2014-2017

Approche stratégique gouvernementale

Sécurité de l'information

Québec

2014-2017

Approche stratégique gouvernementale

Sécurité de l'information

Cette publication a été réalisée par
le Sous-secrétariat du dirigeant principal de l'information
et produite par la Direction des communications.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor
5e étage, secteur 500
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

Dépôt légal – 2014
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-70326-6 (en ligne)

Table des matières

1. Introduction

Le développement accéléré des technologies de l'information ainsi que l'utilisation croissante d'Internet ont considérablement modifié les règles d'échange et de partage de l'information. Dans sa démarche de transformation de la prestation de services aux citoyens et aux entreprises, notamment dans la mise en œuvre de l'administration électronique[1], le gouvernement du Québec a placé la sécurité de l'information au cœur de ses priorités.

La présente approche stratégique, adoptée en vertu de l'article 21 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), fait suite à la Stratégie gouvernementale de sécurité de l'information, adoptée pour la période 2005-2009.

Cette approche définit la mission du gouvernement du Québec en la matière et détermine les éléments essentiels à la réalisation de la vision de l'encadrement de la sécurité de l'information gouvernementale.

2. Contexte

Plus de dix ans se sont écoulés depuis l'adoption, en 2000, de la première directive gouvernementale portant sur la sécurité de l'information numérique et des échanges électroniques. Ces années ont été marquées par une utilisation croissante d'Internet, et, au gouvernement du Québec, par une démarche de transformation de la prestation des services aux citoyens et aux entreprises. Ces changements ont fait en sorte que la sécurité de l'information est devenue un enjeu central et une préoccupation constante dans le cadre de la prestation des services gouvernementaux.

La présente approche s'appuie aussi bien sur les constats des réalisations des dix dernières années de l'Administration gouvernementale que sur les préoccupations et les tendances de l'heure, observées auprès de gouvernements précurseurs en sécurité de l'information, ou découlant d'études spécialisées.

De ces tendances et constats, des enjeux de sécurité de l'information ont été identifiés pour la prochaine décennie, ainsi qu'un positionnement gouvernemental à cet égard. Celui-ci touche principalement la gouvernance de la sécurité de l'information, la cybersécurité, l'authentification, la gestion des risques, la formation et la sensibilisation ainsi que les pratiques de l'information.

1. Administration électronique : Utilisation des technologies de l'information et de la communication et, plus particulièrement, d'Internet comme outils pour arriver à une meilleure administration (Source : OCDE. *Rethinking eGovernment Services: **User-centered Approaches***, le 2 octobre 2000).

Pour répondre à ces enjeux, des mesures ont été définies pour les trois prochaines années. Celles-ci sont détaillées dans quatre documents structurant dont la mise en œuvre requiert la contribution des organismes publics[2] : il s'agit de la présente Approche stratégique gouvernementale 2014-2017, de la nouvelle Directive sur la sécurité de l'information gouvernementale, du Cadre gouvernemental de gestion de la sécurité de l'information et du Cadre de gestion des risques[3] et des incidents[4] à portée gouvernementale.

3. Vision

La vision de l'encadrement de la sécurité de l'information gouvernementale, sur un horizon de dix ans, se précise comme suit :

L'information gouvernementale bénéficie d'une sécurité optimale, peu importe l'endroit où elle est conservée, manipulée ou transmise. Au bout de dix ans, les organismes publics ont atteint un niveau de maturité où la sécurité de l'information est ancrée dans la culture de l'organisation et où les objectifs, les pratiques et les mesures de performance sont définis et les processus, normalisés, intégrés, documentés et mis en œuvre. Tout risque de sécurité est géré en tenant compte des répercussions sur l'ensemble du gouvernement.

4. Mission

La raison d'être de la gouvernance en matière de sécurité de l'information gouvernementale est de protéger l'information gouvernementale, soit d'assurer sa disponibilité et de préserver son caractère confidentiel et son intégrité. Elle vise à maintenir et à accroître la confiance des citoyens à l'égard de l'État et des services publics, en appliquant une gestion optimale des risques en sécurité de l'information.

L'encadrement de la sécurité de l'information gouvernementale s'effectue, d'une part, par le dirigeant principal de l'information (DPI), qui coordonne la mise en œuvre et le suivi des mesures d'encadrement auprès des organismes publics, et, d'autre part, par ces derniers, qui ont la responsabilité d'appliquer ces mesures.

2. Le terme « organisme public » est utilisé pour désigner les ministères et organisme, budgétaires et autres que budgétaires, ainsi que les organisations du réseau de l'éducation, du réseau de l'enseignement supérieur et du réseau de la santé et des services sociaux.
3. Le risque de sécurité de l'information à portée gouvernementale se définit comme étant le risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services fournis par d'autres organismes publics.
4. L'incident de sécurité de l'information à portée gouvernementale se définit comme étant une conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale nécessitant une intervention concertée sur le plan gouvernemental.

5. Cibles visées

La présente section fixe les cibles à atteindre pour les dix prochaines années.

5.1 Gouvernance

Le gouvernement du Québec vise, au bout de dix ans, l'instauration d'un modèle de gouvernance dynamique, favorisant la concertation et permettant de tirer parti de la complémentarité des ressources et des actions. L'adoption de ce modèle exige donc la mise en œuvre d'une approche collaborative, complémentaire et mutuellement fructueuse entre les organismes publics, compte tenu du fait que tout maillon faible dans la chaîne des mécanismes gouvernementaux de sécurité de l'information constitue une vulnérabilité pour l'ensemble des organismes publics.

Le gouvernement du Québec encourage également l'innovation et l'échange des façons de faire, afin de rehausser, à un niveau acceptable, la maturité des organismes publics en matière de sécurité de l'information. Il élargit la concertation en matière de sécurité de l'information à l'ensemble des organismes publics, aux entreprises du gouvernement, aux institutions financières et aux entreprises privées.

Le gouvernement du Québec s'assure de l'application du modèle préconisé, en orchestrant les efforts visant à améliorer les façons de faire et, par conséquent, à instaurer une culture de sécurité de l'information au sein de l'administration publique. Il intervient auprès d'un organisme public lorsque celui-ci ne remplit pas ses obligations en vertu de la Directive sur la sécurité de l'information gouvernementale ou lorsqu'un risque de sécurité de l'information à portée gouvernementale n'est pas adéquatement géré.

De plus, le gouvernement du Québec examine les possibilités de mise en commun des services de sécurité de l'information et en détermine les composantes ainsi que les procédures et les règles de gestion associées.

Le gouvernement du Québec cible également l'étude de nouvelles initiatives législatives, en s'appuyant sur un travail concerté avec d'autres partenaires. Il révise les lois et les règlements actuels ou examine les obstacles à leur application, et ce, dans une perspective de réduction des menaces de sécurité de l'information, particulièrement celles en provenance d'Internet.

Par ailleurs, le gouvernement vise, conformément au modèle préconisé, l'imputabilité des organismes publics, autant dans la prise en charge des exigences de sécurité de l'information relevant de leur autorité que dans leur contribution aux actions gouvernementales en la matière. Dans cette perspective, tous les organismes publics auront à mettre en place les éléments de gouvernance en matière de sécurité de l'information qui leur sont propres. Il s'agit notamment

de la définition des valeurs organisationnelles et des orientations internes, du partage des responsabilités au sein de leur organisation, de la conformité des actions posées en matière de sécurité de l'information avec les orientations gouvernementales, de la définition des mesures de performance, de l'adoption des meilleures pratiques en la matière et de la contribution au processus gouvernemental de concertation et de reddition de comptes.

5.2 Cybersécurité

La cybersécurité est considérée par les experts en sécurité de l'information comme étant le plus grand défi du 21e siècle. À cet égard, plusieurs pays lui allouent d'importants budgets et lui consacrent de nombreuses structures, démontrant ainsi leur engagement en la matière. Cet engagement se justifie par la métamorphose continuelle et rapide des cybermenaces, par leur virulence et par la gravité des conséquences imputables aux cyberattaques.

Le gouvernement du Québec détermine donc des orientations et des objectifs stratégiques en matière de cybersécurité. Ceux-ci permettent, d'une part, de canaliser et de structurer les efforts des principaux intervenants gouvernementaux dans ce domaine et, d'autre part, de mettre en place une veille continue de l'évolution des menaces et des vulnérabilités, y compris celles découlant d'un nouvel usage technologique.

Par ailleurs, le développement de la prestation électronique de services et son utilisation au quotidien par les citoyens et les entreprises exigent un environnement sécuritaire d'échanges. Le gouvernement du Québec vise à accroître la vigilance des citoyens et des entreprises à l'égard des cyberattaques, et ce, en développant des canaux de communication en vue de les conscientiser et de les sensibiliser aux risques qui en découlent. Il instaure des règles de collaboration favorisant le partage, avec les citoyens et les entreprises, de toute information pertinente permettant de contrer les menaces et de remédier aux vulnérabilités.

Le gouvernement du Québec établit également des liens de coopération avec les municipalités et les entreprises du secteur privé se positionnant en tête de file en matière d'innovation technologique et de sécurité de l'information. Ces liens favorisent le partage des connaissances sur les menaces et les vulnérabilités, ainsi que sur les meilleures pratiques à adopter en la matière. Il développe, en outre, des partenariats avec les milieux scolaires, notamment les universités et les collèges, et ce, dans la perspective de favoriser l'émergence d'une main-d'œuvre spécialisée et qualifiée permettant d'accroître et de pérenniser les compétences dans ce domaine.

En vue d'une collaboration mutuellement fructueuse, le gouvernement du Québec adhère à certaines organisations internationales partageant ses préoccupations en matière de cybersécurité ou de cybercriminalité.

5.3 Authentification

Le gouvernement du Québec vise le développement d'une offre de service combinant l'identification, l'authentification et la signature électronique. En effet, la combinaison de ces trois fonctionnalités offre une flexibilité d'utilisation aux citoyens et aux entreprises, les rassurant dans le cadre de leurs transactions électroniques et répondant à leurs besoins spécifiques.

Le gouvernement du Québec unifie, uniformise et harmonise la collecte et l'exploitation des données concernant les citoyens et les entreprises. Il rend ainsi plus facile, plus rapide et plus sécuritaire l'accessibilité des citoyens et des entreprises à l'information. De même, chaque citoyen ou entreprise se voit offrir un identifiant unique permettant à la fois son identification et son authentification.

Le gouvernement du Québec assure la promotion de la mobilité des services gouvernementaux d'authentification. Il examine, à cet égard, les possibilités de coopération entre divers paliers de gouvernement (fédéral, provincial ou municipal) afin de mettre en place des mécanismes permettant une reconnaissance mutuelle des services d'authentification existants.

Par ailleurs, les organisations ont souvent recours, dans la plupart de leurs secteurs d'activité, à l'externalisation. Cette démarche répond à un besoin d'optimisation et de gestion efficace et efficiente des ressources gouvernementales. La maturité et le savoir-faire du secteur privé en matière d'authentification constituent un levier efficace pour la réalisation des objectifs gouvernementaux en la matière. Ainsi, le gouvernement du Québec examine la possibilité de recourir au secteur privé, tout en misant sur la qualité de services aux citoyens et aux entreprises et en préservant la maîtrise et le contrôle permanent de l'offre de service gouvernementale.

5.4 Sensibilisation et formation

Le gouvernement du Québec consolide la culture de sécurité de l'information au sein de l'Administration publique par des actions de sensibilisation à cet égard, à tous les échelons des organismes publics.

Les sous-ministres ou les dirigeants d'organismes, en tant que premiers responsables de la sécurité de l'information relevant de leur autorité, s'assurent de la prise en charge de la sécurité de l'information dans leur organisation. L'information est ainsi considérée à sa juste valeur et sa sécurité est prise en compte au quotidien par les employés de l'État. Ces derniers, en tant que principal maillon de la chaîne de protection, sont conscients des risques de sécurité de l'information auxquels ils sont exposés et s'approprient les meilleures façons de se prémunir contre eux, plus particulièrement en ce qui concerne l'utilisation des nouvelles technologies.

Cette sensibilisation des employés de l'État vise tout autant les citoyens que les entreprises. Pour une meilleure protection de l'information, en particulier des données confidentielles ou sensibles, les citoyens et les entreprises contribuent à la prise de conscience collective des menaces et des vulnérabilités. Ainsi, ils se sentiront concernés et sauront agir, de façon conséquente, en étant vigilants et attentifs envers tout ce qui sort de la normalité.

En tant qu'instigateur de la sécurité de l'information au Québec et dans sa volonté de résorber la pénurie de main-d'œuvre spécialisée, le gouvernement favorise les échanges d'expertises et s'assure des conditions adéquates pour le développement des compétences en la matière. À ce titre, il vise l'élaboration de profils d'emplois et de compétences dans le domaine de la sécurité de l'information, telles l'architecture, la normalisation, l'authentification ou la gouvernance.

Le gouvernement du Québec cible également la mise en place de formations adaptées aux différents intervenants en sécurité de l'information au sein de l'administration publique. Les intervenants ainsi formés pourront répondre aux besoins en matière de sécurité de l'information de leur organisation. De plus, ces formations seront revues, à la faveur d'ententes de partenariat avec des universités, des collèges ou des instituts de recherche.

5.5 Gestion des risques de sécurité de l'information

D'ici dix ans, le gouvernement du Québec instaurera un modèle de gestion des risques de sécurité de l'information qui ira au-delà des façons de faire traditionnelles. Ces dernières sont actuellement limitées au traitement d'un risque au sein d'un organisme public, sans nécessairement se préoccuper outre mesure de ses répercussions sur d'autres entités gouvernementales. Le modèle préconisé vise donc à instaurer une approche de gestion des risques de sécurité de l'information qui serait collaborative, complémentaire et mutuellement fructueuse entre les organismes publics.

Dans cette perspective et dans un même horizon, les organismes publics auront à mettre en place, de façon formelle, un processus unifié intégrant la gestion des risques à portée gouvernementale et la gestion des risques à portée sectorielle. Ce processus intégrera également les mécanismes permettant la reddition de comptes et la concertation avec d'autres organismes publics.

Tous les organismes publics devront donc mettre en place un processus interne d'identification, de traitement et de suivi des risques auxquels est exposée l'information relevant de leur autorité. Un tel processus doit être officialisé et prendre appui sur la connaissance des différentes menaces et de leur impact potentiel sur l'organisation.

Par ailleurs, le gouvernement du Québec instaure une plateforme gouvernementale d'échange et de partage de connaissances sur les risques de sécurité de l'information. Celle-ci contribue à l'amélioration des façons de faire des organismes publics à l'égard des risques et permet, entre autres, une réflexion dynamique sur les risques émergents de sécurité de l'information.

De même, il établit les liens nécessaires entre le processus gouvernemental de gestion des risques et le processus gouvernemental de gestion des incidents. Ces liens assurent une continuité dans la prise en charge d'un risque qui pourrait dégénérer en incident de sécurité de l'information.

Au bout de dix ans, le gouvernement du Québec disposera d'une cartographie des interdépendances entre les processus d'affaires critiques de l'Administration gouvernementale. Celle-ci facilitera l'analyse des conséquences qu'un risque pourrait avoir sur d'autres organismes publics.

5.6 Niveau de maturité

Au cours de la prochaine décennie, les organismes publics devront atteindre un niveau de maturité adéquat au regard de leurs enjeux en sécurité de l'information. Ainsi, normalement, ils se seront approprié les pratiques de sécurité de l'information et les auront mises en œuvre, conformément à leur contexte organisationnel et aux risques de sécurité de l'information qui leur sont propres. Ils auront également normalisé, intégré, documenté et implantés les principaux processus de sécurité de l'information, dont ceux portant sur les incidents, les risques, la disponibilité et l'accès à l'information.

En matière de gestion des incidents de sécurité de l'information, les organismes publics auront à mettre en œuvre les étapes de prévention, de réaction et de rétablissement par rapport à la situation. Ces étapes s'inscrivent dans une perspective de renforcement des mécanismes d'atténuation des risques et assurent, advenant un incident, que les actions appropriées sont posées à tous les niveaux de l'organisation.

Concernant la disponibilité de l'information gouvernementale, les organismes publics devront s'assurer que la personne autorisée a accès à l'information en temps voulu et de la façon appropriée.

Pour ce qui est de l'accès à l'information, des droits d'accès et des privilèges spéciaux seront instaurés de façon formelle par les organismes publics. Ces droits et ces privilèges seront périodiquement révisés afin de tenir compte de la sensibilité de l'information et du mouvement de personnel interne ou externe.

Les organismes publics auront à définir une architecture visant à formaliser leur vision de la sécurité de l'information qui s'inscrit dans une architecture d'entreprise de l'organisation. Ils devront également s'assurer de l'adéquation des mesures de sécurité en vigueur par rapport aux risques encourus.

6. Réduction de l'écart par rapport aux cibles

La présente section constitue une étape visant à formaliser les exigences de sécurité de l'information à l'endroit des organismes publics. Une fois que ces derniers y auront souscrit et qu'ils auront mis en place les mécanismes permettant d'y répondre, ces exigences auront alors contribué, d'une part, à la mise en place d'une base minimale de sécurité de l'information et, d'autre part, à la réduction, sur une période de trois ans, de l'écart entre les cibles identifiées à la section précédente et l'état de situation actuel en matière de sécurité de l'information. Ces exigences sont formalisées au moyen de quatre documents structurants, dont la présente approche stratégique.

6.1 Présentation des documents structurants

L'approche stratégique permet d'asseoir la vision gouvernementale et de définir les objectifs stratégiques pour les trois prochaines années. La mise en œuvre de ces objectifs est appuyée par trois autres documents structurants :

- Une nouvelle directive sur la sécurité de l'information gouvernementale sera proposée en remplacement de la directive actuellement en vigueur depuis 2006. En énonçant des obligations de haut niveau à l'égard des organismes publics, cette nouvelle directive renforce l'encadrement de la sécurité de l'information gouvernementale, contribuant ainsi à l'atteinte des cibles fixées dans le cadre de l'approche stratégique. Elle contribue également à l'instauration d'une gestion optimale du risque d'atteinte à l'information gouvernementale et à l'accroissement de la confiance des citoyens et des entreprises quant à la sécurité de l'information qu'ils confient à l'État.
- Un cadre gouvernemental de gestion de la sécurité de l'information. Celui-ci sert de complément aux dispositions de la nouvelle directive, en précisant l'organisation fonctionnelle de la sécurité de l'information au sein de l'appareil gouvernemental ainsi que les rôles et responsabilités en la matière. Il sert également à définir et à préciser les mandats de divers comités et tables de concertation soutenant les travaux gouvernementaux en matière de sécurité de l'information.
- Un cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information. Ce cadre présente une approche novatrice de gestion des risques et des incidents susceptibles de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peuvent avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux en matière de la protection des renseignements personnels qui les concernent et de respect de leur vie privée,

sur l'image du gouvernement, ou sur la prestation de services fournie par d'autres organismes publics.

6.2 Approche stratégique 2014-2017

Afin de tendre vers l'atteinte des cibles visées pour les dix prochaines années, l'approche stratégique triennale de sécurité de l'information détermine, pour la période 2014-2017, les actions à poser, exprimées sous forme d'exigences, autant à l'endroit des organismes publics que sur le plan gouvernemental. À cette fin, la présente approche identifie les enjeux de sécurité de l'information, détermine les orientations gouvernementales en la matière et définit les objectifs et les cibles à atteindre pour les trois prochaines années.

6.2.1 Exigences sur le plan gouvernemental

Les exigences sur le plan gouvernemental se traduisent par l'adoption et la mise en œuvre d'une stratégie gouvernementale de cybersécurité, d'un processus gouvernemental de gestion des incidents et d'un cadre de gestion des risques et des incidents à portée gouvernementale. Elles se traduisent également par des travaux visant à soutenir les organismes publics dans la prise en charge des exigences de sécurité de l'information. Ces travaux auront comme principal objectif de mettre à la disposition des organismes publics des standards, des outils et des guides des meilleures pratiques en matière de sécurité de l'information.

Les travaux en matière de gestion des risques viendront en appui aux organismes publics pour la conception et la mise en œuvre d'un processus unifié de gestion des risques, intégrant ceux qui sont à portée sectorielle et ceux qui sont à portée gouvernementale. Ils établiront les liens nécessaires avec le processus ministériel ou gouvernemental de gestion des incidents. Ils porteront également sur diverses pratiques recommandées en matière de gestion des risques.

En ce qui concerne la gestion des incidents de sécurité de l'information, les travaux faciliteront la conception et la mise en œuvre d'un processus sectoriel de gestion des incidents ainsi que ses interactions avec un processus gouvernemental en la matière. Ils seront réalisés en fonction des pratiques recommandées aux différentes étapes du processus, comprenant le chiffrement, l'analyse des vulnérabilités ou la détection d'intrusions.

Quant à la gestion de l'accès à l'information, les travaux porteront sur les étapes favorisant une gestion efficace de l'accès à l'information, physiquement, à son lieu d'entreposage, ou logiquement, par l'entremise des technologies de l'information. Ils auront également comme objectif de guider les organismes publics dans le cadre de diverses actions à poser relativement au cycle de vie de l'information, à la sensibilité de l'information et au mouvement du personnel à qui des droits et des privilèges ont été attribués.

En matière de gestion de la disponibilité de l'information, les travaux porteront sur les pratiques à adopter par les organismes publics en vue de permettre l'accessibilité de l'information en temps voulu et de la manière requise par une personne autorisée. Ces pratiques, y compris la mise en place d'un plan de secours informatique ou de sauvegarde des données, devront s'inscrire dans un processus global de gestion de la continuité de l'organisation.

Pour le volet de l'architecture de sécurité de l'information, les travaux porteront sur un modèle d'architecture de sécurité de l'information que les organismes publics pourront adapter à leur contexte. Ce modèle s'inscrira aussi bien dans l'architecture d'entreprise de l'organisation que dans l'architecture d'entreprise gouvernementale.

En ce qui concerne l'audit de sécurité de l'information et le test d'intrusion et de vulnérabilité, les travaux serviront à mettre à la disposition des organismes publics des procédés d'autoévaluation de l'adéquation des mesures de sécurité par rapport aux risques encourus. Ils contribueront également à leur fournir un service d'accompagnement à cet égard.

En matière de formation et de sensibilisation, les travaux auront comme objectif de faciliter l'élaboration et la mise en œuvre d'un programme de formation ou de sensibilisation en sécurité de l'information. Ils permettront aux organismes publics de s'approprier les pratiques et les outils nécessaires, qu'ils pourront adapter à leurs besoins. Il peut s'agir, par exemple, de profils d'emplois, d'outils de sensibilisation ou de modes d'apprentissage.

De plus, un programme gouvernemental de formation à l'intention des employés de l'État sera élaboré et mis en œuvre ; alors que la campagne sur la sécurité de l'information et la protection des renseignements personnels se poursuivra. À cela s'ajoutent des études de positionnement portant, notamment, sur l'évolution de l'infrastructure à clés publiques gouvernementale (ICPG), l'authentification au moyen de procédés biométriques, la centralisation d'une source d'information unique permettant l'authentification des citoyens et des entreprises, l'externalisation de l'offre de service d'authentification, l'intégration de l'identification, l'authentification, la signature électronique et l'impact de l'utilisation des technologies émergentes sur la sécurité de l'information gouvernementale.

6.2.2 Exigences à l'endroit des organismes publics

Pour la prise en charge des exigences de sécurité de l'information, les organismes publics prendront appui sur les orientations et les meilleures pratiques gouvernementales en matière de sécurité de l'information.

Ainsi, sur le plan de la gouvernance de la sécurité de l'information, les organismes publics auront à mettre en place une politique et un cadre de gestion de la sécurité de l'information et devront s'assurer de leur mise à jour et de leur application. De

plus, ils auront à désigner les principaux intervenants en sécurité de l'information et à contribuer aux activités gouvernementales de concertation.

En matière de gestion des incidents, les organismes publics participeront activement au réseau d'alerte gouvernemental.

Pour ce qui est de l'authentification, les organismes publics contribueront à l'accroissement de l'utilisation des offres de service d'authentification gouvernementale.

Sur le plan de la sensibilisation et de la formation en sécurité de l'information, les organismes publics élaboreront et mettront en place un plan de sensibilisation et un programme formel de formation à l'intention de l'ensemble de leur personnel. Les sessions de formation seront adaptées à différents types d'intervenants et porteront tout particulièrement sur les meilleures pratiques en matière de sécurité de l'information.

En ce qui concerne la gestion des risques de sécurité de l'information, les organismes publics identifieront les actifs critiques et mettront en place les mesures de contingence associées.

Quant aux pratiques de sécurité de l'information, les organismes publics définiront et mettront en place des processus formels de sécurité de l'information portant sur la gestion des risques, de l'accès à l'information et des incidents de sécurité de l'information. Ils appliqueront également les meilleures pratiques à utiliser pour l'intégration des clauses contractuelles de sécurité de l'information dans les ententes et les contrats, la mise en place d'un registre d'autorité, l'adoption d'une architecture de sécurité de l'information et l'utilisation sécuritaire des médias sociaux.

Pour obtenir davantage de détails concernant les objectifs et les cibles à l'égard de ces exigences, consultez la section 7.

6.3 Nouvelle directive sur la sécurité de l'information gouvernementale

La nouvelle directive proposée sur la sécurité de l'information gouvernementale tient compte des cibles fixées à la section 5 et comportera de nouvelles obligations sur les plans gouvernemental et sectoriel.

6.3.1 Obligations sur le plan gouvernemental

En matière de gouvernance de la sécurité de l'information, le DPI proposera au Conseil du trésor des approches stratégiques et un cadre gouvernemental de gestion de la sécurité de l'information. De plus, le DPI produira, de concert avec les organismes publics, un rapport annuel sur l'état de situation gouvernemental en matière de gestion de la sécurité de l'information. Par ailleurs, le DPI interviendra

auprès de tout organisme public qui ne se conformera pas à ses obligations en vertu de la directive ou qui ne procédera pas à la gestion adéquate d'un risque de sécurité de l'information à portée gouvernementale.

Pour ce qui est de la gestion des incidents, le CERT/AQ contribuera à l'élaboration d'un processus gouvernemental de gestion des incidents et en assurera la mise en œuvre. Il présentera au DPI, en collaboration avec le ministère de la Sécurité publique (MSP) et la Sûreté du Québec (SQ), un rapport annuel sur les incidents de sécurité de l'information à portée gouvernementale.

En matière de services communs de sécurité de l'information, y compris l'authentification, le DPI proposera des services communs de sécurité de l'information à rendre obligatoires pour les organismes publics. Il en définira les règles de gestion et d'utilisation associées et en identifiera les détenteurs.

Par ailleurs, le DPI présentera annuellement, au Conseil du trésor, un rapport sur les risques de sécurité de l'information à portée gouvernementale.

6.3.2 Obligations à l'endroit des organismes publics

En matière de gouvernance de la sécurité de l'information, les dirigeants d'organismes publics adopteront et mettront en œuvre une politique et un cadre de gestion de la sécurité de l'information au sein de leur organisation. Ils devront également présenter au DPI, tous les deux ans, un plan d'action et un bilan de sécurité de l'information, conformément aux modalités et aux formats fixés par ce dernier. De plus, ils devront désigner leurs principaux intervenants en sécurité de l'information.

Sur le plan de la gestion des incidents, les organismes publics devront déclarer au CERT/AQ les incidents de sécurité de l'information à portée gouvernementale.

En ce qui concerne les services communs de sécurité de l'information, y compris l'authentification, les organismes publics devront utiliser ces services, à moins de démontrer l'existence de circonstances exceptionnelles qui feraient en sorte qu'ils n'auraient pas à se conformer à cette obligation ou à moins qu'un service commun ne réponde pas à leurs préoccupations d'efficience et d'efficacité.

De plus, les organismes publics devront déclarer au DPI les risques de sécurité de l'information à portée gouvernementale.

En matière de pratiques de sécurité de l'information, les organismes publics définiront et mettront en place, de façon formelle, les processus majeurs de sécurité de l'information. Ces processus porteront principalement sur la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents de sécurité de l'information.

6.4 Cadre gouvernemental de gestion de la sécurité de l'information

L'atteinte des cibles fixées pour la prochaine décennie nécessite la définition d'une vision commune de la sécurité de l'information gouvernementale, appuyée par une coordination et une cohérence des interventions en la matière.

Le cadre gouvernemental de gestion de la sécurité de l'information répond à cet objectif, en misant sur la mise en place d'une structure organisationnelle adéquate et sur la définition des rôles et responsabilités sur les plans gouvernemental et sectoriel.

6.4.1 Rôles et responsabilités sur le plan gouvernemental

En ce qui concerne la gouvernance de la sécurité de l'information, le rôle du DPI sera renforcé afin qu'il puisse assurer une coordination efficiente et efficace de la mise en œuvre et du suivi des politiques et des orientations gouvernementales en la matière. À ce titre, il mettra en place les entités de coordination et de concertation et en établira les règles de fonctionnement afférentes. Il agira à titre de détenteur du registre des responsables organisationnels de la sécurité de l'information désignés par les organismes publics. Il apportera également le soutien nécessaire aux organismes publics, notamment au regard de la conformité à la Directive sur la sécurité de l'information gouvernementale.

Quant à la cybersécurité, l'Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale (EIMSIG), créée en 2010 sous la forme d'un partenariat entre le MSP, la SQ et le CERT/AQ, contribuera aux actions gouvernementales de veille et de partage des connaissances sur les menaces et les vulnérabilités. Elle soutiendra le CERT/AQ dans le cadre de la mise en œuvre du processus de gestion des incidents à portée gouvernementale.

En matière de sensibilisation et de formation en sécurité de l'information, le DPI élaborera et mettra en œuvre, de concert avec le Centre de services partagés du Québec, un programme gouvernemental de formation en sécurité de l'information à l'intention du personnel des organismes publics. De plus, il élaborera et tiendra à jour une base de connaissances sur les pratiques de sécurité de l'information d'intérêt pour les organismes publics.

De plus, le DPI élaborera un cadre gouvernemental de gestion des risques et des incidents de sécurité de l'information et en assurera la mise en œuvre.

En matière de pratiques de sécurité de l'information, le DPI sera chargé d'élaborer et de diffuser des documents de référence gouvernementale ayant comme objectif de soutenir les organismes publics dans la prise en charge des exigences de sécurité de l'information. Il assurera, à cet égard, la réalisation, la mise à jour et la diffusion de modèles, de guides et de pratiques en matère de sécurité de l'information.

6.4.2 Rôles et responsabilités sur le plan sectoriel

Sur le plan de la gouvernance de la sécurité de l'information, l'organisme public adoptera et mettra en œuvre une politique et un cadre de gestion de la sécurité de l'information ; il en assurera également l'application. Pour l'aider dans l'exercice de ses fonctions, il se dotera d'un personnel qualifié sur les plans stratégique, tactique et opérationnel. La personne désignée pour le volet stratégique jouera le rôle de porte-parole du DPI auprès de son organisation et lui fera part des orientations et des priorités d'intervention gouvernementales en sécurité de l'information.

En matière de gestion des incidents, l'organisme public devra être représenté, auprès du réseau d'alerte gouvernemental, par une personne responsable de la coordination de la gestion des incidents. Celle-ci aura pour rôle de coordonner une équipe de réponse aux incidents de sécurité de l'information au sein de son organisation et de mettre en œuvre les stratégies de réaction appropriées.

De plus, l'organisme public se dotera d'un programme formel et continu de formation et de sensibilisation de son personnel.

En ce qui concerne la gestion des risques, l'organisme public assurera la mise en place de mesures permettant de réduire les risques de sécurité de l'information à un niveau acceptable pour l'organisation. Il désignera les détenteurs de l'information qui devront s'assurer de l'adéquation de ces mesures par rapport aux risques encourus et contribuera à la mise en œuvre du cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information.

En ce qui concerne les pratiques de sécurité de l'information, l'organisme public aura à définir et à mettre en œuvre, de façon formelle les processus majeurs et les meilleures pratiques de sécurité de l'information.

6.5 Cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information

La mise en œuvre de ce cadre s'appuie sur un processus gouvernemental de gestion des risques et des incidents susceptibles d'avoir des répercussions à l'échelle gouvernementale. Ce cadre apporte aux processus ministériels de gestion des risques de sécurité de l'information un niveau additionnel de gouvernance, qui se traduit par un ensemble d'exigences sur les plans gouvernemental et sectoriel.

6.5.1 Exigences sur le plan gouvernemental

Le concept de risque à portée gouvernementale sera défini et une approche d'identification et de suivi de son traitement sera préconisée. Cette approche permettra d'assurer la prise en charge de cette catégorie de risques par les organismes publics et d'intervenir lorsque les mesures d'atténuation à leur égard sont inadéquates.

Annuellement, un rapport sur les risques à portée gouvernementale en matière de sécurité de l'information sera élaboré et présenté au Conseil du trésor.

6.5.2 Exigences à l'endroit des organismes publics

Un processus formel de gestion des risques en sécurité de l'information sera mis en place par les organismes publics, particulièrement ceux qui sont fortement exposés aux risques. Un tel processus intégrera l'identification des actifs critiques, les risques de sécurité de l'information auxquels ils sont exposés et les mesures d'atténuation correspondantes.

En vue d'une meilleure prise en charge des risques à portée gouvernementale, les organismes publics devront améliorer leurs façons de faire, en adoptant une approche collaborative avec d'autres entités gouvernementales. Ils devront également intégrer, à leur processus interne de gestion de risques, la prise en charge des risques à portée gouvernementale.

Les organismes publics devront déclarer systématiquement les risques à portée gouvernementale inhérents à leurs processus d'affaires et suivre les recommandations du DPI quant à leur traitement.

7. Objectifs stratégiques

La présente section détermine les enjeux et les orientations gouvernementales ainsi que les cibles fixées à l'endroit des organismes publics de grande taille (1 000 employés et plus), de taille moyenne (de 200 à 999 employés) et de petite taille (moins de 200 employés).

Il est à noter que les organismes publics fortement exposés aux risques de sécurité de l'information sont soumis à des exigences plus élevées pour ce qui est des objectifs et des délais de réalisation, puisqu'ils dépendent fortement de leurs ressources informationnelles pour réaliser leur mission, fournissent une importante prestation électronique de services et détiennent de l'information critique ou des renseignements personnels.

7.1 Enjeu 1 : Un encadrement fort et intégré de la sécurité de l'information dans l'Administration gouvernementale

Un encadrement fort et intégré de la sécurité de l'information est déterminant pour assurer la cohérence et la coordination des interventions à tous les niveaux de l'Administration gouvernementale. L'adoption et la mise en œuvre d'une politique et d'un cadre de gestion de la sécurité de l'information ainsi que la formalisation des processus et la conformité aux meilleures pratiques en la matière permettent de répondre efficacement à cet enjeu.

7.1.1 Orientation 1 : Renforcer l'encadrement de la sécurité de l'information

Un encadrement adéquat de la sécurité de l'information passe nécessairement par une définition claire des valeurs organisationnelles et des orientations internes. Il passe également par la définition d'une structure organisationnelle où les rôles et les responsabilités sont précisés à tous les niveaux de l'organisation et par une gestion rigoureuse des risques, particulièrement ceux dont les effets sont préjudiciables pour une prestation de services indispensable à la population, pour la vie, la santé ou le bien-être des citoyens ou pour l'image du gouvernement.

Objectif 1.1 : Gérer efficacement la sécurité de l'information gouvernementale

Indicateur	Cible
Taux d'organismes publics ayant adopté une politique et un cadre de gestion de la sécurité de l'information	100 % des organismes publics, d'ici le 31 mars 2015
Taux d'organismes publics ayant désigné leurs principaux intervenants en sécurité de l'information (responsable organisationnel de la sécurité de l'information et coordonnateur organisationnel de gestion des incidents)	100 % des organismes publics, d'ici le 31 mars 2015
Taux de participation de chacun des organismes publics invités à participer aux activités gouvernementales de concertation	65 % annuellement, pour chacun des organismes publics

Objectif 1.2 : Évaluer les risques à portée gouvernementale

Indicateur	Cible
Taux d'organismes publics ayant identifié leurs actifs critiques	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des autres organismes publics, d'ici le 31 mars 2016
Taux d'actifs critiques identifiés pour lesquels des mesures de contingence sont mises en place	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des autres organismes publics, d'ici le 31 mars 2016

7.1.2 Orientation 2 : Atteindre un niveau de maturité adéquat en sécurité de l'information

Un niveau de maturité en sécurité de l'information convenable pour une organisation est atteint, notamment, lorsque ses processus de sécurité de l'information sont normalisés, intégrés, documentés et mis en œuvre et lorsque l'information qu'elle détient est sécurisée, conformément aux meilleures pratiques de sécurité de l'information. Au gouvernement du Québec, un tel niveau devra être atteint par les organismes publics, en particulier ceux de grande taille et ceux qui sont fortement exposés aux risques.

Objectif 2.1 : Mettre en œuvre des processus formels de gestion de la sécurité de l'information

Indicateur	Cible
Taux d'organismes publics ayant mis en œuvre un processus formel de gestion des risques de sécurité de l'information	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des organismes publics de grande taille, d'ici le 31 mars 2016 100 % des autres organismes publics, d'ici le 31 mars 2017
Taux d'organismes publics ayant mis en œuvre un processus formel de gestion des incidents	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des organismes publics de grande taille, d'ici le 31 mars 2016 100 % des autres organismes publics, d'ici le 31 mars 2017
Taux d'organismes publics ayant mis en œuvre un processus formel de gestion de l'accès à l'information	75 % des organismes publics de grande taille et 25 % des organismes publics de taille moyenne, d'ici le 31 mars 2015 100 % des organismes publics de grande taille, 75 % des organismes publics de taille moyenne et 50 % des organismes publics de petite taille, d'ici le 31 mars 2016 100 % des autres organismes publics, d'ici le 31 mars 2017

Objectif 2.2 : Se conformer aux meilleures pratiques de sécurité de l'information

Indicateur	Cible
Taux d'organismes publics ayant intégré les clauses contractuelles de sécurité de l'information dans leurs ententes ou leurs contrats	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des organismes publics de grande taille, d'ici le 31 mars 2016 100 % des autres organismes publics, d'ici le 31 mars 2017
Taux d'organismes publics ayant effectué un audit en sécurité de l'information au cours des deux dernières années	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des organismes publics de grande taille, d'ici le 31 mars 2016 100 % des autres organismes publics, d'ici le 31 mars 2017

Indicateur	Cible
Taux d'organismes publics qui effectuent, annuellement, des tests d'intrusion et de vulnérabilité en sécurité de l'information	100 % des organismes publics fortement exposés aux risques et des organismes publics de grande taille, d'ici le 31 mars 2015 75 % des organismes publics de taille moyenne et 50 % des organismes publics de petite taille, d'ici le 31 mars 2016 100 % des autres organismes publics, d'ici le 31 mars 2017
Taux d'organismes publics ayant mis en place un registre d'autorité	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des organismes publics de grande taille, d'ici le 31 mars 2016 100 % des autres organismes publics, d'ici le 31 mars 2017
Taux d'organismes publics ayant adopté une architecture de sécurité de l'information	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des organismes publics de grande taille, d'ici le 31 mars 2016 100 % des organismes publics, d'ici le 31 mars 2017

7.2 Enjeu 2 : Des citoyens confiants et protégés quant à l'utilisation des prestations électroniques de services gouvernementaux

Les attaques informatiques, de plus en plus diversifiées, sophistiquées et difficiles à contrer, représentent un facteur qui pourrait nuire à une saine utilisation d'Internet et à l'établissement d'un lien de confiance des citoyens à l'endroit de la prestation électronique de services publics. De ce fait, le gouvernement du Québec privilégie le renforcement de la cybersécurité et le développement de l'offre de service d'authentification gouvernementale des citoyens lorsqu'ils transigent électroniquement avec l'État.

7.2.1 Orientation 3 : Renforcer la cybersécurité

Le renforcement de la cybersécurité sur le plan sectoriel se traduit par la participation des organismes publics au réseau d'alerte gouvernemental, ce qui permettra d'assurer le maintien d'un état d'alerte optimal pour contrer les nouvelles menaces de sécurité de l'information et de coordonner la réaction des organismes publics aux incidents à portée gouvernementale.

Objectif 3.1 : Participer activement au réseau d'alerte gouvernemental

Indicateur	Cible
Taux de participation des organismes publics au réseau d'alerte gouvernemental	100 % des organismes publics fortement exposés aux risques et des organismes publics de grande taille, d'ici le 31 mars 2015 100 % des autres organismes publics, d'ici le 31 mars 2016

7.2.2 Orientation 4 : Développer l'offre de service d'authentification gouvernementale

L'adhésion des citoyens au gouvernement en ligne est tributaire d'un accès facile et sécurisé aux services gouvernementaux. Un tel accès est possible grâce à l'utilisation des services d'authentification gouvernementale, lesquels offrent des fonctionnalités combinées d'identification, d'authentification et de signature électronique.

Les organismes publics devront contribuer à la sécurisation du gouvernement en ligne, en intégrant les services d'authentification gouvernementale dans leurs prestation électronique de services (PES) aux citoyens.

Objectif 4.1 : Augmenter l'utilisation des services d'authentification gouvernementale

Indicateur	Cible
Taux d'adhésion à clicSÉQUR	80 % des nouvelles PES transactionnelles utilisent clicSÉQUR
Taux de comptes clicSÉQUR (Citoyens et Entreprises) actifs	Augmentation de 15 % par année

7.3 Enjeu 3 : Une expertise gouvernementale disponible et confirmée en sécurité de l'information

L'encadrement de la sécurité de l'information gouvernementale et, plus particulièrement, la mise en place des meilleures pratiques reposent avant tout sur la présence d'un personnel compétent. Pour cela, le gouvernement du Québec accorde une attention particulière au développement et au maintien des compétences en sécurité de l'information, notamment dans un contexte de rareté des ressources spécialisées.

7.3.1 Orientation 5 : Développer et maintenir les compétences en sécurité de l'information

L'efficacité des mesures de sécurité déployées par une organisation est en grande partie tributaire du degré de sensibilisation du personnel quant à leur mise en œuvre. En effet, dans diverses circonstances où l'information pourrait être compromise, l'adoption des meilleures pratiques par le personnel pourrait contribuer efficacement à la protection de l'information. C'est le cas de la déclaration, dans les délais requis, d'un incident potentiel ou réel, ce qui pourrait faciliter son traitement par le déclenchement d'une réaction rapide et appropriée.

Outre la sensibilisation du personnel, les organismes publics doivent également s'assurer, par des actions de formation, que celui-ci dispose de l'expertise et du savoir-faire nécessaires à la mise en œuvre des meilleures pratiques de sécurité de l'information.

Objectif 5.1 : Sensibiliser le personnel à la sécurité de l'information

Indicateur	Cible
Taux d'organismes publics ayant mis en place un plan de sensibilisation en matière de sécurité de l'information à l'intention de l'ensemble du personnel	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des organismes publics de grande taille, d'ici le 31 mars 2016 100 % des autres organismes publics, d'ici le 31 mars 2017
Taux d'organismes publics ayant offert une première session de sensibilisation à la sécurité de l'information à l'ensemble du personnel	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des organismes publics de grande taille, d'ici le 31 mars 2016 100 % des autres organismes publics, d'ici le 31 mars 2017

Objectif 5.2 : Accroître l'expertise et le savoir-faire en sécurité de l'information

Indicateur	Cible
Taux d'organismes publics ayant mis en œuvre un programme formel de formation à l'intention de l'ensemble du personnel	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des organismes publics de grande taille, d'ici le 31 mars 2016 100 % des autres organismes publics, d'ici le 31 mars 2017
Taux des ROSI ayant suivi une formation générale en sécurité de l'information	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des organismes publics de grande taille, d'ici le 31 mars 2016 100 % des autres organismes publics, d'ici le 31 mars 2017
Taux des COGI ayant suivi une formation sur les meilleures pratiques de sécurité de l'information, dont la gestion des risques, des incidents ou de l'accès à l'information	100 % des organismes publics fortement exposés aux risques, d'ici le 31 mars 2015 100 % des organismes publics de grande taille et 50 % des organismes publics de taille moyenne et de petite taille, d'ici le 31 mars 2016 100 % des autres organismes publics, d'ici le 31 mars 2017

8. Annexe

Documents de référence gouvernementale

Modèles

- Modèle de gestion de la sécurité de l'information gouvernementale
- Modèle de gestion de la sécurité de l'information gouvernementale – Synthèse
- Modèle détaillé d'habilitation et de contrôle d'accès
- Modèle d'habilitation et de contrôle d'accès – Application de la norme XACML

Guides et pratiques

- Architecture gouvernementale de la sécurité de l'information numérique (AGSIN) – Architecture cible globale
- Architecture gouvernementale de la sécurité de l'information numérique (AGSIN) – Architecture cible globale synthèse
- Précis SCPRP[5], versions Web 1,3 et Word 1,3
- Guide de déploiement du Précis SCPRP
- Guide d'utilisation du Précis SCPRP
- Guide pour faciliter la gestion du processus SCPRP
- Guide d'évaluation de la sécurité des sites Web gouvernementaux
- Mesures de réduction du risque pour des sites Web publics
- Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité
- Pratique de vérification de la sécurité de l'information numérique
- Cadre gouvernemental d'élaboration de clauses contractuelles en matière de sécurité de l'information et de protection des renseignements personnels
- Guide d'utilisation sécuritaire des assistants numériques personnels (ANP)
- Guide d'utilisation sécuritaire des assistants numériques personnels (ANP) – Synthèse
- Guide de destruction sécuritaire de l'information
- Guide d'élaboration d'un cadre normatif ministériel de sécurité de l'information

5. SCPRP : Sécurité, contrôle et protection des renseignements personnels

- Guide sur la gestion de la continuité des services
- Guide sur la gestion des incidents de sécurité de l'information gouvernementale
- Gestion des risques – Guide d'utilisation de la méthodologie Méhari et de l'outil Risicare
- Guide de sensibilisation à la sécurité de l'information numérique et des échanges électroniques
- Modèles et domaines de confiance de la sécurité et guide de conception – Pratique recommandée
- Contenu type et guide d'élaboration d'une entente de sécurité
- Contenu type et guide d'élaboration d'une interface sécuritaire – Pratique recommandée

Juin 2014

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique