APPROCHE STRATÉGIQUE TRIENNALE 2014-2017 EN SÉCURITÉ DE L'INFORMATION GOUVERNEMENTALE

Octobre 2013

Version 1.0

UN QUÉBEC POUR TOUS

Québec

Table des matières

1 Sommaire exécutif

Le développement accéléré des technologies de l'information ainsi que l'utilisation croissante de l'Internet ont considérablement modifié les règles d'échanges 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, prise 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. Elle définit la mission du gouvernement du Québec en cette matière et détermine les éléments essentiels à la réalisation de la vision de l'encadrement de la sécurité de l'information gouvernementale.

Cette approche s'appuie sur les résultats de l'analyse des contextes interne et externe au gouvernement du Québec. Elle tient compte, d'une part, des préoccupations et des tendances de l'heure observées auprès de gouvernements précurseurs en matière de sécurité de l'information ou découlant d'études spécialisées. D'autre part, elle se base sur des constats observés à la suite d'une analyse détaillée des réalisations des dix dernières années de l'Administration gouvernementale.

L'analyse de ces contextes a permis de dégager les principaux enjeux de sécurité de l'information et, par conséquent, le positionnement gouvernemental à cet égard pour la prochaine décennie. Ce positionnement est principalement exprimé en termes de gouvernance de la sécurité de l'information, de cybersécurité, d'authentification, de gestion des risques, de formation et de sensibilisation ainsi que de pratiques de sécurité de l'information.

Pour répondre à ces enjeux, des mesures ont été identifiées pour les trois prochaines années. Celles-ci sont traduites dans quatre documents structurants dont la mise en œuvre requiert la contribution des organismes publics[2]: il s'agit de la présente approche stratégique, 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.

Enfin, la présente approche fixe les objectifs stratégiques en matière de sécurité de l'information à l'endroit des organismes publics. Ces objectifs sont accompagnés d'indicateurs permettant de mesurer la performance des organismes publics à l'égard des cibles fixées.

---

[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 e-Government Services: User-centered Approaches*, 2 octobre 2000).

[2] Le terme « organisme public » est utilisé pour désigner les ministères et les organismes, budgétaires et autres que budgétaires, ainsi que les organisations du réseau de l'Éducation, du réseau de l'Enseignement supérieur, de la Recherche, de la Science et de la Technologie 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 fournie 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 au plan gouvernemental.

2 Préambule

Plus de dix années se sont écoulées 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 de l'Internet, et au gouvernement du Québec, par une démarche de transformation de la prestation de services aux citoyens et aux entreprises. À travers ces changements, la sécurité de l'information est devenue un enjeu central et une préoccupation constante dans la livraison des services gouvernementaux.

Ainsi, la présente approche stratégique triennale, prise 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), établit la vision de la sécurité de l'information gouvernementale et précise des orientations et des objectifs qui guideront les actions des organismes publics, ainsi que des indicateurs qui permettront de mesurer l'atteinte des objectifs fixés. Elle prend appui, d'une part, sur une analyse détaillée des réalisations en matière de sécurité de l'information des dix dernières années et, d'autre part, sur les préoccupations et les tendances de l'heure en matière de sécurité de l'information communes à plusieurs gouvernements ou résultant d'études spécialisées.

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. À terme, 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 implémentés. Tout risque de sécurité est géré en tenant compte des impacts sur l'ensemble du gouvernement.

4 Mission

La raison d'être de la gouvernance en 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 renforcer la confiance des citoyens à l'égard de l'État et des services publics en réalisant 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 les mesures.

5 Tendances mondiales et bilan gouvernemental

Cette section présente les préoccupations et les tendances en matière de sécurité de l'information, communes à plusieurs gouvernements ou résultant d'études spécialisées, ainsi qu'une analyse des réalisations au plan sectoriel et gouvernemental. Elle a pour objectif de dégager les cibles ainsi que les moyens permettant de les atteindre.

5.1 Tendances mondiales (environnement externe)

Des préoccupations et des tendances sont observées auprès de gouvernements précurseurs dans le domaine de la sécurité de l'information. Celles-ci se rapportent principalement aux thématiques ayant trait à la gouvernance, à la cybersécurité, à l'authentification, à l'infrastructure à clés publiques, à la formation et à la sensibilisation, à la gestion des risques, au cadre normatif, au niveau de maturité des organisations et à l'impact des technologies émergentes.

5.1.1 Gouvernance

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[5] assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. L'ANSSI est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées. La gouvernance de l'Agence s'exerce par le biais d'un comité stratégique constitué de responsables de haut niveau de l'Administration. En matière de suivi et de reddition de comptes, des inspections locales en sécurité des systèmes d'information[6], planifiées annuellement en collaboration étroite avec des ministères sélectionnés, sont réalisées par l'ANSSI. Celles-ci sont destinées à donner, au premier ministre et aux ministres concernés, une appréciation du niveau de sécurité des systèmes d'information de l'État. Elles permettent, à l'issue d'un cycle de réalisation triennal, d'obtenir une vision globale et synthétique du niveau de sécurité de l'ensemble des ministères.

Au Royaume-Uni, le Centre de l'encadrement de la sûreté de l'information (CSIA)[7] assure la mise en œuvre de la stratégie nationale de sécurité de l'information, alors que l'Autorité technique nationale pour la sûreté de l'information (CESG)[8] développe des outils, des standards ou des guides de bonnes pratiques au niveau national. Le Bureau du Conseil des ministres reçoit, des ministères, un rapport annuel sur l'évaluation de l'application de la Politique nationale de sécurité, dont l'un des sept volets traite de la sécurité de l'information.

En Finlande, le ministère des Finances est responsable de la direction, du développement et de la coordination de la sécurité de l'information gouvernementale[9]. Il est appuyé par le Conseil de gestion en sécurité de l'information gouvernementale (VAHTI)[10]. Celui-ci assure la coordination de la mise en œuvre et du suivi des politiques et des orientations gouvernementales dans le but d'améliorer la continuité et la qualité des services gouvernementaux et d'assurer l'intégration de la sécurité de l'information au sein des activités gouvernementales.

Au Japon[11], la sécurité de l'information est assurée par le Centre national de sécurité de l'information (NISC) et le Conseil des politiques en sécurité de l'information, tous deux créés en

---

[5] http://www.ssi.gouv.fr/
[6] http://www.ssi.gouv.fr/site_rubrique8.html
[7] http://webarchive.nationalarchives.gov.uk/20080906101500/cabinetoffice.gov.uk/csia
[8] http://www.cesg.gov.uk/
[9] Government Resolution on Enhancing Information Security in Central Government - December, 1st 2009.
[10] http://www.vm.fi/vm/en/13_public_management_reforms16746/06_information_security/index.jsp
[11] http://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf

2005 et rattachés au Cabinet du Premier ministre. Dans le but de devenir le leader mondial en sécurité de l'information en 2020, le Japon a élaboré, en février 2009, une seconde stratégie nationale en la matière complétée par des plans annuels.

À Singapour, l'Autorité du développement de l'info-communication (IDA)[12] tient le rôle de dirigeant principal de l'information gouvernementale. Celui-ci, en plus d'assurer la sécurité des infrastructures critiques de l'État, élabore et diffuse des plans stratégiques, des normes et des lignes directives en matière de sécurité de l'information.

En Australie, les agences doivent réaliser annuellement un audit sur le respect des exigences de sécurité et en faire rapport au procureur général. Il est à noter qu'une autre entité centrale (AGIMO, Australian Government Information Management Office)[13] a la responsabilité de conseiller et d'assister les ministères et les organismes (MO) en matière de gestion des risques en sécurité de l'information.

Aux États-Unis, la gestion de la sécurité de l'information est régie, depuis 2002, par une loi intitulée « FISMA »[14]. Cette loi attribue au ministère de la Sécurité intérieure la coordination gouvernementale de la gestion de la sécurité de l'information. Elle assigne à l'Institut national des standards et de la technologie (NIST)[15] la responsabilité de développer des standards et des procédures visant à renforcer le niveau de sécurité des systèmes d'information des agences gouvernementales américaines. En termes de suivi, le Bureau de la gestion et du budget (OMB)[16] présente annuellement au Congrès américain les résultats des évaluations de l'application de la FISMA dans les agences gouvernementales.

Au Canada, la Direction du dirigeant principal de l'information (DDPI)[17] fournit des conseils stratégiques et de l'aide aux institutions fédérales, surveille et supervise la mise en œuvre des politiques, des directives, des normes et des lignes directrices gouvernementales de sécurité de l'information.

Les provinces canadiennes, tels la Colombie-Britannique[18], l'Alberta[19] et Terre-Neuve-et-Labrador[20], possèdent une structure de gouvernance semblable à celle du Québec et du Canada, où un DPI joue un rôle de coordonnateur central de la sécurité de l'information.

La tendance qui se dégage dans la majorité des gouvernements, précurseurs en matière de sécurité de l'information, se reflète dans la mise en place de structures centrales d'encadrement et de coordination. Celles-ci ont notamment pour mandat de s'assurer de la mise en œuvre d'une politique ou d'une stratégie nationale de sécurité de l'information, de jouer un rôle-conseil auprès des organismes publics et de mettre à leur disposition des outils, des standards et des guides de bonnes pratiques. Elles ont également pour mandat d'apprécier le niveau de sécurité des systèmes d'information et des infrastructures critiques et d'en faire rapport à l'État.

---

[12] http://www.ida.gov.sg/About%20us/20060406102431.aspx
[13] http://www.finance.gov.au/agimo/index.html
[14] FISMA : Federal Information Security Management Act. http://www.marcorsyscom.usmc.mil/sites/pmia%20documents/documents/Federal%20Information%20Security%20Management%20Act%20(FISMA).htm
[15] NIST : National Institute of Standards and Technology http://www.nist.gov/index.html
[16] OMB : Office of management and budget http://www.whitehouse.gov/omb/
[17] http://www.tbs-sct.gc.ca/sim-gsi/index-fra.asp
[18] http://www.cio.gov.bc.ca/cio/index.page
[19] Le Bureau du dirigeant principal de l'information a été établi par Service Alberta lors de l'exercice 2009-2010 : http://www.servicealberta.gov.ab.ca/pdf/annual/SA_Annual_Report_09-10.pdf
[20] http://www.ocio.gov.nl.ca/index.html

5.1.2 Cybersécurité

La cybersécurité se trouve en tête des préoccupations mondiales de sécurité de l'information, et ce, en raison de la gravité des impacts que peuvent engendrer les cyberattaques. En effet, une enquête, menée par McAfee[21] auprès de 14 pays répartis à travers le monde, estime à six millions de dollars par jour le coût lié aux cyberattaques. Elle révèle également que plus de la moitié des infrastructures dites « hautement sensibles » sont régulièrement victimes d'attaques à grande échelle ou d'infiltrations furtives de la part du crime organisé, de terroristes ou d'États, et que ces attaques peuvent même ébranler la sécurité nationale d'un pays.

Plusieurs pays situent la cybersécurité au centre de leur stratégie gouvernementale de sécurité de l'information. C'est ainsi que le Royaume-Uni, l'Australie et le Canada ont publié récemment leur propre plan de protection du cyberespace.

La stratégie britannique[22] a permis, notamment, la création, en mars 2010, de deux organismes : le Bureau de la cybersécurité (OCS) et le Centre opérationnel de cybersécurité (CSOC). L'OCS joue un rôle de leadership stratégique gouvernemental en cybersécurité, assure la cohérence des actions pour l'ensemble du gouvernement et supervise les programmes gouvernementaux prioritaires en la matière. Le CSOC veille activement à la sécurité de l'espace cybernétique, coordonne la réponse aux incidents de sécurité de l'information de l'ensemble du pays et fournit, aux citoyens et aux entreprises, une assistance et des conseils sur les risques.

La stratégie du gouvernement australien considère la cybersécurité comme une priorité pour la sécurité nationale et, à cet égard, cible son renforcement en misant sur la sensibilisation des citoyens et sur l'instauration de partenariats au plan national et international.

Quant à la stratégie du Canada[23], elle s'articule autour des axes suivants : protéger les systèmes gouvernementaux, nouer des partenariats pour protéger les cybersystèmes essentiels et aider les Canadiens à se protéger en ligne.

La tendance observée est à la mise en œuvre de stratégies de cybersécurité. Celles-ci visent à se prémunir contre les cyberattaques en misant sur la sensibilisation des citoyens, l'instauration de partenariats au plan national et international et la mise en place d'entités centrales ayant pour vocation de prodiguer assistance et conseils et de coordonner la réaction en cas d'incidents.

5.1.3 Authentification

Plusieurs initiatives dans le monde ont été prises afin de proposer aux citoyens, dans une même offre de service, les trois fonctions essentielles d'authentification : l'identification, l'authentification et la signature électronique. Ainsi, des pays comme la France, la Belgique, l'Italie, la Suède, les Émirats Arabes Unis et la Chine offrent un accès facile et sécurisé à de nombreux services administratifs relatifs à la santé[24], à l'état civil ou à l'éducation requérant une signature électronique. Ces projets ont été réalisés avec le concours du secteur privé[25].

En Europe, certains pays, à l'instar de la Finlande[26], de l'Estonie, de la Belgique[27] ou de la France[28], misent sur l'instauration de la carte nationale d'identité numérique. En remplissant les fonctions

[21] http://www.3dcommunication.fr/pdf/McAfee%200CIP%20report.pdf
[22] http://www.enisa.europa.eu/act/sr/files/country-reports/UK.pdf/view
[23] http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-fra.aspx
[24] http://fr.wikipedia.org/wiki/Carte_Vitale
[25] Gemalto, Oberthur ou Safran.
[26] http://fineid.fi/
[27] http://eid.belgium.be/fr/.
[28] http://www.interieur.gouv.fr/sections/a_votre_service/vos_demarches/carte-nationale-d-identite

d'identification, d'authentification et de signature électronique, cette carte a pour objectif d'authentifier les citoyens désirant utiliser les services en ligne du gouvernement. La compatibilité de la technologie utilisée avec plusieurs applications et systèmes d'exploitation commerciaux confère, à cette carte, une flexibilité accrue et lui permet une utilisation dans plusieurs entreprises, notamment dans le secteur financier.

Aux États-Unis, le système d'authentification « E-authentification » a été mis en place en décembre 2003 dans le but de soutenir efficacement le développement du gouvernement en ligne. Ce système s'inscrit dans le cadre de la mise en œuvre d'une circulaire[29] émise par le bureau exécutif du Président des États-Unis à l'endroit des départements et des agences gouvernementales. Celle-ci, présentée sous forme de lignes directrices, instaure les bases de l'E-authentification.

De nombreux États, dont le Canada, ont développé leur propre système d'authentification[30], conformément aux principes de l'Organisation de coopération et de développement économique (OCDE) présentés dans le rapport intitulé « *Recommandation de l'OCDE sur l'authentification électronique et Orientations pour l'authentification électronique* »[31]. Ce rapport préconise, notamment, l'instauration d'approches technologiquement neutres pour une authentification électronique efficace des personnes et des entités au plan intérieur et transfrontalier, et pour la fourniture et l'utilisation de produits et de services d'authentification intégrant de solides pratiques commerciales répondant à un besoin de sécurité et de confidentialité de l'information et encourageant la compatibilité commerciale et juridique ainsi que l'interopérabilité technique des dispositifs d'authentification.

Au Canada, le système d'authentification « ePass » est en voie de remplacement, transitoirement, par un autre système appelé « Clé d'accès ». Ce dernier offre aux MO un mécanisme d'authentification plus économique, plus souple et plus efficace.

La tendance mondiale dégage une préférence pour les technologies d'authentification forte. Ces technologies sont souvent matérialisées par un déploiement massif de cartes d'identité électroniques aux citoyens. Cette offre de service présente plusieurs fonctionnalités combinées : identification, authentification et signature électronique. Plusieurs autres fonctionnalités peuvent également être intégrées sur demande, notamment le portefeuille électronique[32]. Le déploiement de ces solutions est souvent réalisé avec le concours de firmes privées.

5.1.4 Infrastructure à clés publiques

L'infrastructure à clés publiques (ICP) est un ensemble de moyens matériels, de logiciels et de composants cryptographiques permettant de créer, de gérer, de conserver, de distribuer et de révoquer des certificats numériques. Le certificat est utilisé pour sécuriser les fichiers lors de transferts ou de stockages, pour signer numériquement des documents et des transactions financières, pour accéder en toute sécurité à des réseaux éloignés ou encore pour s'authentifier auprès d'applications sécurisées. L'ICP garantit la confidentialité et l'intégrité des transactions électroniques ainsi que la possibilité de vérifier et d'authentifier chaque entité impliquée dans ces transactions.

En Europe, c'est l'Estonie[33] qui possède la plus large infrastructure à clés publiques. Son infrastructure a été déployée en utilisant des certificats numériques sur la carte d'identité nationale

[29] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf
[30] Authentification : fonction destinée à établir la validité et l'assurance de l'identité déclarée par une entité (Source : OCDE).
[31] http://www.oecd.org/dataoecd/31/63/38924785.pdf
[32] http://www.gemalto.com/php/pr_view.php?id=465
[33] http://www.riso.ee/en/system/files/Estonian%20Information%20Society%20Strategy%202013.pdf

depuis 2002 et sur le téléphone mobile depuis février 2011. Les domaines d'utilisation des certificats touchent, notamment, l'identification des personnes sur Internet, la signature électronique, le chiffrement des données et le vote électronique. À ce jour, plus de 80 % de la population estonienne bénéficient de la carte d'identité électronique et plus de 135 millions d'utilisations ont été enregistrées pour la signature électronique et les transactions électroniques utilisant l'ICP[34].

Aux États-Unis, c'est le dirigeant principal de l'information[35] qui est chargé d'établir les standards du certificat numérique pour l'authentification de l'identité entre les organismes fédéraux ainsi qu'entre les organismes fédéraux et les organismes externes. Ainsi, depuis son adoption en 2002, l'architecture fédérale d'ICP des États-Unis continue d'évoluer afin de répondre aux besoins des organismes et de tenir compte des lois en vigueur. En 2003, une note de loi exige que les organismes fédéraux cessent le développement d'une ICP et les invite plutôt à acquérir une solution auprès d'un fournisseur commercial certifié[36]. Actuellement, il existe quatre autorités de certification.

Toujours aux États-Unis, l'application directe de l'ICP figure dans le programme USAccess[37] offrant une solution à la vérification d'identité personnelle (PIV). Elle permet aux agences du gouvernement fédéral américain d'authentifier les employés, les prestataires et les sociétés affiliées, en utilisant des cartes d'accès électroniques comportant des certificats numériques. Au 1er décembre 2010, 80 % des employés possédaient une carte USAccess leur donnant à la fois un accès physique et un accès logique aux ressources gouvernementales.

Au Canada, c'est le Bureau de la gestion des justificatifs internes, relevant du ministère des Travaux publics et Services gouvernementaux Canada, qui offre le service d'ICP pour les activités internes du gouvernement. Ce service permet notamment aux employés du gouvernement fédéral d'accéder à des applications sécurisées et de faciliter ainsi l'échange de documents protégés.

La tendance suivie par les gouvernements est au recours aux prestataires privés pour la mise en œuvre d'une solution d'ICP et pour offrir ce service aussi bien aux employés qu'aux citoyens et aux entreprises. Cette tendance est également à l'utilisation des certificats pour les téléphones mobiles.

5.1.5 Formation et sensibilisation

Dans un contexte mondial de rationalisation des moyens et de rareté des ressources spécialisées, la formation et la sensibilisation en matière de sécurité de l'information sont devenues une priorité pour de nombreux gouvernements. À l'image de l'Australie, des campagnes nationales de sensibilisation des citoyens ou des programmes de formation du personnel de l'administration publique sont inscrits dans les plans stratégiques gouvernementaux. La Finlande et Singapour, quant à eux, ont mis en œuvre des initiatives, comme la création d'associations de professionnels en sécurité de l'information et l'octroi de bourses d'études spécialisées en sécurité de l'information sous l'égide d'universités ou d'instituts de recherche.

Il ressort donc que plusieurs gouvernements partagent les mêmes préoccupations en ce qui a trait au développement des compétences des employés de l'État et à la sensibilisation des citoyens en matière de sécurité de l'information.

[34] http://www.id.ee/
[35] Chief Information Officers (CIO).
[36] http://www.idmanagement.gov/documents/RealizedValueFederalPKI.pdf
[37] http://www.fedidcard.gov/

5.1.6 Gestion des risques

La gestion des risques est un acte de gestion incontournable qui ne doit pas être perçu comme une contrainte, mais comme un défi qu'il faut constamment relever. C'est ainsi que des approches en la matière ont été adoptées par plusieurs pays.

Au Royaume-Uni[38], le département exécutif du gouvernement britannique « HM Treasury » a développé un cadre d'évaluation du risque à haut niveau. Destiné aux départements, il leur permet d'augmenter leur capacité organisationnelle à apprécier et à gérer les risques.

En Australie, le gouvernement de l'État de Victoria[39] a élaboré un cadre gouvernemental de gestion des risques, dans lequel il a clairement identifié les conséquences de certains risques qui peuvent déborder du domaine d'un organisme. Par ailleurs, la problématique de l'interdépendance de ces risques a été également abordée. Cette notion est identifiée sous le terme « risques des interagences gouvernementales et risques horizontaux »[40]. Ce cadre préconise que chaque agence produise un rapport annuel dans lequel elle certifie qu'elle dispose d'un processus de gestion des risques effectif et qu'elle est à un niveau satisfaisant. Une entité centrale supervise les activités du processus de gestion de risques en tenant à jour un registre des risques horizontaux et en apportant un soutien-conseil en la matière.

Aux États-Unis, le département de la sécurité intérieure[41] « United States Department of Homeland Security » a élaboré, en 2009, des orientations en gestion de risques mettant l'emphase sur les fonctions essentielles du secteur des technologies de l'information. De son côté, l'Institut national des standards et de la technologie[42] « National Institute of Standards and Technologies » a élaboré un cadre de référence pour l'identification des risques dans les systèmes d'information de l'Administration.

Au Canada, la Stratégie de cybersécurité[43], adoptée en 2010, confie à Sécurité publique Canada la responsabilité de coordonner, de manière centrale, l'évaluation des nouvelles menaces complexes. À cette fin, elle doit élaborer et promouvoir des approches complètes et harmonisées afin de faire face aux risques de sécurité de l'information au sein du gouvernement et partout au Canada.

Au niveau provincial, la Colombie-Britannique[44] a créé, dans sa structure administrative, une entité[45] dédiée à l'encadrement de la gestion du risque pour l'ensemble de ses organisations.

Il résulte de ces constats que la gestion des risques de sécurité de l'information est, pour plusieurs pays, un processus incontournable. Toutefois, une attention particulière est accordée au développement et à la mise en place d'un cadre d'évaluation des risques de haut niveau. Globalement, ce cadre promeut des approches complètes et harmonisées de gestion des risques de sécurité de l'information. Il met ainsi l'emphase sur les fonctions essentielles de l'État où les risques horizontaux résultant d'interdépendances entre les institutions peuvent avoir des conséquences qui débordent du domaine propre à une organisation et qui, par conséquent, finissent par affecter d'autres organisations.

---

[38] http://www.hm-treasury.gov.uk/psr_governancerisk_index.htm
[39] http://www.dtf.vic.gov.au/CA25713E0002EF43/WebObj/VicGovtRiskMgmtFramework/$File/VicGovt%20Risk%20Mgmt%20Framework.pdf
[40] Interagency and statewide risks.
[41] http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf
[42] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
[43] http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-fra.pdf
[44] http://www.fin.gov.bc.ca/pt/rmb/erm.shtml
[45] Risk Management Branch and Government Security Office.

5.1.7 Cadre normatif en matière de sécurité de l'information

La normalisation, la standardisation ainsi que la mise en place des bonnes pratiques de sécurité de l'information sont préconisées par la majorité des institutions gouvernementales.

Travaillant en partenariat étroit, la Nouvelle-Zélande et l'Australie unissent leurs efforts en vue de l'élaboration de guides de bonnes pratiques, de normes et de standards. En effet, sous ce partenariat, plusieurs travaux portant sur les bonnes pratiques de sécurité de l'information ont été élaborés et diffusés. Citons, notamment, le code de bonnes pratiques AS/NZS 18044:2006 traitant de la gestion des incidents de sécurité de l'information ou encore le guide HB 231:2004 abordant les principes fondamentaux d'implémentation d'un processus de gestion des risques de sécurité de l'information.

Les États-Unis, par le biais de l'Institut national des standards et de la technologie (NIST), tendent à développer des standards et des procédures visant à renforcer le niveau de sécurité des systèmes d'information des agences gouvernementales américaines.

L'Europe et le Royaume-Uni se distinguent dans le domaine des référentiels de sécurité de l'information par la publication des normes BS 7799. Depuis 2005, l'Organisation internationale de normalisation (ISO) a pris le relais avec la famille 27000 des normes de sécurité de l'information. Ces normes sont appuyées par les pays européens et par d'autres gouvernements de par le monde, dont le Canada et le Québec.

La tendance est donc à la conformité aux bonnes pratiques comme préconisées par les normes internationales de sécurité de l'information. Une attention particulière est toutefois accordée au volet Encadrement de la sécurité de l'information et à la mise en place de pratiques relevant de domaines particulièrement sensibles, comme la gestion des risques, la gestion des incidents ou la gestion de l'accès à l'information.

5.1.8 Niveau de maturité des organisations

En termes de niveau de maturité en matière de sécurité de l'information, une approche méthodologique[46], adoptée en 2007 par le gouvernement français, stipule qu'un niveau de maturité convenable n'est pas nécessairement le niveau le plus élevé. C'est le niveau adéquat au regard d'enjeux en sécurité de l'information des organisations, tels le niveau de conséquences potentielles en cas de sinistre, la sensibilité du patrimoine informationnel, le degré d'exposition aux menaces et l'importance des vulnérabilités.

De plus, se basant sur le modèle de maturité de la sécurité de l'information à six niveaux (de 0 à 5), développé par Gartner[47], des experts ont, en 2009, analysé l'évolution, depuis 2007, du niveau de maturité d'un large éventail de grandes organisations. Ils en ont déduit que l'atteinte d'un niveau de maturité dépasse souvent les échéanciers impartis. Le manque d'attention au développement des processus de gestion de sécurité et la tendance à considérer comme facultatifs les projets pour améliorer la maturité sont évoqués. Les experts déduisent également qu'une maturité moyenne de niveau 3 ou de niveau 4 pourrait être une cible appropriée pour ces organisations.

Une organisation se situe au niveau 3 du modèle de Gartner si ses objectifs, ses pratiques et ses mesures de performance sont définis et si les processus de sécurité de l'information sont normalisés, intégrés, documentés et implémentés. Elle se situe au niveau 4 si, de plus, la sécurité de l'information est intégrée dans toutes les opérations et dans la culture de l'organisation.

---

[46] Maturité SSI, approche méthodologique, Direction Centrale des Systèmes d'informations, France, 2007 http://www.ssi.gouv.fr/IMG/pdf/maturitessi-methode-2007-11-02.pdf

[47] Security Program Maturity Timeline Update, 2009. Gartner Inc., 2009.

5.1.9 Impacts des technologies émergentes

L'infonuagique[48], les médias sociaux[49] ou les technologies mobiles constituent des enjeux importants de sécurité de l'information. La quasi-totalité des gouvernements leur accordent un intérêt certain et étudient les meilleures approches quant à leur déploiement.

Infonuagique

Tirant profit des progrès technologiques liés à la virtualisation des serveurs informatiques, l'infonuagique semble s'installer durablement dans le paysage informatique de nombreuses organisations. En 2006, Gartner[50] prévoyait que plus de 25 % des applications utilisées en 2011 seraient des applications informatiques dématérialisées. En 2010, la firme Cloud Hypermarket team avance un taux de 29 % d'applications infonuagiques. La tendance générale quant à l'utilisation de cette technologie est en hausse constante.

Au niveau de l'administration américaine, l'infonuagique s'est imposée comme la solution adéquate, répondant à un objectif de réduction des coûts informatiques liés à la multitude de solutions souvent similaires adoptées par les différentes agences d'États. Ce revirement gouvernemental se traduit par la mise en place d'un site Web qui met, à la disposition des agences gouvernementales, différents services en technologie de l'information, des capacités informatiques (capacités de stockage ou serveurs virtuels) et des applications infonuagiques.

Au niveau du gouvernement français, dans le cadre d'un projet appelé « Grand emprunt »[51], 700 millions d'Euros seront alloués au développement des infrastructures infonuagiques, sur les 11 milliards d'Euros destinés à la recherche scientifique.

Quant aux éditeurs majeurs en informatique, ils sont de plus en plus nombreux à proposer des solutions basées sur l'infonuagique. Toutefois, une réticence majeure subsiste quant à l'adoption, par les organisations, d'une telle technologie, dont le déploiement doit être associé à une gestion rigoureuse des risques de sécurité de l'information. Afin de remédier à cet état de fait, une association formée des principaux acteurs dans ce domaine a été créée en 2009, la Cloud Security Alliance (CSA). Cette association a comme objectif de promouvoir l'infonuagique sous l'angle de la sécurité, et ce, par la diffusion de bonnes pratiques de sécurité visant à rassurer les entreprises quant à l'utilisation de cette technologie.

Ainsi, de par son caractère réducteur de coût et de par la grande flexibilité qu'elle offre, de nombreuses organisations gouvernementales adoptent et développent cette technologie. Néanmoins, il est recommandé que cette mutation soit précédée d'une étude des risques inhérente à son déploiement.

Technologies mobiles

Les technologies mobiles (téléphones intelligents et autres) sont à la base du développement du gouvernement mobile[52], désigné aussi sous le nom de m-gouvernement. Cette technologie permet au gouvernement de rejoindre le citoyen en tous lieux et à tout moment.

---

[48] Infonuagique : Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services évolutifs, adaptables dynamiquement et facturés à l'utilisation. (Source : Grand dictionnaire terminologique)

[49] Médias sociaux : Groupe d'applications collaboratives en ligne basé sur les techniques du Web 2.0. Ils permettent la création et l'échange de contenus générés par des utilisateurs et se déclinent sous différentes formes : les plateformes collaboratives, les blogues, les wikis, le vidéo-partage, les réseaux sociaux. (Source : Wikipédia)

[50] http://www.gartner.com/it/page.jsp?id=496886

[51] http://www.grandemprunt.net/

Les technologies mobiles sont prônées par un grand nombre de gouvernements, d'autant plus que le taux de pénétration du mobile est de loin supérieur à celui de l'Internet[53]. Des pays, comme les États-Unis[54] ou Singapour[55], mettent à la disposition, de leurs citoyens, un large éventail de services gouvernementaux ainsi que des applications mobiles.

Selon une étude effectuée en 2010 auprès de 56 pays, par le Cabinet d'expertise Ernst & Young[56], environ les deux tiers (64 %) des répondants avancent que la perte ou la fuite de données sensibles figure parmi les principaux risques liés à l'utilisation de ce genre de technologie. Par conséquent, ils préconisent des ajustements dans leur politique de sécurité de l'information, des campagnes de sensibilisation et la considération des risques liés aux technologies mobiles dans leurs processus de gestion de sécurité de l'information.

La tendance globale est au déploiement de services basés sur les technologies mobiles au sein des administrations gouvernementales. De par le potentiel que peut procurer une telle technologie à applications multiples, son encadrement et son accompagnement ne peuvent qu'instaurer un climat de confiance et d'ouverture pour le citoyen.

Médias sociaux

Les médias sociaux sont définis comme un groupe d'applications collaboratives en ligne permettant la création et l'échange de contenus générés par des utilisateurs. Ils se déclinent sous différentes formes (plateforme collaborative, blogue, wiki, vidéo-partage ou réseaux sociaux[57]) et sont reconnus par plusieurs organisations pour leur utilité comme outils collaboratifs.

L'utilisation des médias sociaux comporte des risques de sécurité de l'information qui peuvent découler d'un comportement inadéquat des utilisateurs ou de la sécurité des sites abritant les médias sociaux eux-mêmes. À titre d'exemple, un utilisateur, par inadvertance ou par manque de discernement, peut être à l'origine de la divulgation d'information sensible. De même, les sites des médias sociaux sont des cibles de choix pour les pirates informatiques qui, au moyen de techniques d'hameçonnage[58], peuvent y trouver des voies d'accès privilégiées à des réseaux entiers de connaissances et ainsi usurper l'identité des membres, individuels ou corporatifs, ou infecter les réseaux d'une organisation avec du code malicieux[59].

Par ailleurs, une étude commandée en 2010 par McAfee[60], auprès de 1055 organisations réparties dans 17 pays, indique que la sécurité de l'information est un obstacle majeur à l'utilisation des médias sociaux. Citons quelques chiffres de cette étude qui révèlent des pratiques actuelles quant à l'utilisation des médias sociaux : 25 % des organisations n'accordent l'accès aux médias sociaux qu'à des personnes spécifiquement autorisées et 13 % des entreprises bloquent l'accès aux médias

---

[52] Gouvernement mobile ou m-government : diffusion d'informations et de l'offre de service par l'intermédiaire des technologies sans fil et portables. (Source : Bulletin *e-Veille* du CEFRIO)

[53] ITU World Telecommunication/ICT Indicators (WTI) database.

[54] http://www.usa.gov/

[55] http://www.ecitizen.gov.sg/mobile/index.html

[56] Borderless security Global Information Security Survey, Ernst & Young's 2010.

[57] http://fr.wikipedia.org/wiki/M%C3%A9dias_sociaux

[58] Hameçonnage ou phishing et parfois filoutage : technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale (sécurité de l'information). L'hameçonnage peut se faire par courrier électronique, par des sites Web falsifiés ou par d'autres moyens électroniques. (Source : Wikipedia)

[59] To Facebook Or Not To Facebook, Chenxi Wang, Forrester, March 30th, 2010.

[60] http://www.3dcommunication.fr/pdf/McAfeeSecuriteWeb2.pdf

sociaux au niveau de l'infrastructure. Le blocage de l'utilisation est plus courant dans le secteur public et au sein des grandes entreprises.

Cette étude et plusieurs autres sources, dont Gartner[61] ou Govtech[62], recommandent de mettre en place des mesures d'encadrement de l'utilisation des médias sociaux, comme une politique ou un plan de sensibilisation du personnel. Outre la sécurité de l'information, ces mesures devront considérer d'autres enjeux connexes à l'instar de l'éthique ou de la protection de la vie privée.

[61] Roundup of Security Research, 1Q10 : Understanding and Controlling Social-Media Security Risks, Gartner Research January 14, 2010.

[62] http://www.govtech.com/pcio/CIOs-Social-Media-Security-Risks-021111.html

5.2 Bilan gouvernemental (environnement interne)

Depuis 2000, plusieurs actions visant à encadrer la sécurité de l'information gouvernementale ont été réalisées, tant au plan sectoriel qu'au plan de la coordination gouvernementale. La présente section décrit le bilan de ces réalisations réparties selon plusieurs thèmes.

5.2.1 Directives, politiques et normes

Une directive portant sur la sécurité de l'information numérique et des échanges électroniques est adoptée en février 2000. C'est en mai 2006 qu'elle a été remplacée par la directive actuellement en vigueur, visant l'information quel que soit son support ou son moyen de communication et ne se limitant pas à l'information numérique. Il est à noter que la directive en vigueur ne se réduit pas à l'énoncé d'obligations des intervenants concernés, mais précise également leurs rôles et leurs responsabilités.

Au plan sectoriel, les MO se sont progressivement dotés d'une politique de sécurité de l'information, passant du tiers d'entre eux en 2000 aux trois quarts au dernier bilan de l'exercice 2009-2010. Ce progrès dénote de la volonté d'un grand nombre de MO de s'acquitter pleinement de leurs obligations en matière de sécurité de l'information.

En matière de normalisation en sécurité de l'information, le Secrétariat du Conseil du trésor (SCT) a établi une entente avec le Bureau de normalisation du Québec, afin que ce dernier le représente auprès d'organismes généralement reconnus de normalisation et de certification de normes en matière de sécurité de l'information.

5.2.2 Meilleures pratiques

En vue d'apporter le soutien nécessaire aux MO dans la prise en charge des exigences de sécurité de l'information, plusieurs documents de référence gouvernementale (modèles de sécurité de l'information, guides et pratiques) ont été élaborés et diffusés. De plus, une trentaine de sessions de formation sur ces documents de référence ont été dispensées.

Les modèles élaborés[63], colligeant les façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale, portent sur la gestion de la sécurité de l'information gouvernementale et sur l'habilitation et le contrôle d'accès. Ces modèles de référence visent à soutenir les MO dans la mise en œuvre des dispositions de la Directive sur la sécurité de l'information gouvernementale, à simplifier la gestion des droits d'accès et à favoriser l'interopérabilité.

Les guides et les pratiques conçus[64] ont pour objectif la mise en place efficiente des processus de gestion de la sécurité de l'information. Ceux-ci portent notamment sur les incidents, les risques, la disponibilité de l'information gouvernementale, la destruction sécuritaire de l'information et l'utilisation sécuritaire des assistants numériques personnels (ANP).

Il est à signaler, par ailleurs, que le gouvernement du Québec ne dispose actuellement d'aucun standard[65] en matière de sécurité de l'information approuvé par le Conseil du trésor.

[63] Une liste détaillée des modèles, des guides et des pratiques est jointe en annexe.

[64] Une liste détaillée des modèles, des guides et des pratiques est jointe en annexe.

[65] Un standard se définit comme étant une norme qui n'a pas été définie ni entérinée par un organisme officiel de normalisation, comme l'Organisation internationale de normalisation (ISO) ou le Conseil canadien des normes (CCN), mais qui s'est imposée par la force des choses, parce qu'elle fait consensus auprès des utilisateurs, d'un groupe d'entreprises ou encore d'un consortium.

Au niveau sectoriel, des pratiques de sécurité de l'information sont appliquées depuis plusieurs années, sans nécessairement avoir été adoptées de façon formelle. C'est le cas de la gestion des risques, de la gestion des droits d'accès et de la gestion des incidents.

5.2.3 Cadre de gestion de la sécurité de l'information

Structure de gouvernance

Dans leur grande majorité, les MO mettent en place une structure de gouvernance de la sécurité de l'information qui répond à leurs besoins propres, sans nécessairement envisager son efficacité au plan gouvernemental. Souvent, la structure mise en place ne favorise que très peu la fluidité des communications avec le DPI et, par conséquent, la prise en compte des orientations et des priorités d'intervention gouvernementales. À titre d'exemple, le responsable de la sécurité de l'information (RSI) désigné par un MO, dans plusieurs cas, dispose d'une faible capacité d'influence, est placé dans une situation de conflits d'intérêts, réels ou potentiels, ou se trouve dans une position hiérarchiquement éloignée du pouvoir décisionnel.

Cette situation semble avoir légèrement évolué depuis la diffusion par le DPI, en mars 2009, d'un modèle de référence intitulé « Modèle gouvernemental de gestion de la sécurité de l'information », lequel, entre autres éléments, argumente le choix de plusieurs variantes de structures de gouvernance. Toutefois, n'étant pas d'application obligatoire, ce modèle ne semble pas avoir efficacement contribué à l'instauration de liens de communication efficaces avec le DPI.

Rôles et responsabilités

Comme précédemment signalé, la directive en vigueur, en plus d'énoncer des obligations, définit les rôles et les responsabilités des intervenants concernés. Or, les bonnes pratiques préconisent de définir ces rôles et ces responsabilités dans un document distinct : le cadre gouvernemental de gestion de la sécurité de l'information. La directive devra alors se limiter aux seuls énoncés d'obligations à l'endroit des entités gouvernementales visées.

Au dernier bilan de l'exercice 2009-2010, environ les deux tiers déclarent avoir adopté un cadre de gestion de la sécurité de l'information, mais seulement un peu moins du tiers l'ont formalisé.

5.2.4 Comités de gouverne en sécurité de l'information

Au plan gouvernemental, deux entités ont été créées : Le Comité d'orientation stratégique de la sécurité de l'information gouvernementale (COSSIG) et le Réseau des responsables de la sécurité de l'information (RSI).

Le Comité d'orientation stratégique de la sécurité de l'information gouvernementale (COSSIG)

Créé en 2001, le Comité d'orientation stratégique de la sécurité de l'information gouvernementale (COSSIG) a pour mandat de conseiller le DPI et les MO en matière de sécurité de l'information. Il agit à titre consultatif et réunit ses membres selon une fréquence moyenne de quatre rencontres par année, au cours desquelles de nombreux thèmes de sécurité de l'information sont abordés.

Les membres du COSSIG proviennent de MO à qui des responsabilités particulières sont attribuées et de représentants de sociétés d'État. Cette composition hétérogène fait en sorte que les thématiques abordées n'étaient pas toujours d'intérêt pour l'ensemble des membres. À noter également que ces derniers n'ont pas la même compréhension du mandat du COSSIG et demeurent partagés entre sa nature consultative ou décisionnelle.

Le Réseau des responsables de la sécurité de l'information

Créé en 2001, le Réseau des responsables de la sécurité de l'information (RSI) constitue une plateforme d'échanges et de partage de connaissances entre les RSI des MO. Il permet au DPI de présenter ses travaux et aux membres d'échanger sur diverses problématiques de sécurité de l'information. Il se réunit selon une fréquence moyenne de quatre fois par année.

En termes de participation à ce réseau, il est à noter qu'un grand nombre de RSI se font fréquemment remplacer par leurs substituts, souvent hiérarchiquement éloignés de l'instance décisionnelle de leur organisation. Cela défavorise l'instauration de canaux de communication permettant de véhiculer, adéquatement à l'endroit des MO, les orientations et les objectifs stratégiques et de s'assurer qu'ils sont adoptés et appliqués.

À l'échelle sectorielle, les deux tiers des MO ont mis en place un comité chargé de la sécurité de l'information. Ce dernier est présidé par le sous-ministre ou le dirigeant d'organisme. Il a notamment pour rôle de favoriser la cohérence des actions en sécurité de l'information au sein d'un MO et d'assurer le suivi des orientations stratégiques et des priorités d'intervention en la matière.

5.2.5 Planification et suivi

Planification en sécurité de l'information

La première stratégie gouvernementale de sécurité de l'information, adoptée pour 2005-2009, est articulée autour des axes suivants : analyse de risques, plan d'action, gestion des incidents, continuité des services, formation et sensibilisation, contrôle d'accès et journalisation. À signaler que cette stratégie fixe les mêmes objectifs à l'endroit des MO, et ce, sans égard à la gravité des risques auxquels ils sont exposés. Elle se distingue également par l'absence d'orientations qui sous-tendent les objectifs fixés et d'indicateurs permettant de les mesurer.

Au plan sectoriel et en vertu de la directive en vigueur, les MO doivent présenter un plan d'action annuel en matière de sécurité de l'information. Au dernier bilan de l'exercice 2009-2010, les plans d'action sont adoptés par la moitié des MO seulement. Ce ratio laisse entrevoir que des efforts en matière de planification d'actions visant la réduction de risques restent à déployer.

Suivi de la sécurité de l'information

Depuis 2001, un rapport sur l'état de situation gouvernemental en matière de sécurité de l'information est annuellement présenté au Conseil du trésor. Ce rapport, réalisé avec la contribution active des MO, dresse un portrait d'ensemble de la sécurité de l'information gouvernementale et permet d'évaluer l'application des dispositions de la directive en vigueur.

La participation des MO au bilan gouvernemental de la sécurité de l'information est en constante progression et s'élève à 93 % de répondants pour l'exercice 2009-2010, comparativement à 89 % en 2008-2009 et à 79 % en 2007-2008. Toutefois, certaines organisations éprouvent encore des difficultés à respecter les délais fixés.

De plus, les constats énoncés dans les rapports sont basés sur les réponses fournies par les MO, lesquels sont individuellement responsables d'en assurer l'exactitude. En effet, il n'existe actuellement aucun moyen de contrôle ni d'intervention auprès des MO.

5.2.6 Cybersécurité

La création, en 2002, de l'Équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise (CERT/AQ), relevant du Centre de services partagés du Québec (CSPQ), a permis le renforcement des réseaux informatiques gouvernementaux à l'égard des cyberattaques. Le CERT/AQ, en plus d'apporter aux MO le soutien nécessaire dans la gestion des incidents, assure

la coordination d'un réseau d'alerte gouvernemental, auquel participent les coordonnateurs organisationnels de gestion des incidents (COGI) désignés par les MO. Ce réseau constitue une plateforme de communication qui favorise un échange d'information et une réaction concertée en cas d'incident cybernétique.

La création, en 2010, de l'Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale (EIMSIG) est le fruit d'un partenariat regroupant des représentants du CERT/AQ, du ministère de la Sécurité publique (MSP) et de la Sûreté du Québec (SQ). Coordonnée par le CERT/AQ, cette équipe contribue au renforcement de la sécurité de l'information gouvernementale en améliorant la connaissance des menaces et des incidents en la matière.

Toutefois, il est à constater l'absence d'un processus gouvernemental de gestion des incidents de sécurité de l'information. La mise en œuvre d'un tel processus faciliterait les communications entre les MO et définirait les stratégies de réaction appropriées incluant la gestion de crise.

5.2.7 Authentification

Infrastructure à clés publiques

L'Infrastructure à clés publiques (ICP) est un système de gestion qui, en permettant notamment à des personnes de se reconnaître à distance, leur permet d'effectuer en toute sécurité des transactions électroniques et d'échanger de l'information à caractère sensible. L'ICP permet notamment de confirmer l'identité d'une personne, d'assurer l'intégrité des documents, de préserver la confidentialité des données échangées et d'établir un lien clair entre une personne et un document.

En mai 1999, le Registre des droits personnels et réels mobiliers (RDPRM) met en opération son ICP permettant ainsi à sa clientèle de déposer électroniquement ses réquisitions d'inscription. Forte de cette expertise acquise en matière d'ICP, en février 2001, la Direction générale des services de justice (de laquelle relève le RDPRM) est mandatée par le Conseil du trésor pour exploiter un service d'ICP de portée gouvernementale. Pour ce faire, le RDPRM doit élargir ses services aux employés des autres ministères ou organismes publics ainsi qu'aux mandataires de l'État et de ses clients, et ce, afin de sécuriser leurs échanges électroniques. L'Infrastructure à clés publiques gouvernementale (ICPG) prend alors forme.

Actuellement, l'ICP du RDPRM et l'ICPG comptent 4 166 clés et certificats (2 071 pour le RDPRM et pour l'ICPG 2 095 pour 27 prestations électroniques de services (PES) réparties dans 50 ministères et organismes publics).

« Bien que l'ICPG constitue la solution commune gouvernementale en matière de certification, le ministère des Ressources naturelles et le ministère des Transports sont autorisés à recourir aux services d'un autre prestataire afin de répondre aux besoins spécifiques de certains de leurs employés tels les ingénieurs et arpenteurs-géomètres, ou de certains clients de leur prestation électronique de services. »

ClicSÉQUR[66]

Depuis 2005, le gouvernement du Québec a mis en place et fait évoluer, au bénéfice des citoyens, des entreprises et de l'ensemble des MO, le service commun d'authentification gouvernementale clicSÉQUR. Ce service, amélioré et diversifié depuis sa création, a permis d'augmenter le nombre d'inscriptions pour ses volets Citoyens et Entreprises.

[66] Les chiffres avancés datent du 31 mars 2011.

La version « Citoyens » de clicSÉQUR a été mise en ligne en 2005. Depuis, plus de 711 000 identifiants ont été délivrés aux citoyens afin d'accéder aux treize PES appartenant à huit MO. Proposée en juin 2010, une version ne nécessitant aucune vérification préalable de l'identité du demandeur et permettant un accès limité aux services en ligne, la version « Limité »[67], compte déjà plus de 24 000 inscriptions.

La version « Entreprises » de clicSÉQUR a été mise en ligne en 2008. Depuis, plus de 113 000 entreprises y sont inscrites et utilisent les sept PES. D'autres PES sont prévues ou en cours d'arrimage pour 2011 et 2012. À noter qu'une version « Express »[68], mise en ligne en juillet 2010, compte déjà plus de 81 000 inscriptions. Cette version se limite à la transmission, par les entreprises, d'information destinée aux MO participants.

En février 2011, une table regroupant les MO utilisateurs de clicSÉQUR est créée dans le but de recueillir leurs besoins d'affaires. Elle permet également d'échanger sur le fonctionnement de clicSÉQUR et sur son évolution.

Par ailleurs, clicSÉQUR n'a pas fini d'évoluer, puisque de nouveaux besoins ont été identifiés. Ceux-ci feront l'objet d'études de développement et viseront à contribuer davantage au déploiement du gouvernement en ligne et à la modernisation de l'offre de service gouvernementale.

5.2.8 Formation et sensibilisation

Au plan gouvernemental, des efforts en matière de formation ont été déployés à l'endroit des employés de l'État. À cet égard, une trentaine de sessions de formation ont été dispensées et du matériel de formation générale et spécifique a été élaboré et diffusé.

De plus, dans le but de sensibiliser le citoyen québécois aux risques liés à l'utilisation de l'Internet, trois campagnes annuelles d'information et de sensibilisation sur la sécurité de l'information et la protection des renseignements personnels ont été réalisées. Organisées sous le thème « Je protège mon identité sur Internet », ces campagnes ciblaient les adultes québécois qui transigent sur Internet et visaient notamment à augmenter leur compréhension des enjeux et des dangers associés à la sécurité de l'information, ainsi que l'adoption, au quotidien, de bonnes pratiques de sécurité de l'information. À noter, cependant, que ces campagnes excluaient une partie de la population constituée de jeunes adultes plus enclins à l'utilisation d'Internet.

Par ailleurs, au dernier bilan de l'exercice 2009-2010, le ratio des MO ayant mis en œuvre un plan de formation et de sensibilisation du personnel a plus que doublé par rapport à l'exercice précédent, pour s'établir aux deux tiers des MO environ. À noter, cependant, que le tiers des MO seulement ont adopté ce plan de façon formelle. D'autre part, bien que les MO aient une préférence à l'apprentissage en ligne, l'apprentissage classique reste le mode le plus utilisé.

5.2.9 Gestion des risques et des incidents de sécurité de l'information

Gestion des risques

Bien que la gestion des risques soit à la base de toute action de sécurité de l'information, environ le tiers seulement des MO l'ont mise en œuvre au sein de leur organisation. De plus, le processus de

[67] https://www.clicsequr.gouv.qc.ca/sqag-aide/web/FichierAide/fr/identifiant.html#typeCompteLimite
[68] https://www.info.clicsequrexpress.gouv.qc.ca/pour_tout_savoir_sur_clicsequr_express.html

gestion des risques n'est instauré que par la moitié des MO fortement exposés aux risques[69], d'où l'importance de fixer à leur endroit des exigences ciblées en la matière.

Rappelons également qu'au plan gouvernemental, la Stratégie gouvernementale de sécurité de l'information 2005-2009 avait fixé, comme date butoir, le 31 mars 2008 pour la réalisation, par les MO, des analyses de risques de sécurité des systèmes essentiels et stratégiques. Au dernier bilan de l'exercice 2009-2010, un peu plus de la moitié seulement ont réalisé au moins une analyse de risque et environ le tiers de ces analyses datent de plus de trois ans. Sur cette base, nous pouvons conclure que les risques de sécurité de l'information ne sont pas suffisamment pris en charge au plan sectoriel.

De plus, la gestion du risque de sécurité de l'information est principalement assurée en silo, puisqu'elle tient compte de la gravité du risque pour un MO, sans nécessairement se préoccuper de son impact au plan gouvernemental. Par conséquent, la problématique associée à un risque, susceptible d'avoir des incidences sur d'autres entités gouvernementales, reste entière et plaide en faveur de la mise en place d'un cadre gouvernemental qui permettra son identification et le suivi de son traitement.

Gestion des incidents

La mise en place d'un processus de gestion des incidents de sécurité de l'information permet de renforcer les mécanismes d'atténuation des risques et, advenant un incident, de s'assurer que les actions appropriées sont posées.

Au plan gouvernemental, le DPI a mis, à la disposition des MO, un guide de référence pour l'élaboration et la mise en œuvre d'un processus de gestion des incidents de sécurité de l'information qu'ils détiennent dans le cadre de leur mission.

Au dernier bilan de l'exercice 2009-2010, la majorité des MO ont mis en place un processus de gestion des incidents de sécurité de l'information, dont environ la moitié de façon formelle.

Concernant la participation au réseau d'alerte gouvernemental, un nombre insuffisant de MO (une cinquantaine environ) participent à ce réseau, et une proportion insuffisante déclare les incidents au CERT/AQ.

5.2.10 Gestion des droits d'accès

La nécessité de contrôler l'accès au patrimoine informationnel d'une organisation, en vue de parer aux risques d'usurpation d'identité ou d'accès non autorisés à l'information, fait de cette pratique une priorité gouvernementale. À cet effet, un modèle détaillé d'habilitation et de contrôle d'accès a été élaboré et diffusé afin de simplifier la gestion des droits d'accès et de favoriser l'interopérabilité.

Depuis 2000, la gestion des droits d'accès semble bien ancrée dans les processus de gestion des MO (78 % des MO en 2000-2001 contre la quasi-totalité en 2009-2010). En revanche, la proportion est moindre quant à la formalisation d'un tel processus (65 %). De plus, une proportion insuffisante de MO (54 %) procède périodiquement à la révision des droits d'accès et des privilèges spéciaux.

[69]Les entités fortement exposées aux risques sont celles qui 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.

6 Cibles visées

Partant des tendances mondiales et du bilan gouvernemental (voir section 5), la présente section fixe les cibles à atteindre pour les dix prochaines années.

6.1 Gouvernance

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

Également, le gouvernement du Québec encourage 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 géré adéquatement.

De plus, le gouvernement du Québec examine les opportunités de mise en commun des services de sécurité de l'information et détermine leurs 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 utilisation, 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 l'alignement des actions de sécurité de l'information dans le sens des orientations gouvernementales, de la définition des mesures de performance, de l'adoption des bonnes pratiques en la matière et de la contribution au processus gouvernemental de concertation et de reddition de comptes.

6.2 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 de larges budgets et lui consacrent de nombreuses structures, démontrant ainsi leur engagement dans ce domaine. Cet engagement se

justifie par la métamorphose continuelle et rapide des cybermenaces, par leur virulence et par la gravité des conséquences imputables aux cyberattaques.

Ainsi, le gouvernement du Québec détermine 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 sur l'évolution des menaces et des vulnérabilités, incluant celles découlant d'un nouvel usage technologique.

Par ailleurs, le développement de la prestation électronique de services (PES) et son utilisation au quotidien par les citoyens et les entreprises exigent un environnement d'échanges sécuritaire. 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 visant à échanger, avec les citoyens et les entreprises, toute information pertinente permettant de contrer les menaces et de remédier aux vulnérabilités.

Également, le gouvernement du Québec établit 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, et sur les bonnes pratiques à adopter en la matière. Il développe, en outre, des partenariats avec les milieux académiques, 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.

6.3 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 confortant dans 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 à l'information par les citoyens et les entreprises. 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, diverses opportunités de coopération interjuridictionnelle (fédérale, provinciale ou municipale) afin de mettre en place des mécanismes permettant une reconnaissance mutuelle des services d'authentification existants.

Par ailleurs, les organisations ont souvent recours à l'externalisation dans la plupart des secteurs d'activité. 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 l'opportunité 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.

6.4 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 en la matière à tous les échelons dans les 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 conscientisés des risques de sécurité de l'information auxquels ils font face et s'approprient les meilleures façons de s'y prémunir, 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. Ils se sentiront ainsi concernés et sauront agir, de façon conséquente, en étant vigilants et suspicieux 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 au 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.

Également, le gouvernement du Québec cible 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 sécurité de l'information de leur organisation. De plus, ces formations seront ajustées à la faveur d'ententes de partenariat avec des universités, des collèges ou des instituts de recherche.

6.5 Gestion des risques de sécurité de l'information

Le gouvernement du Québec vise, à terme, l'instauration d'un modèle de gestion des risques de sécurité de l'information qui va 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 impacts sur d'autres entités gouvernementales. Ainsi, le modèle préconisé vise à instaurer une approche de gestion des risques de sécurité de l'information collaborative, complémentaire et mutuellement fructueuse entre les organismes publics.

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

Ainsi, tous les organismes publics auront à 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 formel 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'échanges 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.

Également, le gouvernement du Québec 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.

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

6.6 Niveau de maturité

La prochaine décennie vise l'atteinte, par les organismes publics, d'un niveau de maturité adéquat au regard de leurs enjeux en sécurité de l'information. À terme, les organismes publics 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 spécifiques. Ils auront également normalisé, intégré, documenté et implémenté 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 de la situation. Ces étapes s'inscrivent dans une perspective de renforcement des mécanismes d'atténuation des risques et, advenant un incident, s'assurent 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 de l'accessibilité à l'information en temps voulu et de la manière requise par une personne autorisée.

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.

7 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 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.

7.1 Présentation des documents structurants

L'approche stratégique permet d'asseoir la vision gouvernementale et de définir les objectifs stratégiques pour les trois ans à venir. 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 l'approche stratégique. Elle contribue également à l'instauration d'une gestion optimale du risque d'atteinte à l'information gouvernementale et au renforcement de la confiance des citoyens et des entreprises quant à la sécurité de leur information confiée à l'État.
- Un cadre gouvernemental de gestion de la sécurité de l'information. Celui-ci vise à compléter les 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 les responsabilités en cette matière. Il vise également à définir et à préciser les mandats de divers comités et de 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 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 fournie par d'autres organismes publics.

7.2 Approche stratégique 2014-2017

Afin de tendre vers les 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 engager, exprimées en termes d'exigences, autant à l'endroit des organismes publics qu'au 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.

7.2.1 Exigences au plan gouvernemental

Les exigences au 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. Ceux-ci viseront, notamment, à mettre à la disposition des organismes publics des standards, des outils et des guides de bonnes pratiques de sécurité de l'information.

C'est ainsi que les travaux en matière de gestion des risques appuieront les organismes publics dans la conception et la mise en œuvre d'un processus unifié de gestion des risques, intégrant ceux à portée sectorielle ou 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 matière de 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 porteront également sur des pratiques recommandées aux différentes étapes du processus, comprenant le chiffrement, l'analyse des vulnérabilités ou la détection d'intrusion.

En matière de 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 viseront également à guider les organismes publics dans diverses actions en la matière appropriées 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, incluant 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.

En matière d'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 matière d'audit de sécurité de l'information et de test d'intrusion et de vulnérabilité, les travaux viseront 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 viseront également à leur fournir un service d'accompagnement en la matière.

En matière de formation et de sensibilisation, les travaux viseront à 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 en la matière 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 des employés de l'État sera élaboré et mis en œuvre et 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, l'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 et la signature électronique et l'impact de l'utilisation des technologies émergentes sur la sécurité de l'information gouvernementale.

7.2.2 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 bonnes pratiques gouvernementales en matière de sécurité de l'information.

C'est ainsi qu'en matière de 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.

En matière d'authentification, les organismes publics contribueront à l'accroissement de l'utilisation des offres de service d'authentification gouvernementale.

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

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

En matière de pratiques de sécurité de l'information, les organismes publics définiront et mettront en place les 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 bonnes pratiques relatives à l'intégration des clauses contractuelles de sécurité de l'information dans les ententes et les contrats, à la mise en place d'un registre d'autorité, à l'adoption d'une architecture de sécurité de l'information et à l'utilisation sécuritaire des médias sociaux.

Pour davantage de détails concernant les objectifs et les cibles à l'égard de ces exigences, vous pouvez vous reporter à la section 8.

7.3 Nouvelle directive sur la sécurité de l'information gouvernementale

Une nouvelle directive sera proposée en remplacement de l'actuelle directive sur la sécurité de l'information gouvernementale en vigueur depuis 2006. Elle tiendra compte des cibles fixées à la section 6 en y intégrant de nouvelles obligations au plan gouvernemental et sectoriel.

7.3.1 Obligations au 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. Également, le DPI réalisera, de concert avec les organismes publics, un rapport annuel sur l'état de situation gouvernemental en la matière. De plus, le DPI interviendra auprès d'un organisme public,

lorsque celui-ci ne remplit pas ses obligations en vertu de la directive ou lorsqu'un risque de sécurité de l'information à portée gouvernementale n'est pas géré adéquatement.

En matière de 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, conjointement avec le MSP et la 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, incluant 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.

En matière de gestion de risques de sécurité de l'information, le DPI déposera annuellement, au Conseil du trésor, un rapport sur les risques de sécurité de l'information à portée gouvernementale.

7.3.2 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, selon une périodicité bisannuelle, 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.

En matière de gestion des incidents, les organismes publics déclareront 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, incluant l'authentification, les organismes publics devront utiliser ces services, à moins de démontrer l'existence de circonstances exceptionnelles pour ne pas se conformer à cette obligation ou qu'un service commun ne réponde pas à leur préoccupation en termes d'efficience et d'efficacité.

En matière de gestion des risques de sécurité de l'information, les organismes publics déclareront, 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.

7.4 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 des responsabilités au plan gouvernemental et sectoriel.

7.4.1 Rôles et responsabilités au plan gouvernemental

En matière de gouvernance de la sécurité de l'information, le rôle du DPI sera renforcé afin d'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 en matière de conformité à la Directive sur la sécurité de l'information gouvernementale.

En matière de cybersécurité, l'Équipe intégrée sur les menaces à la sécurité de l'information gouvernementale (EIMSIG), créée en 2010, sous forme d'un partenariat impliquant 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 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 CSPQ, un programme gouvernemental de formation en sécurité de l'information à l'endroit du personnel des organismes publics. De plus, il développera et tiendra à jour une base de connaissances sur les pratiques de sécurité de l'information d'intérêt pour les organismes publics.

En matière de gestion gouvernementale des risques et des incidents de sécurité de l'information, le DPI élaborera un cadre gouvernemental de gestion en cette matière 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 visant à soutenir les organismes publics dans la prise en charge des exigences de sécurité de l'information. Il poursuivra, à cet égard, la réalisation, la mise à jour et la diffusion de modèles, de guides et de pratiques de sécurité de l'information.

7.4.2 Rôles et responsabilités au plan sectoriel

En matière de gouvernance de la sécurité de l'information, l'organisme public adoptera, mettra en œuvre et assurera l'application d'une politique et d'un cadre de gestion de la sécurité de l'information. Il assumera ses responsabilités par un personnel qualifié au plan stratégique, tactique et opérationnel. La personne désignée au plan stratégique jouera le rôle de porte-parole du DPI auprès de son organisation et lui relaiera les orientations et les 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.

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

En matière de 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 matière de 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 bonnes pratiques de sécurité de l'information.

7.5 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 de produire des conséquences à l'échelle gouvernementale. Il 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 au plan gouvernemental et sectoriel.

7.5.1 Exigences au plan gouvernemental

Le concept de risque à portée gouvernementale sera défini et une approche d'identification et de suivi de son traitement sera préconisée. Celle-ci permettra de s'assurer de 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.

7.5.2 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 en la matière avec d'autres entités gouvernementales. Ils devront également intégrer, dans 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.

8 Objectifs stratégiques

Cette section détermine les enjeux et les orientations gouvernementales ainsi que les cibles fixées à l'endroit des organismes publics de grande taille (1000 employés et plus), de taille moyenne (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 en termes d'objectifs et de 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.

8.1 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 de processus et la conformité aux bonnes pratiques en la matière permettent de répondre efficacement à cet enjeu.

8.1.1 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 identifiés 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 : Taux d'organismes publics ayant adopté une politique et un cadre de gestion de la sécurité de l'information	**Cible :** 100 % des organismes publics, le 31 mars 2015
Indicateur : Taux d'organismes publics ayant désigné leurs principaux intervenants en sécurité de l'information (ROSI et COGI)	**Cible :** 100 % des organismes publics, le 31 mars 2015
Indicateur : Taux de participation de chacun des organismes publics invités aux activités gouvernementales de concertation	**Cible :** 65 % annuellement pour chacun des organismes publics
Objectif 1.2 : Évaluer les risques à portée gouvernementale	
Indicateur : Taux d'organismes publics ayant identifié leurs actifs critiques	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics, le 31 mars 2016
Indicateur : Taux d'actifs critiques identifiés pour lesquels des mesures de contingence sont mises en place	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics, le 31 mars 2016

8.1.2 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 implémentés et lorsque l'information qu'elle détient est sécurisée, conformément aux bonnes 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 ou ceux fortement exposés aux risques.

Objectif 2.1 : Mettre en œuvre des processus formels de gestion de la sécurité de l'information	
Indicateur : Taux d'organismes publics ayant mis en œuvre un processus formel de gestion des risques de sécurité de l'information	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics de grande taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017
Indicateur : Taux d'organismes publics ayant mis en œuvre un processus formel de gestion des incidents	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics de grande taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017
Indicateur : Taux d'organismes publics ayant mis en œuvre un processus formel de gestion de l'accès à l'information	**Cible :** 75 % des organismes publics de grande taille et 25 % de taille moyenne, le 31 mars 2015 **Cible :** 100 % des organismes publics de grande taille, 75 % de taille moyenne et 50 % de petite taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017
Objectif 2.2 : Se conformer aux bonnes pratiques de sécurité de l'information	
Indicateur : Taux d'organismes publics ayant intégré les clauses contractuelles de sécurité de l'information dans leurs ententes ou leurs contrats	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics de grande taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017
Indicateur : Taux d'organismes publics ayant effectué un audit en sécurité de l'information au cours des deux dernières années	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics de grande taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017
Indicateur : Taux d'organismes publics qui effectuent, annuellement, des tests d'intrusion et de vulnérabilité en sécurité de l'information	**Cible :** 100 % des organismes publics fortement exposés aux risques et ceux de grande taille, le 31 mars 2015 **Cible :** 75 % des organismes publics de taille moyenne et 50 % de petite taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017
Indicateur : Taux d'organismes publics ayant mis en place un registre d'autorité	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics de grande taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017
Indicateur : Taux d'organismes publics ayant adopté une architecture de sécurité de l'information	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics de grande taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017

8.2 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 de l'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.

8.2.1 Orientation 3 : Renforcer la cybersécurité

Le renforcement de la cybersécurité au plan sectoriel se traduit par la participation des organismes publics au réseau d'alerte gouvernemental. Ceci permet d'assurer le maintien d'un état d'alerte optimal face aux 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 : Taux de participation des organismes publics au réseau d'alerte gouvernemental	**Cible :** 100 % des organismes publics fortement exposés aux risques ainsi que ceux de grande taille, le 31 mars 2015 **Cible :** 100 % des organismes publics, le 31 mars 2016

8.2.2 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 PES aux citoyens.

Objectif 4.1 : Augmenter l'utilisation des services d'authentification gouvernementale	
Indicateur : Taux d'adhésion à clicSÉQUR	**Cible :** 80 % des nouvelles PES transactionnelles utilisent clicSÉQUR
Indicateur : Taux de comptes clicSÉQUR (Citoyens et Entreprises) actifs	**Cible :** Augmentation de 15 % par année

8.3 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 de bonnes 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.

8.3.1 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 de bonnes pratiques par le personnel pourrait contribuer efficacement à sa protection. C'est le cas de la déclaration, dans les délais requis, d'un incident potentiel ou réel, 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 de bonnes pratiques de sécurité de l'information.

Objectif 5.1 : Sensibiliser le personnel à la sécurité de l'information	
Indicateur : Taux d'organismes publics ayant mis en place un plan de sensibilisation de l'ensemble du personnel en matière de sécurité de l'information	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics de grande taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017
Indicateur : Taux d'organismes publics ayant dispensé une première session de sensibilisation à la sécurité de l'information à l'ensemble du personnel	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics de grande taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017
Objectif 5.2 : Accroître l'expertise et le savoir-faire en sécurité de l'information	
Indicateur : Taux d'organismes publics ayant mis en œuvre un programme formel de formation de l'ensemble du personnel	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics de grande taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017
Indicateur : Taux des ROSI ayant suivi une formation générale en sécurité de l'information	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics de grande taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017
Indicateur : Taux des COGI ayant suivi une formation sur les bonnes pratiques de sécurité de l'information, dont la gestion des risques, des incidents ou de l'accès à l'information	**Cible :** 100 % des organismes publics fortement exposés aux risques, le 31 mars 2015 **Cible :** 100 % des organismes publics de grande taille et 50% des organismes publics de taille moyenne et de petite taille, le 31 mars 2016 **Cible :** 100 % des organismes publics, le 31 mars 2017

9 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[70], 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;
- 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;

[70] SCPRP : Sécurité, contrôle et protection des renseignements personnels.

- 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.

Québec

UN
QUÉBEC
POUR TOUS