Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Stratégie intégrée de cybersécurité du gouvernement du Canada

Publié : le 2024-05-20

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

No de catalogue BT48-44/2024F-PDF
ISBN: 978-0-660-72249-8

Ce document est disponible sur le site Web du gouvernement du Canada à l'adresse www.canada.ca

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: GC Enterprise Cyber Security Strategy

Stratégie intégrée de cybersécurité du gouvernement du Canada

Sur cette page

Message de la présidente

Stratégie intégrée de cybersécurité du gouvernement du Canada

La sécurité de la population canadienne est et a toujours été notre priorité absolue. Les Canadiennes et Canadiens comptent sur le gouvernement du Canada pour offrir des programmes et des services, dont bon nombre sont de plus en plus numériques en cette ère moderne. Comme de nombreuses institutions publiques dans le monde, le gouvernement a été la cible de cyberattaques qui peuvent avoir des répercussions importantes sur les activités gouvernementales et la sécurité des Canadiens et Canadiennes.

Nous adaptons constamment les mesures de sécurité et nous mettons en place des outils qui permettront de protéger nos systèmes, ainsi que les renseignements personnels des Canadiennes et Canadiens.

Des outils comme les exercices de simulation du Plan de gestion des événements de cybersécurité du gouvernement du Canada, et la surveillance de la sécurité des sites Web constituent des mesures proactives qui nous aident à prévoir les événements de cybersécurité et à y réagir efficacement.

Nous prenons maintenant d'autres mesures pour renforcer notre approche et avoir une idée plus précise des mesures de cyberdéfense actuelles au gouvernement. Cette toute première Stratégie intégrée de cybersécurité du gouvernement du Canada, élaborée par le Secrétariat du Conseil du Trésor du Canada, le Centre de la sécurité des télécommunications Canada et Services partagés Canada, adopte une approche pangouvernementale fondée sur le risque qui va améliorer la collaboration entre les ministères, ainsi que la cybersécurité dans son ensemble.

Cette stratégie intégrée de cybersécurité est la première du genre et témoigne de notre engagement à assurer la sécurité des Canadiens et Canadiennes à l'ère numérique. Elle permettra de réduire les redondances, de cerner les lacunes et de réaliser des tests et des examens à longueur d'année.

Elle améliorera également la façon dont le gouvernement se prépare aux cyberattaques, y répond et reprend ses activités par la suite, tout en contribuant à favoriser un effectif diversifié, qui possède les compétences, les connaissances et la culture requises pour soutenir la cybersécurité. La fonction publique du Canada est l'une des meilleures au monde, et cette stratégie nous aidera à nous assurer que nous avons un effectif doté des bons outils pour réagir aux cyberattaques complexes.

La cybersécurité est un travail de longue haleine, et cette stratégie sera régulièrement examinée et mise à jour afin qu'elle suive l'évolution des menaces.

Les Canadiennes et Canadiens peuvent avoir l'assurance que le gouvernement met continuellement en œuvre des mesures efficaces pour protéger leurs renseignements et contrer les événements de cybersécurité qui se produisent.

Je vous invite à lire la stratégie pour en apprendre davantage sur la façon dont le gouvernement du Canada renforce la cybersécurité dans toute l'administration publique.

L'honorable Anita Anand, C. P., députée
Présidente du Conseil du Trésor

1. Introduction

▶ Dans cette section

1.1 Contexte

La population canadienne compte sur des institutions publiques telles que le gouvernement du Canada (GC) pour la prestation de programmes et de services. En tant que secteur d'infrastructures essentielles, les services publics sont essentiels à la santé, à la sécurité et au bien-être économique de la population canadienne. Le caractère de plus en plus numérique du GC et sa dépendance à l'égard de la technologie de l'information font du GC une cible attrayante en raison des informations personnelles, des données de recherche précieuses et d'autres informations sensibles qu'il détient.

En conséquence, les événements liés à la cybersécurité peuvent avoir un effet significatif sur les opérations gouvernementales, soit par l'interruption de services critiques et essentiels, soit par l'exposition d'informations

classifiées ou personnelles. Cet effet significatif peut exposer les personnes à un risque d'usurpation d'identité ou à d'autres types de fraude, ce qui peut éroder la confiance dans les institutions gouvernementales et avoir une incidence négative sur l'ensemble de l'économie et de la société canadiennes. L'Évaluation des cybermenaces nationales 2023-2024 souligne l'augmentation significative du nombre et de la sophistication des auteurs de cybermenace qui profitent de la dépendance à l'égard des technologies connectées à Internet pour mener des activités malveillantes. En raison de la complexité croissante des menaces et de la rapidité de l'innovation et de l'adoption de la technologie, il sera encore plus difficile pour les ministères et les organismes du GC de comprendre les risques auxquels ils sont confrontés et la manière dont ils peuvent et doivent se protéger.

À cette fin, compte tenu de la sophistication et de la fréquence croissantes des cyberattaques, le GC doit rester vigilant et continuer à renforcer sa défense pour améliorer sa résilience. Le fait de garantir la confidentialité, l'intégrité et l'accessibilité des informations et des réseaux du GC est essentiel pour la prestation de services numériques sûrs et fiables. Afin de procéder à la mise en place et au maintien d'un GC numérique résilient, il faudra mieux comprendre la nature des cyberrisques**,** et prendre des mesures pour moderniser et sécuriser les systèmes afin de prévenir les cyberattaques et d'y résister. Lorsque des cyberévénements se produisent, le GC doit être en mesure de les détecter rapidement afin d'en limiter l'incidence. La position résiliente en matière de cybersécurité permettra au GC de réagir efficacement aux cyberévénements et de s'en remettre en temps voulu, afin d'assurer la prestation continue des programmes et des services gouvernementaux.

1.2 Objectif et portée

La Stratégie intégrée de cybersécurité du GC (la « Stratégie ») a pour objet de :

- définir la vision et les objectifs stratégiques du GC, en tenant compte de l'évolution du contexte des risques liés à la cybersécurité, améliorer la maturité en matière de cybersécurité et optimiser les investissements du GC dans ce domaine;
- développer un état futur pour la cybersécurité des opérations gouvernementales, avec une gouvernance de soutien, une surveillance et des rôles et responsabilités clairs;
- déterminer les initiatives et les investissements nécessaires afin d'appuyer la mise en œuvre de la Stratégie.

La Stratégie s'applique aux ministères et organismes sous l'autorité du Conseil du Trésor, en particulier dans le cadre de la Politique sur les services et le numérique et de la Politique sur la sécurité du gouvernement. En outre, le champ d'application de la Stratégie vise les systèmes d'information désignés (Protégé B), ainsi que les systèmes d'information classifiés (secrets) qui visent à appuyer les opérations gouvernementales, tout en respectant les besoins uniques de l'écosystème plus large des systèmes classifiés.

Même si les organismes et ministères fédéraux qui ne sont pas sous l'autorité du Conseil du Trésor ne sont pas tenus, pour l'instant, de mettre en œuvre et d'adopter les exigences et les orientations de la politique du Conseil du Trésor, il leur est conseillé d'adopter les objectifs et les buts définis dans le cadre de la Stratégie, dans toute la mesure du possible, afin d'améliorer la situation en matière de cybersécurité à l'échelle des institutions fédérales.

1.3 Environnement actuel

1.3.1 Facteurs

Comme le souligne l'Ambition numérique du Canada, le paysage numérique d'aujourd'hui est marqué par des changements d'une rapidité et d'une portée sans précédent. La transformation rapide des technologies, du

numérique et des données fait désormais partie de la vie quotidienne de la population canadienne, révolutionnant la façon dont ils accèdent à l'information et aux services et la façon dont ils vivent, socialisent et travaillent. La population canadienne veut pouvoir avoir confiance en leur gouvernement et avoir accès à n'importe quel service gouvernemental, à tout moment et sur n'importe quel appareil, de façon sécuritaire et accessible. Toutefois, la réalisation de cette attente présente une série de défis et de points en matière de sécurité qui doivent être pris en compte dans le cadre d'un environnement cybernétique en constante évolution :

> **Énoncé de l'Ambition numérique du Canada**
>
> Faciliter la prestation de services gouvernementaux à l'ère numérique pour tous les Canadiens et toutes les Canadiennes en fournissant des outils modernisés et accessibles afin d'appuyer une prestation de services qui expriment le meilleur du Canada dans l'espace numérique.

- **Prestation de services numériques**
    - Le Canada compose avec des cybercampagnes malveillantes persistantes et de plus en plus sophistiquées qui menacent le secteur public et, en fin de compte, la sécurité et la vie privée de la population canadienne.
    - La numérisation entraîne une augmentation des risques de violation et de perte de données. L'augmentation du nombre de renseignements personnels numérisés et l'amélioration des services par l'entremise d'approches numériques doivent s'accompagner de mesures visant à garantir la protection de la vie privée de la population canadienne et la prestation de services gouvernementaux dans un environnement de menaces en évolution rapide.
    - Conformément au Guide sur les Normes relatives au numérique du GC, les services doivent être créés pour répondre aux besoins des

utilisateurs. Pour ce faire, on doit notamment adopter une approche équilibrée de la gestion des risques en appliquant les mesures appropriées en matière de protection des renseignements personnels et de sécurité. Veiller à ce que les mesures de sécurité ne causent pas de friction, afin qu'elles ne deviennent pas un fardeau pour les utilisateurs.

- **Engagements environnementaux, sociaux et de gouvernance (ESG)**
    - Comme le GC met de plus en plus sur la prestation de services numériques responsables et durables, la protection de ses actifs et des renseignements personnels des Canadiens et des Canadiennes fait partie intégrante de l'exercice de la responsabilité sociale du GC.
    - Les préoccupations environnementales soulignent la nécessité de réduire au minimum l'empreinte carbone associée aux cyberattaques et aux atteintes à la protection des données, car ces incidents entraînent souvent une importante consommation d'énergie.
    - De solides pratiques en matière de cybersécurité témoignent d'un engagement en faveur de la gouvernance en appuyant la transparence, la responsabilité et la conduite éthique, et en consolidant ainsi la fiabilité et la confiance des Canadiens et des Canadiennes à l'égard du GC.
- **L'avenir du travail**
    - La pandémie de la COVID-19 a mis en lumière le besoin d'outils et de pratiques de travail plus modernes pour favoriser un environnement de travail hybride. Dans les jours qui ont suivi la déclaration de la pandémie en mars 2020, la plupart des fonctionnaires fédéraux avaient commencé à travailler à distance.
    - Avec l'introduction de mesures permettant le travail à distance pendant la pandémie, une plus grande tolérance au risque a été

nécessaire pour assurer la continuité des opérations du gouvernement. Pour l'avenir, cette tolérance au risque et/ou les mesures d'atténuation correspondantes devront être réexaminées et réharmonisées pour refléter le nouvel environnement de travail.

- **Modernisation des technologies**
  - La technologie évolue à un rythme sans précédent, avec de nouvelles innovations et avancées introduites régulièrement (par exemple, l'Internet des objets [IdO], l'intelligence artificielle [IA], l'informatique quantique, la chaîne de blocs). Si cette évolution rapide présente de nombreux avantages et possibilités, elle crée également de nouveaux vecteurs de menace et de nouveaux défis en matière de cybersécurité. La rapidité des changements technologiques signifie que les mesures de sécurité qui étaient autrefois efficaces peuvent rapidement devenir obsolètes. Cela souligne la nécessité pour une approche adaptative à la cybersécurité, qui en est une où les organisations évaluent et améliorent constamment leurs mesures de sécurité pour suivre le rythme d'un environnement de menaces en constante évolution. La vitesse à laquelle on applique ces changements peut causer des difficultés en matière de surveillance, créant ainsi des lacunes en matière de reddition de comptes et de responsabilité pour les risques liés à la cybersécurité.
  - L'adoption et l'intégration des appareils IdO) ont entraîné la convergence des systèmes cybernétiques et physiques, ce qui élargit le champ d'attaque et permet à un vecteur de menace cybernétique d'avoir des incidences physiques ou à un vecteur de menace physique d'avoir des incidences cybernétiques.
  - La manière dont les services de la technologie de l'information (TI) sont fournis et utilisés a considérablement changé ces dernières années et continue d'évoluer. L'utilisation répandue des appareils mobiles et l'adoption de services basés sur l'informatique en nuage

modifient l'environnement technologique du GC et doivent être prises en compte du point de vue de la cybersécurité.
    - Si le modèle de sécurité traditionnel axé sur le périmètre a bien servi le GC, l'idée que les actifs numériques et les utilisateurs à l'intérieur d'un périmètre défini sont dignes de confiance n'est pas adaptée au « nouveau monde numérique » où le périmètre de confiance ne peut pas être défini. La connectivité accrue, le risque de menaces internes et la nécessité de protéger et de stocker les données dans divers référentiels internes et tiers (par exemple, dans le nuage) ont conduit à de nouveaux concepts de sécurité qui ne reposent pas uniquement sur une approche de sécurité axée sur le périmètre (c'est-à-dire aucune confiance).
- **Les événements et incidents liés à la cybersécurité continuent d'avoir une incidence sur les gouvernements**
    - Le nombre de vulnérabilités de type « jour zéro » nécessitant une mesure immédiate de la part du GC augmente chaque année.
    - Les compromissions au sein de la chaîne d'approvisionnement (par exemple, SolarWinds) ont une incidence sur le GC et introduisent des risques opérationnels lorsque des services tiers sont utilisés. Il est nécessaire que les institutions d'infrastructures essentielles (notamment des secteurs de ressources naturelles, financier, de la santé, des télécommunications) doivent être au premier plan des discussions sur la cybersécurité et la résilience lors de l'analyse de la vulnérabilité. Le GC doit veiller à ce que toutes les activités de cybersécurité soient menées en collaboration avec ces institutions d'infrastructures essentielles afin de garantir une approche cohérente et collective de la cybersécurité et de la résilience.
    - Les cyberattaques sophistiquées [1] qui ont une incidence sur les ministères et les organismes démontrent que le GC continue d'être une cible, d'où la nécessité de remédier rapidement à toute faille dans l'architecture des systèmes d'information du GC.

- Les cyberattaques et les atteintes à la protection des données offrent également l'occasion aux fraudeurs d'exploiter les vulnérabilités et de mener des activités frauduleuses en utilisant des techniques comme le piratage psychologique, l'hameçonnage ou l'énumération des justificatifs d'identité volés qui permettent d'obtenir un accès non autorisé aux systèmes et qui peuvent entraîner du vol d'identité ou de la fraude financière.

1.3.2 Progrès à ce jour

La mise en place et le maintien de cyberdéfenses gouvernementales sont donc essentiels à la protection des fonctions et des services dont dépend la société canadienne. Au cours de la dernière décennie, des progrès ont été réalisés dans l'amélioration de la position du gouvernement en matière de cybersécurité, des capacités de sécurité centralisées ayant été mises en œuvre dans une certaine mesure au sein du GC. En voici des exemples :

- la création du ministère Services partagés Canada (SPC) dans le cadre des efforts déployés afin de normaliser l'infrastructure de la TI du GC, notamment l'intégration des services de cyberdéfense au périmètre intégrée du GC;
- la création du Centre canadien pour la cybersécurité (Cybercentre), dans le cadre du Centre de la sécurité des télécommunications (CST), afin de consolider l'expertise opérationnelle en matière de cybersécurité au sein du gouvernement fédéral et d'offrir une source unique et unifiée en matière de conseils, d'orientation, de services et de soutien quant aux questions opérationnelles liées à la cybersécurité;
- la mise en place de mécanismes de gouvernance clairs afin d'appuyer l'élaboration d'une politique stratégique de cyberdéfense, la gestion efficace des initiatives en matière de sécurité de la technologie de l'information ayant une incidence sur les opérations à l'échelle du gouvernement, et la réaction du gouvernement aux cyberincidents;

- le plus de conseils, d'orientations et d'autres outils et mise en œuvre d'exigences minimales en matière de configuration en 2022 dans le cadre de la Politique sur les services et le numérique, qui a été initialement publiée en 2020, ainsi que le renouvellement de la Politique sur la sécurité du gouvernement en 2019.

1.3.3 Lacunes persistantes

Malgré ces progrès, il reste des lacunes quant à l'état actuel de la cyberrésilience du gouvernement, et de l'état dans lequel il doit se trouver.

- **Niveaux variables de cybermaturité**
    - L'outil d'autoévaluation de la cybermaturité (AECM) du SCT a été lancé à l'automne de 2021 afin d'aider les ministères et organismes à évaluer leur niveau de cybermaturité à l'aide de pratiques exemplaires reconnues, et il est basé sur la méthodologie ayant été dérivée du cadre de cybersécurité de la National Institute of Standards and Technology (NIST) des États-Unis.
    - La comparaison des résultats pour 2021-2022 avec ceux de 2022-2023 a permis de démontrer que les ministères et organismes ont réalisé peu de progrès en matière d'amélioration de leur cybersécurité, et qu'ils demeurent, dans la moyenne, en deçà de la cible fixée dans le cas des organisations ayant des processus récurrents pour ce qui est de déceler et d'atténuer les risques de façon à se défendre adéquatement contre les menaces nouvelles et émergentes.
- **Manque de sensibilisation à l'environnement des risques liés à la cybersécurité**
    - Le niveau de maturité, de capacité, d'investissement et de compréhension de la sécurité dans les ministères et organismes fédéraux n'est toujours pas homogène. De plus, la taille et la complexité du patrimoine du gouvernement fédéral en matière de

numérique, notamment la présence d’applications et de technologies anciennes, compliquent considérablement le défi à relever.
    - Le recours accru aux services de tiers a fait naître le besoin d’approches et de solutions plus efficaces en matière de gestion des risques liés aux tiers en raison de la gravité potentielle des faiblesses de la chaîne d’approvisionnement pour le GC.
    - La capacité à se protéger contre les vulnérabilités et les menaces en constante évolution est encore plus limitée par la présence d’anciens systèmes d’information du GC. Cette contrainte renforce le besoin de poursuivre les efforts de gestion, de mise à niveau ou de suppression de ces systèmes, et de mettre en place les mesures de protection nécessaires ainsi que des investissements continus afin de veiller à ce que les systèmes d’information du CG soient suffisamment sûrs tout au long de leur cycle de vie. Cependant, le suivi et l’entretien des actifs technologiques et des données (sur place et dans le nuage) ne sont pas compris ou gérés de manière exhaustive, ce qui a pour effet de limiter la visibilité et la connaissance des actifs devant être protégés. De nombreux ministères et organismes s’appuient sur des processus manuels, qui peuvent prendre du temps, causer des erreurs et être inefficaces. Ces limites imposées aux processus manuels sont particulièrement importantes pour les nombreux actifs pour lesquels il est nécessaire de suivre correctement les détails de la configuration (par exemple, les algorithmes cryptographiques exacts et leurs paramètres).
- **Des approches disparates et l’absence d’investissements coordonnées en ce qui concerne les différentes capacités de sécurité peuvent entraîner des incohérences, des inefficacités et des zones d’ombre dans la position globale en matière de sécurité du GC.**

- Gestion de l’identité et des justificatifs en matière d’accès (GIJA)
    - Il est de la plus haute importance pour le GC de gérer les justificatifs numériques de manière à atténuer les risques pour la sécurité du personnel, de l’organisation et de l’État, tout en protégeant l’intégrité des programmes et en permettant la prestation de services de confiance axés sur le citoyen. À cette fin, il est nécessaire de moderniser les solutions actuelles de la GIJA du GC afin de garantir que l’identité est gérée de manière cohérente et collaborative à l’échelle du GC pour les services internes et externes, tout en augmentant le niveau d’assurance nécessaire pour atténuer les risques en matière d’authentification.
- Surveillance de la sécurité
    - Les ministères et les organismes utilisent une combinaison d’outils, de méthodes et/ou de services différents pour surveiller leurs systèmes, ce qui peut compliquer l’obtention d’une vue d’ensemble des menaces potentielles pour la sécurité et donner lieu à un chevauchement ou à des lacunes non intentionnels en matière de surveillance. Il est donc nécessaire d’améliorer la visibilité et l’accès aux données mises à disposition pour permettre un suivi de bout en bout, où les ministères et les organismes peuvent analyser les données selon leurs propres perspectives opérationnelles. Il faut tenir compte du fait que de nombreux ministères ne sont pas formés, équipés ou dotés de personnel afin d’appuyer cette fonction.
    - Bien que la portée des services sur place soit claire en ce qui a trait au mandat (par exemple, lorsque SPC est chargé de la prestation de services de messagerie, de réseau et de centre de données, et que les ministères et organismes sont responsables des points d’extrémité et des applications),

l’adoption rapide de l’informatique en nuage a entraîné un manque de clarté quant aux rôles et responsabilités et à la mesure dans laquelle les rôles et responsabilités existants sont étendus à l’informatique en nuage. En raison de ce manque de clarté, les ministères et les organismes sont censés gérer leurs environnements en nuage, notamment les opérations de cybersécurité. Cette attente a entraîné une répétition des efforts, des approches incohérentes, un manque de partage de renseignements, et une visibilité réduite pour l’organisation du GC en ce qui concerne l’analyse d’un événement de cybersécurité et l’atténuation des risques.

- Services communs
  - Bien que des fonds aient été reçus pour mettre en place les capacités de cybersécurité intégrées, toutes ces capacités n’ont pas été pleinement mises en œuvre à l’échelle du GC pour différentes raisons, y compris les approches en cascade pour la livraison du projet et un long processus d’approvisionnement.
  - Le rapport spécial du comité des Parlementaires sur la sécurité nationale et le renseignement portant sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques met en évidence l’obstacle global que représente le fait que le gouvernement est de plus en plus géré horizontalement, alors que ses pouvoirs fondamentaux demeurent verticaux, ce qui crée des divergences importantes. En particulier, les politiques du Conseil du Trésor visant à sécuriser les systèmes gouvernementaux ne sont pas appliquées de manière uniforme étant donné que :
    - les ministères et organismes individuels conservent une grande latitude sur le choix d’adhérer au cadre ou d’accepter des technologies défensives spécifiques;

        - un grand nombre d’organisations, notamment des sociétés d’État et potentiellement certains intérêts gouvernementaux, ne sont pas tenues d’adhérer aux politiques du Conseil du Trésor ni de se servir du cadre de cyberdéfense.
    - Bien que l’utilisation de l’application de services centralisés à l’échelle du gouvernement contribuerait à réduire les risques, il existe un besoin de partager un plus grand nombre d’informations afin d’appuyer une telle utilisation, notamment en améliorant la coordination dans l’élaboration des activités stratégiques, de mise en œuvre et opérationnelles. Ce besoin est également amplifié en raison de l’absence de suivi et de gestion normalisés dans le cas des services communs.

- **Les modèles traditionnels d’architecture de sécurité sont moins efficaces, car les utilisateurs et les applications sont désormais présents en dehors du périmètre traditionnel du réseau.**
    - La menace croissante de cyberattaques sophistiquées a mis en évidence le fait que le GC ne peut pas compter uniquement sur les mécanismes de défense traditionnels basés sur le périmètre pour protéger les systèmes et les données critiques. Une approche axée sur l’information où il n’y a pas de confiance implicite et où tous les accès sont vérifiés (également appelée zéro confiance), et une défense du réseau fondé sur l’hôte et le nuage existants, permettra aux ministères et aux organismes de détecter et d’isoler ces types de menaces, et d’y répondre rapidement.
- **Décalage entre les approches traditionnelles en matière d’évaluation de la sécurité et les méthodologies de prestation agile.**
    - Alors que le GC s’oriente vers un environnement de travail plus agile avec des pratiques de gestion de projets et de développement, les processus d’évaluation et d’autorisation de la sécurité (E et AS)

du GC continuent de fonctionner selon une approche en cascade, basée sur la conformité, ce qui entraîne de longs retards dans le déploiement opérationnel des solutions des systèmes d'information. Le GC doit évoluer vers une approche fondée sur les risques et les menaces, qui réduira les frictions avec les méthodologies de livraison agiles tout en équilibrant la sécurité.

- **Faibles pratiques de gestion de l'information**
    - Les processus de protection des données existants sont manuels et n'ont pas fait l'objet d'une normalisation complète, de la création à la destruction. En outre, il y a un manque de sensibilisation aux procédures appropriées liées à la manipulation, au traitement et à la classification des informations (par exemple, sous-classification ou surclassification), résultant en une application qui n'est pas cohérente à l'échelle du GC.
    - La protection des informations est insuffisante en raison d'outils de la TI dépassés, résultant en une augmentation des incidents de cybersécurité ou à des atteintes à la vie privée, entraînant ainsi une érosion de la confiance quant à la sécurité de la gestion de l'information au sein du GC.
- **Pratiques peu évoluées de gestion des événements liés à la cybersécurité**

Exercices de simulation cybernétique

Les exercices de simulation cybernétique (également appelés exercices sur table) contribuent à améliorer la préparation, la communication et la prise de décisions, et constituent une formation rentable qui renforce la confiance dans la gestion des événements liés à la cybersécurité. Au cours de l'exercice financier de 2021-2022, seuls 25 % des ministères ont effectué des exercices de simulation cybernétique.

- Bien que le GC ait amélioré sa gestion centrale des cyberévénements, grâce à la mise en place du Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC), les capacités de chaque ministère sont limitées et les services accessibles à l'échelle du gouvernement ne sont pas toujours clairs. En outre, les solutions actuelles tendent à être autonomes et manquent d'intégration, d'automatisation des flux de travail et de capacité à générer des dossiers d'incident afin d'appuyer la gestion des incidents liés à la cybersécurité.
- Les ministères et les organismes sont confrontés à toute une série d'importants événements ou d'importantes crises dont la complexité et la portée varient. Ils sont responsables de la détermination, de la planification et de la récupération, ainsi que de la restauration de leurs services critiques, de leurs opérations internes, de leurs systèmes d'information et de leurs applications de soutien. Toutes ces responsabilités deviennent de plus en plus difficiles à respecter en raison du vieillissement des systèmes d'information et de l'augmentation de la décentralisation des actifs technologiques. Des ressources suffisantes sont nécessaires pour assurer la continuité des services critiques et appuyer les efforts de récupération en cas d'incident.

- **Défis associés à la sécurité des personnes et culture en matière de sécurité**
    - La demande mondiale pour des talents en cybersécurité dépasse largement l'offre, ce qui entraîne une pénurie de professionnels qualifiés dans ce domaine en général. Le GC n'est pas épargné, car les ministères et les organismes ont toujours du mal à pourvoir les postes vacants dans ce domaine. De plus, le GC doit établir un modèle de dotation de taille appropriée dans le domaine de la cybernétique pour les ministères et organismes centraux, afin de combler les postes de façon prioritaire. Le GC a également ajouté des niveaux de complexité en raison des exigences en matière d'habilitation de sécurité, de profil linguistique et d'un environnement de travail hybride pour de nombreux postes dans le domaine de la TI.
    - Il y a également un manque général de formation en cybersécurité pour le personnel du GC, tant du point de vue du domaine de la cybernétique (par exemple, sécurité de l'informatique en nuage, intervention en cas d'incident, surveillance de la sécurité, utilisation d'outils de cybersécurité existants, etc.) que du point de vue des employés en général. Pour limiter les cyberévénements dus à l'erreur humaine, il est indispensable de renforcer les compétences de l'ensemble du personnel afin de promouvoir le leadership et les connaissances en matière de cybersécurité à l'échelle du GC.
    - Les travailleurs en place disposant d'un accès autorisé à des données sensibles peuvent représenter un risque important pour le GC, que ce soit par une divulgation ou une utilisation abusive, intentionnelle ou non. En l'absence de processus modernisés d'enquête de sécurité et d'assurance continue pour les employés et les sous-traitants, d'un accès fiable et fondé sur l'identité aux ressources et aux renseignements de la TI, ainsi que de pratiques

de gestion antifraude rigoureuses, le risque de menace interne est accru.

Pour composer avec l'évolution constante des risques liés à la cybersécurité, le GC devra mobiliser ses forces collectives afin de mettre en place des systèmes d'information sûrs et résistants. Ces forces seront appuyée par des politiques axées sur l'action, une plus grande agilité, ainsi qu'une planification des investissements visant à combler les lacunes, afin que la population canadienne ait la certitude que ses données sont protégées, et que la prestation de services critiques se fasse sans interruption.

2. Approche pangouvernementale en matière de cybersécurité des opérations gouvernementales

▶ Dans cette section

2.1 Vision

L'adoption d'une approche pangouvernementale en matière de cybersécurité des opérations gouvernementales viendra appuyer la prestation de services gouvernementaux pour permettre à l'ensemble de la population canadienne de bénéficier des services gouvernementaux à l'ère numérique. Pour ce faire, le GC doit fournir des outils modernisés et accessibles à l'appui de la prestation de services. La cybersécurité est une composante fondamentale qui assure la prestation de services et d'avantages gouvernementaux de manière simple, sûre et efficiente.Par conséquent, le GC doit donner la priorité aux efforts visant à concrétiser sa vision globale de :

Construire un GC de classe mondiale, durable et résilient pour réduire les risques liés à la cybersécurité afin que les ministères et les organismes fédéraux puissent fournir des services numériques sûrs et fiables.

Pour concrétiser cette vision, le GC doit accorder la priorité aux efforts visant à réduire les risques liés à la cybersécurité afin que ses ministères et ses organismes puissent maximiser les avantages de la technologie numérique. Cela signifie également un effort concerté pour optimiser l'utilisation de ses ressources, la mise à profit de solutions communes lorsque possible pour améliorer la cohérence et réduire les risques de configuration inadéquate. Pour ce faire, le GC aura besoin des politiques, personnes, processus et technologies appropriés pour relever et gérer les risques connus et inconnus ou émergents, tout en maintenant un niveau proportionné et efficace de cybersécurité dans tous ses ministères et organismes.

Cette approche permettra également au GC de passer d'une position réactive à une approche proactive en relevant et en traitant les vulnérabilités en matière de sécurité et les lacunes en matière de capacités, tout en suivant le rythme d'évolution des menaces. En outre, le GC doit miser sur la sauvegarde de ses données sensibles, en veillant à protéger et à sécuriser ses systèmes d'information, quel que soit l'environnement dans lequel ils se trouvent. L'intégration de la protection de la vie privée et de la sécurité dès le départ et l'utilisation d'une approche axée sur l'information permettront de fournir des services fiables et d'appuyer des systèmes d'information qui accordent un accès aux actifs protégés à des utilisateurs, des dispositifs et des services fiables et vérifiés qui ont besoin de savoir.

2.2 Principaux intervenants

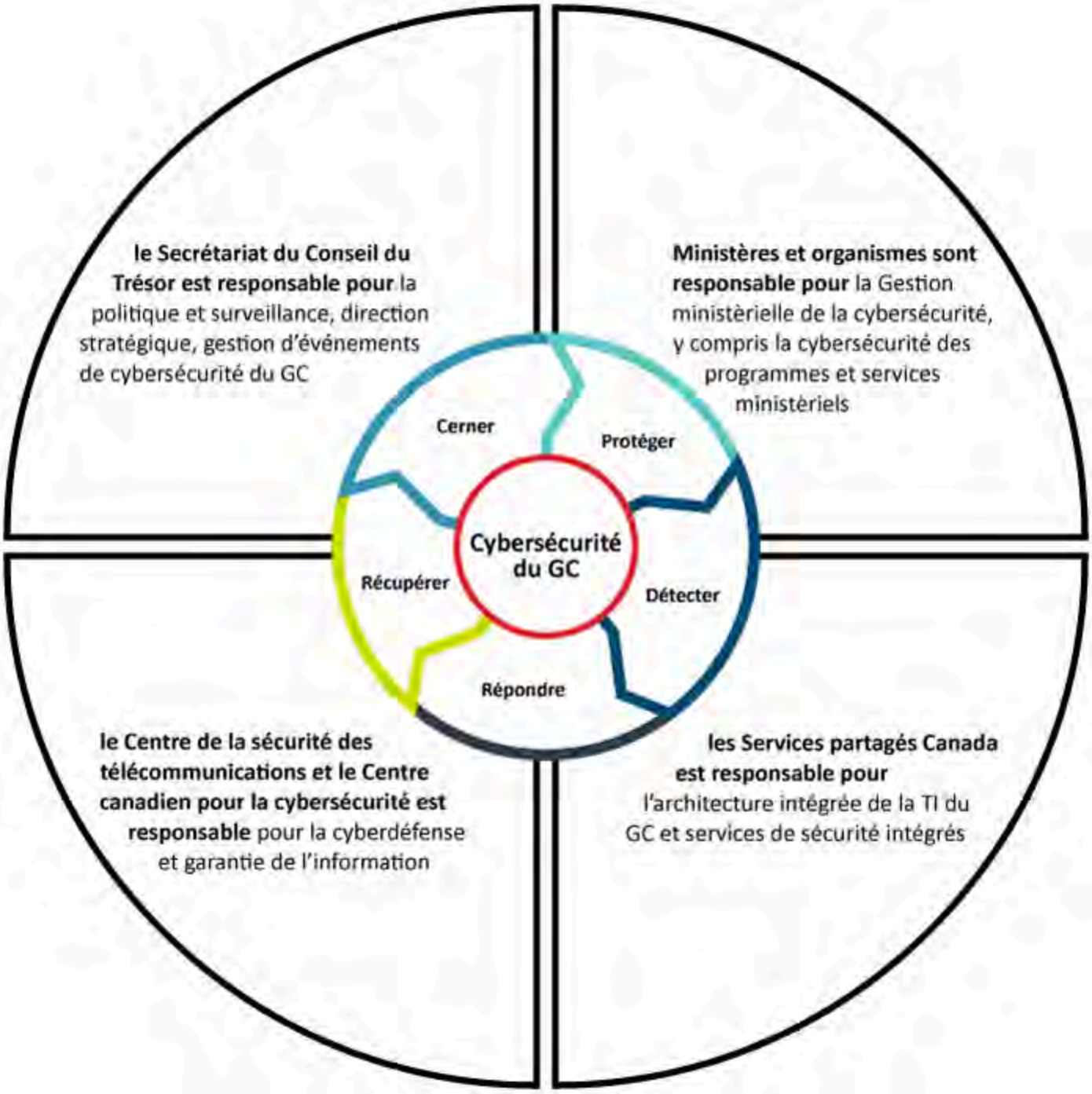
Le GC se doit d'assurer la gestion et la coordination de la cybersécurité au sein du GC pour aller au-devant des cybermenaces et fournir le leadership et le soutien nécessaires pour le Canada. Le renforcement de la gouvernance

et de la surveillance seront nécessaires pour assurer la collaboration et l'harmonisation des ministères et organismes qui ont un rôle clé à jouer dans la gestion de la cybersécurité. Chaque intervenant du GC a un rôle à jouer dans le cadre de la mission fédérale.

Pour parvenir à ses fins, le GC doit faire en sorte que les principaux intervenants unissent leurs efforts. Parmi les principaux intervenants, on compte :

- le **Secrétariat du Conseil du Trésor** — Politique et surveillance, direction stratégique, gestion d'événements de cybersécurité du GC;
- le **Centre de la sécurité des télécommunications** et le **Centre canadien pour la cybersécurité** (CCCS) — Cyberdéfense et garantie de l'information;
- **Services partagés Canada** — Architecture intégrée de la TI du GC et services de sécurité intégrés.
- les **ministères et organismes** — Gestion ministérielle de la cybersécurité, y compris la cybersécurité des programmes et services ministériels.

Figure 1 : Principaux intervenants



▶ Figure 1 - Version textuelle

De façon centrale, le Comité directeur tripartite (Comité tripartite) sur la sécurité de la TI, formé de représentants du Secrétariat du Conseil du Trésor (SCT), de Services partagés Canada (SPC) et du Centre canadien pour la cybersécurité (Cybercentre), joue un rôle important pour ce qui est de fournir des conseils, des renseignements, de la surveillance et une orientation en ce qui concerne les initiatives gouvernementales en matière de sécurité, et d'appuyer les ministères et organismes en vertu des pouvoirs du Conseil du Trésor. Le Comité tripartite poursuivra ses efforts en vue de

coordonner les activités opérationnelles de cybersécurité, de transformer la façon dont les données en matière de cybersécurité et les renseignements sur les menaces sont partagés, utilisés et traités au sein du gouvernement.

Les ministères et organismes sont tenus de gérer les risques liés à la cybersécurité dans leurs secteurs de programme, au fur et à mesure que le gouvernement adopte une approche intégrée en matière de cybersécurité et que les programmes et services deviennent de plus en plus intégrés, il sera essentiel que les risques liés à la cybersécurité soient gérés de façon efficace et globale à l'échelle du GC, selon les responsabilités indiquées dans les instruments politiques du Conseil du Trésor.

En se basant sur les attentes et pouvoirs prévus dans la Politique sur la sécurité du gouvernement et la Politique sur les services et le numérique, les rôles et responsabilités seront clarifiés dans le contexte du modèle opérationnel envisagé sur le plan de la sécurité et de ses variations technologiques. Des relations étroites entre les dirigeants principaux de l'information (DPI) des ministères, les dirigeants principaux de la sécurité (DPS) des ministères, ainsi que l'agent désigné pour la cybersécurité seront nécessaires afin de :

- procéder à la mise en œuvre des priorités et des activités liées à la cybersécurité dans le cadre des plans de sécurité ministériel;
- veiller de façon collective à la gestion des risques liées à la cybersécurité afin d'appuyer la position de cybersécurité dans son ensemble.

2.3 Objectifs stratégiques

Pour concrétiser cette vision, des objectifs stratégiques ont été définis, accompagnés de mesures clés. Les objectifs stratégiques sont :

- Expliquer clairement les risques liés à la cybersécurité et leur incidence sur les opérations, afin de permettre une prise de décisions efficace, axée sur l'action et responsable

- Prévenir les cyberattaques et y résister plus efficacement pour mieux protéger les informations et les actifs du GC.
- Renforcer les capacités et la résilience à l'échelle du GC afin de se préparer de manière proactive à des événements liés à la cybersécurité, d'y répondre et de s'en remettre
- Favoriser l'émergence d'une main-d'œuvre diversifiée au sein du GC, dotée des compétences, des connaissances et de la culture nécessaires en matière de cybersécurité

Ces objectifs stratégiques sont décrits plus en détail dans la section ci-dessous. En outre, l'annexe A comprend un premier jeu d'indicateurs de rendement clé pour permettre d'évaluer les progrès accomplis dans à les mesures présentées.

2.3.1 Objectif no 1 : Expliquer clairement les risques liés à la cybersécurité et leur incidence sur les opérations, afin de permettre une prise de décisions efficace, axée sur l'action et responsable.

L'environnement des cybermenaces étant complexe, évolutif et extrêmement sophistiqué, le GC doit mieux le comprendre afin de mettre au point des mécanismes de défense de sécurité plus complets et à plusieurs niveaux. Pour gérer les risques liés à la cybersécurité, les ministères et les organismes fédéraux doivent mettre en place des processus de gestion des risques, une gouvernance et une responsabilité permettant de relever, d'évaluer et de gérer de manière proactive et efficace ces risques. Les stratégies de cybersécurité ministérielles pluriannuelles, seront soumises au Bureau du dirigeant principal de l'information du SCT (BDPI) à des fins d'approbation, chaque année. Grâce à cette approche axée sur les risques, il y aura une visibilité globale suffisante avec un accès aux données pour effectuer des analyses, ce qui permettra au GC de gérer et de mesurer efficacement les risques liés à la cybersécurité de façon holistique et d'harmoniser les stratégies d'atténuation avec les objectifs à l'échelle du

GC. En outre, le GC disposera de mécanismes permettant de relever, d'évaluer et de gérer rapidement les vulnérabilités à l'échelle de l'organisation.

Les mesures et objectifs clés sont les suivants :

- **Planifier et gouverner pour une gestion durable et intégrée de la cybersécurité.**
  - Définir une approche, une méthodologie, des solutions et des outils communs pour évaluer la position du GC en matière de cybersécurité, qui soient harmonisés avec la politique du GC et au contexte de gouvernance de la TI et qui appliquent une approche basée sur les risques, conformément à la Gestion des risques à la sécurité de la TI : Une approche au cycle de vie (ITSG-33) du Centre canadien pour la cybersécurité.
  - Mener des évaluations indépendantes continues (à l'année longue), des mises à l'essai ou des examens approfondis de la position de cybersécurité des ministères, afin d'aider à cerner et à prioriser les risques à la cybersécurité.
  - Renforcer la gouvernance en ce qui concerne les garanties numériques et technologiques et, dans le cadre du cycle pangouvernemental de planification des investissements en matière de TI, veiller à ce que les dépenses proposées en matière de cybersécurité soient harmonisées avec les priorités et la Stratégie du gouvernement.
  - Utiliser une plateforme intégrée de gestion des risques qui se sert des données pour relever et évaluer et communiquer les risques liés à la cybersécurité qui sont communiqués d'une manière :
    - qui trouve un écho auprès de la haute direction;
    - qui fournit des recommandations réalisables afin d'améliorer la correction des risques, la hiérarchisation des investissements, l'orientation des ressources;

        - qui permet l’adoption d’approches qui préconisent l’assurance agile de la sécurité.
    - Veiller à ce que les ministères et les organismes disposent de ressources et d’un soutien pour améliorer leur position en matière de cybersécurité, conformément à la Stratégie et au MOSC.
- **Mieux comprendre l’exposition à l’échelle du GC et renforcer la gestion de la vulnérabilité.**
    - Mettre en place des outils permettant de relever, de surveiller et de gérer en permanence la surface d’attaque du GC, et mettre à profit des outils existants lorsque possible.
    - Élaborer des répertoires précis des actifs et établir un plan des liens et dépendances entre les actifs, de façon à faciliter les efforts de correction.
    - S’attaquer de manière proactive aux vulnérabilités de l’infrastructure, des systèmes et des applications et aux risques liés à la cybersécurité qu’ils présentent grâce à un programme de gestion des vulnérabilités organisationnelles du GC, afin de veiller à ce que les vulnérabilités relevées soient gérées de manière efficace à l’échelle du patrimoine du GC en matière de numérique, y compris l’intégration dans notre personnel, nos processus et nos technologies de la redondance et de l’approfondissement des capacités résultant des évaluations de la vulnérabilité.
- **Améliorer la gestion des risques liés à la cybersécurité concernant les tiers.**
    - Rechercher des mesures pour améliorer la visibilité du système et la gestion des stocks de logiciels et de matériel de la chaîne d’approvisionnement afin de protéger les informations et les actifs du GC dans le cadre d’une approche solide de gestion des risques liés à la cybersécurité concernant les tiers.
    - Normaliser et renforcer les exigences en matière de cybersécurité et les modalités des accords contractuels avec les fournisseurs

externes, et vérifier régulièrement si les fournisseurs se conforment aux clauses de sécurité contractuelles.

Résultat escompté :

- **La cybersécurité est considérée comme une organisation pangouvernementale, dans le cadre de laquelle les risques liés aux systèmes d'information du GC sont surveillés en permanence, communiqués et corrigés efficacement et rapidement.**

2.3.2 Objectif no 2 : Prévenir les cyberattaques et y résister plus efficacement pour mieux protéger les informations et les actifs du GC.

Le GC s'appuie sur une série de technologies pour remplir ses fonctions et fournir des services numériques, ce qui exige essentiellement une approche qui préconise la sécurité dès la conception afin de veiller à ce que les fonctions et les services se conforment aux pratiques exemplaires de façon systématique et continue, et qu'ils se conforment à des normes robustes. En outre, les ministères et organismes fédéraux utiliseront davantage les capacités, outils et services partagés pour régler les problèmes communs de cybersécurité, ce qui améliorera la cybersécurité à l'échelle du gouvernement et favorisera l'efficacité et l'optimisation des ressources.

Les mesures et objectifs clés sont les suivants :

- **Accélérer la mise en œuvre d'architectures modernes de cybersécurité et d'applications.**
    - Moderniser les systèmes de gestion de l'identité et des justificatifs en matière d'accès à l'échelle du gouvernement, notamment l'authentification multifacteur partout, pour permettre au personnel de travailler en mode hybride.
    - Moderniser les applications et les méthodes de prestation de services numériques sécurisés à l'aide d'architectures de référence pour assurer la sécurité des services numériques.
    - Adopter une approche qui préconise la sécurité dès la conception au moyen de ressources d'architecture et d'ingénierie intégrées

aux projets pour faire en sorte que les aspects de la sécurité et les menaces potentielles soient pris en compte.
    - Améliorer et normaliser les pratiques d'évaluation et d'autorisation de sécurité (E et AS), en partageant les résultats de cet audit à l'échelle de l'organisation afin de réduire le chevauchement dans le cadre de l'évaluation des composantes communes.
    - Poursuivre l'expansion des services de cyberdéfense pour tous les ministères et organismes fédéraux autant que possible.
    - Effectuer la transition des systèmes du GC de façon à ce qu'ils utilisent une cryptographie post-quantique normalisée pour se protéger de la menace quantique.
    - Améliorer la capacité du GC de prévenir, détecter, réagir et se remettre de toute activité frauduleuse contre les applications du GC.
- **Déployer des outils et des dispositifs sécurisés, modernes et accessibles en milieu de travail.**
    - Fournir des solutions communes et sécurisées de référence pour les points d'extrémité, partout où cela est possible, afin qu'elles tiennent compte des besoins spécifiques du personnel du GC comme la mobilité, la collaboration et l'accessibilité. Ce qui comprend :
        - établir des protections qui sont toujours actives et qui sont harmonisées avec les politiques, les directives, les normes et les lignes directrices du GC, et qui sont facilement vérifiables afin d'améliorer la confiance à l'échelle du gouvernement;
        - élaborer des profils de protection faciles à utiliser et des guides à l'appui indiquant les exigences en matière de sécurité et proposant une série de mesures de protection pour garantir une protection adéquate correspondant à la catégorisation de sécurité de l'information et de l'environnement des menaces.
- **Renforcer les mesures de protection des données.**

- Améliorer les pratiques de sécurité de l’information grâce à un modèle de catégorisation de la sécurité actualisé.
- Mettre en place une application automatisée de la politique de sécurité des données afin de prévenir les accès non autorisés et les pertes de données.
- Améliorer la gestion et la sensibilisation aux risques internes afin d’appuyer l’assurance et les pratiques d’après-soins de façon continue.

Résultats escomptés :

- **Des outils, des dispositifs et des services de cybersécurité normalisés et modernes sont déployés et exploités à l’échelle du GC.**
- **Une approche sécurisée dès la conception est appliquée pour garantir la sécurité des services numériques et la protection des actifs numériques tout au long de leur cycle de vie.**

2.3.3 Objectif no 3 : Renforcer les capacités et la résilience à l’échelle du GC afin de se préparer de manière proactive à des événements liés à la cybersécurité, d’y répondre et de s’en remettre.

Même si des mesures de protection et de détection robustes sont en place, le GC sera touché par des incidents liés à la cybersécurité. Il est donc essentiel que le GC puisse réagir rapidement aux incidents liés à la cybersécurité lorsqu’ils se produisent, afin d’en limiter les conséquences et d’assurer la continuité des fonctions et des services essentiels. Les essais et les exercices des plans de réponse aux incidents, tant à l’échelle de l’organisation qu’à l’échelle du gouvernement, ainsi que la capacité à tirer des leçons des incidents et à partager ces leçons constituent un élément clé de l’approche. Une approche de surveillance holistique avec des capacités des mesures de la sécurité proportionnelles à la taille de l’organisation, au contexte commercial et à la maturité contribuera à faciliter la détection

proactive des cybermenaces. En outre, une surveillance et un soutien centralisés de la reprise après les incidents liés à la cybersécurité les plus graves permettront de déterminer et d'atténuer les risques systémiques.

Les mesures et objectifs clés sont les suivants :

- **Améliorer les capacités de surveillance et de détection de la sécurité afin de faciliter la mise en place d'options efficaces et personnalisables pour les ministères et les organismes.**
    - Accroître la clarté des rôles et des responsabilités en matière de surveillance parmi les organisations, les ministères et les organismes de services internes intégrés du GC.
    - Mettre en place une architecture fédérée de centre des opérations de sécurité (COS) permettant une couverture proportionnelle aux besoins opérationnels des ministères et des organismes afin d'accroître l'efficacité, de limiter la répétition des efforts et d'assurer une coordination efficace, notamment :
        - un COS centralisé ou « de commandement » au Cybercentre qui surveille l'infrastructure globale du GC (y compris des réseaux sur place, l'informatique en nuage et d'autres paramètres) dans lequel les ministères tirent profit de l'écosystème de cyberdéfense et obtiennent un accès à leurs données par l'entremise d'une plateforme d'analyse de la sécurité;
        - un centre des opérations de réseau et d'infrastructure multifonctionnel de sécurité (CORIMS) au sein de SPC, afin de permettre une surveillance efficace du bon fonctionnement du réseau des principaux ministères et organismes sous le mandat de SPC, ainsi que la cybersécurité des solutions communes fournies par SPC, tout en appuyant le Cybercentre et les équipes de sécurité des ministères;
        - des COS locaux spécialisés pour certains ministères et organismes ayant atteint un niveau de maturité suffisant et nécessitant une visibilité accrue et des mesures nuancées en

raison de leurs mandats particuliers et/ou de leurs besoins opérationnels qui nécessitent une surveillance accrue afin d'appuyer la cybersécurité de la prestation de programmes et de services;
        - fournir des services de COS gérés aux ministères et organismes qui ne disposent pas d'une maturité suffisante en matière de capacités ou de ressources de surveillance et qui ont besoin d'un soutien pratique en matière de coordination.
    - Faciliter le partage des journaux et autres informations essentielles détenus à l'échelle du gouvernement afin de fournir aux ministères et organismes une visibilité de bout en bout sur les flux réseau appuyant leurs systèmes d'information, ce qui permettra aux ministères et aux organismes d'assumer leurs responsabilités respectives en matière de sécurité.
- **Améliorer l'harmonisation avec le Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) afin d'être en mesure de mieux se préparer aux cyberattaques, d'y répondre et de s'en remettre.**
    - Préparer les ministères par l'entremise d'une meilleure planification des incidents et des exercices réguliers avec des outils qui permettent de faciliter les exercices de cybersécurité (également appelés exercices de simulation) et de partager les rapports après action de manière centralisée afin d'appuyer la hiérarchisation des recommandations à prendre en compte à l'échelle du GC. Au minimum, les ministères et les organismes organiseront chaque année un exercice de simulation sur la cybernétique pouvant aller jusqu'au niveau du sous-ministre.
    - Favoriser la collaboration de la collectivité grâce à une plateforme de gestion des réponses aux incidents liés à la sécurité afin d'automatiser les réponses à et l'établissement de rapports sur les demandes de mesures provenant des ministères et des organismes.

    - Élaborer des outils et des modèles supplémentaires afin d'améliorer les activités ministérielles de Plan de gestion des événements de cybersécurité et appuyer l'exécution du cadre général du PGEC GC.
    - Mettre en place des équipes d'intervention rapide et à grande échelle en cas d'incident répondre et compromettre dotées de compétences diverses, afin d'appuyer les activités de reprise des ministères.
- **Améliorer la résilience des services critiques du GC en renforçant les pratiques de gestion de la continuité des activités.**
    - Établir un plan de continuité des activités à l'échelle du GC afin de veiller à ce qu'il y ait une approche coordonnée pour la gestion des événements qui affectent plusieurs services critiques du GC, afin de veiller à une prestation continue des programmes et des services du GC.

Résultats escomptés :

- **Les réseaux, systèmes, applications et points d'extrémité du GC sont surveillés afin de fournir une capacité de détection proportionnée et de bout en bout, tout en respectant la vie privée.**
- **Les systèmes d'information et les services critiques du GC touchés par des incidents liés à la cybersécurité sont rapidement rétablis et reprennent leurs activités avec un minimum de perturbations.**

2.3.4 Objectif no 4 : Favoriser l'émergence d'une main-d'œuvre diversifiée au sein du GC, dotée des compétences, des connaissances et de la culture nécessaires en matière de cybersécurité.

Pour atteindre la vision et les objectifs de la présente Stratégie, le GC doit cultiver une culture de la cybersécurité qui permette à son personnel d'apprendre, de s'interroger et de se remettre en question afin de s'améliorer de façon continue. Pour favoriser un changement de culture en matière de cybersécurité à l'échelle du gouvernement, il faut améliorer la

sensibilisation à la cybersécurité et les connaissances en la matière de l'ensemble du personnel du GC, afin de s'attaquer de manière proactive aux risques organisationnels liés à la cybersécurité. Selon les normes relatives au numérique du GC, les mesures de sécurité doivent être sans heurts, de sorte qu'elles ne représentent pas une charge pour les utilisateurs. La mise en place d'une solide culture en matière de cybersécurité à l'échelle du GC qui conduira à la maturation des carrières en cybersécurité au sein du GC, et permettra à ce dernier d'attirer des ressources qualifiées, et de permettre à celles-ci de perfectionner et d'entretenir leurs compétences, en offrant des parcours de carrière durables de manière plus efficace. Le fait de procéder ainsi viendra assurer une plus grande sensibilisation et une vigilance accrue de la part de tous les employés du GC.

Les mesures et objectifs clés sont les suivants :

- **Perfectionner les compétences en matière de cybersécurité.**
  - Amener les ministères et organismes concernés à mettre en œuvre des programmes de formation interfonctionnels faisant appel à diverses solutions d'apprentissage qui permettent d'améliorer les compétences des employés de différents ministères qui sont dotés de divers niveaux d'expérience en matière de cybersécurité afin d'augmenter les redondances et la couverture stratégique pour protéger les actifs du GC.
  - Mettre en place une formation normalisée et obligatoire de sensibilisation à la cybersécurité à l'échelle du gouvernement pour tous les employés du GC.
- **Attirer et maintenir en poste des talents de la diversité dans le domaine de la cybersécurité.**
  - Établir des partenariats stratégiques avec des établissements d'enseignement, des groupes industriels et d'autres organisations ou collectivités externes afin de perfectionner les compétences et d'acquérir une expérience pratique qui pourra être utilisée à l'échelle du GC.

- Mettre en place un Centre de perfectionnement de la main-d'œuvre en cybersécurité qui aura pour but de :
  - favoriser une culture de gestion des talents dont l'un des principaux objectifs est de recruter et de maintenir en poste les candidats possédant les compétences et l'expertise requises en matière de cybersécurité;
  - réduire le dédoublement des efforts, stimuler la collaboration interministérielle et le partage des connaissances en vue du perfectionnement et du maintien en poste efficaces des talents et des ressources;
  - appuyer la mise en place d'une progression de carrière claire pour le personnel, notamment des possibilités d'avancement et de responsabilités accrues, en mettant l'accent sur la promotion d'une culture inclusive intégrée, grâce aux programmes d'égalité, de diversité et d'inclusion de l'ensemble du GC.
- **Accélérer l'embauche de fonctionnaires en transformant le filtrage de sécurité du personnel et en permettant une assurance continue.**
  - Moderniser le filtrage de sécurité du personnel grâce à une politique renforcée, à l'automatisation et à l'habilitation de la technologie.

Résultats escomptés :

- **Une culture de la cybersécurité à l'échelle du CG tout entier qui encourage les comportements favorisant l'apprentissage et l'amélioration, avec un bassin de talents en cybersécurité partagé stratégiquement à l'échelle du gouvernement.**
- **Un régime de filtrage solide qui équilibre la prise de décisions fondée sur des preuves et l'assurance continue pour atténuer les risques de menaces internes tout en améliorant les délais d'embauche.**

2.4 Modèle logique

Le modèle logique ci-dessous a été créé pour illustrer les résultats escomptés, ainsi que les principaux intrants et activités, de même que les extrants connexes.

Tableau 1 : Modèle logique

Résultat final	Un Canada sécuritaire et résilient		
Résultats à long terme	Un CG de premier ordre, durable et résilient, qui cherche à réduire les r numériques sécuritaires et fiables.		
Résultats intermédiaires (5 à 10 ans)	Les ministères et les organismes utilisent des renseignements fondés sur des données pour déterminer les cyberrisques et l'incidence des activités, ce qui favorise la prise de décisions efficaces et responsables.	Les ministères et les organismes acquièrent une plus grande maturité cybernétique, ce qui leur permet de mieux prévenir les cyberattaques et d'y réagir plus efficacement.	Les ministères et déployé les capa se préparer de m événements liés répondre à ces é la situation.

Résultats immédiats (2 à 5 ans)	La cybersécurité est une initiative pangouvernementale, dans laquelle les risques liés aux systèmes d'information du GC sont surveillés en permanence, transmis et corrigés de manière efficace et opportune.	Utilisation d'outils, de dispositifs et de services de cybersécurité normalisés et modernes à l'échelle du GC.	Une approche sécuritaire est adoptée dès la conception afin d'assurer la sécurité des services numériques et la protection des actifs numériques tout au long de leur cycle de vie.	La surveillance des réseaux, des systèmes, des applications et des points finaux du GC assure une capacité de détection appropriée et intégrale qui respecte la protection de la vie privée.

Extrants (2 ans)	Plateforme intégrée de gestion des risques. Programme intégré de gestion de la vulnérabilité du GC. Clauses de sécurité contractuelles types afin de gérer les risques liés aux tiers.	Artéfacts, outils et modèles de l'architecture de sécurité intégrée (ASI) de la CG Stratégie et feuille de route de la gestion de l'identité et des justificatifs en matière d'accès (GIJA) du GC. Guides de sécurité. Mise en œuvre de services de cybersécurité intégrés.	Artéfacts de mise en œuvre du modèle opérationnel de sécurité cible (MOSC). Pratiques en matière d'ingénierie des systèmes sécurisés et de modélisation des menaces. Cadre DevSecOps. Modèle moderne de catégorisation de la sécurité. Politiques sur la protection des données numériques.	Architecture du centre d'opérations de sécurité fédérées (COS). Cadre de surveillance continue. Cas d'utilisation de la surveillance de la sécurité.
Activités (2 ans)	Gouvernance simplifiée, responsabilités claires, développement de capacités et d'outils fonctionnels, mesure du rendement et de la maturité cybernétiques.	Mise en place des éléments constitutifs, élaboration de lignes directrices, mise en œuvre de projets agiles.	Mise en œuvre du cycle d'élaboration de systèmes sécurisés, élaboration de processus de modèles opérationnels de sécurité.	Élaborer les exigences et les cas d'utilisation, mettre au clair les rôles et les responsabilités.
Intrants (2 ans)	Informations sur les ressources humaines et financières des partenaire			

3. Approche de la mise en œuvre

Pour concrétiser la vision et atteindre les objectifs stratégiques, il est essentiel de mettre en place un modèle opérationnel de sécurité cible (MOSC) afin d'adopter une approche efficace de la conduite des opérations en matière de cybersécurité qui permettent la prestation de services numériques. Ce modèle doit prendre en compte les dimensions de la politique, des personnes, des processus et de la technologie, ainsi que l'approche de gestion de la cybersécurité du GC. Cette approche comprend les fonctions de sécurité que sont l'identification, la protection, la détection, la réaction et la récupération, qui constituent les principaux piliers d'un programme de cybersécurité holistique. Cette approche fournit également des orientations aux ministères et aux organismes pour mieux comprendre, gérer, réduire et communiquer les risques liés à la cybersécurité, et complète les pratiques existantes décrites en vertu du Cadre stratégique de gestion du risque du SCT et du Cadre de gestion des risques liés à la sécurité de la TI du Cybercentre : Une approche au cycle de vie (ITSG-33).

Par conséquent, le MOSC est un outil permettant d'appuyer l'opérationnalisation de la Stratégie et fournit un plan directeur pour des opérations de cybersécurité réussies. Le MOSC illustre l'éventail des processus et activités de sécurité nécessaires pour disposer d'une capacité de sécurité complète, et fournit une répartition des intervenants qui sont responsables de chaque processus et activité ou qui les appuient. En outre, le MOSC fournit le cadre permettant de clarifier les responsabilités et la mesure dans laquelle des pouvoirs supplémentaires peuvent être nécessaires pour atteindre l'état cible en matière de cybersécurité des opérations gouvernementales.

De plus, le SCT, SPC, le CSC, ainsi que les ministères et organismes, utilisent le MOSC pour orienter l'élaboration de leurs plans ministériels respectifs axés sur cette Stratégie. Il est attendu que ces plans prévoient une approche intégrée de planification des investissements tenant compte de la

cybersécurité, et qui accorde la priorité à l'utilisation de solutions communes et de services intégrés lorsque cela s'avère possible, en fonction de leur disponibilité. Les plans ministériels appuient également l'établissement de feuilles de route. De telles feuilles de route technologiques sont élaborées par les organisations internes comme SPC en tant que principal intervenant pour ce qui est de la prestation de solutions communes sécuritaires.

Il faudra surveiller et mener une évaluation de la Stratégie générale pour assurer le respect de la vision et des objectifs de celle-ci. Le Comité tripartite continuera de jouer un rôle clé dans la gouvernance et la surveillance dans le cas des initiatives stratégiques, mais une gouvernance plus vaste sera également nécessaire pour superviser et obtenir des garanties accrues en ce qui concerne les investissements en cyber sécurité. Cette gouvernance plus vaste, qui sera bâtie sur les autorisations du SCT qui ont trait à la surveillance, comprendra des examens précoces des propositions de dépenses pour assurer le respect de la Stratégie et des priorités du gouvernement. En établissant des garanties en matière de numérique et de technologies, incluant la cybersécurité, le gouvernement sera en mesure d'adopter une approche holistique pour promouvoir la réutilisation de solutions et technologies communes, et d'améliorer l'interopérabilité, ainsi que l'utilisation des actifs de façon efficiente et collaborative. Cela aidera le gouvernement à réaliser des économies et à accroître l'efficience, à améliorer la confiance dans la prestation de services, à réduire les risques, à appuyer l'amélioration de la capacité et à contribuer à l'amélioration des résultats du GC.

4. Conclusion

Si le gouvernement a progressé dans l'amélioration de la cybersécurité au cours des dernières années, l'évolution constante de l'environnement des menaces et des technologies a été encore plus rapide. Les ministères et

organismes doivent faire preuve d'un nouvel engagement pour servir la population canadienne de manière crédible et transparente et pour maintenir la confiance en fournissant des services numériques sûrs et fiables. Il faut trouver un juste équilibre entre la sécurité, le coût associé et l'expérience de l'utilisateur final. Si la sécurité est une préoccupation majeure, le GC doit adopter une solide culture des cyberrisques pour veiller à ce que les mécanismes de sécurité nécessaires correspondant à la sensibilité et à la valeur des informations soient mis en place de manière rentable et avec un minimum d'incidence sur l'utilisateur final.

Annexe A : Indicateurs clés de rendement

Le tableau suivant présente un ensemble proposé d'indicateurs clés de rendement pour surveiller l'avancement de la Stratégie dans la réalisation de la vision et des objectifs stratégiques qui sont exposés de la Stratégie. Ces indicateurs feront l'objet d'un examen plus approfondi dans le cadre de l'élaboration du cadre de gestion du rendement de la Stratégie.

Tableau A.1 : Objectifs stratégiques, mesures clés et indicateurs clés de rendement

Objectif stratégique	Mesures clés	Indicateurs clés de rendement

Objectif stratégique	Mesures clés	Indicateurs clés de rendement
Objectif no 1 : Expliquer les risques liés à la cybersécurité, de même que ses incidences importantes aux activités, en vue d'une prise de décisions efficace, orientée vers l'action, et responsable.	Planifier et gouverner pour la gestion durable et intégrée de la cybersécurité.	• Pourcentage des changements apportés dans les problèmes de conformité aux politiques en suspens chez les ministères ayant terminé leur autoévaluation
	Améliorer la compréhension de l'exposition au risque à l'échelle du GC, et renforcer la gestion de la vulnérabilité.	• La compréhension de l'exposition est améliorée et les vulnérabilités sont atténuées dans l'ensemble du GC : 1) dans une certaine mesure; 2) dans une mesure modérée; 3) dans une grande mesure
	Améliorer la gestion des risques à la cybersécurité des tiers.	• Pourcentage des applications essentielles du GC qui sont gérées dans le cadre du nouveau processus de visibilité de la chaîne d'approvisionnement des logiciels et de la gestion des stocks • Pourcentage des contrats/entrepreneurs échantillonnés dans l'ensemble du GC dont le respect des obligations contractuelles en matière de cybersécurité a fait l'objet d'une vérification

Objectif stratégique	Mesures clés	Indicateurs clés de rendement
Objectif no 2 : Prévenir les cyberattaques et y résister plus efficacement pour mieux protéger les informations et les actifs du CG.	Accélérer la mise en œuvre d'architectures modernes de cybersécurité et d'applications.	• Pourcentage des ministères et organismes qui ont adopté le processus agile d'évaluation et d'autorisation de sécurité • Pourcentage des ministères et organismes qui ont réalisé des progrès vers l'achèvement du plan de transition vers la cryptographie postquantique • Pourcentage des ministères et organismes qui ont intégré au moins un service de capteur du CCCS (capteurs au niveau de l'hôte, capteurs au niveau du réseau, capteurs au niveau du nuage)
	Déployer des outils et des appareils sécurisés, modernes et accessibles en milieu de travail.	• Des outils et des dispositifs sécuritaires, modernes et accessibles en milieu de travail sont déployés 1) dans une certaine mesure; 2) dans une mesure modérée; 3) dans une grande mesure
	Renforcer les mesures de protection des données.	• Pourcentage des ministères et organismes qui tirent parti de la Norme sur la catégorisation de sécurité de l'information à jour

Objectif stratégique	Mesures clés	Indicateurs clés de rendement
Objectif no 3 : Renforcer les capacités et la résilience à l'échelle du GC afin de se préparer de manière proactive à des événements liés à la cybersécurité, d'y répondre et de s'en remettre.	Améliorer les capacités de surveillance et de détection de la sécurité afin d'aider les ministères et les organismes avec des options efficaces et personnalisables.	• Pourcentage des ministères et organismes qui utilisent le Cadre de surveillance et d'exploitation de la sécurité du GC
	Renforcer les pratiques de gestion de cyberévénements pour se préparer aux cyberattaques, y répondre et s'en récupérer.	• Les pratiques de gestion des événements de cybersécurité sont appliquées dans l'ensemble du GC : 1) dans une certaine mesure; 2) dans une mesure modérée; 3) dans une grande mesure
	Améliorer la résilience des services critiques du GC avec des pratiques renforcées de gestion de la continuité des activités.	• Les applications qui permettent d'offrir des services essentiels dans l'ensemble du GC sont bien comprises : 1) dans une certaine mesure; 2) dans une mesure modérée; 3) dans une grande mesure

Objectif stratégique	Mesures clés	Indicateurs clés de rendement
Objectif no 4 : Favoriser l'émergence d'une main-d'œuvre diversifiée au sein du GC, dotée des compétences, des connaissances et de la culture nécessaires en matière de cybersécurité.	Perfectionner les compétences en matière de cybersécurité.	• Pourcentage du personnel du GC ayant suivi, année après année, sa formation sur la sensibilisation à la sécurité (obligatoire)
	Attirer et maintenir en poste des talents diversifiés en matière de cybersécurité.	• Pourcentage de réduction du taux de postes vacants dans des rôles de cybersécurité au GC
	Accélérer l'embauche de fonctionnaires en transformant le filtrage de sécurité du personnel et en permettant une assurance continue.	• Temps médian pour embaucher de nouveaux fonctionnaires

Annexe B : Glossaire

Service ou activité critique

Service ou activité dont la perturbation porterait un préjudice très élevé à la santé, à la sûreté, à la sécurité ou au bien-être économique des Canadiens et des Canadiennes, ou encore au fonctionnement efficace du gouvernement du Canada.(Source : Politique sur la sécurité du gouvernement)

Cybersécurité

La cybersécurité a trait à la sécurité de la transmission des données électroniques et de l'information à travers le cyberespace. Elle couvre la technologie, les processus, les pratiques, la réponse et les mesures d'atténuation ayant été conçus pour protéger l'information électronique, les données et l'infrastructure de l'information contre les méfaits, l'utilisation non autorisée ou les perturbations dans le cyberespace. La cybersécurité vient compléter la sécurité de la TI. La cybersécurité vient opérationnaliser les mesures de sécurité de la TI qui sont établies dans la sous-section B.2.3 de l'annexe B de la Directive sur la gestion de la sécurité.

(Source : Ligne directrice sur les services et le numérique du gouvernement du Canada, sous-section 4.6.1)

Événement de cybersécurité

Un événement, un acte, une omission ou une situation pouvant nuire à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité, dont :

- la divulgation d'une nouvelle vulnérabilité;
- une information indiquant qu'on menace de lancer une attaque contre un système d'information du gouvernement du Canada;
- une tentative de déjouer le périmètre du réseau;
- des courriels suspects ou ciblés avec liens ou pièces jointes que n'ont pu détecter les mesures de sécurité existantes;
- une activité sur le réseau suspecte ou non autorisée qui s'écarte de la norme.

(Source : Plan de gestion des événements de cybersécurité du gouvernement du Canada [PGEC GC] - Canada.ca, sous--section 1.5)

Incident de cybersécurité

Tout événement ou série d'événements, tout acte, toute omission ou toute situation qui a entraîné une compromission. Exemples d'incidents de cybersécurité :

- la violation de données ou la compromission ou corruption de renseignements;
- des attaques par bourrage d'identifiants;
- des tentatives d'hameçonnage;
- l'introduction intentionnelle ou accidentelle d'un logiciel malveillant dans un réseau;
- des attaques par déni de service;
- la défiguration ou la compromission de pages Web ou d'une présence en ligne (y compris l'utilisation non autorisée de comptes de médias sociaux du GC);
- les tentatives réussies de rançongiciel.

(Source : Plan de gestion des événements de cybersécurité du gouvernement du Canada [PGEC GC] - Canada.ca, sous-section 1.5)

Cybermenace

Une activité visant à compromettre la sécurité d'un système d'information en altérant la confidentialité, l'intégrité ou la disponibilité d'un système ou des renseignements qu'il contient.

(Source : Plan de gestion des événements de cybersécurité du gouvernement du Canada [PGEC GC] - Canada.ca, sous-section 1.5)

Technologie de l'information

Tout équipement ou système qui sert à l'acquisition, au stockage, à la manipulation, à la gestion, au déplacement, au contrôle, à l'affichage, à la commutation, aux échanges, à la transmission ou à la réception d'information ou de données. Elle comprend tous les éléments concernant la conception, l'élaboration, l'installation et la mise en œuvre des systèmes d'information et des applications.

(Source : Politique sur les services et le numérique, annexe A)

Menace interne

Menace à une organisation qui vient de personnes de l'organisation, comme les employés, les anciens employés, les entrepreneurs ou les associés, qui détiennent de l'information privilégiée concernant les pratiques de sécurité de l'organisation, les données et les systèmes informatiques.

(Source : Stratégie nationale de cybersécurité du gouvernement du Canada, glossaire)

Services internes intégrés

Un service livré par un ministère du gouvernement du Canada à d'autres ministères du gouvernement du Canada à des fins d'utilisation pangouvernementale.

(Source : Politique sur les services et le numérique, annexe A)

Sécurité de la TI

La sécurité de la TI est une discipline qui désigne l'application de mesures de sécurité, de solutions de sécurité, d'outils et de techniques qui cherchent à protéger les actifs de la TI contre les menaces qui viendraient engendrer une compromission tout au long de leur cycle de vie. La sécurité de la TI mise sur la sécurité des actifs liés aux données électroniques et aux actifs

physiques de la TI. En d'autres termes, elle couvre, à titre d'exemple, la sécurité des fichiers qui sont sauvegardés sur des appareils, la sécurité des systèmes qui servent à les sauvegarder, de même que la sécurité des appareils comme tels.

(Source : Ligne directrice sur les services et le numérique du gouvernement du Canada, sous-section 4.6.1.)

Vulnérabilité

Une faiblesse dans un système d'information, des procédures de sécurité, des mesures de contrôle internes ou la mise en œuvre d'un système qui pourrait être exploitée ou déclenchée par une source de menace.

(Source : Plan de gestion des événements de cybersécurité du gouvernement du Canada [PGEC GC] - Canada.ca, sous-section 1.5.)

Exploit de jour zéro

Une attaque à l'encontre d'une vulnérabilité de jour zéro.

(Source : Plan de gestion des événements de cybersécurité du gouvernement du Canada [PGEC GC] - Canada.ca, sous-section 1.5.)

Vulnérabilités de jour zéro

Une vulnérabilité logicielle qui n'est pas encore connue du fournisseur et qui n'a donc pas été atténuée.

(Source : Plan de gestion des événements de cybersécurité du gouvernement du Canada [PGEC GC] - Canada.ca, sous-section 1.5.)

Notes de bas de page

1 Ottawa enquête sur une cyberattaque contre Affaires mondiales Canada, Le Devoir, le 24 janvier 2022; Un « cyberincident » touche le Conseil national de recherches du Canada , les affaires, le 22 mars 2022; Un groupe de pirates prorusses revendique l'attaque, La Presse, le 11 avril 2023.

ISBN : 978-0-660-72249-8

Date de modification :

2024-06-13