PLAN STRATÉGIQUE
2023-2027

MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE

Votre gouvernement

Québec

PLAN STRATÉGIQUE
2023-2027

MINISTÈRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE

Cette publication a été réalisée par le Sous-ministériat adjoint à la gouvernance et au financement en collaboration avec la Direction des communications du ministère de la Cybersécurité et du Numérique.

Une version accessible de ce document est disponible en ligne.
Si vous éprouvez des difficultés techniques ou pour obtenir une version adaptée, veuillez communiquer avec la Direction des communications à l'adresse dcom@mcn.gouv.qc.ca.

Pour plus d'information :

Direction des communications
du ministère de la Cybersécurité et du Numérique
800, place D'Youville, 4e étage
Québec (Québec) G1R 3P4

Dépôt légal – Mai 2023
Bibliothèque et Archives nationales du Québec
ISBN 978-2-550-94498-0 (version imprimée)
ISBN 978-2-550-94499-7 (version électronique)

MESSAGE DU MINISTRE

Madame Nathalie Roy
Présidente de l'Assemblée nationale
Hôtel du Parlement
Québec

Madame la Présidente,

Je suis très fier de présenter le Plan stratégique 2023-2027 du ministère de la Cybersécurité et du Numérique.

Ce plan ambitieux, le premier depuis la création du Ministère, vient confirmer une fois de plus l'importance qu'accorde le gouvernement du Québec à l'amélioration des services qu'il offre à sa population, en utilisant au mieux le potentiel des technologies du numérique. Les Québécoises et les Québécois doivent pouvoir compter sur des services publics plus simples et plus accessibles, qui allient rapidité, convivialité et sécurité. Les entreprises qui font affaire au Québec méritent d'avoir accès à des services numériques qui leur permettent de consacrer moins de temps aux formalités administratives et plus de temps à créer de la richesse pour l'ensemble de notre société.

Les prochaines années seront très stimulantes pour quiconque s'intéresse à l'univers des technologies et à l'impact qu'elles auront sur la qualité de vie de notre population : automatisation, intelligence artificielle, objets connectés, technologies quantiques, autant de sujets qui pourraient faire du Québec un leader reconnu dans le monde.

L'État québécois n'échappe malheureusement pas à un contexte géopolitique plus tendu et à l'évolution inquiétante des cybermenaces et des cyberattaques partout dans le monde. C'est la raison pour laquelle la cybersécurité prend une importance particulière dans ce plan.

Le ministère de la Cybersécurité et du Numérique coordonne l'action de plus de 300 organismes publics en vue d'accélérer la transformation numérique de l'État et de rehausser la protection des actifs informationnels du gouvernement et de sa population. Le Plan stratégique reflète l'importance que nous accordons au personnel du Ministère, sans qui il ne serait pas possible de réaliser nos ambitions. Les prouesses du numérique sont le fruit du génie humain et l'humain doit en profiter.

Veuillez agréer, Madame la Présidente, l'expression de mes sentiments distingués.

Original signé

Éric Caire
Québec, mai 2023

MESSAGE DU SOUS-MINISTRE

Monsieur Éric Caire

Ministre de la Cybersécurité et du Numérique
900, place D'Youville, 9e étage
Québec (Québec) G1R 3P7

Monsieur le Ministre,

Le Plan stratégique 2023-2027 du ministère de la Cybersécurité et du Numérique résulte de la réflexion et des efforts de toute une équipe dédiée à l'amélioration des services à la population et à la performance de l'État. Le gouvernement du Québec consacre plus de 4 G$ annuellement à ses ressources informationnelles. Une gestion plus efficace de ces ressources fait partie de nos priorités, en s'assurant qu'elles génèrent le maximum de bénéfices pour la population. Le maintien de services publics de qualité constitue un défi, alors que le Québec subit une rareté de main-d'œuvre importante, susceptible de se prolonger encore plusieurs années. Les technologies du numérique, dans ce contexte, permettent à l'État de mieux servir sa population.

En ce qui concerne le risque grandissant que représentent les cybermenaces, le Ministère doit maintenir une étroite collaboration avec l'ensemble de l'écosystème, qu'il s'agisse des universités, des centres de recherche, des autres gouvernements ou de l'entreprise privée, et ce, afin de demeurer à l'affût des nouvelles menaces et d'être en mesure d'y faire face efficacement.

L'un de nos chantiers prioritaires sera évidemment celui de l'expertise de notre personnel. Pour devenir un leader dans ses domaines de compétences, le Ministère se doit de disposer de compétences de pointe qui vont évoluer aussi rapidement que le développement des technologies.

Je tiens à remercier chaleureusement tout le personnel du Ministère pour son professionnalisme, qui s'avère essentiel à la réussite de nos ambitions. Rien ne serait possible sans le dévouement quotidien et l'expertise de nos équipes.

Je me dois également de souligner la collaboration exceptionnelle de l'équipe des dirigeants de l'information, qui sont nommés pour chacun des portefeuilles ministériels et des grands organismes, qui m'appuient dans l'exercice de mes responsabilités de dirigeant principal de l'information et qui rendront possible la réalisation de ce plan stratégique.

Le sous-ministre et dirigeant principal de l'information,

Original signé

Pierre E. Rodrigue

Québec, mai 2023

TABLE DES MATIÈRES

L'ORGANISATION EN BREF

Mission

Le ministère de la Cybersécurité et du Numérique (ci-après « le Ministère ») a pour mission d'animer et de coordonner les actions de l'État dans les domaines de la cybersécurité et du numérique, de proposer au gouvernement les grandes orientations en ces domaines, de déterminer les secteurs d'activités où il entend agir en priorité et de lui proposer des mesures en vue d'accroître l'efficacité de la lutte contre les cyberattaques et les cybermenaces au Québec.

Secteurs d'activité

Le Ministère :

- énonce la vision globale et intégrée de la transformation numérique gouvernementale en veillant à l'arrimage entre les besoins d'affaires et les ressources informationnelles, et ce, tout en visant à transformer l'accès des citoyennes et des citoyens aux services publics;
- assure le développement, l'implantation et le déploiement de l'administration publique numérique de même que la promotion et la mise en œuvre de toute mesure favorisant l'adaptation à cette fin des services publics;
- regroupe les activités d'élaboration des politiques, des stratégies et des orientations ainsi que les activités de conception, de réalisation et d'exploitation des projets numériques et technologiques communs ou à portée gouvernementale;
- réunit des expertises de pointe favorisant l'innovation et l'excellence au sein de l'administration publique, notamment par l'entremise du Centre québécois d'excellence numérique et du Centre gouvernemental de cyberdéfense;
- est responsable de la gouvernance ainsi que de la planification et de la performance des investissements en ressources informationnelles;
- est responsable de la gestion des données numériques gouvernementales, notamment dans le but de favoriser leur mobilité et leur valorisation au sein de l'administration publique, et ce, au profit des citoyennes et des citoyens;
- soutient les organismes publics dans le rehaussement de la sécurité de l'information à l'échelle gouvernementale et assure la coordination ainsi que la concertation des actions dans ces domaines, dont celles du Réseau gouvernemental de cyberdéfense;
- assure la cybersécurité des services qu'il offre aux organismes publics;
- établit des exigences en matière de sécurité de l'information applicables aux organismes publics et ordonne à ces derniers, lorsque requis, de mettre en œuvre ces exigences afin d'assurer la protection de leurs actifs informationnels et des informations qui leur sont confiées;
- offre des services de télécommunication, de radiocommunication, de téléphonie et de communication mobile;

- agit à titre de Courtier en infonuagique pour le compte des organismes publics en rendant accessibles, grâce à son catalogue, une multitude d'offres infonuagiques et en les accompagnant dans le processus;
- développe un ensemble de moyens visant à offrir aux citoyens et aux entreprises une prestation de services numériques de qualité, en s'assurant autant que possible de ne pas causer de fracture numérique;
- assure l'exploitation de solutions d'affaires administratives pour le compte de nombreux organismes publics et pourvoit également à l'entretien et à l'évolution de ces solutions;
- offre des services en opérations financières et contractuelles SAGIR (solutions d'affaires en gestion intégrée des ressources) ainsi que le service de soutien et de formation aux utilisateurs;
- fournit aux organismes publics clients une gamme complète de services liés à la rémunération, aux avantages sociaux et à la retraite du personnel.

Clientèles

Le Ministère, en application de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03; ci-après « LGGRI »), intervient auprès de plus de 300 organismes publics assujettis à celle-ci. Ses activités s'exercent notamment dans les sphères de gouvernance, d'orientation, d'encadrement normatif, de contrôle et de vérification.

Il offre également un éventail de services d'infrastructures technologiques, de services de télécommunication, de solutions bureautiques et de solutions d'affaires aux multiples organismes publics qui y ont recours.

Par ailleurs, en matière de cybersécurité, les actions du Ministère sont susceptibles de s'étendre à l'ensemble de la société civile.

Vision

Nous sommes le chef de file dans les services numériques sécuritaires qui propulsent l'administration publique de demain.

Valeurs

Le Ministère adhère pleinement aux valeurs de l'administration publique québécoise, soit la compétence, l'intégrité, l'impartialité, la loyauté et le respect.

En 2022, le Ministère a amorcé des travaux de définition de sa vision et de ses valeurs organisationnelles. Ces travaux, qui ont inclus une consultation du personnel, ont résulté par la proposition, d'une part, de la vision organisationnelle et, d'autre part, de quatre valeurs, soit l'innovation, l'excellence, la considération et la collaboration, desquelles résulte un sentiment de fierté.

Des activités se poursuivent afin d'intégrer la vision et les valeurs dans le quotidien de l'organisation, ce qui permettra leur appropriation et leur concrétisation.

CHIFFRES CLÉS	DESCRIPTION
7 715,2 M$	Investissements totaux pour le Plan québécois des infrastructures en ressources informationnelles 2023-2033
25 493	Nombre de personnes faisant partie de la main-d'œuvre en ressources informationnelles au gouvernement en 2022
2 144	Nombre de projets qualifiés en ressources informationnelles à l'échelle gouvernementale
5 400	Nombre de points d'accès Wi-Fi dans le Réseau intégré de télécommunication multimédia
2 039 034	Nombre de paies traitées pour l'ensemble du gouvernement en 2021-2022
26	Nombre de centres opérationnels de cyberdéfense faisant partie du Réseau gouvernemental de cyberdéfense

ANALYSE DE L'ENVIRONNEMENT

Contexte externe

Le Ministère a été constitué le 1er janvier 2022 en vertu de la Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions (LQ 2021, c. 33). À cet effet, les responsabilités et les ressources d'Infrastructures technologiques Québec (ITQ) et celles du Sous-secrétariat du dirigeant principal de l'information et de la transformation numérique (SSDPITN) du Secrétariat du Conseil du trésor (SCT) lui ont été transférées. La préparation du Plan stratégique 2023-2027 constitue donc le premier exercice de planification stratégique du Ministère depuis sa création.

La démarche de planification stratégique du Ministère a été étroitement associée à celle de la définition de la vision et des valeurs organisationnelles, et ce, afin d'établir des priorités stratégiques qui lient la raison d'être du Ministère aux préoccupations que celui-ci doit traiter.

L'analyse de l'environnement du Ministère repose sur plusieurs sources d'informations, dont :

- les rapports annuels de gestion d'ITQ et du SCT;
- le bilan du premier plan d'action ministériel du Ministère 2022-2023;
- les résultats de sondages de satisfaction des clientèles menés dans les dernières années par ITQ et le Centre de services partagés du Québec;
- des données opérationnelles provenant de diverses sources d'information de gestion au Ministère;
- les résultats de l'analyse de maturité numérique organisationnelle menée auprès d'ITQ et du SSDPITN en 2021;
- les résultats de la consultation du personnel du Ministère sur la vision et les valeurs organisationnelles.

La somme des informations recueillies, analysées sous le prisme des opportunités, des menaces, des forces et des faiblesses du Ministère, et notamment lors d'ateliers de réflexion stratégique menés en 2022, permet de brosser un portrait des contextes externe et interne dans lesquels celui-ci réalisera ses interventions stratégiques suivant sa création. Ces interventions stratégiques se veulent tout aussi pertinentes au regard de sa mission que respectueuses à l'égard des attentes de ses clientèles et des autres parties prenantes.

Les nouvelles attentes de la société numérique

De nos jours, le numérique est bien intégré dans la société : il a transformé les habitudes de vie, les interactions avec la famille et les amis ainsi que la manière de consommer et de travailler. D'ailleurs, en 2020, 92 % des citoyennes et des citoyens du Québec avaient accès à Internet à leur domicile[1]. La présence du numérique a contribué ainsi 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, ceux-ci s'attendent désormais à ce que l'administration publique s'adapte à leurs façons de faire. Ils souhaitent ainsi bénéficier d'expériences plus simples, personnalisées et requérant moins d'interactions pour réaliser des démarches de la vie courante auprès de l'État, voire d'expériences numériques de bout en bout. Les services publics doivent donc s'adapter pour répondre à ces nouvelles attentes.

La transformation des services publics

La transformation numérique des services publics et privés a une incidence sur l'administration publique de multiples façons. Par exemple, l'utilisation répandue des services en ligne se traduit par une demande pour une identité numérique gouvernementale afin d'accéder à des services, de même que par une demande de services gouvernementaux en ligne efficaces et efficients. En outre, il s'avère nécessaire d'augmenter les liens réseau et le déploiement de points d'accès à Internet sans fil afin de répondre aux besoins des organismes publics. Il en résulte que la transformation numérique de l'État représente une occasion pour rehausser la qualité des services fournis aux citoyennes et aux citoyens, mais aussi pour créer des économies d'échelle pour le gouvernement en augmentant l'efficience de ses infrastructures et en misant sur la mutualisation. Toutefois, afin de s'assurer que les organismes publics ont les moyens de leurs ambitions en matière de transformation numérique, et afin d'offrir une bonne qualité de services aux citoyennes et aux citoyens, il est indispensable que les investissements publics en ressources informationnelles soient alloués en concordance avec les priorités gouvernementales, et concourent à la matérialisation de bénéfices.

L'organisation du travail hybride

Au-delà des infrastructures elles-mêmes, la pérennisation de l'organisation du mode de travail hybride constitue un facteur important dans l'environnement de la cybersécurité et du numérique. De ce fait, le télétravail a intégré l'utilisation massive d'outils de collaboration dans les organisations de toute taille et a modifié la façon dont le personnel communique et interagit. Ce mode permet du même coup des possibilités de gain d'efficacité et de productivité au travail, qui font et continuent de faire l'objet d'études sur le sujet[2]. D'autres outils font également partie de l'éventail de solutions qu'apporte la transformation numérique, comme la robotique, l'automatisation et l'intelligence artificielle. Non seulement ces moyens permettent de numériser les lieux de travail, mais ils sont de plus en plus évoqués comme des facteurs qui peuvent contribuer à répondre aux défis liés à la rareté de main-d'œuvre actuelle. L'administration publique québécoise, le plus grand employeur public du Québec, doit donc mettre en place des actions structurantes pour soutenir et baliser ce virage.

1. INSTITUT DE LA STATISTIQUE DU QUÉBEC. *L'accès à Internet à domicile au Québec en 2020*, [En ligne], [https://statistique.quebec.ca/fr/produit/publication/acces-internet-domicile-quebec], (Consulté en avril 2023).
2. STATISTIQUE CANADA. *Étude : Travail à domicile : productivité et préférences*, [En ligne], [https://www150.statcan.gc.ca/n1/daily-quotidien/210401/dq210401b-fra.htm], (Consulté en avril 2023).

Les cyberattaques et la cybersécurité publique

Les événements internationaux des dernières années ont placé les problématiques de cybersécurité au cœur des agendas diplomatiques et stratégiques. Les piratages successifs de grands acteurs de la technologie et d'organisations publiques ainsi que l'apparition de nouvelles menaces, comme les rançongiciels, démontrent la volatilité d'un contexte politique international qui doit, lui aussi, s'adapter à la transformation numérique de la société. Les soupçons d'ingérence dans les processus électoraux et les tensions entre certains pays font en sorte que la cybersécurité est devenue un enjeu prioritaire pour les décideurs publics.

À ce titre, le gouvernement du Québec se doit d'agir pour protéger ses actifs informationnels et ses infrastructures et, surtout, pour éviter tout bris de service dû à des activités malveillantes. La surveillance et le renforcement des actifs, de même qu'une communication efficace des renseignements de sécurité, doivent être au cœur des priorités gouvernementales. Il en va de même de la protection des renseignements personnels des citoyennes et des citoyens, lesquels doivent pouvoir avoir confiance en la robustesse des systèmes utilisés dans les services gouvernementaux.

Une croissance des besoins en ressources informationnelles

Les enjeux de la rareté de main-d'œuvre dans la société québécoise de manière générale ne sont plus à démontrer. Plus précisément, dans un domaine en plein développement comme les ressources informationnelles, le besoin en ressources au sein des organismes gouvernementaux est criant. En effet, en 2022, on dénotait un taux de postes vacants de 12,1 %[3], soit un peu plus de 2 700 postes. Dans un tel contexte, il s'avère essentiel d'assurer l'attraction et la rétention de la main-d'œuvre en ressources informationnelles pour préserver la sécurité des actifs gouvernementaux et la mission de transformation numérique de l'État, mais aussi soutenir le virage numérique à l'échelle du Québec. De plus, considérant l'aspect innovant et en constante évolution du monde numérique, le développement et la consolidation des compétences des ressources humaines en ressources informationnelles constituent des enjeux prioritaires.

La création d'un intervenant public fédérateur

Les défis en matière de cybersécurité et de transformation numérique dans le domaine public sont de taille et prennent de l'ampleur avec le temps. Considérant leur importance indéniable dans la société, le gouvernement s'est doté d'un ministère dédié exclusivement à ces préoccupations, le ministère de la Cybersécurité et du Numérique, créé le 1er janvier 2022.

Plusieurs leviers sont induits par l'institution d'un nouvel intervenant public dans le domaine de la cybersécurité et de la transformation numérique. Nommément, les leviers juridiques du dirigeant principal de l'information, appuyé par ses équipes, favorisent la mise en œuvre de stratégies de cybersécurité et de numérique dans les organismes publics. Par ailleurs, la posture fédératrice du Ministère soutient la mise en œuvre de projets innovants en la matière dans la société, entre autres en collaboration avec les universités et l'ensemble de l'écosystème s'intéressant au monde numérique. Finalement, la création d'un tel intervenant ayant pour mission de favoriser la sécurité de l'information publique et le virage numérique de l'État crée des occasions

3. DONNÉES QUÉBEC. *Portraits de la main-d'œuvre en ressources informationnelles 2022*, [En ligne], [https://www.donneesquebec.ca/recherche/dataset/portrait-de-la-main-d-oeuvre-en-ti-de-la-fonction-publique-du-quebec/resource/58d29796-401e-4826-8413-0a27b2988db3], (Consulté en avril 2023).

de partage d'informations stratégiques pertinentes avec d'autres paliers de gouvernements à l'échelle locale, nationale et internationale, et ce, dans une optique de sécurité nationale.

Contexte interne

Dans le contexte de l'élaboration du premier plan stratégique du Ministère, les résultats de l'analyse du diagnostic organisationnel prennent une dimension des plus importantes. Le présent contexte interne tient ainsi compte des forces et des faiblesses cernées pouvant avoir un impact sur les activités du Ministère. Cette analyse démontre toute l'importance que ce dernier accorde au développement et à la mobilisation de son personnel, de même qu'aux processus de travail internes, et ce, dans l'optique d'offrir des services performants, sécuritaires et de qualité.

Ressources humaines

Le Ministère s'appuie sur l'expertise des 1 815[4] membres de son personnel. Dans un esprit d'exemplarité en ce qui concerne la Politique-cadre en matière de télétravail pour le personnel de la fonction publique ainsi que la régionalisation des emplois, la majorité des postes du Ministère sont offerts ou pourvus dans l'ensemble des régions du Québec.

Ce faisant, le Ministère redouble d'efforts pour attirer et retenir les meilleurs talents en ressources informationnelles, tant dans les opérations que dans la gouvernance, surtout dans un contexte de grand changement organisationnel. Signe de l'importance accordée à la mobilisation du personnel, le taux de départ volontaire des employés du Ministère n'était que de 5,3 % au 31 mars 2022, soit bien en deçà de celui de la fonction publique du Québec (13 %)[5].

L'expertise nichée de certains postes du Ministère et l'innovation inhérente aux domaines de la transformation numérique et de la cybersécurité font en sorte que de nouvelles connaissances et de nouvelles compétences professionnelles sont recherchées continuellement, notamment pour les métiers d'avenir. Considérant les enjeux de la rareté de main-d'œuvre et ses préoccupations d'expertises en constante évolution, le Ministère se doit d'être une organisation apprenante qui favorise la rétention et la mobilisation de son personnel.

Rehaussement de processus de travail axés sur l'efficience et la qualité des services

La qualité des ressources informationnelles et des infrastructures mêmes du Ministère a un impact direct sur l'efficience et la qualité des services qui sont ensuite fournis à ses clientèles. Dans cette perspective, il est pertinent et louable que le Ministère soit en posture exemplaire. Or, pour ce faire, le diagnostic organisationnel démontre que la mise en place de nouveaux processus de travail et l'optimalisation de certains d'entre eux pourront contribuer positivement à ces visées ultimes, notamment en réduisant certains délais de service. Des actions internes seront donc mises en place à cet effet dans les prochaines années dans le but de soutenir activement l'atteinte des objectifs stratégiques du Ministère.

4. Donnée au 28 février 2023.
5. SECRÉTARIAT DU CONSEIL DU TRÉSOR. *Effectif de la fonction publique*. [En ligne], [https://www.tresor.gouv.qc.ca/ressources-humaines/effectifs-gouvernementaux/effectif-de-la-fonction-publique/], (Consulté en avril 2023).

CHOIX STRATÉGIQUES

Enjeu stratégique 1 – Un Québec cybersécuritaire en partenariat avec l'écosystème

L'omniprésence du numérique et des technologies de l'information dans la vie des citoyennes et des citoyens ainsi que la transformation des services de l'État qui s'en accompagne ont comme incidence d'augmenter les risques et les dangers liés à l'utilisation du numérique. Les cyberrisques et les cyberincidents ont un impact considérable dans tous les pans de la société.

En 2021, les dépenses effectuées en cybersécurité dans les entreprises canadiennes étaient de près de 10 G$[6], et ce chiffre ira en augmentant. De plus, pour cette même année, près du cinquième des entreprises canadiennes ont été victimes d'un incident de cybersécurité et cette proportion atteint plus du tiers lorsque l'on parle uniquement des grandes entreprises. Selon un rapport d'IBM de 2022, un cyberincident coûte en moyenne 7,3 M$ au Canada[7], ce qui place ce dernier parmi les cinq pays avec un coût moyen le plus élevé. De plus, malgré le fait que la majorité des entreprises adoptent des pratiques de cyberhygiène, plus de 90 % de celles-ci ne déclarent pas aux autorités pertinentes qu'elles ont été victimes d'un cyberincident[8].

Les citoyennes et les citoyens ne sont pas en reste : en 2020, 32 % des Canadiens ont été victimes d'une cybermenace et 56 % ont déjà été victimes d'un virus, d'un logiciel espion ou malveillant. Il n'est donc pas surprenant de voir que 85 % des Canadiens sont inquiets à propos de la sécurité de leurs renseignements personnels. Ces chiffres peuvent surprendre, mais il est important de souligner que pour cette même année, 93 % des Canadiens avaient un ordinateur portable ou de bureau, 76 % des téléphones intelligents et 58 % des tablettes électroniques[9].

Il s'avère nécessaire d'effectuer énormément de sensibilisation, de prévention et d'optimisation de la lutte aux cybermenaces afin de conserver un environnement numérique sécuritaire qui favorise la confiance de la population et qui assure un développement économique durable.

Dans cette optique, il est essentiel que les différents acteurs de la société civile agissent avec une vision commune et concertée pour assurer l'intégrité des ressources informationnelles au Québec. Ainsi, les différents paliers de gouvernement, les entreprises, les universités et centres de recherche unissent leurs forces pour établir et appliquer les mêmes standards et les mêmes pratiques en cybersécurité, ce qui permet de garantir la cybersécurité au Québec et de positionner ce dernier comme un leader dans ce domaine.

6. STATISTIQUE CANADA. *L'incidence du cybercrime sur les entreprises canadiennes, 2021*, [En ligne], [https://www150.statcan.gc.ca/n1/daily-quotidien/221018/dq221018b-fra.htm], (Consulté en avril 2023).
7. IBM. *Cost of a data breach 2022*, [En ligne], [https://www.ibm.com/reports/data-breach], (Consulté en avril 2023).
8. STATISTIQUE CANADA. *L'incidence du cybercrime sur les entreprises canadiennes, 2021*, [En ligne], [https://www150.statcan.gc.ca/n1/daily-quotidien/221018/dq221018b-cansim-fra.htm], (Consulté en avril 2023).
9. GOUVERNEMENT DU CANADA. *Fiche d'information : comment fonctionnent les cybermenaces*, [En ligne], [https://www.pensezcybersecurite.gc.ca/fr/ressources/fiche-dinformation-comment-fonctionnent-les-cybermenaces], (Consulté en avril 2023).

Orientation 1 – Accroître l'efficacité de la lutte contre les cybermenaces

En plus de s'imposer comme un vecteur de changement pour une société plus cybersécuritaire, l'État doit s'assurer que ses propres infrastructures et services ne sont pas menacés. Le gouvernement du Québec devra donc faire preuve de prudence pour assurer la protection des renseignements et des infrastructures dont il a la charge. Ainsi, au cours des prochaines années, le Ministère mettra en place des actions afin d'accroître l'efficacité de la lutte contre les cybermenaces, et ce, dans une perspective de protection des biens collectifs et des renseignements personnels des citoyennes et des citoyens.

Objectif 1.1 – Réduire l'efficacité des attaques de rançongiciels par l'adoption de comportements cybersécuritaires

Considérant l'importance du facteur humain dans la protection contre les attaques de rançongiciels, le Ministère prend des engagements afin de rehausser la sécurité de l'information des actifs gouvernementaux en améliorant les connaissances des utilisateurs au sujet de ceux-ci.

Suivant cette logique, le Ministère s'est engagé, dans un premier temps, à favoriser la connaissance des citoyennes et des citoyens en matière de sécurité de l'information par l'entremise de campagnes d'information et de sensibilisation qui seront lancées dans les prochaines années. De manière efficiente et concertée, le Ministère vise à fournir du contenu d'information et de sensibilisation destiné aux utilisateurs des services numériques gouvernementaux, et ce, afin d'augmenter l'efficacité de la cyberprotection des services et la protection des renseignements des systèmes utilisés.

De plus, le Ministère poursuivra ses efforts afin que la forte majorité du personnel de la fonction publique québécoise maîtrise des connaissances en sécurité de l'information pour que celle-ci puisse contribuer activement à l'accroissement de l'efficacité de la lutte contre les cybermenaces. À cette fin, le Ministère mettra à la disposition des organismes publics du matériel de formation actualisé régulièrement et les membres du personnel devront démontrer annuellement leurs connaissances en cybersécurité. À court et à moyen termes, les risques de bris de service et de violation de confidentialité causés par des activités cybercriminelles ayant un impact sur les services rendus aux citoyennes et aux citoyens seront amenuisés.

INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
1. Taux d'utilisateurs de services numériques sensibilisés aux comportements cybersécuritaires (valeur de départ en 2022-2023 : S. O.)	30 %	45 %	65 %	85 %
2. Taux du personnel de la fonction publique ayant suivi et réussi une formation sur les comportements cybersécuritaires (valeur de départ en 2022-2023 : S. O.)	70 %	75 %	80 %	85 %

Objectif 1.2 – Rehausser le niveau de protection des actifs informationnels de l'État contre les cyberattaques

La détection des failles ou des vulnérabilités dans les services numériques est considérée comme une bonne pratique pour favoriser la protection et la résilience des systèmes informatiques. En effet, une vulnérabilité est une faiblesse qui est susceptible d'être exploitée lors d'une cyberattaque et d'ainsi porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité d'un système ou d'une infrastructure technologique. C'est pourquoi le Ministère, par l'entremise du Centre gouvernemental de cyberdéfense, a mis en place différentes actions afin de s'assurer de rehausser le niveau de protection des actifs informationnels, comme :

- la Plateforme de signalement de vulnérabilité;
- le Programme de prime aux bogues;
- des tests d'intrusion;
- des balayages de vulnérabilités.

Afin de maintenir le plus haut taux de confiance envers les actifs informationnels et de prévenir les incidents de sécurité dus à des activités cybercriminelles, le Ministère s'engage à rehausser le taux de correction dans les délais prescrits des vulnérabilités détectées dans les actifs informationnels de l'État.

INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
3. Pourcentage des vulnérabilités détectées dans les actifs informationnels de l'État corrigées conformément aux délais prévus dans le processus de gestion des menaces, des vulnérabilités et des incidents (valeur de départ en 2022-2023 : 75 %)	80 %	85 %	88 %	90 %

Enjeu stratégique 2 – Une administration publique numérique et performante

Le numérique occupe désormais une place primordiale dans les divers aspects de la vie courante, notamment dans les communications, la consommation et le travail. Aujourd'hui, en plus de l'utilisation d'Internet, 71 % des Canadiens utilisent les réseaux sociaux et 82 % effectuent des achats en ligne[10]. Le numérique a considérablement transformé toutes les structures de la vie quotidienne autant en la simplifiant qu'en apportant des enjeux nouveaux. Cette omniprésence du numérique dans la vie des citoyens nécessite que l'administration publique s'adapte, se renouvelle et évolue dans ses façons de faire. Le numérique doit contribuer à une offre de services publics performants et de qualité qui répondent aux besoins des citoyens et des entreprises.

10. STATISTIQUE CANADA. *Enquête canadienne sur utilisation d'Internet, 2020*, [En ligne], [https://www150.statcan.gc.ca/n1/daily-quotidien/210622/dq210622b-fra.htm], (Consulté en avril 2023).

Devant ce virage numérique, l'administration publique doit adopter de nouvelles stratégies qui permettent d'augmenter son efficacité et sa productivité dans une perspective d'amélioration des services offerts aux citoyennes et aux citoyens et de la performance de l'État.

Orientation 2 – Maximiser la valeur des investissements des organismes publics dans les projets en ressources informationnelles

Le Ministère appuie les organismes publics dans la planification et le suivi des dépenses de projets en ressources informationnelles. Par l'entremise du Plan québécois des infrastructures – secteur des ressources informationnelles, il s'assure que les sommes investies concordent avec les priorités gouvernementales, maximisent la transformation numérique, renforcent la cybersécurité et génèrent des bénéfices récurrents.

Objectif 2.1 – Réduire les délais de planification des projets

Les projets qualifiés en ressources informationnelles des organismes publics assujettis à la LGGRI font l'objet d'un suivi par le Ministère afin d'en assurer une bonne gouvernance.

Lorsqu'un délai de planification plus long que la normale est observé, la cause est généralement attribuable à une gouvernance du portefeuille de projets en ressources informationnelles de l'organisme public concerné qui doit être rehaussée. Ce portefeuille de projets doit prendre en considération plusieurs facteurs, comme la capacité financière et humaine en ressources informationnelles. En priorisant les projets en ressources informationnelles d'un organisme public en fonction de ces facteurs, le délai de planification de chaque projet peut être maintenu sous les six mois, ce qui permet d'amorcer plus rapidement l'exécution et de livrer en temps opportun les résultats attendus au sein de l'organisation.

INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
4. Proportion des projets qualifiés en ressources informationnelles dont la planification est réalisée en moins de six mois (valeur de départ en 2022-2023 : 64 %)	67,5 %	70 %	72,5 %	75 %

Objectif 2.2 – Augmenter le respect des paramètres d'autorisation des projets

La santé des projets en ressources informationnelles des organismes publics assujettis à la LGGRI constitue une priorité gouvernementale dont la vue d'ensemble fait l'objet d'une diffusion publique dans le Tableau de bord des projets en ressources informationnelles du gouvernement du Québec[11], et ce, dans un souci de transparence. De ce fait, le Ministère souhaite contribuer activement à l'amélioration du taux de respect des paramètres d'autorisation des projets des organismes publics, tant en ce qui concerne la variation du coût de réalisation par rapport au montant autorisé que la variation de la durée du projet par rapport à celle prévue et autorisée, toujours dans un esprit de bonne gouvernance et de bonne performance des organismes publics.

11. Pour les projets dont le coût est supérieur à 500 000 $ et dont la phase d'exécution est débutée.

INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
5. Taux de respect des paramètres d'autorisation des projets qualifiés en ressources informationnelles quant au coût (valeur de départ en 2022-2023 : 90,3 %)	91 %	92 %	93 %	95 %
6. Taux de respect des paramètres d'autorisation des projets qualifiés en ressources informationnelles quant à l'échéancier (valeur de départ en 2022-2023 : 60,5 %)	61 %	63 %	65 %	67 %

Objectif 2.3 – Générer des bénéfices quantifiables et récurrents

Les ressources informationnelles représentent une valeur stratégique pour l'État. Considérant l'importance des dépenses et des investissements dans ce domaine, il est primordial d'en assurer une utilisation optimale, permettant ainsi aux organismes publics d'offrir notamment aux citoyennes et aux citoyens les meilleurs services au moindre coût. C'est en voulant s'assurer d'une saine gestion des fonds publics, et parce que l'utilisation et la contribution des ressources informationnelles aux activités gouvernementales sont essentielles à la performance de l'État, qu'a été pris l'arrêté numéro 2022-01 du ministre de la Cybersécurité et du Numérique en date du 27 mai 2022, concernant le Cadre gouvernemental de gestion des bénéfices des projets en ressources informationnelles, lequel est entré en vigueur le 15 juin 2022 à la suite de sa publication à la *Gazette officielle du Québec*.

Puisque les initiatives et les projets en ressources informationnelles doivent permettre aux organismes publics de dégager des bénéfices, ceux-ci doivent être définis pour pouvoir les estimer, les mesurer, voire les réinvestir. Le cadre est donc un outil indispensable à cet égard. Il renforce la priorisation des projets en ressources informationnelles en encadrant la gestion des bénéfices, en définissant les bénéfices attendus des projets en ressources informationnelles et en suivant la performance des organismes publics.

Par son rôle de soutien à la gouvernance des projets en ressources informationnelles, le Ministère s'engage à accompagner les organismes publics de manière à dégager des bénéfices quantifiables et récurrents qui permettront de réduire le budget des organismes publics, soit par des économies, soit par des recettes supplémentaires.

INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
7. Somme des bénéfices quantifiables et récurrents identifiés dans les plans de matérialisation des bénéfices des projets qualifiés des organismes publics (valeur de départ en 2022-2023 : 0 $)	50 M$	100 M$	150 M$	200 M$

Orientation 3 – Soutenir la performance des services publics

Le Ministère a pour mandat d'augmenter l'efficacité et l'efficience de l'État étant donné son rôle de coordonnateur de l'action gouvernementale en matière de numérique. Pour ce faire, il apporte un soutien aux organismes publics dans leur transition numérique par des moyens comme la sensibilisation, le partage d'expertise, la communication, la formation et l'accompagnement. Au cours des prochaines années, le Ministère réalisera des actions concertées qui permettront aux organismes publics d'adopter une culture du numérique, et ce, dans un esprit de collaboration et de mutualisation des services au bénéfice des citoyennes et des citoyens.

Objectif 3.1 – Permettre aux citoyennes et aux citoyens d'accéder de manière optimale aux services numériques

La transformation numérique de l'administration publique favorisera l'augmentation de l'utilisation des services numériques au cours des prochaines années. Pour ce faire, le Ministère continuera de soutenir les organismes publics dans la mise en place de services numériques simplifiés et efficaces qui tiennent compte des différentes particularités des utilisateurs.

Le Ministère s'engage à ce que le déploiement du Service d'authentification gouvernementale fasse partie de ses actions prioritaires. Ce service permettra une meilleure accessibilité numérique aux services gouvernementaux tout en répondant à des exigences de sécurité rehaussées pour protéger les renseignements personnels des citoyennes et des citoyens. La réussite de cette transformation s'illustrera par le taux de citoyennes et de citoyens utilisant le service pour accéder aux prestations électroniques de services d'organismes publics.

INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
8. Taux de citoyennes et de citoyens utilisant le Service d'authentification gouvernementale (valeur de départ en 2022-2023 : 0 %)	40 %	45 %	75 %	80 %

Objectif 3.2 – Réduire les coûts de fonctionnement de l'État par l'utilisation de services communs performants

L'une des priorités gouvernementales à laquelle le Ministère contribue activement est d'augmenter la performance des services gouvernementaux, notamment en matière de coûts de fonctionnement. Le Ministère soutient cette priorité, notamment en mutualisant des services qui peuvent être combinés dans un souci d'efficience. L'offre de service du Ministère permet également de dégager les organismes publiques de la gestion d'infrastructures technologiques et de systèmes afin qu'elles puissent concentrer leurs efforts sur leur mission et la transformation numérique de leurs opérations.

Le Ministère s'engage de manière prioritaire à proposer des services communs de base qui seront offerts aux organismes publics dans les prochaines années, selon les besoins d'affaires qui seront identifiés, de manière à susciter l'utilisation de ces services. De plus, la migration de la desserte policière de la Sûreté du Québec vers le Réseau national intégré de radiocommunication (RENIR) est une priorité du Ministère afin d'assurer l'adhésion et la satisfaction de ses services de communication.

INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
9. Taux d'organismes publics utilisant au moins deux des services communs de base (valeur de départ en 2022-2023 : S. O.)	S. O.	10 %	15 %	20 %
10. Taux d'unités opérationnelles existantes de la Sûreté du Québec migrées vers le Réseau national intégré de radiocommunication (RENIR) (valeur de départ en 2022-2023 : 51 %)	70 %	75 %	80 %	90 %

Objectif 3.3 – Augmenter le niveau de maturité numérique des organismes publics

Le Ministère accompagne les organismes publics dans leur transformation numérique. Pour mesurer et suivre l'évolution de la maturité numérique organisationnelle de ceux-ci, le Ministère utilisera un outil basé entre autres sur les 18 bonnes pratiques numériques gouvernementales. Le portrait dégagé permettra d'obtenir une vue d'ensemble de la situation actuelle et ciblera les pistes d'améliorations potentielles. Plus les organismes publics seront avancés dans leur plan de transformation numérique, plus leur indice de maturité numérique devrait être élevé. Le Ministère souhaite suivre annuellement l'indice moyen de maturité numérique des organismes publics afin de s'assurer que son soutien suscite un véritable virage dans leur transformation numériqu. La valeur de départ est alimentée par le résultat moyen des organismes publics au Baromètre numériQc en 2022.

INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
11. Indice moyen de maturité numérique des organismes publics (valeur de départ en 2022-2023 : 62,7 %)	63 %	65 %	67 %	70 %

Objectif 3.4 – Utiliser le plein potentiel de l'infonuagique

Toujours dans un souci d'optimisation des services de l'État, le Ministère utilise des moyens innovants pour favoriser la performance organisationnelle. Ainsi, il s'engage à poursuivre son Programme de consolidation des centres de traitement informatique et de l'optimisation du traitement et du stockage, dont l'objectif est notamment de déplacer le traitement et le stockage visé des organismes publics vers des offres de nuages externes qui ont été préalablement qualifiées par le Courtier en infonuagique.

Les évaluations du dossier d'affaires démontrent que l'utilisation du plein potentiel de l'infonuagique pour faire évoluer les pratiques des organisations pourrait générer des économies, en plus de permettre d'augmenter le degré de protection des actifs informationnels gouvernementaux.

INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
12. Taux d'organismes publics ayant terminé leur migration vers l'infonuagique externe (valeur de départ au 31 mars 2022 : 6 %)	35 %	73 %	95 %	S. O.

Orientation 4 – Implanter un modèle de gestion des données numériques gouvernementales

Découlant de son rôle de gardien de la saine gouvernance des ressources informationnelles du gouvernement, le Ministère veille à mettre en place une gestion performante des données numériques gouvernementales afin de favoriser la transformation numérique de l'État. Accroître la gestion efficace et efficiente des données numériques se fera dans un esprit de valorisation de l'information auprès des citoyennes, des citoyens, des entreprises et de l'administration publique elle-même.

Objectif 4.1 – Augmenter l'utilisation des données numériques gouvernementales au sein de l'administration publique

L'accès à des données numériques cohérentes et de qualité en temps opportun est essentiel pour le bon fonctionnement de plusieurs prestations de services gouvernementales. Les sources officielles de données numériques gouvernementales et de référence offrent aux organismes publics une version unique de certaines données communes à plusieurs organismes publics. Ainsi, l'utilisation de ces sources officielles de données par les organismes publics contribue non seulement à réduire le nombre de copies de ces données communes, mais également à accroître l'efficacité et l'efficience de l'administration publique, notamment par une meilleure protection de celles-ci. Par ailleurs, le Ministère s'engage à accompagner les organismes publics à mieux utiliser et à augmenter la mobilité des données numériques dont ils ont l'intendance, ce qui se traduira par l'augmentation de leur performance dans la gestion des données, mais aussi dans les services offerts aux citoyennes, aux citoyens de même qu'aux entreprises.

Dans le même esprit, le Ministère souhaite encourager l'utilisation du Service d'authentification gouvernementale et en bonifier l'accès pour les citoyennes et les citoyens. Ainsi, il vise à rendre disponible un portefeuille numérique, une innovation technologique permettant par application mobile de démontrer son identité, une compétence et/ou une autorisation de manière fiable et sécuritaire, le tout afin de favoriser l'efficience de l'utilisation des services gouvernementaux par les citoyennes et les citoyens.

INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
13. Nombre d'organismes publics qui utilisent des sources officielles de données numériques et de référence (valeur de départ en 2022-2023 : 2)	10	15	30	50
14. Taux de citoyennes et de citoyens utilisant le portefeuille d'attestations numériques gouvernementales (valeur de départ en 2022-2023 : S. O.)	S. O.	5 %	12 %	18 %

Enjeu stratégique 3 – Une expertise de haut calibre dans une organisation modèle

Par son rôle et sa mission, le Ministère est une organisation qui se doit de miser sur l'innovation et de se positionner comme leader en la matière auprès des autres organismes publics. Néanmoins, pour ce faire, il doit se doter de pratiques exemplaires et ainsi servir de réel modèle auprès des organismes publics afin de les accompagner dans le développement de leur propre culture de transformation numérique et de cybersécurité.

Pour devenir une organisation modèle, le Ministère mise sur l'instauration d'une culture de l'innovation et du changement qui guidera ses activités. En effet, par sa raison d'être et sa volonté d'être un chef de file, le Ministère se doit d'être à l'avant-garde des grandes tendances en matière de cybersécurité et de transformation numérique, tant dans leur connaissance que dans leur application.

La mise en place d'une organisation modèle dans un domaine innovant passe d'abord et avant tout par une main-d'œuvre détenant une expertise hautement qualifiée et mobilisée autour de la mise en œuvre de transformation structurante.

Orientation 5 – Créer une organisation apprenante qui fidélise ses talents

Le Ministère a à cœur d'offrir des services innovants, performants et de qualité pour contribuer à la transformation de l'administration publique. Au centre de la prestation de ses services se trouve un personnel hautement qualifié qui doit demeurer à la fine pointe des connaissances dans des domaines en constante évolution. Ainsi, le Ministère est un milieu de travail où plusieurs secteurs peuvent être appelés à recourir à des métiers d'avenir.

Considérant les défis d'envergure que pose la rareté de main-d'œuvre, le Ministère doit mettre de l'avant des actions structurantes qui permettront de susciter la mobilisation de son personnel tout en favorisant le développement de ses compétences. Il entend ainsi implanter une culture d'apprentissage en continu et faire vivre des expériences positives à son personnel, et ce, à chacune des phases de leur expérience en tant qu'employés.

Objectif 5.1 – Se positionner comme un employeur exemplaire en matière de développement d'expertises de pointe

De manière proactive, le Ministère s'engage à évaluer en continu ses besoins en matière de métiers d'avenir dans le domaine des ressources informationnelles et à y répondre afin d'apporter une contribution croissante à sa capacité d'accomplir sa mission. Il veillera à identifier la présence, actuelle ou potentielle, de ces métiers d'avenir dans l'organisation.

Ainsi, dans une perspective de fidélisation et de développement des compétences de son personnel, le Ministère identifiera chaque année des candidats présentant un potentiel pour occuper un métier d'avenir et mettra en place des plans de développement individuels enrichis pour ceux-ci.

INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
15. Taux d'employés dont l'emploi est appelé à se transformer en métier d'avenir en ressources informationnelles qui bénéficient d'un plan de développement individuel enrichi (valeur de départ en 2022-2023 : S. O.)	25 %	50 %	75 %	95 %

Objectif 5.2 – Se positionner comme un employeur exemplaire en matière de fidélisation

Le Ministère entend miser sur la fidélisation de son personnel afin de susciter l'adhésion à une culture de l'innovation et de favoriser une prestation de services efficiente et de qualité. Il s'engage à mesurer, puis à augmenter l'indice de mobilisation de son personnel. Les facteurs de cet indice font référence à l'engagement ainsi qu'à l'implication émotionnelle et intellectuelle des membres du personnel envers l'organisation, et ce, dans l'optique de contribuer de manière optimale à la performance du Ministère. Les mesures annuelles seront réalisées par des sondages et des actions concrètes et axées sur les constats seront mises en œuvre afin de favoriser l'augmentation annuelle prévue de l'indice.

INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
16. Indice de mobilisation du personnel (valeur de départ en 2022-2023 : S. O.)	Mesure initiale	Augmentation de 2 % par rapport à la mesure initiale	Augmentation de 4 % par rapport à la mesure initiale	Augmentation de 6 % par rapport à la mesure initiale

TABLEAU SYNOPTIQUE DU PLAN STRATÉGIQUE 2023-2027

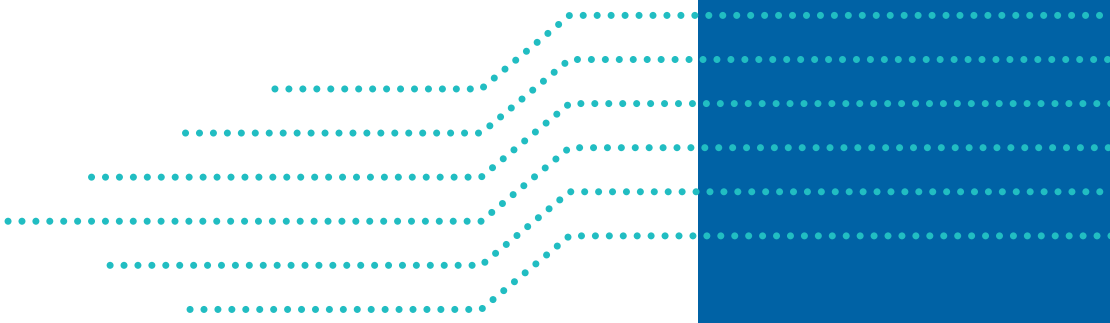
MISSION : Le ministère de la Cybersécurité et du Numérique a pour mission d'animer et de coordonner les actions de l'État dans les domaines de la cybersécurité et du numérique, de proposer au gouvernement les grandes orientations en ces domaines, de déterminer les secteurs d'activités où il entend agir en priorité et de lui proposer des mesures en vue d'accroître l'efficacité de la lutte contre les cyberattaques et les cybermenaces au Québec.

VISION : Nous sommes le chef de file dans les services numériques sécuritaires qui propulsent l'administration publique de demain.

VALEURS : Innovation, excellence, considération et collaboration

OBJECTIF	INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
Enjeu 1 : Un Québec cybersécuritaire en partenariat avec l'écosystème					
Orientation 1 : Accroître l'efficacité de la lutte contre les cybermenaces					
1.1 Réduire l'efficacité des attaques de rançongiciels par l'adoption de comportements cybersécuritaires	**1.** Taux d'utilisateurs de services numériques sensibilisés aux comportements cybersécuritaires Valeur de départ : S. O.	30 %	45 %	65 %	85 %
	2. Taux du personnel de la fonction publique ayant suivi et réussi une formation sur les comportements cybersécuritaires Valeur de départ : S. O.	70 %	75 %	80 %	85 %
1.2 Rehausser le niveau de protection des actifs informationnels de l'État contre les cyberattaques	**3.** Pourcentage des vulnérabilités détectées dans les actifs informationnels de l'État corrigées conformément aux délais prévus dans le processus de gestion des menaces, des vulnérabilités et des incidents Valeur de départ : 75 %	80 %	85 %	88 %	90 %
Enjeu 2 : Une administration publique numérique et performante					
Orientation 2 : Maximiser la valeur des investissements des organismes publics dans les projets en ressources informationnelles					
2.1 Réduire les délais de planification des projets	**4.** Proportion des projets qualifiés en ressources informationnelles dont la planification est réalisée en moins de six mois Valeur de départ : 64 %	67,5 %	70 %	72,5 %	75 %
2.2 Augmenter le respect des paramètres d'autorisation des projets	**5.** Taux de respect des paramètres d'autorisation des projets qualifiés en ressources informationnelles quant au coût Valeur de départ : 90,3 %	91 %	92 %	93 %	95 %

OBJECTIF	INDICATEUR	CIBLE 2023-2024	CIBLE 2024-2025	CIBLE 2025-2026	CIBLE 2026-2027
	6. Taux de respect des paramètres d'autorisation des projets qualifiés en ressources informationnelles quant à l'échéancier Valeur de départ : 60,5 %	61 %	63 %	65 %	67 %
2.3 Générer des bénéfices quantifiables et récurrents	**7.** Somme des bénéfices quantifiables et récurrents identifiés dans les plans de matérialisation des bénéfices des projets qualifiés des organismes publics Valeur de départ : 0 $	50 M$	100 M$	150 M$	200 M$
Orientation 3 : Soutenir la performance des services publics					
3.1 Permettre aux citoyennes et aux citoyens d'accéder de manière optimale aux services numériques	**8.** Taux de citoyennes et de citoyens utilisant le Service d'authentification gouvernementale Valeur de départ : 0 %	40 %	45 %	75 %	80 %
3.2 Réduire les coûts de fonctionnement de l'État par l'utilisation de services communs performants	**9.** Taux d'organismes publics utilisant au moins deux des services communs de base Valeur de départ : S. O.	S. O.	10 %	15 %	20 %
	10. Taux d'unités opérationnelles existantes de la Sûreté du Québec migrées vers le Réseau national intégré de radiocommunication (RENIR) Valeur de départ : 51 %	70 %	75 %	80 %	90 %
3.3 Augmenter le niveau de maturité numérique des organismes publics	**11.** Indice moyen de maturité numérique des organismes publics Valeur de départ : 62,7 %	63 %	65 %	67 %	70 %
3.4 Utiliser le plein potentiel de l'infonuagique	**12.** Taux d'organismes publics ayant terminé leur migration vers l'infonuagique externe Valeur de départ : 6 %	35 %	73 %	95 %	S. O.
Orientation 4 : Implanter un modèle de gestion des données numériques gouvernementales					
4.1 Augmenter l'utilisation des données numériques gouvernementales au sein de l'administration publique	**13.** Nombre d'organismes publics qui utilisent des sources officielles de données numériques et de référence Valeur de départ : 2	10	15	30	50
	14. Taux de citoyennes et de citoyens utilisant le portefeuille d'attestations numériques gouvernementales Valeur de départ : S. O.	S. O.	5 %	12 %	18 %
Enjeu 3 : Une expertise de haut calibre dans une organisation modèle					
Orientation 5 : Créer une organisation apprenante qui fidélise ses talents					
5.1 Se positionner comme un employeur exemplaire en matière de développement d'expertises de pointe	**15.** Taux d'employés dont l'emploi est appelé à se transformer en métier d'avenir en ressources informationnelles qui bénéficient d'un plan de développement individuel enrichi Valeur de départ : S. O.	25 %	50 %	75 %	95 %
5.2 Se positionner comme un employeur exemplaire en matière de fidélisation	**16.** Indice de mobilisation du personnel Valeur de départ : S. O.	Mesure initiale	Augmentation de 2 % par rapport à la mesure initiale	Augmentation de 4 % par rapport à la mesure initiale	Augmentation de 6 % par rapport à la mesure initiale



Cybersécurité
et Numérique
Québec