qu'ils évoluent de manière à ne pas poser de risque pour la sécurité de l'information ou à la continuité des services.

Les infrastructures technologiques, quant à elles, assurent notamment la connectivité nécessaire au fonctionnement des technologies numériques, la sécurité et la mobilité des données, en plus de permettre le stockage sécuritaire des données. Elles constituent les fondations qui permettent de développer des services numériques qu'ils soient en lien avec la mission d'une organisation ou en soutien à celle–ci. Des infrastructures à jour permettent à l'État de se transformer et d'évoluer en tenant compte des exigences qui sont notamment tributaires des enjeux de sécurité.

Dans cette perspective, il importe que le ministère de la Cybersécurité et du Numérique s'assure du **développement et de l'évolution des infrastructures technologiques pour garantir la pérennité et la sécurité numérique de l'administration publique.**

Les infrastructures numériques : des actifs stratégiques vitaux pour le Québec

Les technologies issues de la transformation numérique permettront de relever plusieurs défis sociaux, économiques et environnementaux, notamment d'accroître le développement économique des régions, d'augmenter la productivité et l'innovation de tout le Québec, d'agir à titre de solution à la rareté de main–d'œuvre grâce à l'intelligence artificielle et à l'automatisation des processus, d'accélérer le développement d'une économie numérique verte, d'augmenter la compétitivité économique du Québec et de stimuler l'émergence de nouvelles entreprises québécoises.

La transformation numérique de l'État et de la société québécoise entraînera l'interconnexion numérique et technologique de milliards de personnes et d'objets. Il est donc impératif, pour le gouvernement du Québec et au bénéfice de l'ensemble de sa population, que ces interconnexions se fassent de façon sécuritaire. Les infrastructures numériques devront assurer une puissance de traitement ainsi qu'une capacité de stockage sécuritaire des données sans précédent, améliorant les modes de production et la productivité tout en permettant de réaliser des économies.

Développer des actifs favorisant l'autonomie numérique

La portabilité d'un actif informationnel désigne la capacité de déplacer cet actif d'une infrastructure informatique à une autre sans perte de fonctionnalité ou d'intégrité.

Afin de permettre la portabilité de ses actifs informationnels, le gouvernement veillera à instaurer des politiques et des normes, lesquelles viseront à assurer sa pleine et entière autonomie numérique par l'accroissement de l'utilisation des technologies libres et ouvertes.

Par exemple, grâce à la conteneurisation, un organisme public pourrait encapsuler ses logiciels dans un format ouvert et standardisé. Cette action simplifierait leur transfert et leur exécution entre le nuage externe, le nuage gouvernemental du Québec ou encore un centre de traitement informatique tout en garantissant la sécurité de l'actif et l'intégralité de ses fonctionnalités.

Rappelons, au passage, que le logiciel libre ne constitue pas une fin en soi, mais plutôt un moyen d'obtenir notamment le contrôle d'un système technologique et d'en faciliter le partage. Ce contrôle permet d'assurer une certaine indépendance à l'égard des manufacturiers de logiciels, de gérer sainement les cycles de vie, d'augmenter la pérennité des solutions, de simplifier la mutualisation et de consolider les investissements.

Pour ce faire, l'administration publique se donne les trois objectifs suivants :

OBJECTIFS DE L'AXE III

OBJECTIF 8

Consolider les actifs technologiques

OBJECTIF 9

Résorber la désuétude des actifs informationnels de l'administration publique

OBJECTIF 10

Soutenir le déploiement des infrastructures de télécommunication

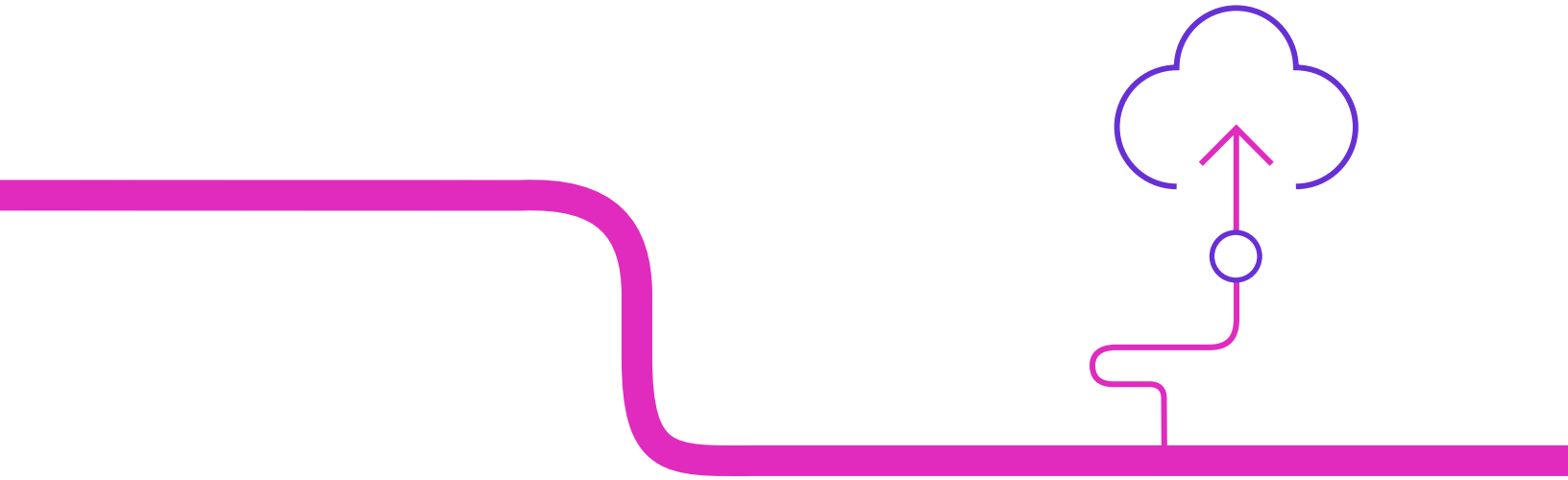
OBJECTIF 8

CONSOLIDER LES ACTIFS TECHNOLOGIQUES

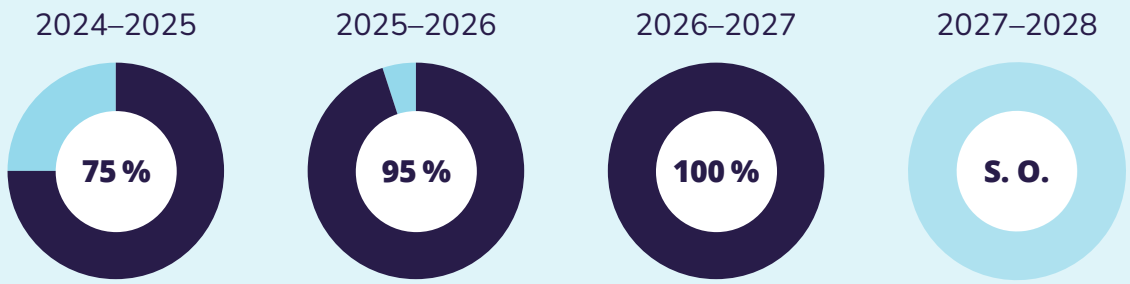
La migration des systèmes technologiques des ministères et organismes publics vers l'infonuagique constitue un levier important pour accroître la performance et l'agilité de l'État. Le gouvernement du Québec doit accélérer ce virage vers l'infonuagique tout en assurant la protection des données qu'il détient.

Il importe de distinguer trois types d'offres en infonuagique et en hébergement auxquelles l'administration publique a recours en fonction de ses besoins.

- **Nuage externe :**
  le nuage externe est une offre infonuagique qui permet la création et le déploiement des applications en bénéficiant des innovations et des infrastructures matérielles infonuagiques d'un fournisseur externe.
- **Nuage gouvernemental du Québec (NGQ) :**
  le NGQ est un service infonuagique offert par le MCN et basé sur le modèle IaaS (*Infrastructure as a Service*). Hébergé dans des environnements physiques sécurisés conçus pour les données importantes pour le service aux citoyennes et aux citoyens, il consiste en un service automatisé pouvant être consommé en mode libre–service par les ministères et organismes publics.
- **Centre de traitement informatique (CTI) :**
  un CTI est un lieu physique, situé au Québec, qui héberge des infrastructures technologiques, sous la responsabilité du MCN.



CIBLES



Indicateur Pourcentage d'organismes publics dont la stratégie respecte l'orientation gouvernementale de consolidation des centres de traitement informatique

8.1 CONSOLIDER L'OFFRE INFONUAGIQUE GOUVERNEMENTALE

Le Courtier en infonuagique est un outil qui permet aux organismes publics d'accélérer leurs acquisitions de solutions en infonuagique et des ressources professionnelles en qualifiant des offres de fournisseurs et en permettant à de tels organismes de conclure des contrats avec ces fournisseurs qui figurent dans un catalogue élaboré par le Courtier.

Cet outil sera bonifié afin de maximiser son utilisation et de rendre le catalogue plus facile d'utilisation par les organismes publics.

8.2 CONSOLIDER LES CENTRES DE TRAITEMENT INFORMATIQUE

L'administration publique détient une grande quantité d'informations, dont des renseignements personnels et des données confidentielles. Dans un souci d'optimisation des services de l'État, l'utilisation des moyens innovants pour favoriser la performance gouvernementale est essentielle. Ainsi, le Programme de consolidation des centres de traitement informatique et de l'optimisation du traitement et du stockage vise à réduire significativement le nombre de CTI.

Pour atteindre cet objectif, le Courtier en infonuagique a préalablement qualifié des offres infonuagiques externes qui permettront aux organismes publics d'y déplacer prioritairement les charges pertinentes. En complément, le MCN rend également disponible le NGQ pour l'information jugée sensible. L'utilisation du plein potentiel de l'infonuagique pour faire évoluer les pratiques des organisations permettra d'augmenter le degré de protection des actifs informationnels gouvernementaux.

OBJECTIF 9

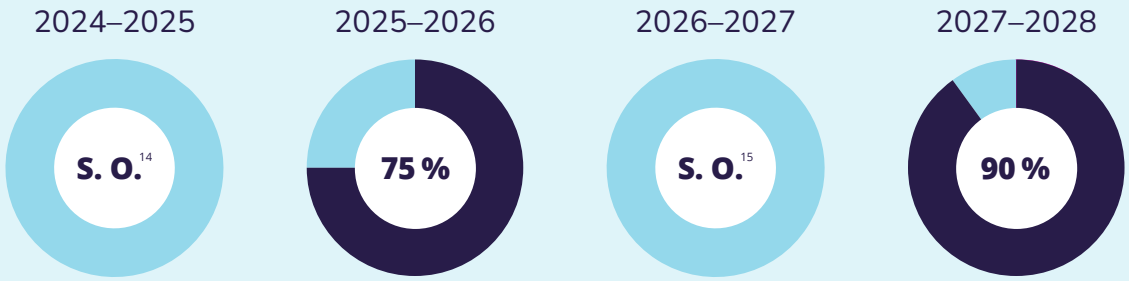
RÉSORBER LA DÉSUÉTUDE DES ACTIFS INFORMATIONNELS DE L'ADMINISTRATION PUBLIQUE

Le gouvernement du Québec dispose actuellement d'infrastructures technologiques et de solutions d'affaires numériques qui rendent difficile leur interopérabilité avec d'autres actifs informationnels. Cet état constitue un frein à l'amélioration des services offerts aux citoyennes, aux citoyens et à la transformation numérique.

La désuétude des systèmes peut également créer un risque relatif à la continuité des opérations. Par ailleurs, les technologies sont parfois rendues obsolètes en raison d'un manque d'expertise pour soutenir et faire évoluer les solutions.

Dans ces situations, il importe que les organismes publics déploient des mesures d'atténuation afin de se protéger de ces risques.

CIBLES



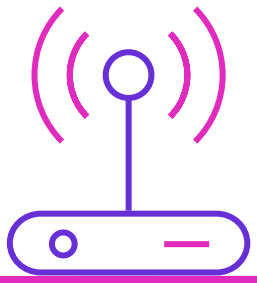
Indicateur Pourcentage des actifs informationnels en voie d'être désuets ou désuets faisant l'objet d'une stratégie d'intervention

14. Collecte tous les deux ans.

15. Collecte tous les deux ans.

9.1 ASSURER UNE GESTION RESPONSABLE DE LA DÉSUÉTUDE DES ACTIFS INFORMATIONNELS DE L'ADMINISTRATION PUBLIQUE

Le maintien, la modernisation et le développement des infrastructures technologiques de l'administration publique représentent une part importante des ressources consacrées aux technologies de l'information dans un contexte où l'on souhaite tirer profit du numérique pour gagner en efficacité. Les organismes publics doivent donc prendre des mesures concrètes de modernisation et de remplacement de leurs infrastructures désuètes ou obsolètes dans le cadre de leur transformation, soutenant ainsi le passage des services vers le numérique, mais également pour assurer la sécurité de ces actifs et des informations qu'ils détiennent.



OBJECTIF 10

SOUTENIR LE DÉPLOIEMENT DES INFRASTRUCTURES DE TÉLÉCOMMUNICATION

La connectivité joue désormais un rôle crucial dans la transformation numérique de l'État québécois ainsi que dans le développement économique et social de tout le Québec. Elle repose sur des réseaux de télécommunication performants, sécuritaires et résilients. La révolution numérique sera ainsi rendue possible par le développement accéléré de nouvelles technologies innovatrices et le rehaussement des infrastructures de télécommunication qui permettent d'en soutenir l'utilisation. Ces technologies transformeront les modes de production de l'économie québécoise.

Moteur du développement économique dont bénéficieront toutes les régions du Québec, la performance des infrastructures de télécommunication doit occuper un rôle central dans la *Stratégie 2024–2028*. À cet effet, les résultats de l'Opération haute vitesse sont probants : une augmentation totale annuelle estimée du produit intérieur brut québécois de 1,0 % et jusqu'à 3,8 %[16] pour certaines régions.

Afin que toute la population puisse profiter de services publics de qualité, soutenus par des technologies issues de la transformation numérique, et pour éviter la création d'un fossé numérique entre les différentes régions du Québec, l'État doit pouvoir compter sur des infrastructures de haut calibre soutenant la connectivité sur l'ensemble de son territoire. Considérant que la consommation de données et les besoins en connectivité augmentent exponentiellement d'année en année, les réseaux de télécommunication constituent ainsi des actifs névralgiques pour toute la société québécoise.

Étant donné la hausse des cyberattaques dont sont victimes les gouvernements et la population, l'importance de pouvoir miser sur des réseaux sécuritaires et résilients est plus que jamais démontrée.

16. KPMG. *Étude sur l'impact économique des mesures gouvernementales mises en place afin de déployer l'Internet haut débit au Québec*, [En ligne], 2022, [https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/MCE/IHV/etudes/Etude_impact_economique_IHV_2022.pdf] (Consulté en mai 2024).

La fibre optique au Québec

Le secteur d'avenir sur lequel l'économie du futur se déploiera est la fibre optique[17]. L'État québécois, incluant les réseaux de la santé et des services sociaux, de l'éducation et de l'enseignement supérieur, ainsi que les entreprises et les organismes privés comptent sur une connexion performante afin de mieux servir leur clientèle, d'accroître leur productivité et d'augmenter leur compétitivité internationale.

De plus, des enjeux importants de cybersécurité sont à considérer, car les données des citoyennes, des citoyens et des entreprises du Québec, ainsi que leurs communications, circulent sur ces réseaux. C'est pourquoi le ministère de la Cybersécurité et du Numérique s'assurera que les réseaux et les infrastructures de télécommunication, ainsi que les données qui y transitent, bénéficient de la plus haute protection contre les cyberattaques.

Actuellement, le ministère de la Cybersécurité et du Numérique est responsable d'offrir des services de télécommunication à la grande majorité des organismes publics ainsi qu'au réseau de la santé et des services sociaux, par l'intermédiaire de prestataires de services privés. Toutefois, un certain nombre d'entreprises du gouvernement ou d'organismes publics utilisent des réseaux distincts pour soutenir leurs activités. Le ministère de la Cybersécurité et du Numérique jouera donc un rôle actif pour optimiser l'utilisation de ces infrastructures, contribuer à la cohérence de leur déploiement et permettre la mise en place des mesures visant à assurer leur sécurité.

L'amélioration de la couverture cellulaire

Pour des raisons liées à la sécurité et à la vitalité économique des régions, l'amélioration de la qualité des services cellulaires sur tout le territoire est l'objet d'efforts soutenus de l'État québécois. Ainsi, des aides financières importantes sont accordées à des entreprises de télécommunication en vue de la construction de nouveaux sites cellulaires partout au Québec, dans des zones où la couverture est inexistante ou mauvaise. Ce soutien financier permet de rehausser la qualité des réseaux et des services qu'ils rendent à leur clientèle. Le déploiement de nouveaux sites cellulaires se fait en s'assurant que toute possibilité de mutualisation avec des équipements du Réseau national intégré de radiocommunication (RENIR) est prise en considération.

Par ailleurs, le ministère de la Cybersécurité et du Numérique poursuivra les travaux visant le transfert de la desserte policière vers le RENIR et la mise à niveau de celui-ci.

17. ANALYSYS MASON. *Full-Fibre access as strategic infrastructure : strenghtening public policy for Europe*, [En ligne], 2020, [https://www.analysysmason.com/contentassets/ae94d4d039a144529906c1a8ca58d1ea/analysys_mason_full_fibre_europe_rdfi0.pdf] (Consulté en mai 2024).

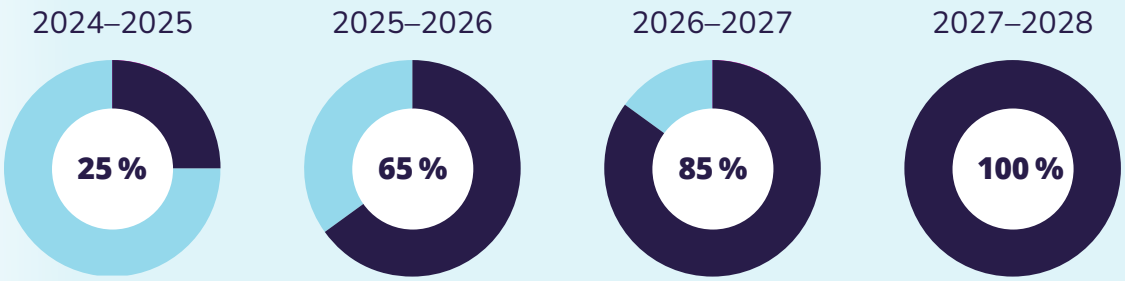
10.1 DÉVELOPPER ET PÉRENNISER LE RÉSEAU GOUVERNEMENTAL DE TÉLÉCOMMUNICATION

La nécessité d'offrir une nouvelle gamme de services répondant aux besoins évolutifs de l'administration publique et d'optimiser les dépenses gouvernementales de télécommunication a amené le gouvernement à réviser en profondeur les modèles d'affaires et technologiques. Ces travaux ont donné lieu à la création du programme de Réseau gouvernemental de télécommunication (RGT), dont les services remplaceront progressivement ceux du Réseau intégré de télécommunication multimédia (RITM) qui procure actuellement des services aux 34 établissements du réseau de la santé et des services sociaux et à près de 100 autres organismes publics.

Sous la responsabilité du ministère de la Cybersécurité et du Numérique, le RGT offrira une gamme de services de pointe afin de soutenir la mise en œuvre de projets structurants tels que le Programme de consolidation des centres de traitement informatique et de l'optimisation du traitement et du stockage et le virage infonuagique. Il a pour but l'élaboration de solutions d'affaires et technologiques soutenant la transmission de données de toute nature. Les services offerts permettront des transmissions sécurisées de données à haut débit tant filaires que sans fil. En introduisant des technologies permettant sa virtualisation, le RGT s'affranchit un peu plus des infrastructures des fournisseurs privés de services de télécommunication puisque le ministère de la Cybersécurité et du Numérique sera propriétaire de ces équipements.

Les organismes publics seront appelés à collaborer avec le ministère de la Cybersécurité et du Numérique dans la migration des services du RITM vers le RGT en fournissant les ressources locales requises.

CIBLES



Indicateur Pourcentage des services du Réseau intégré de télécommunication multimédia (RITM) ayant migré vers le Réseau gouvernemental de télécommunication (RGT)

CONCLUSION

Cette stratégie gouvernementale représente une opportunité réelle pour l'administration publique de tirer le meilleur du numérique, notamment pour augmenter sa performance, mais surtout améliorer son offre de service au bénéfice des citoyennes et des citoyens. Dans un contexte où la vie quotidienne se numérise de plus en plus, que ce soit par le télétravail, la télémédecine ou même la formation, les services publics doivent se transformer pour répondre aux attentes de la population. D'ici 2028, la mise en oeuvre de cette stratégie permettra de répondre à ces attentes, notamment en améliorant de façon significative l'expérience citoyenne à l'égard des services numériques offerts par l'administration publique.

Les orientations proposées représentent également des opportunités pour l'optimisation des services offerts par l'État. Par exemple, en intégrant de façon responsable, sécuritaire et innovante des processus d'automatisation et d'intelligence artificielle, les organismes publics seront en mesure de développer tout le potentiel d'optimisation et d'efficience dans leurs opérations.

Si des services de qualité engendrent la confiance, des services sécuritaires consolident cette dernière. Ainsi, la transformation numérique qui se poursuivra dans les prochaines années devra se faire sur des bases solides en matière de sécurité de l'information et de cybersécurité. Les services publics n'en seront que plus durables et résilients.

Finalement, même s'il existe maintenant un ministère de la Cybersécurité et du Numérique pour assurer le leadership de cette transformation, celle–ci doit être portée par l'ensemble des organismes publics. C'est en effet collectivement que l'administration publique doit assumer la responsabilité de se transformer, mais également de démontrer aux citoyennes et aux citoyens l'impact positif d'un État numérique. Ainsi, la collaboration entre les organismes publics est un élément clé du succès de cette transformation par le numérique qui se poursuit, toujours dans l'objectif de faire mieux pour les citoyennes et les citoyens du Québec.

Québec