Gouvernement du Canada

Plan de gestion des incidents en matière de technologie de l'information

No de catalogue
ISBN

On peut se procurer ce document sur médias substituts
et sur le site Internet du Secrétariat du Conseil du Trésor du Canada, à l'adresse suivante
www.tbs-sct.gc.ca

Historique des révisions du document

Date	Version	Commentaires (ou source)	Auteur

Préface

Les incidents en matière de technologie de l'information (TI) et de sécurité de TI (STI) qui touchent les réseaux et l'infrastructure du gouvernement du Canada (GC) peuvent avoir de lourdes répercussions sur les opérations gouvernementales et, par conséquent, sur les services assurés à la population canadienne et la confiance envers le gouvernement. Pour gérer de manière opportune et efficiente ces incidents, un programme de gestion des incidents doit avoir en place des services de soutien, des activités et un leadership stratégique assurant la prise de décisions éclairées.

Le Plan de gestion des incidents (PGI) du gouvernement du Canada (GC) représente un cadre opérationnel de la gestion d'incidents relatifs à la TI qui ont eu ou qui pourraient avoir des répercussions sur le GC. Comme le PGI a trait aux incidents relatifs à la TI ou à la STI, dans ce contexte, un incident relatif à la TI se définit comme tout événement présentant les caractéristiques suivantes :

- il perturbe les activités habituelles d'un organisme et cause (ou risque de causer) une diminution de la qualité des services, une interruption ou une réduction de la productivité;
- il constitue une tentative d'accès non autorisé, réussie ou non, à un réseau informatique ou à une ressource de système, en vue de modifier, de détruire ou d'éliminer un tel réseau ou une telle ressource ou encore de le rendre inaccessible.[1]

Le PGI vise à rétablir le service normal le plus rapidement possible et à minimiser les effets défavorables sur les services offerts aux Canadiennes et aux Canadiens, sur les activités gouvernementales et sur la confiance du public envers le gouvernement. Il assure le maintien des niveaux de service, de qualité et de disponibilité les plus élevés possible.[2]

Pour obtenir de l'aide pour la gestion de l'incident communiquer avec **CENTRE DES OPÉRATIONS DU GOUVERNEMENT (COG) :**

Courrier électronique : GOC-COG@ps-sp.gc.ca
Téléphone : 613-991-7000
Télécopieur : 613-996-0995

1. Bureau de la protection des infrastructures essentielles et de la protection civile, Vocabulaire des communications dans les situations d'urgence et de crise, Bulletin terminologique 252.
2. Détails du cadre BITI (v2), http://en.wikipedia.org/wiki/ITIL#Incident_Management

Table des matières

1. Introduction

Le programme de sécurité du GC et la continuité de ses opérations reposent sur la capacité des ministères[3] voire de l'administration fédérale dans son ensemble, de gérer les incidents réels et éventuels en matière de technologie de l'information (TI). Des événements qui touchent ou menacent les services et les opérations du gouvernement surviennent dans tous les ministères. Le GC dépend de plus en plus de la TI pour fournir les services à la population canadienne et maintenir ses opérations, et il doit intervenir avec rapidité et efficacité chaque fois que se produit un incident en matière de TI susceptible de nuire aux services offerts à la population canadienne, aux opérations gouvernementales ou de miner la confiance envers ce dernier.

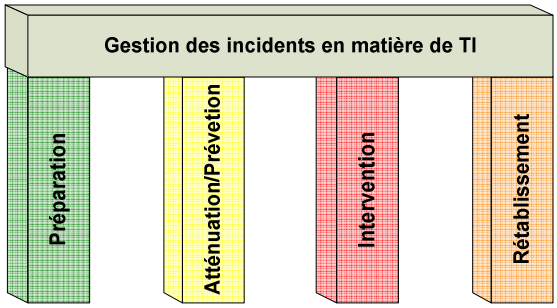

Figure 1 : Les quatre piliers du PGI

Le GC doit se doter de protocoles et de procédures officiels de gestion des incidents en matière de TI et d'assurance de la continuité de ses services et de ses opérations à l'échelle pangouvernementale, étant donné que la capacité et l'infrastructure de prestation des services du gouvernement sont de plus en plus partagées et intégrées. Lorsque surviennent des menaces ou des pannes opérationnelles ou de services, le GC doit alors établir des priorités et réduire le temps d'intervention. C'est pour cela que le PGI du GC en matière de TI décrit les processus de gestion des incidents du GC et détermine les rôles et responsabilités des ministères au chapitre de la présentation de rapports sur les incidents réels et éventuels, de même que leurs interventions en cas de panne des services ou des opérations du gouvernement ou lorsque ses services ou ses opérations sont par ailleurs touchés par un incident en matière de TI. Le PGI officialise les protocoles pangouvernementaux de présentation de rapports, d'avertissement et d'intervention pour assurer la mobilisation adéquate de tous les ministères compétents.

La *Politique du gouvernement sur la sécurité* stipule que les ministères doivent établir des mécanismes pour intervenir judicieusement en cas d'incidents reliés aux TI et pour partager rapidement les détails de l'incident avec les ministères responsables désignés. Une solide coordination horizontale des activités de gestion des incidents s'impose si l'on veut réussir à régler les incidents qui ont une incidence sur le GC.

Le PGI s'harmonise directement avec les quatre piliers généralement acceptés de la gestion des urgences : préparation, atténuation ou prévention, intervention et rétablissement, et énonce les

3. L'utilisation généralisée du terme ministère dans le plan inclut les organismes.

activités de l'analyse postérieure à l'incident afin de cerner et de mettre en œuvre les leçons apprises. Le PGI est un plan propre à un type d'incidents particuliers dans le Plan fédéral d'intervention d'urgence (PFIU). Le cadre du PGI, en mettant l'accent sur les éléments qui sont les plus urgents et les plus susceptibles d'avoir de lourdes répercussions sur le GC, assurera une gestion efficace et efficiente des incidents en matière de TI.

Objectifs

- Permet au GC de mieux connaître la situation.
- Permet de régler rapidement les incidents qui ont des répercussions sur les services et les opérations du gouvernement ou ébranler la confiance à son égard.
- Mise sur les connaissances et les compétences au sein du GC et les partage.
- Permet de réduire les répercussions sur les Canadiennes et les Canadiens, les partenaires et la confiance générale à l'égard du gouvernement.
- Accroît la confiance du public canadien à l'égard de l'efficacité du GC.
- Permet d'améliorer les décisions et les mesures d'atténuation et d'intervention.
- Permet une meilleure planification de la coordination et de la gestion au sein du GC.
- Suscite chez les collectivités de la TI et de la STI au GC un sens des responsabilités partagées.

1.1 Pouvoirs

Ce plan est dressé à la lumière des pouvoirs délégués que confère au ministre de la Sécurité publique la Loi sur la gestion des urgences de même que de ceux qui sont délégués au Secrétariat du Conseil du Trésor du Canada en vertu de la *Loi sur la gestion des finances publiques* et de la *Politique du gouvernement sur la sécurité* qui s'y rapporte.[4]

1.2 But

Ce PGI en matière de TI a pour but d'offrir un cadre opérationnel adapté aux incidents afin d'intégrer l'intervention du gouvernement fédéral, en cas de menaces à la TI, de vulnérabilités et d'incidents qui influent sur le GC ou qui seraient susceptibles de le faire.

4. Ces pouvoirs stipulent que Sécurité publique Canada fasse la promotion des efforts du gouvernement fédéral en matière de préparation (y compris les interventions et les opérations de rétablissement) pour des situations d'urgence de tous types, notamment celles du domaine de la TI, et que le Secrétariat du Conseil du Trésor du Canada assure la supervision des incidents qui influent sur les opérations gouvernementales ou qui pourraient nécessiter des révisions des normes opérationnelles ou de la documentation technique.

Le PGI fait converger toutes les responsabilités au GC en ce qui a trait à la gestion des incidents de TI en un tout cohérent qu'appuient tous les ministères, organismes centraux, organismes responsables et les fournisseurs de service du GC[5] ayant un mandat se rapportant à l'incident.

Le PGI :

- établit des mesures et des processus pour seconder sa mise en place et son exécution;
- énonce des critères et des processus clairs pour mettre en place et exécuter ses rapports et ses interventions;
- identifie clairement les rôles et les responsabilités en matière d'orientation horizontale, de coordination et de communication;
- identifie les liens qu'il a avec les PGI ministériels;
- fournit un modèle opérationnel souple qui s'harmonise au Plan fédéral d'intervention d'urgence (PFIU) et qui facilite la gestion horizontale de l'intervention du GC à la suite d'incidents en matière de TI.

1.3 Portée

Le Plan s'applique à toutes les institutions fédérales assujetties à la Politique du gouvernement sur la sécurité et porte sur les éléments suivants :

- menaces, vulnérabilités, incidents dans le contexte de la TI qui ont une incidence ou qui pourraient en avoir une sur les services offerts à la population canadienne, sur les opérations du GC ou sur le degré de confiance envers le gouvernement;
- incidents survenant dans le contexte de la TI qui nécessitent une intervention concertée à l'échelle du GC (section 1.8).

Le plan ne vise pas ce qui suit :

- activités ministérielles d'intervention, de règlement ou de gestion à la suite d'un incident de TI ou toute autre forme d'activités de planification de la continuité des opérations, parce que chaque ministère doit harmoniser et coordonner ses propres processus de gestion des incidents de TI et plans de continuité avec le PGI du GC;
- coordination d'incidents en matière de TI à l'échelle nationale et internationale, sauf lorsque l'incident influe sur les services assurés à la population canadienne, sur les opérations gouvernementales ou sur la confiance envers le gouvernement et nécessite une intervention du gouvernement fédéral;

5 L'utilisation généralisée de l'expression fournisseur de service du GC inclut les ministères et les organismes qui fournissent des services communs au GC.

- autres formes de gestion des crises et des situations d'urgence.

1.4 Hypothèses

Les hypothèses suivantes ont été formulées pendant l'élaboration du plan :

- S'ils estiment que l'incident est de nature criminelle, les ministères le déclareront directement à la Gendarmerie royale du Canada ou au service de police local.
- Tous les ministères du GC collaboreront et contribueront s'il y a lieu.
- Les rôles et les responsabilités des ministères et des organismes varieront selon la nature et la portée de l'incident.
- Toutes les organisations ont des plans de gestion des incidents et de continuité des opérations et des processus connexes, conformément à la *Politique du gouvernement sur la sécurité*.
- Tous les ministères connaissent le contenu du PFIU.
- Les mandats et les responsabilités actuels des ministères seront respectés.
- Les incidents de TI se rapportant à la divulgation de renseignements personnels suivent les procédures établies en ce qui a trait à la protection des renseignements personnels.
- Les ministères cotent, désignent, communiquent et gèrent l'information selon les mécanismes appropriés. Pour de plus amples renseignements à cet égard, communiquez avec l'agent de sécurité ministériel

1.5 Environnement des risques auxquels le GC est exposé en matière de TI

Jusqu'à maintenant, il a toujours existé un écart entre la perception de la sécurité en matière de TI à l'échelle pangouvernementale et la communication d'une approche intégrée pour assurer et maintenir les services de TI. Les données existantes montrent que l'environnement des risques auxquels le GC est exposé en matière de TI est en constante évolution. Les risques augmentent, parce que les attaques sont bien ciblées et plus complexes et nécessitent une coordination pangouvernementale. De plus, les citoyens sont conscients des répercussions que les menaces et les incidents en matière de TI ont sur leur vie et, par conséquent, sur leur bien-être.

Le GC dépend de plus en plus sur les systèmes de TI pour appuyer ses opérations essentielles, et il dépend comme jamais auparavant sur Internet pour assurer ses services à la population canadienne. Les systèmes de TI deviennent de plus en plus complexes et demeurent malgré tout vulnérables. La menace évolue constamment dans un environnement mondial de plus en plus interrelié, les attaques devenant de plus en plus ciblées et complexes.

La gestion des incidents de TI dans ce contexte mondial est un défi de tous les instants, à cause de la foule incessante de nouvelles vulnérabilités, de codes malveillants et d'incidents concrets. Outre cette vulnérabilité aux menaces nouvelles et émergentes, des facteurs comme l'entretien des systèmes, les pannes de courant, les catastrophes naturelles et les pandémies doivent être pris en compte dans les plans d'urgence, car ils peuvent aussi avoir des répercussions sur les systèmes du GC. Les organisations doivent faire preuve de vigilance constante et être prêtes à intervenir. Étant donné l'interdépendance des ministères fédéraux et l'incidence globale qu'un seul incident peut avoir sur le degré de confiance envers le gouvernement, aucun ministère ne peut gérer à lui seul les incidents de TI.

Même si le GC n'a pas les données adéquates sur la situation pour être en mesure d'évaluer complètement l'état de la sécurité en TI et les mécanismes pour assurer la continuité, de récents incidents ont fait ressortir que le GC n'était pas à l'abri des incidents de TI et qu'il devait se préparer. En outre, le GC lutte contre le crime et les menaces à la sécurité nationale. Comme les incidents qui touchent la prestation des services du CG font les manchettes des médias, le public canadien est au courant des risques qui menacent l'environnement de TI du GC. De plus en plus, les incidents ne peuvent être gérés isolément; ils nécessitent une approche concertée au GC.

1.6 Objectifs

Voici les principaux objectifs du PGI :

- Permet de régler rapidement les incidents pour limiter les répercussions sur les services et les opérations du gouvernement et sur la confiance à son égard.
- Assure un meilleur accès au savoir et à l'expertise qui se trouvent au GC en ce qui a trait à la gestion des incidents à l'échelle pangouvernementale.
- Permet de mieux comprendre les répercussions des incidents sur le GC, afin de mieux les prioriser pour minimiser les conséquences négatives sur la population canadienne et les partenaires et aussi sur la confiance globale envers le gouvernement.
- Fournit une information précise et des rapports d'étape sur les incidents de TI, réels ou potentiels, afin d'améliorer le processus décisionnel, de même que les mesures d'atténuation et d'intervention.
- Permet une meilleure planification de la coordination et de la gestion des incidents de TI au sein du GC.
- Permet au GC de mieux connaître la situation pour étayer une vision intégrée de l'état de la sécurité de la TI à l'échelle pangouvernementale.
- Permet au GC d'améliorer ses activités pour atténuer les risques d'incidents de TI et de se préparer à les prévenir et à s'en protéger.

- Suscite chez les collectivités de la TI et de la STI au GC un sens des responsabilités partagées.
- Améliore la perception qu'a le public canadien de l'efficacité avec laquelle le GC serait en mesure d'intervenir à la suite d'incidents de TI qui influent ou qui pourraient influer sur la prestation des services à la population canadienne, sur les opérations gouvernementales ou sur la confiance envers le gouvernement.

1.7 Modèle de gouvernance

Lorsque se produit un incident, la mobilisation au bon moment des cadres supérieurs est un élément clé pour assurer une intervention musclée, proactive ou réactive, selon le cas. Le modèle de gouvernance du PGI renferme les comités de la haute direction et les responsables qui interviendront lorsque les critères de déclenchement et de gravité s'appliqueront.

La figure 2 montre l'orientation et les conseils que les comités de gestion assureront en ce qui a trait aux quatre piliers du PGI : préparation, atténuation ou prévention, intervention et rétablissement. Les circonstances et la gravité de chaque situation dicteront qui, au nombre des comités et des responsables suivants, devront participer :

- Équipe de gestion
- Agent de coordination fédéral
- Comité de gestion des urgences des sous-ministres adjoints
- Comité des sous-ministres sur la sécurité nationale
- Comité du Cabinet chargé des opérations

Les rôles et les responsabilités des comités sont décrits plus en détail à la section 1.8.

Les activités à court et à long terme seront prévues dans le cadre de la structure de gouvernance assurée par les comités et les responsables cités dans le PGI. La structure de gouvernance assurée par les comités et les responsables cités dans le PGI. Les activités à court terme sont celles que dictent les incidents et qui sont menées pour atténuer la menace ou la vulnérabilité, pour intervenir pendant l'incident ou pour rétablir les opérations après coup. Leur calendrier d'exécution est souvent serré et nécessite la prise de mesures rapides et concertées.

Quant aux activités à long terme, elles se rapportent à l'analyse postérieure à l'incident et aux leçons apprises, à la préparation et aux mesures d'atténuation, pour lesquelles le Comité des sous-ministres adjoints chargé de la sécurité (SMA Sécurité) et le Conseil des dirigeants principaux de l'information (CDPI) assureront le leadership stratégique à plus long terme, l'orientation et la gouvernance concernant la sécurité et la TI respectivement.

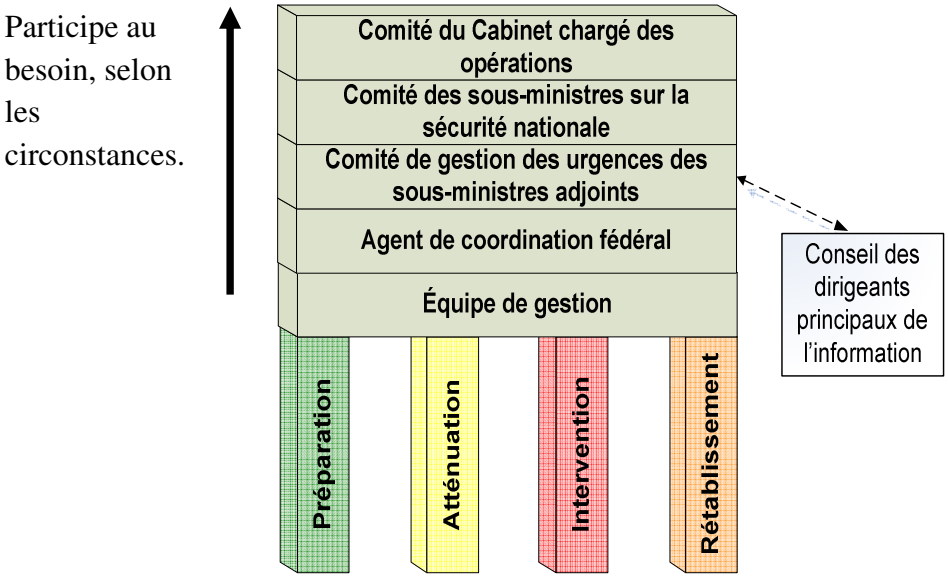

Figure 2 : Gouvernance horizontale du PGI

1.8 Rôles et responsabilités

Pour assurer l'orientation horizontale, la coordination et la communication nécessaires pour que le GC intervienne de manière concertée et uniforme lorsque se produisent des incidents de TI, Sécurité publique Canada (SPC) supervisera les incidents et les menaces possibles nuit et jour, coordonnera les activités et fournira son soutien. La figure 3 montre l'intégration des volets orientation horizontale, coordination et communication.

Participe au besoin, selon les circonstances.

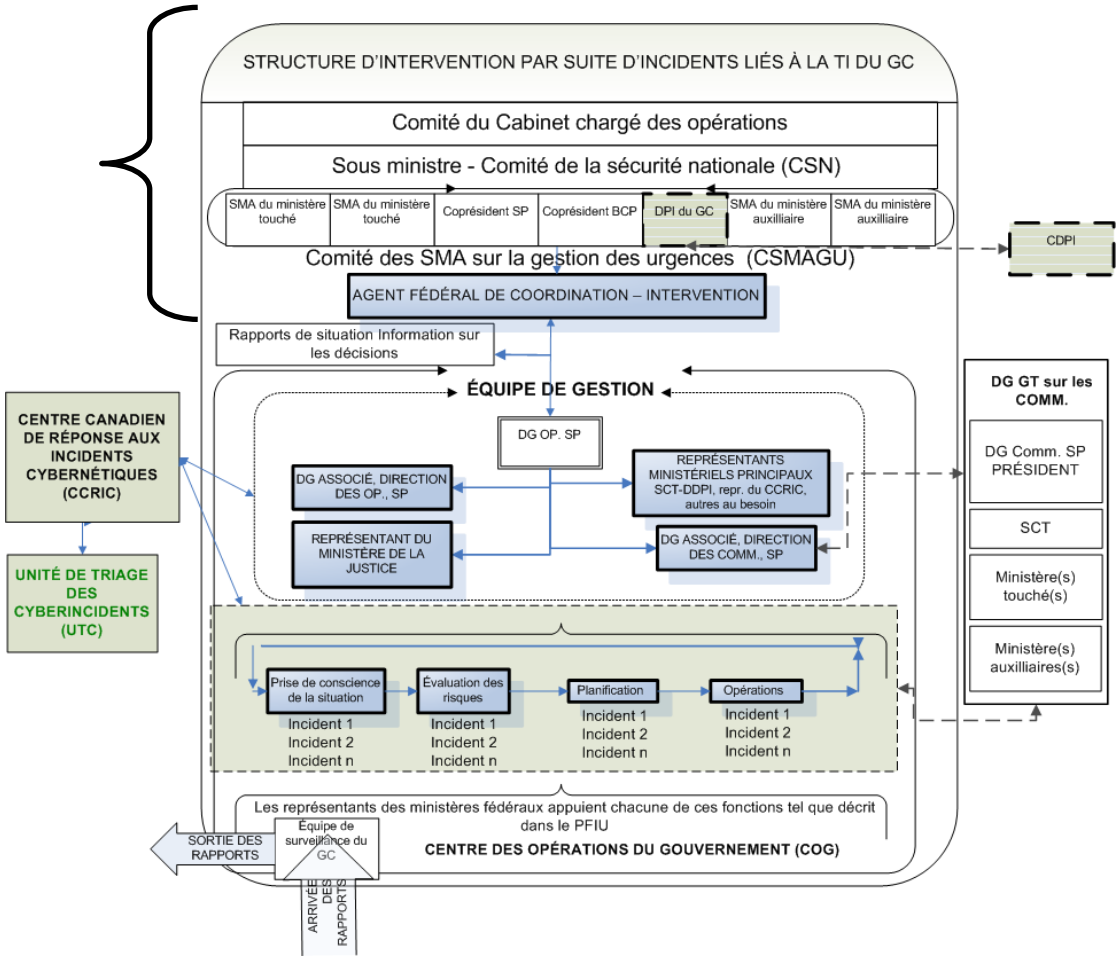

Figure 3 : Structure d'intervention en cas d'incident de TI au GC

1.8.1 Orientation horizontale

Le PGI s'harmonise à la structure des comités de la haute direction déjà en place et utilisée dans le PFIU; il inclut de surcroît les personnes et les comités clés nécessaires pour gérer les incidents de TI qui influent ou qui pourraient influer sur le GC. Une menace, une vulnérabilité ou un incident sera porté à l'attention de ces comités au besoin, si les circonstances le justifient. Voici la liste des comités de la haute direction et des responsables :

- Le **Comité du Cabinet chargé des opérations (Comité Ops)** supervise l'intervention du GC à la suite d'un incident qui touche durement le GC[6] et il participera sur demande du Comité des sous-ministres adjoints sur la sécurité nationale (CSMASN). Le Comité Ops donne des

6 Annexe C : Matrice de la gravité de l'impact

directives aux hauts fonctionnaires et peut assigner une partie ou la totalité de ses responsabilités concernant l'incident au Comité du Cabinet chargé des affaires étrangères et de la sécurité.

- Le **Comité des sous-ministres adjoints sur la sécurité nationale (CSMASN)** donne des directives au Comité de gestion des urgences des sous-ministres adjoints (CGU-SMA) et à l'agent de coordination fédéral (ACF) lorsque surviennent des incidents qui touchent durement le GC1 et qui nécessitent l'intervention concertée du GC. Le CSMASN participera sur demande du CGU-SMA ou du conseiller en matière de sécurité nationale. Ce comité est le principal comité responsable de la coordination de l'intervention du GC et de la prestation de conseils aux ministres. Sa composition peut varier selon la nature de l'incident. Le CSMASN détermine aussi le contenu des notes d'information destinées aux ministres, examine, approuve et recommande les mesures d'intervention à porter à l'attention des ministres.
- Le **Comité de gestion des urgences des sous-ministres adjoints (CGU-SMA)** assure en parallèle à tous les ministères fédéraux et au sein de ceux-ci un soutien pour gérer les incidents. Le CGU-SMA donne une orientation stratégique et des conseils à l'ACF dans le cas d'incidents dont les répercussions varient de moyennes à élevées1 (telles que déterminées par l'ACF) et donne des directives aux responsables du Centre des opérations du gouvernement (COG). Le CGU-SMA interviendra sur demande de l'équipe de gestion ou de l'agent de coordination fédéral (ACF). La figure 4 montre comment circule l'information entre le COG et le CGU-SMA. Ce comité approuve le contenu et la substance des notes d'information destinées aux sous-ministres, coordonne et recommande des options d'intervention au CSMASN ou au Comité des opérations.

  Comme la composition de ce comité est variable, le dirigeant principal de l'information du gouvernement du Canada est le membre permanent pour tout incident de TI qui influe ou qui pourrait influer sur les opérations ou les services du GC ou sur la confiance envers le gouvernement.
- Le **dirigeant principal de l'information pour le gouvernement du Canada (DPI du GC)** conseille le CGU-SMA sur des questions se rapportant à des incidents qui influent sur la sécurité ou le fonctionnement des systèmes et réseaux de TI du GC, ou encore sur la prestation des services ou sur la confiance envers le gouvernement. Le DPI du GC est le président du Conseil des DPI (CDPI) et l'intermédiaire avec la collectivité élargie des DPI au GC. Le DPI du GC :
  - approuve le débranchement des infrastructures ou des systèmes ministériels s'il faut confiner un incident et réduire son incidence à l'échelle pangouvernementale, après avoir consulté le CDPI* et le(s) ministère(s) touché(s). Il peut notamment s'agir d'interconnexions de réseaux, de services communs ou partagés, de systèmes essentiels et d'autres infrastructures ministérielles;

- approuve le blocage ou le débranchement de services limités, lorsque des mesures de confinement s'imposent sur-le-champ et que l'incidence sur les opérations gouvernementales ou les services essentiels est minimale;
- approuve la directive du GC d'appliquer des mesures pour atténuer les risques, à titre préventif, pour réduire l'incidence ou l'exposition aux menaces, aux vulnérabilités ou aux incidents.

- Le **Conseil des dirigeants principaux de l'information (CDPI)** est l'organe consultatif du DPI du GC et il appuie la gestion des incidents de TI qui touchent la sécurité, les systèmes, les réseaux, la prestation des services ou la confiance envers le gouvernement. Ce comité prodigue des avis, des directives et des conseils en ce qui a trait à la gestion des incidents au GC, notamment aux plans d'intervention et de rétablissement, sans toutefois s'y limiter.
- L'**agent de coordination fédéral (ACF)**, au nom du ministre de la Sécurité publique, assume la responsabilité générale de coordonner une intervention fédérale s'il survient une urgence.[7] En ce qui concerne le PGI, cela inclut tout incident qui répond aux critères de déclenchement et de gravité que renferme le plan. Le sous-ministre de la Sécurité publique ou le sous-ministre adjoint principal de la Sécurité publique peut jouer ce rôle.
- L'**équipe de gestion**, sous le leadership du directeur général, Direction générale des opérations de SPC, gère les mesures et les fonctions qui se rapportent au Système fédéral de gestion des interventions d'urgence (SFGIU), établit et supervise l'atteinte des objectifs fixés pour chaque période opérationnelle.[8] En ce qui a trait au PGI du GC, l'équipe de gestion est l'équipe de la haute direction qui fournit une orientation stratégique au COG et au CCRIC, lorsque les incidents de TI répondent aux critères de déclenchement et de gravité du PGI. C'est également l'équipe de la haute direction qui sert d'interface avec l'ACF et qui approuve les produits destinés aux cadres supérieurs fédéraux, comme les documents d'information en vue d'une décision (voir l'annexe F). En plus des représentants de l'équipe de gestion décrits dans le PFIU, dans le cadre du PGI, l'équipe de gestion inclut aussi un représentant ministériel de la Direction du dirigeant principal de l'information du Secrétariat du Conseil du Trésor du Canada (DDPI du SCT) et d'autres ministères primaires, selon la nature de l'incident de TI.

7 Plan fédéral d'intervention d'urgence
*lorsque les impératifs opérationnels le permettent

8 Plan fédéral d'intervention d'urgence

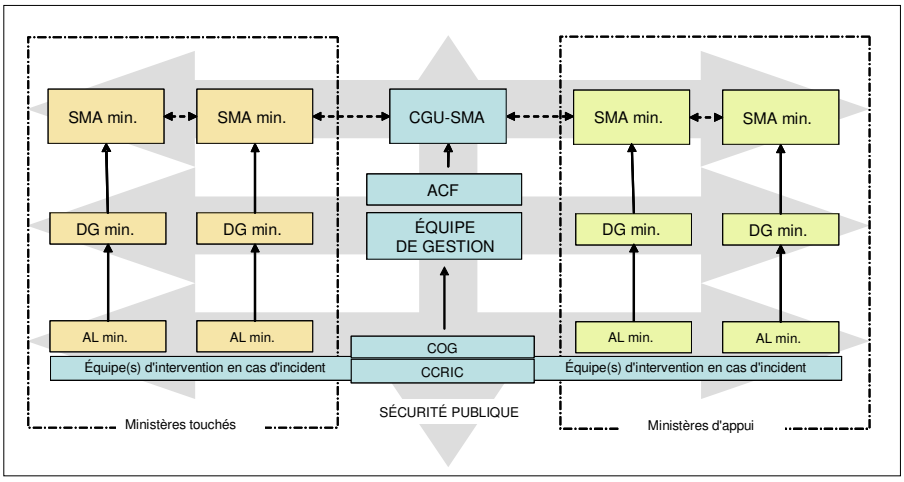

Figure 4 : Flux d'information entre le COG et le CGU-SMA

1.8.2 Coordination et analyse

- Le **Centre canadien de réponse aux incidents cybernétiques (CCRIC)** est la ressource centrale qui assure la supervision et la coordination de l'intervention à la suite de tout incident de TI afin de protéger le GC[9]. Le Centre des opérations du gouvernement (COG) assure des fonctions correspondantes nuit et jour au reste du GC. Pour étayer son mandat dans le cadre du PGI, le CCRIC doit fournir soutien et coordination aux intervenants suivants :
- Le **Centre des opérations du gouvernement (COG)** qu'abrite Sécurité publique Canada au nom du GC est le principal noyau de spécialistes du domaine et d'agents de liaison des ministères, des organismes non gouvernementaux et du secteur privé (s'il y a lieu) qui exécutent les fonctions primaires du SFGIU. Les centres d'opérations de chaque ministère appuient les rôles et les mandats de leur ministère respectif et participent à l'intervention concertée du gouvernement du Canada par l'intermédiaire du COG. Le COG, dont l'effectif chargé des opérations quotidiennes est formé d'**agents de surveillance** de SPC, assure l'interface entre le CCRIC et le GC.
- Lorsqu'un incident correspond au niveau d'intervention 2[10] ou 3[11] du PFIU, les représentants ministériels peuvent être appelés à venir se joindre à l'effectif du COG. C'est le directeur général, Direction générale des opérations qui, à la lumière des circonstances, détermine, après avoir consulté l'équipe de gestion et l'ACF, si un incident de TI répond aux critères de déclenchement (section 1.9) et aux critères de gravité moyenne à élevée. Tout dépendant des circonstances de l'incident de TI, le COG inclura des spécialistes du domaine ou des agents

9 C'est un sous-ensemble de son mandat élargi qui inclut la protection des infrastructures nationales essentielles.

10 Le niveau d'intervention 2 du PFIU fait référence à l'augmentation de l'effectif du COG.

11 Le niveau d'intervention 3 du PFIU fait référence à une augmentation marquée de l'effectif du COG.

de liaison des ministères primaires et des ministères d'appui, pour seconder les fonctions liées aux opérations, à la connaissance de la situation, à l'évaluation des risques et à la planification, comme le mentionne le PFIU. Lorsque le niveau du PFIU est majoré, ces représentants ministériels seconderont temporairement le COG et l'équipe de gestion, mais ils continueront de relever avant tout de leur ministère d'attache.

- Le **Centre canadien de réponse aux incidents cybernétiques (CCRIC)** est le centre de coordination au niveau national des interventions à tout incident cybernétique. Il reçoit des rapports d'incident de partout au GC, ainsi que de ses partenaires nationaux et internationaux et de gouvernements étrangers[12]. Le CCRIC analyse ces données à la lumière des vulnérabilités et des risques et accroît ses capacités d'analyse et d'intervention en faisant appel à l'Unité de triage des cyberincidents (UTC) et au COG. Pour atteindre les objectifs stratégiques, le CCRIC informera, de manière continue et permanente, la DDPI du SCT des incidents qui répondent aux critères de déclenchement du PGI.
- L'**Unité de triage des cyberincidents (UTC)**, dirigée par le CCRIC, veille à assurer une intervention rapide et ciblée à la suite d'un cyberincident. Elle est formée de représentants de Sécurité publique Canada, de la Gendarmerie royale du Canada, du Service du renseignement de sécurité, du ministère de la Défense nationale[13] et du Centre de la sécurité des télécommunications Canada. L'UTC est chargée de ce qui suit :
  - analyser les incidents et les cyberalertes déclarés par des sources fédérales, nationales et internationales;
  - évaluer la nature d'un incident pour identifier les rôles d'un ministère primaire et des ministères de soutien;
  - veiller à ce que l'information soit échangée entre les ministères.
- Les **ministères primaires** sont ceux dont le mandat est relié à un élément principal de l'incident. Certains représentants de ces ministères peuvent être appelés par SPC à remplir diverses fonctions au COG, à agir comme agents de liaison entre SPC et leur ministère respectif ou à assurer la communication dans leur ministère d'attache sur l'évolution de l'intervention liée à un incident.
- Les **ministères d'appui** sont ceux qui assurent une aide générale ou spécialisée à un ministère primaire dans le cadre d'une intervention à la suite d'un incident. Certains représentants de ces ministères peuvent être appelés par SPC à remplir diverses fonctions au COG, à agir

12 Le PGI reconnaît l'importance d'analyser l'information provenant de diverses sources; les rapports d'incidents des partenaires qui débordent de la portée du PGI sont jugés être un apport direct au PGI lorsqu'ils évaluent les répercussions réelles ou potentielles sur le GC.

13 Le ministère de la Défense nationale a été proposé comme membre de l'UTC (à l'étude).

comme agents de liaison entre SPC et leur ministère respectif ou à assurer la communication dans leur ministère d'attache sur l'évolution de l'intervention liée à un incident.

- Les **ministères touchés** sont ceux qui répondent aux critères de déclenchement et aux critères de gravité moyenne ou élevée du PGI (voir l'annexe C).

1.8.3 Communication

L'interface entre le GC et le CCRIC se fait par l'intermédiaire du COG, qu'abrite SPC. Les activités de communication, dont les stratégies et les communications publiques, seront dirigées par SPC, par l'intermédiaire des personnes suivantes :

- Le **directeur général, Communications de Sécurité publique Canada (DG, Communications de SPC)** - Conformément au PFIU, SPC est le ministère primaire chargé des fonctions de soutien des communications en cas d'urgence et de liaison avec les directeurs généraux des Communications des autres ministères.
- Le **Groupe de travail chargé des communications du directeur général (GT, DG Comm)** – Il relève du DG, Communications de SPC. Il regroupe les représentants des communications du SCT et des ministères touchés et d'appui, pour coordonner les aspects des communications de l'incident, s'il y a lieu.

1.8.4 Continuité et surveillance

Pour exécuter certaines activités permanentes de soutien et de gestion du PGI :

- La **DDPI du SCT** prendra en charge la supervision du PGI du GC. Dans le cadre de cette responsabilité, afin que les objectifs stratégiques du GC soient atteints, le CCRIC informera, de manière continue et permanente, la DDPI du SCT des incidents qui répondent aux critères de déclenchement et de gravité du PGI. De plus, la DDPI du SCT recevra tous les plans d'action postérieurs à l'incident et, s'il y a lieu, effectuera des examens rétrospectifs des activités liées à l'incident, fera le suivi des rapports postérieurs à l'incident, dressera et exploitera un dépôt des leçons apprises au GC, élaborera, tiendra à jour et, au besoin, rajustera les instruments stratégiques et le PGI.
- Le **CDPI**, l'organe consultatif du DPI du GC, donnera des avis et des conseils relativement à la gestion des incidents au GC. De plus, il assurera une orientation stratégique et son leadership en ce qui a trait aux activités de préparation, d'atténuation et d'analyse postérieure à l'incident. Il recevra régulièrement les rapports sommaires sur les incidents de TI qui influent sur le GC.
- Le **Comité des sous-ministres adjoints sur la sécurité (SMA Sécurité)**, à titre d'organe consultatif du GC pendant les activités normales, fournit une gouvernance et des conseils stratégiques, dont les mesures stratégiques relevées dans l'analyse postérieure à l'incident et le suivi. De plus, il assurera une orientation stratégique et un leadership en ce qui a trait aux

activités de préparation, d'atténuation et d'analyse postérieure à l'incident en matière de sécurité et recevra régulièrement les rapports sommaires sur les incidents de TI qui influent sur le GC.

1.9 Mise en œuvre - Critères de déclenchement

Bien que le PGI du GC prévoit que la responsabilité d'assurer la préparation continuelle contre les menaces, les vulnérabilités et les incidents incombe à tous les ministères fédéraux, leur gravité pourrait justifier de les porter à l'attention du niveau fédéral advenant l'une ou plusieurs des conditions suivantes :

- La menace, la vulnérabilité ou l'incident influe sur les services ou les infrastructures essentiels du ministère, tels qu'identifiés dans les plans ministériels de la continuité des activités.
- La menace, la vulnérabilité ou l'incident nécessite une intervention concertée du GC, notamment lorsque les circonstances suivantes se produisent :
  - la menace, la vulnérabilité ou l'incident a des répercussions intersectorielles, c'est-à-dire qu'il se produit dans un ministère et a ou pourrait avoir sur d'autres ministères une incidence négative ou inconnue;
  - la menace, la vulnérabilité ou l'incident influe ou pourrait influer sur plus d'un ministère;
  - il est très probable que les services communs soient touchés.
- La menace, la vulnérabilité ou l'incident influe sur d'autres instances, sur les secteurs d'infrastructure essentiels ou sur d'autres partenaires importants alors qu'il faut dégager un point d'entrée unique du GC.
- La menace, la vulnérabilité ou l'incident a des répercussions sur les employés, sur la prestation des services à la population canadienne ou sur la confiance à l'égard du GC.
- La menace, la vulnérabilité ou l'incident touche la population canadienne ou la sécurité nationale, selon qu'il s'agit de la divulgation non autorisée de renseignements de nature délicate détenus, traités, transmis ou stockés électroniquement.[14]

Nota : En cas d'incertitude, les ministères devraient communiquer avec le CCRIC pour qu'il les aide à mieux définir les caractéristiques de la menace, de la vulnérabilité ou de l'incident et précise les rapports à produire. Le CCRIC fera participer les cyberspécialistes de l'UTC, pour évaluer la nature de l'incident et son incidence possible, de même que pour mettre en place les mesures qui aideront à défendre tout le gouvernement.

14 Conformément à l'Avis signalement d'incident SPIN 2008-02 en matière de TI

Critères de déclenchement

La menace, la vulnérabilité ou l'incident de TI :

- Influe ou pourrait influer sur des services ou des infrastructures ministériels essentiels.
- A ou pourrait avoir des répercussions intersectorielles (impact qu'un incident dans un ministère a ou pourrait avoir sur d'autres ministères).
- Influe ou pourrait influer sur plus d'un ministère.
- Influe ou pourrait influer sur les services communs.
- Influe ou pourrait influer sur les fonctionnaires, sur la prestation de services à la population canadienne ou sur la confiance envers le GC.
- Influe ou pourrait influer sur la sécurité nationale ou a ou pourrait avoir une incidence sur la vie privée de la population canadienne à cause de la divulgation non autorisée de renseignements de nature délicate détenus, traités, transmis ou stockés électroniquement.
- Influe ou pourrait influer sur d'autres instances, secteurs d'infrastructure essentiels ou partenaires importants, lorsqu'il faut dégager un point d'entrée unique du GC.

2 Concept d’opération

Le PGI du GC fournit une approche complète pour gérer les menaces, les vulnérabilités et les incidents. Tout en respectant l’autorité de chaque administrateur général, le GC dans son ensemble doit tenir compte des répercussions plus étendues que les menaces, les vulnérabilités et les incidents ont ou pourraient avoir sur les services à la population canadienne, les opérations gouvernementales ou la confiance envers le GC. Ceci étant dit, les ministères continueront de protéger les activités de TI et de veiller à ce que les mécanismes d’intervention en cas d’incident et de continuité des opérations de TI soient en place pour étayer toutes les étapes de la gestion des incidents, en tenant compte également de l’approche intégrée du PGI du GC.

2.1 Modèle opérationnel

Pour concrétiser les objectifs du PGI du GC, les ministères et le gouvernement doivent l’appuyer et participer à l’élaboration des éléments suivants se son modèle opérationnel (figure 5), notamment :

- un ensemble de vastes processus continus liés à la préparation,
- les mesures préventives liées à l’atténuation des risques,
- les activités réactives liées à l’intervention,
- le retour à la normale après le rétablissement des opérations.

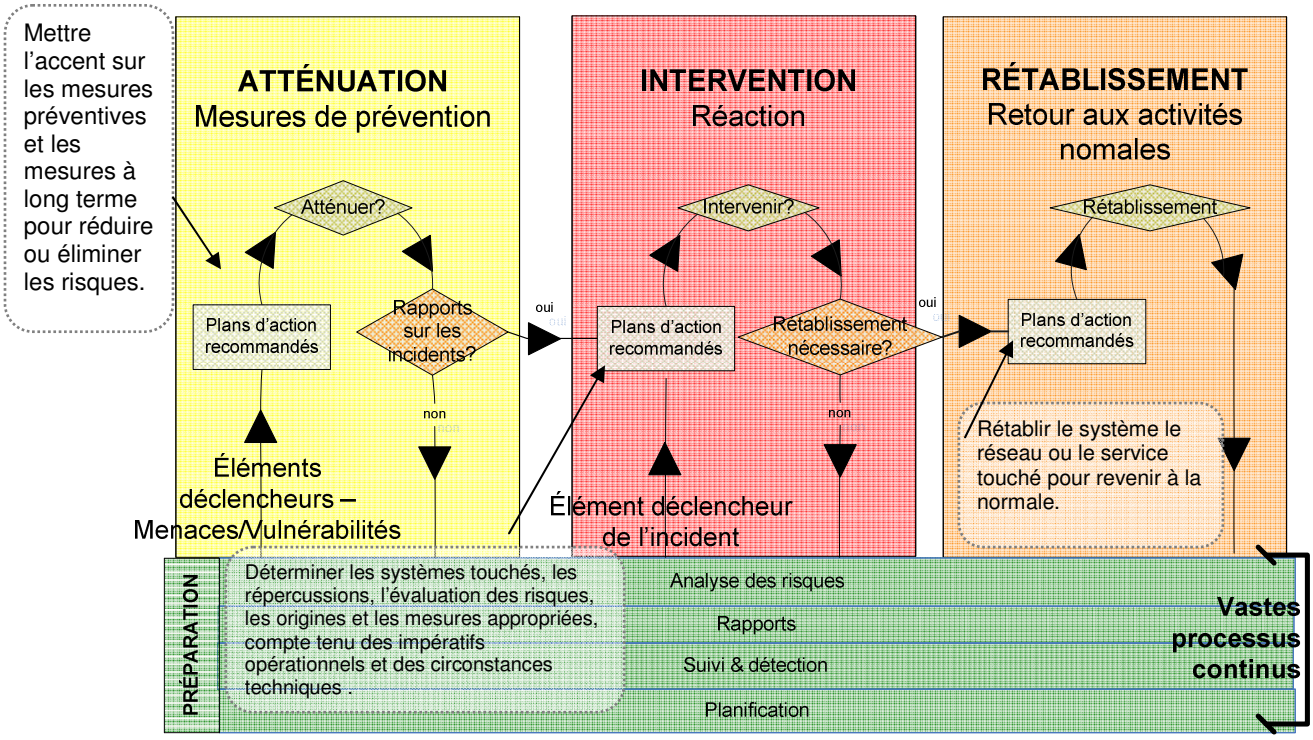

Figure 5 : Modèle opérationnel de la gestion des incidents de TI

Préparation – Il s'agit de la mise en place du fondement du modèle opérationnel et elle consiste en des processus continus de planification, de supervision, d'analyse des risques et de rapports, lesquels font partie des opérations normales d'un environnement de TI. Les activités de préparation servent à prévoir des situations ou des incidents précis ou même imprévisibles et à identifier les menaces, les vulnérabilités ou les incidents qui déclenchent des mesures d'atténuation, d'intervention et de rétablissement à l'échelle pangouvernementale. Ces processus sont permanents. Par exemple, les activités de supervision se poursuivent pendant les activités d'atténuation, d'intervention et de rétablissement. De la même manière, les activités stratégiques à plus long terme dans le cadre de la planification tiennent compte de manière typique des tendances en matière d'incidents ou des autres changements survenus dans l'environnement de TI qui influent sur les risques et qui appellent des mesures d'atténuation.

Atténuation – On englobe les mesures préventives qui sont prises pour éviter l'exposition à des menaces et les vulnérabilités découlant d'incidents ou pour réduire les effets de ces incidents lorsqu'ils se produisent. L'étape de l'atténuation est différente des autres, parce que les mesures qui sont prises visent à réduire ou à éliminer les risques de manière proactive contrairement aux mesures réactives qui sont prises aux étapes de l'intervention et du rétablissement. Idéalement, les activités d'atténuation sont déclenchées assez tôt pour permettre de prendre des mesures de

protection à long terme. Les menaces et les vulnérabilités seront portées à l'attention du GC par les ministères, le CCRIC ou les membres de l'UTC dès que les critères du PGI sont déclenchés.

Intervention – C'est l'étape à laquelle on décide des mesures appropriées pour protéger des services qui ont été touchés ou qui pourraient l'être par l'incident. Les incidents seront portés à l'attention du GC aux fins d'intervention lorsqu'une menace, une vulnérabilité ou l'incident répond à au moins un des critères de déclenchement. Cette étape a pour objectif immédiat de contenir rapidement l'incident et d'en analyser l'origine. D'autres analyses seront effectuées pendant l'étape du rétablissement.

Rétablissement – C'est l'étape au cours de laquelle on rétablit le système, le réseau ou le service touché pour qu'il revienne à la normale. Il arrive parfois que des services essentiels soient rétablis temporairement à un niveau moindre, tel que défini dans les plans de continuité des opérations. Au cours de cette étape, on examine des problèmes et on doit prendre des décisions dès que la menace immédiate liée à l'incident a disparu et que l'incident est confiné.

2.2 Étape de la préparation

But

Dans le cadre des opérations normales, l'étape de la préparation correspond à un ensemble de vastes processus permanents qui font que le GC est prêt à faire face à des incidents ou à des événements précis ou imprévisibles, et à cerner les menaces, les vulnérabilités ou les incidents qui déclenchent les mesures d'atténuation, d'intervention ou de rétablissement à l'échelle pangouvernementale.

Activités

Planification – Cette activité décrit comment le personnel, l'équipement et d'autres ressources sont utilisés pour appuyer les activités de gestion des incidents. Les plans du GC renferment les mécanismes et les systèmes pour établir les priorités, intégrer de multiples organisations et fonctions, et veiller à ce que les communications et les autres systèmes soient accessibles et intégrés à l'appui de l'éventail complet des besoins liés à la gestion des incidents. Les plans des ministères et des fournisseurs de services au GC doivent s'harmoniser au plan pangouvernemental dès qu'un critère du PGI est déclenché. De plus, les plans de gestion des incidents doivent être pris en compte dans les ententes sur les niveaux de service (ENS) s'il y a lieu.

Supervision et détection – Ces activités visent à identifier et à déceler les changements dans l'environnement opérationnel qui influent ou qui pourraient influer sur les services à la population canadienne, sur les opérations gouvernementales ou sur la confiance envers

le gouvernement. Il pourrait s'agir d'événements ou de signes avant-coureurs d'incidents, de nouvelles menaces et vulnérabilités, ou d'incidents à proprement parler, qui pourraient être décelés grâce à la supervision et à la détection.

Rapport – Cette activité garantit la communication au bon moment des nouvelles menaces et vulnérabilités en TI et d'incidents qui influent ou qui pourraient influer sur les services et les opérations du GC ou sur la confiance envers le gouvernement. Les ministères doivent signaler les anomalies ou les événements qui déterminent ou qui pourraient déterminer qu'un incident répond aux critères de déclenchement du PGI.

Analyse des risques – Dans le cadre de cette activité, on utilise les rapports que les ministères envoient au CCRIC, lorsque l'analyse ministérielle déclenche les critères du PGI. Le CCRIC partagera ce rapport avec l'UTC qui effectuera une analyse du risque à l'échelle pangouvernementale (y compris des répercussions et des probabilités). Cette information sera transmise aux comités de la haute direction aux fins d'examen et d'approbation de mesures de suivi à l'échelle pangouvernementale.

2.2.1 Planification

But

Au cours de l'étape de la planification, on décrit comment le personnel, l'équipement et d'autres ressources sont utilisés pour appuyer les activités de gestion des incidents et on jette les bases pour que ces plans puissent être exécutés. Les plans du GC renferment les mécanismes et les systèmes pour établir les priorités, intégrer de multiples organisations et fonctions, et veiller à ce que les communications et les autres systèmes soient accessibles et intégrés à l'appui de l'éventail complet des besoins liés à la gestion des incidents. Les plans des ministères doivent s'harmoniser au plan pangouvernemental dès qu'un critère du PGI est déclenché. De plus, les plans de gestion des incidents doivent être pris en compte dans les ententes sur les niveaux de service (ENS) s'il y a lieu.

Activités

L'identification et la compréhension des systèmes essentiels sont deux activités fondamentales pour appuyer les activités de gestion des incidents. Faute de comprendre ce qui est le plus essentiel au GC, l'évaluation des risques ne permettrait pas de caractériser les répercussions. Pour identifier les systèmes essentiels, les impératifs opérationnels, comme l'information et les services, doivent être compris à la lumière des points forts et des lacunes des systèmes, c'est-à-dire qu'il faut comprendre les mesures de protection en place, les vulnérabilités du système et les attaques connues dans le domaine public.

2.2.2.1 Identification

2.2.1.1.1 Les **ministères** identifieront leurs systèmes essentiels.

2.2.1.1.2 **Sécurité publique Canada** identifiera les systèmes essentiels du GC en se fondant sur ceux que les ministères ont identifiés et répertoriés.

2.2.1.1.3 Le **Secrétariat** dirigera et mobilisera les comités stratégiques de la haute direction pour s'assurer qu'ils identifient les problèmes de planification et de préparation au sein du GC et prennent les mesures qui s'imposent.

2.2.1.2 Élaboration

L'élaboration des instruments stratégiques (dont les plans) doit appuyer les activités de gestion des incidents et clairement préciser les rôles et les responsabilités. Il est essentiel de formuler les plans, les attentes et les règles d'engagement des principaux acteurs avant, pendant et après la menace de TI, la vulnérabilité ou l'incident.

2.2.1.2.1 Les **ministères** intégreront les processus du PGI du GC dans leurs propres plans de TI.

2.2.1.2.2 **Sécurité publique Canada** élaborera et tiendra à jour des procédures opérationnelles normalisées pour le PGI en ce qui a trait aux éléments connexes (comme les communications, le COG et le CCRIC).

2.2.1.2.3 Le **Secrétariat** dressera et tiendra à jour le PGI du GC.

2.2.1.2.4 Le **Secrétariat** intégrera les résultats sur les leçons apprises des incidents antérieurs, des stratégies d'atténuation, des exercices et des essais concernant les instruments stratégiques du GC.

2.2.1.2.5 Le **Secrétariat** promulguera les pratiques exemplaires et veillera à la mise en œuvre des plans d'action du GC axés sur les leçons apprises.

2.2.1.3 Formation

Les principaux acteurs et ministères doivent être renseignés et formés relativement aux processus du PGI du GC, à l'organigramme connexe et aux procédures opérationnelles afin de réagir de manière efficace et efficiente en présence de menaces, de vulnérabilités ou d'incidents possibles ou réels. Ils doivent notamment bien comprendre les rôles, les responsabilités et les attentes en menant des exercices interministériels et en appliquant des scénarios qui amélioreront

l'intégration et l'interopérabilité et qui optimiseront l'utilisation des ressources pendant la gestion d'un incident.

2.2.1.3.1 Les **ministères** participeront à la formation sur le PGI du GC.

2.2.1.3.2 Le **Secrétariat** veillera à mettre au point des séances de formation sur le PGI à l'intention des représentants ministériels.

2.2.1.4 Essai

Les plans de gestion des incidents du GC doivent être mis à l'essai dans le cadre d'exercices et de scénarios multidisciplinaires et interministériels réalistes pour améliorer l'intégration et l'interopérabilité et pour optimiser l'utilisation des ressources pendant les activités liées à un incident.

2.2.1.4.1 Les **ministères** participeront à des exercices, à des scénarios et à des essais du PGI du GC.

2.2.1.4.1 **Sécurité publique Canada** mènera des exercices pour faire l'essai du PGI du GC en appliquant des scénarios réalistes pour en valider l'efficacité et cerner ses lacunes.

2.2.1.4.1 Le **Secrétariat** veillera à ce qu'on mène des exercices relatifs au PGI et qu'on en fasse l'essai pour tirer des leçons qui seront examinées et mises en œuvre.

Intrants	Extrants
• Information sur les leçons apprises d'incidents antérieurs, de stratégies d'atténuation, d'exercices et de scénarios d'essai • Stratégies d'atténuation • Pratiques exemplaires	• Répertoire du GC des services essentiels, des dépendances sur la TI et de la position défensive connexes • Stratégies, politiques, plans et processus pangouvernementaux pour la gestion des incidents • Séances de formation sur le PGI du GC à l'intention des représentants ministériels • Exercices et scénarios d'essai pour valider l'efficience et l'efficacité du PGI du GC et des plans ministériels • PGI ministériels intégrant le PGI du GC • Pratiques exemplaires

2.2.2 Suivi et détection

But

Être constamment à l'affût des événements ou des signes avant-coureurs d'une nouvelle menace, d'une vulnérabilité ou d'incidents et déceler et évaluer la validité et l'impact d'un incident concernant la sécurité ou de la panne de TI sur les services à la population canadienne, sur les opérations gouvernementales ou sur la confiance envers le gouvernement.

Activités

La supervision continue (et l'analyse) des menaces et des vulnérabilités, de même que des indicateurs d'incidents possibles dans chaque ministère et pour tout le GC s'impose pour pouvoir identifier les effets négatifs, réels ou potentiels, qu'ils pourraient avoir sur l'infrastructure du GC. La détection découle directement de la supervision. Si la supervision est inadéquate ou incomplète, le processus de détection passera sûrement outre certaines anomalies ou certains événements qui pourraient révéler une menace, une vulnérabilité ou un incident réel ou potentiel. Conformément à la *Politique du gouvernement sur la sécurité*, les ministères doivent continuellement superviser le fonctionnement de leurs systèmes pour déceler les anomalies ou les événements qui sont ou qui pourraient être des indicateurs d'un incident réel ou d'une forte probabilité qu'il s'en produise un. Sans supervision, la détection des anomalies ou des événements qui sont un signe avant-coureur d'un incident ou qui pourraient l'être s'avérerait pratiquement impossible. La détection d'une menace, d'une vulnérabilité ou d'un incident dans un ministère pourrait permettre de signifier un avis anticipé relativement à une grave infraction à la sécurité ou à une panne de TI susceptible de durement toucher d'autres ministères, les services à la population canadienne, les opérations gouvernementales ou la confiance à l'égard du gouvernement et de l'ensemble du GC.

2.2.2.1 Suivi et analyse

2.2.2.1.1 Les **ministères** se chargeront des activités de suivi et de détection, conformément à la *Politique du gouvernement sur la sécurité* (soit suivre et analyser les menaces et les vulnérabilités, les événements et les incidents qui pourraient toucher les systèmes ministériels de TI).

2.2.2.1.2 En cas d'incertitude, les **ministères** s'adresseront au CCRIC qui les aidera à caractériser un événement, une menace, une vulnérabilité ou un incident.

2.2.2.1.3 Les **ministères** suivront l'information (par ex. les rapports d'étape du GC, les demandes d'information (DI), les rapports d'incidents du GC, les rapports de situation en cas d'incident au GC, les avertissements et la connaissance de la

situation qui prévaut au GC) fournie par le CCRIC et y donneront suite selon le cas.

2.2.2.1.4 L'**UTC** supervisera l'environnement du GC conformément au mandat respectif de ses membres (voir la liste qui suit), en ce qui a trait aux menaces, vulnérabilités ou incidents réels ou potentiels :

2.2.2.1.4.1 La **Gendarmerie royale du Canada** supervisera les sources de surveillance criminelles.

2.2.2.1.4.2 Le **Service canadien du renseignement de sécurité** supervisera les sources de surveillance du renseignement de sécurité.

2.2.2.1.4.3 Le **Centre de la sécurité des télécommunications du Canada** suivra les menaces technologiques en matière de TI et fournira une analyse technique des menaces et des incidents ainsi que des conseils en matière de mesures d'atténuation.

2.2.2.1.4.4 Le **Centre de la sécurité des télécommunications du Canada** colligera et fournira des rapports sur les renseignements d'origine électromagnétique de source primaire (ROEM) au sujet des cybermenaces.

2.2.2.1.4.5 Le **ministère de la Défense nationale** suivra l'information fournie par des sources alliées, dont l'OTAN.

2.2.2.1.4.6 Le **ministère de la Défense nationale** suivra les menaces technologiques en matière de TI.

2.2.2.1.5 Les membres de l'**UTC** collaboreront avec le CCRIC pour évaluer l'information sur les nouvelles menaces, les vulnérabilités et les incidents qui pourraient influer sur la disponibilité des biens et des services essentiels du GC, à la lumière des critères de déclenchement et de gravité de l'impact du PGI.

2.2.2.2 Coordination et analyse

2.2.2.2.1 Afin de déceler une menace, une vulnérabilité ou un incident réel ou potentiel, le **CCRIC** suivra et analysera les sources et les renseignements techniques qui ont été signalées par :

2.2.2.2.1.1 les ministères fédéraux;

2.2.2.2.1.2 les membres de l'UTC;

2.2.2.2.1.3 des sources ouvertes;

2.2.2.2.1.4 des partenaires nationaux et internationaux[15]

2.2.2.2.2 Le **CCRIC** consultera l'UTC pour évaluer la probabilité que des renseignements sur une nouvelle menace ou sur une vulnérabilité puissent déboucher sur un incident répondant aux critères de déclenchement et de gravité du PGI.

2.2.2.2.3 Le **CCRIC** enverra aux ministères une demande d'information (DI) pour qu'ils brossent le tableau de la menace du GC afin de déterminer si d'autres ministères relèvent les mêmes indicateurs de menace, de vulnérabilité ou d'incident.

2.2.2.2.4 Le **CCRIC** donnera suite aux demandes des ministères fédéraux qui désirent obtenir des avis techniques précis, des conseils et des renseignements sur la détection d'incidents en matière de TI.

Intrants	Extrants
• Source ouverte • Rapports d'incidents et de menaces influant sur la disponibilité de biens et de services essentiels du GC • Rapports d'incidents susceptibles de s'avérer des infractions criminelles • Rapports d'incidents mettant en cause des menaces aux intérêts nationaux • Produits d'information du CCRIC distribués par l'intermédiaire du COG • Rapports d'incidents initiaux envoyés par les ministères au CCRIC	• Identification de menaces, de vulnérabilités ou d'incidents, nouveaux ou potentiels, qui nécessitent la prise de mesures à l'échelle pangouvernementale

15 Bien que l'interaction et les processus entre le CCRIC et les partenaires nationaux et internationaux débordent de la portée du PGI, l'information qui est déclarée et partagée avec le CCRIC sera analysée à la lumière des critères de déclenchement et de gravité du PGI.

2.2.3 Rapport

But

Il est essentiel de produire au moment opportun des rapports sur les menaces, les vulnérabilités, les événements et les incidents de TI qui influent ou qui pourraient influer sur les services à la population canadienne, les opérations gouvernementales ou la confiance envers le gouvernement.

Activités

2.2.3.1 Rapport

2.2.3.1.1 Les ministères enverront au CCRIC, par l'intermédiaire du COG, un rapport sur les menaces, les vulnérabilités et incidents de TI qui répondent aux critères de déclenchement, aussitôt qu'ils les auront décelés, au :

CENTRE DES OPÉRATIONS DU GOUVERNEMENT (COG)

Courriel : GOC-COG@ps-sp.gc.ca
Téléphone : 613-991-7000
Télécopieur : 613-996-0995
Télécopieur protégé : 613-991-7094

Les **ministères** enverront leur rapport initial d'incident au CCRIC, par l'intermédiaire du COG, lorsque le critère de déclenchement aura été satisfait et incluront :

2.2.3.1.1.1 les renseignements sur la personne-ressource chargée des rapports, aux fins de suivi;

2.2.3.1.1.2 la description de l'incident, y compris le moment et l'endroit où il s'est produit;

2.2.3.1.1.3 les répercussions estimées, en fonction des critères déclenchés;

2.2.3.1.1.4 la situation des mesures d'atténuation et une indication qu'ils ont besoin d'aide.

2.2.3.1.2 Si un **ministère** doute qu'un événement constitue une menace, une vulnérabilité ou un incident, il communiquera avec le CCRIC pour qu'il l'aide à caractériser l'événement et précise clairement les rapports d'incident qu'il doit soumettre.

2.2.3.1.3 Les **ministères** enverront au CCRIC, par l'intermédiaire du COG, d'autres renseignements dans un rapport ministériel d'incident, lorsque ces renseignements seront disponibles (annexe D).

2.2.3.1.4 Les membres de l'**UTC** enverront au CCRIC de l'information au sujet d'une menace, d'une vulnérabilité ou d'un incident, réel ou potentiel, qui influe ou qui pourrait influer sur les services à la population canadienne, sur les opérations gouvernementales ou sur la confiance envers le gouvernement, dans leur domaine d'expertise respectif (voir 2.2.2.1.4).

2.2.3.2 Rapports et coordination

2.2.3.2.1 Le **CCRIC** fera office de point de convergence des rapports ministériels sur les menaces, les vulnérabilités ou les incidents, réels ou potentiels, qui influent ou qui pourraient influer sur les services à la population canadienne, sur les opérations gouvernementales ou sur la confiance envers le gouvernement.

2.2.3.2.2 Le **CCRIC** effectuera une analyse initiale de l'information à la lumière des critères de déclenchement du PGI. Les rapports peuvent provenir des sources suivantes :

2.2.3.2.2.1 Sources externes – dont tout partenaire national, international ou allié du Canada.

2.2.3.2.2.2 Ministères – tout ministère du gouvernement fédéral.

2.2.3.2.2.3 Membres de l'UTC – chargés d'analyser l'information provenant des sources qui relèvent du mandat de chaque ministère membre.

2.2.3.2.2.4 CCRIC – chargé de comprendre la situation et d'analyser l'information provenant de diverses sources.

2.2.3.2.3 S'il y a lieu, le **CCRIC** enverra une confirmation à tous les ministères qui ont déclaré un incident afin que ces derniers sachent que l'incident est analysé et évalué dans le contexte de tout le GC.

2.2.3.2.4 Le **CCRIC** publiera à l'intention des ministères des produits de cyberinformation (cybercapsules, alertes, avis, documents techniques, autres directives, renseignements ou avis se rapportant à ces menaces, vulnérabilités et incidents). La figure 6 montre le flux d'information entre le CCRIC (par l'intermédiaire du COG) et les ministères touchés. Ces produits d'information électronique seront partagés avec tous les ministères, sauf si les circonstances entourant un incident dictent le contraire. Il s'agira entre autres :

2.2.3.2.4.1 *Alertes* : produits cruciaux qui décrivent un problème de sécurité immédiat ou actif.

2.2.3.2.4.2 Avis : pas aussi urgents que les alertes, mais décrivent néanmoins des menaces à la sécurité et des problèmes qui pourraient menacer la sécurité informatique de l'infrastructure essentielle du Canada et renferment aussi des conseils pour les atténuer.

2.2.3.2.4.3 Cybercapsules : produits ayant un contenu et un degré d'urgence semblables à ceux des avis, à la différence qu'elles ne sont accompagnées d'aucun conseil officiel pour parer à la vulnérabilité. Contrairement aux alertes et aux avis, elles ne sont pas affichées publiquement.

2.2.3.2.4.4 Mises à jour : servent à compléter, à corriger ou à actualiser n'importe quel produit de cyberinformation que diffuse le CCRIC pour garantir que le GC dispose de toute l'information disponible.

2.2.3.2.4.5 Rapports de situation : envoyés par le COG, donnent de l'information actualisée sur l'incident et les mesures d'intervention qui seront prises sur-le-champ et dans le futur (annexe E). Incluent aussi une analyse des répercussions de l'incident sur le GC et l'identification des problèmes à régler. De manière typique, sont émis pour chaque période opérationnelle ou sur demande du directeur général, Direction des opérations.

2.2.3.2.5 Les **ministères** donneront suite aux produits de cyberinformation du CCRIC sur demande.

2.2.3.2.6 Le **CCRIC** donnera suite aux demandes émanant des ministères qui solliciteront des avis techniques, des conseils et des renseignements sur les rapports d'incident en matière de TI.

2.2.3.2.7 Le **CCRIC** confirmera l'existence d'un incident touchant l'ensemble du GC et en informera l'équipe de gestion.

2.2.3.2.8 Le **CCRIC** soumettra à la DDPI du SCT un rapport sur les statistiques, les tendances, les nouveaux problèmes et les incidents.

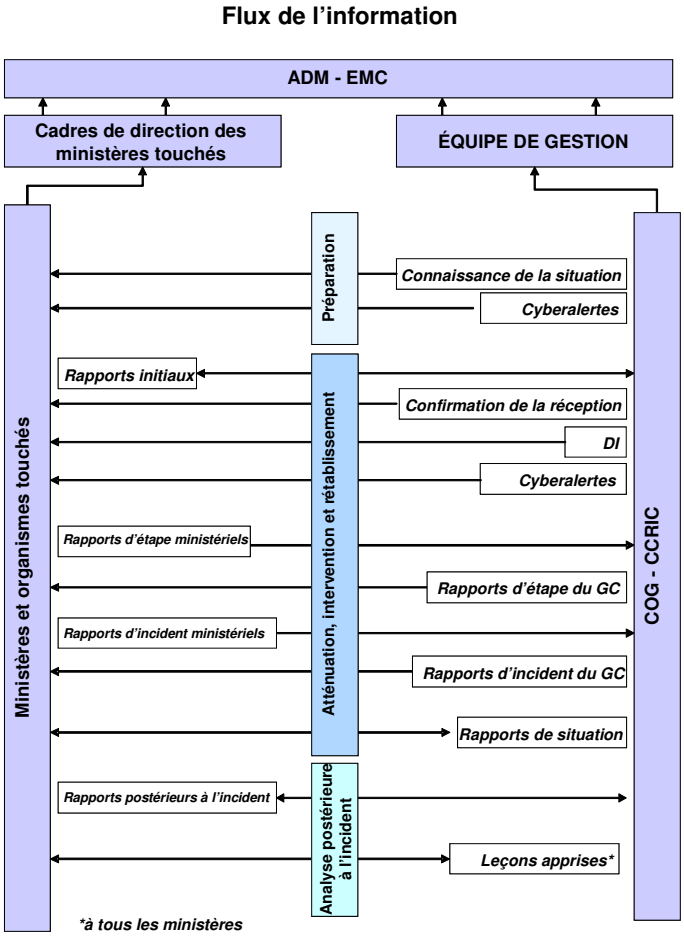

Figure 6 : Flux de l'information entre le CCRIC (par l'intermédiaire du COG) et les ministères touchés

Intrants	Extrants
• Produits d'information publiés par le CCRIC par l'intermédiaire du COG • Rapports d'incident initiaux soumis par les ministères au CCRIC • Rapports envoyés par les membres de l'UTC au CCRIC	• Rapports d'incidents et de menaces influant sur la disponibilité de biens et de services essentiels du GC • Rapports d'incidents susceptibles de s'avérer des infractions criminelles • Rapports d'incidents mettant en cause des menaces aux intérêts nationaux • Signification à l'équipe de gestion d'un incident qui a déclenché l'étape de l'intervention du PGI du GC

2.2.4 Analyse des risques

But

L'analyse des risques est un processus continu qui appuiera directement les étapes de l'atténuation, de l'intervention et du rétablissement du PGI du GC. Elle garantit que des événements douteux ou des menaces, des vulnérabilités ou des incidents nouveaux sont examinés dans le contexte de tout le GC, en se fondant sur des évaluations à jour et, s'il y a lieu, des évaluations ministérielles, pouvant inclure des évaluations de sources externes qui sont soumises au CCRIC (voir 2.2.3.2.2).

Activités

2.2.4.1 Analyse continue

2.2.4.1.1 Les **ministères** analyseront les risques auxquels sont exposés leurs systèmes respectifs et leurs activités opérationnelles pour déceler les menaces, les vulnérabilités et les incidents qui répondent aux critères de déclenchement du PGI et partageront cette information avec le CCRIC, par l'intermédiaire du COG.

2.2.4.1.2 Les membres de l'**UTC** partageront constamment avec le CCRIC l'information découlant de leur analyse afin de produire un tableau coordonné et complet du GC (voir 2.2.3.1.4).

2.2.4.1.3 Le **CCRIC** partagera l'analyse des risques ministériels avec l'UTC.

2.2.4.1.4 L'**UTC** effectuera une analyse plus vaste des répercussions réelles ou potentielles sur l'ensemble du GC.

2.2.4.1.5 Le **CCRIC** évaluera continuellement toute l'information reçue des diverses sources et, s'il y a lieu, identifiera les tendances ou les domaines de préoccupations possibles qui ont déclenché le PGI ou qui pourraient le faire.

2.2.4.1.6 Si le CCRIC décèle par son analyse une menace, une vulnérabilité ou un incident réel ou potentiel, il déclenchera aussitôt une mesure d'atténuation ou d'intervention (voir 2.3.1 et 2.4.1 respectivement) selon les circonstances.

Intrants	Extrants
• Information découlant des évaluations ministérielles des risques • Information découlant des évaluations de l'UTC des risques	• Vaste tableau d'ensemble des risques auxquels est exposé le GC • Indications d'incidents et de menaces pouvant influer sur la disponibilité de biens et de services essentiels du GC • Indications d'incidents susceptibles de s'avérer des infractions criminelles • Indications d'incidents pouvant mettre en cause des menaces aux intérêts nationaux • Information sur les menaces, les risques et les mesures d'atténuation • Évaluation de la nature et de la portée de la menace, de la vulnérabilité ou de l'incident nouveau à la lumière des critères de déclenchement du PGI

2.3 Atténuation

But

Empêcher que les vulnérabilités et les menaces deviennent des incidents ou réduire les effets des incidents lorsqu'ils se produisent. L'étape de l'atténuation est différente des autres, parce que les mesures qui sont prises visent à réduire ou à éliminer les risques de manière proactive contrairement aux mesures réactives qui sont prises aux étapes de l'intervention et du rétablissement. Idéalement, les activités d'atténuation sont déclenchées assez tôt pour permettre de prendre des mesures de protection à long terme. Les ministères, le CCRIC ou les membres de l'UTC porteront les menaces et les vulnérabilités à l'attention du GC dès que les critères du PGI sont déclenchés.

Activités

2.3.1 Prise de mesures d'atténuation

2.3.1.1 L'étape de l'atténuation est amorcée lorsque le CCRIC reçoit des ministères (ou d'autres sources énoncées à la rubrique 2.2.3.2.2.) un rapport sur une menace ou une vulnérabilité répondant aux critères de déclenchement du PGI (section 1.9). Les rapports sont soumis au CCRIC par l'intermédiaire du COG. Le **CCRIC** effectuera une analyse initiale de l'information à la lumière des critères de déclenchement.

2.3.2 Signification d'avis à l'équipe de gestion

2.3.2.1 Dès qu'il est confirmé qu'une vulnérabilité ou une menace répond aux critères de déclenchement ou lorsque l'UTC a été activée, le **CCRIC** transmettra à l'équipe de gestion l'information dont il dispose.

2.3.2.2 Le **chef de l'équipe de gestion (directeur général, Direction des opérations de SPC)** informera les membres de l'équipe suivants :

2.3.2.2.1 Directeur général adjoint, Direction des opérations de SPC;

2.3.2.2.2 Représentant du ministère de la Justice;

2.3.2.2.3 DG, Communications de SPC (activation du cycle de communication);

2.3.2.2.4 Représentants des ministères primaires :

2.3.2.2.2.1 DDPI du SCT

2.3.2.2.2.2 Directeur du CCRIC

2.3.2.2.2.3 Autres personnes déterminées par le directeur général, Direction des opérations, selon les circonstances

2.3.3 Connaissance de la situation

2.3.3.1 L'information sur la menace ou la vulnérabilité est validée à la lumière des critères de déclenchement du PGI, et le **CCRIC** :

2.3.3.2 Activera l'UTC conformément à ses procédures de fonctionnement normalisées (le cas échéant, il doit consulter l'UTC ou coordonner avec celle-ci l'analyse mentionnée à la rubrique 2.3.3.4).

2.3.3.2.1 L'**UTC** analysera d'une manière ciblée les circonstances atténuantes (après avoir effectué l'analyse mentionnée à la rubrique 2.2.4.1.4).

2.3.3.2.2 L'**UTC** identifiera les ministères primaires et les ministères d'appui et formulera une recommandation à l'équipe de gestion quant aux principaux intervenants qui devraient participer à l'étape de l'atténuation de la menace ou de la vulnérabilité.

2.3.3.2.3 La **Gendarmerie royale du Canada** mènera en parallèle une enquête criminelle pendant l'intervention du GC.

2.3.3.2.4 Le **ministère de la Défense nationale** mènera en parallèle une analyse des options et des interventions militaires pendant l'intervention au GC, s'il s'agit d'une menace à ses systèmes ou à ceux des Forces canadiennes ou de toute cybermenace militaire d'un gouvernement étranger.

2.3.3.2.5 Le **Service canadien du renseignement de sécurité** mènera en parallèle une enquête pendant l'intervention du GC, s'il s'agit d'un événement d'envergure ou d'une question de sécurité nationale.

2.3.3.2.6 Le **Centre de la sécurité des télécommunications Canada** suivra en parallèle les menaces de TI pendant l'intervention du GC, effectuera une analyse de la menace et de l'incident, fournira des conseils sur les mesures d'atténuation et secondera les enquêtes.

2.3.3.3 Fera participer à l'analyse les ministères touchés, les ministères primaires et les ministères d'appui.

2.3.3.4 Analysera la menace ou la vulnérabilité pour identifier les systèmes et les utilisateurs touchés, de même que les répercussions opérationnelles :

2.3.3.4.1 en identifiant l'origine de la menace ou de la vulnérabilité;

2.3.3.4.2 en analysant les répercussions permanentes et potentielles sur les services, les biens et les infrastructures essentiels du GC, à la lumière de la Matrice de la gravité de l'impact (annexe C);

2.3.3.4.3 en évaluant la probabilité qu'un incident se produise à la lumière des renseignements et des évaluations des menaces disponibles;

2.3.3.4.4 en établissant l'ordre de priorité des mesures, en présence de multiples menaces ou vulnérabilités simultanées;

2.3.3.4.5 en élaborant des mesures et en déterminant pour chacune les risques connexes, le niveau d'effort anticipé et les jalons pour atténuer la menace ou la vulnérabilité.

2.3.3.5 Le **CCRIC** collaborera avec l'agent de liaison en communication (au besoin).

2.3.3.6 Le **CCRIC** recommandera à l'équipe de gestion la mesure qui convient le mieux aux fins d'examen et d'approbation.

2.3.4 Points de décision relatifs à la mesure d'atténuation

2.3.4.1 L'**équipe de gestion** sera le premier niveau de gestion supérieure à exiger la prise des mesures nécessaires pour atténuer la menace ou la vulnérabilité à laquelle fait face le GC.

2.3.4.2 L'**équipe de gestion** approuvera une option recommandée parmi celles que lui a proposées le CCRIC à la lumière du niveau de tolérance au risque et de l'environnement actuel du GC.

2.3.4.3 L'**équipe de gestion** dressera le plan de communications. Le DG, Communications de SPC coordonnera et dirigera cet effort de communication et pourrait faire participer en parallèle le Groupe de travail du DG, Communications de SPC.

2.3.4.4 Selon les circonstances, l'**équipe de gestion** pourra décider de porter la situation à un niveau supérieur :

2.3.4.4.1 au niveau d'intervention 2 ou 3 du PFIU à cause de sa gravité, de la probabilité qu'elle nécessite des mesures d'atténuation et de leur portée;

2.3.4.4.2 à l'attention des comités exécutifs, dont les suivants :

2.3.4.4.2.1 ACF,

2.3.4.4.2.2 CGU-SMA,

2.3.4.4.2.3 CSMASN,

2.3.4.4.2.4 Comité des opérations.

2.3.4.5 L'**équipe de gestion** approuvera des documents d'information en vue d'une décision (s'il y a lieu) et des rapports de situation préparés par le COG pour conseiller les comités exécutifs à propos des répercussions possibles sur les services à la population canadienne, sur les opérations gouvernementales ou sur la confiance envers le gouvernement.

2.3.4.6 L'**équipe de gestion** déterminera la mesure à prendre à partir de celles que lui aura proposées le CCRIC (voir 2.3.3.6) et établira son orientation. Cela débouchera sur l'approbation du Plan d'atténuation du GC, comme l'aura déterminé l'équipe de gestion seule ou en consultation avec les comités exécutifs.

2.3.4.7 L'**équipe de gestion** demandera au CCRIC, par l'intermédiaire du COG, de coordonner la mise en œuvre du plan d'atténuation à l'échelle pangouvernementale. Cela pourra inclure, sans toutefois s'y limiter, la signification d'un avis aux ministères à propos des

mesures d'atténuation précises et de l'obligation de soumettre au CCRIC, par l'intermédiaire du COG, un rapport d'étape ou un rapport de situation.

2.3.5 Mise en œuvre du plan d'atténuation des risques du GC

2.3.5.1 Tel que demandé par l'équipe de gestion, le **CCRIC** coordonnera, par l'intermédiaire du COG, la mise en œuvre du plan d'atténuation à l'échelle pangouvernementale et collaborera avec les ministères pour s'assurer qu'ils sont au fait de la situation et qu'ils peuvent prendre des mesures d'atténuation en connaissance de cause s'il y lieu.

2.3.5.2 Au besoin, le **CCRIC**, par l'intermédiaire du COG, informera les ministères de certaines mesures d'atténuation précises et de tout rapport d'étape ou rapport de situation qu'ils doivent lui soumettre par l'intermédiaire du COG.

2.3.5.3 Les **ministères touchés** (et s'il y a lieu tous les ministères) collaboreront pour mettre en œuvre dans leur organisation respective toute mesure d'atténuation pertinente du GC.

2.3.5.4 Au besoin, les **ministères** soumettront des rapports au CCRIC par l'intermédiaire du COG (voir 2.2.3.2.5).

2.3.5.5 Le **CCRIC** évaluera le risque résiduel en se servant des rapports ministériels sur la situation et informera l'équipe de gestion du risque, de la situation ou du changement à la lumière de cette évaluation.

2.3.5.6 Le **CCRIC** analysera de manière permanente la situation et les risques pour déterminer si la portée de la menace ou de la vulnérabilité est atténuée dans les ministères touchés désignés et soumettra ses constatations dans un rapport à l'équipe de gestion.

2.3.5.6.1 Dans le rapport d'étape ou de situation concernant les mesures d'atténuation qu'il a soumis à l'équipe de gestion, le **CCRIC** l'informera si la menace ou la vulnérabilité a été atténuée avec succès. Le **CCRIC** identifiera également tout incident connexe qui répondrait aux critères de déclenchement du PGI et informera l'équipe de gestion d'activer l'étape de l'intervention (voir 2.4.2).

2.3.6 Points de décision relatifs à la confirmation de l'atténuation

2.3.6.1 L'**équipe de gestion** examinera le rapport d'étape et le rapport de situation concernant les mesures d'atténuation que lui a soumis le CCRIC et, au besoin, consultera davantage les ministères touchés.

2.3.6.2 L'**équipe de gestion** informera ensuite les comités exécutifs, selon leur degré de participation (voir 2.3.4.4.2). Les comités exécutifs du PGI qui participent donneront d'autres directives.

2.3.6.3 L'**équipe de gestion** décidera s'il y a lieu ou non de clore le volet atténuation ou de continuer à assurer un suivi relativement à des menaces ou à des vulnérabilités particulières ou connexes.

2.3.6.3.1 S'il est décidé de continuer à assurer le suivi relativement à des menaces ou à des vulnérabilités particulières, tout renseignement additionnel sera validé et analysé (voir 2.3.3.1).

2.3.6.3.2 Si l'équipe de gestion décide de clore le volet atténuation, l'analyse postérieure à l'incident (voir 2.6) sera alors menée en parallèle, pendant que l'on revient à l'ensemble des vastes processus continus de l'étape de la préparation.

Intrants	Extrants
• Rapports ministériels et rapports de situation • Rapports sur le renseignement de sécurité (s'il y a lieu) • Renseignements de surveillance criminelle (s'il y a lieu) • Information sur un événement d'envergure (s'il y a lieu) • Vulnérabilités et menaces connues du public • Journaux du système (s'il y a lieu) • Répertoire des systèmes essentiels et des services du GC • Ressources techniques • Aspects politiques à prendre en compte • Aspects juridiques à prendre en compte • Objectifs opérationnels	• Analyse détaillée de la menace ou de la vulnérabilité • Rapports de connaissance de la situation (bidirectionnels, des ministères au CCRIC et du CCRIC aux ministères) • Signification d'un avis à la haute direction et aux comités exécutifs du PGI • Mobilisation des représentants des ministères primaires, des ministères d'appui et des ministères touchés • Plan d'atténuation du GC approuvé • Atténuation de la menace ou de la vulnérabilité • Produits d'information • Produits de communication • S'il y a lieu, élimination validée de la menace ou de la vulnérabilité

2.4 Intervention

But

Prendre les mesures, mener les activités et mobiliser les services appropriés lorsque l'impact d'un ou de plusieurs incidents répond à au moins un des critères de déclenchement. L'objectif immédiat de cette étape est de contenir rapidement l'incident et d'en analyser l'origine. Selon l'étendue des dommages, une autre analyse peut être menée à l'étape du rétablissement.

Activités

2.4.1 Prise de mesures d'intervention

2.4.1.1 L'étape de l'intervention est activée lorsque le CCRIC reçoit des ministères (ou d'autres sources mentionnées à la rubrique 2.2.3.2.2) des rapports sur des incidents, réels ou potentiels, qui répondent aux critères de déclenchement du PGI (section 1.9). Le **CCRIC** effectuera une analyse initiale de l'information à la lumière des critères de déclenchement.

2.4.2.2 Si les critères de déclenchement ne sont pas satisfaits, la **coordination horizontale du GC (CCRIC)** retombera à l'étape de la préparation.

2.4.2 Signification d'avis à l'équipe de gestion

2.4.2.1 Dès qu'on aura confirmé que l'incident répond aux critères de déclenchement ou lorsque l'UTC a été activée, le **CCRIC**, par l'intermédiaire du COG, transmettra à l'équipe de gestion l'information dont il dispose.

2.4.2.2 Le **chef de l'équipe de gestion (directeur général, Direction des opérations de SPC)** informera les membres suivants de l'équipe de gestion :

2.4.2.2.1 Directeur général adjoint, Direction des opérations de SPC

2.4.2.2.2 Représentant du ministère de la Justice

2.4.2.2.3 DG adjoint, Communications de SPC (activation du cycle de communication)

2.4.2.2.4 Représentants des ministères primaires :

2.4.2.2.4.1 DDPI du SCT

2.4.2.2.4.2 Directeur du CCRIC

2.4.2.2.4.3 Autres personnes déterminées par le directeur général, Direction des opérations, selon les circonstances

2.4.3 Connaissance de la situation

2.4.3.1 En se servant de l'information tirée des rapports d'incidents et de l'ensemble des vastes processus continus décrits à l'étape de la préparation, le **CCRIC** :

2.4.3.2 Validera le rapport d'incident à la lumière des critères de déclenchement du PGI.

2.4.3.3 Activera l'UTC selon les procédures opérationnelles normalisées de l'UTC (le cas échéant, il doit consulter l'UTC ou coordonner avec celle-ci les mesures mentionnées à la rubrique 2.4.3.5).

2.4.3.3.1 L'**UTC** analysera les circonstances pour déterminer la nature et la portée de l'incident.

2.4.3.3.2 L'**UTC** identifiera les ministères primaires et les ministères d'appui et recommandera à l'équipe de gestion les principaux intervenants qui devraient participer aux étapes de l'intervention et du rétablissement pour l'incident.

2.4.3.3.3 La **Gendarmerie royale du Canada** mènera en parallèle une enquête criminelle pendant l'intervention du GC.

2.4.3.3.4 Le **ministère de la Défense nationale** mènera en parallèle une analyse des options et des interventions militaires pendant l'intervention du GC, s'il s'agit d'une menace à ses systèmes ou à ceux des Forces canadiennes ou de toute cybermenace militaire d'un gouvernement étranger.

2.4.3.3.5 Le **Service canadien du renseignement de sécurité** mènera en parallèle une enquête pendant l'intervention du GC, s'il s'agit d'un événement d'envergure ou d'une question de sécurité nationale.

2.4.3.3.6 Le **Centre de la sécurité des télécommunications Canada** suivra en parallèle les menaces de TI pendant l'intervention du GC, effectuera une analyse de la menace et de l'incident, fournira des conseils sur les mesures d'atténuation et secondera les enquêtes.

2.4.3.4 Fera participer à l'analyse les ministères touchés, les ministères primaires et les ministères d'appui.

2.4.3.5 Analysera l'incident pour identifier les systèmes et les utilisateurs touchés, de même que les répercussions opérationnelles :

2.4.3.5.1 en identifiant l'origine de la menace ou de la vulnérabilité (l'analyse peut se poursuivre pendant l'étape du rétablissement dans le cas d'incidents complexes);

2.4.3.5.2 en analysant les répercussions permanentes et potentielles sur les services, les biens et les infrastructures essentiels du GC, à la lumière de la Matrice de la gravité de l'impact (annexe C);

2.4.3.5.3 en évaluant la probabilité qu'un incident se produise à la lumière des renseignements et des évaluations des menaces disponibles;

2.4.3.5.4 en établissant l'ordre de priorité des mesures, en présence de multiples menaces ou vulnérabilités simultanées;

2.4.3.5.5 en élaborant des mesures possibles et en déterminant pour chacune les risques connexes, le niveau d'effort anticipé et les jalons pour contenir l'incident et minimiser les répercussions sur les autres systèmes et services.

2.4.3.6 Le **CCRIC** collaborera avec l'agent de liaison en communication (au besoin).

2.4.3.7 Le **CCRIC** recommandera à l'équipe de gestion les mesures qui conviennent le mieux et le plan d'intervention connexe aux fins d'examen et d'approbation.

2.4.4 Points de décision relatifs à la mesure d'intervention

2.4.4.1 L'**équipe de gestion** sera le premier niveau de la gestion supérieure à exiger la prise des mesures nécessaires pour contenir l'incident rapidement.

2.4.4.2 L'**équipe de gestion** examinera les mesures proposées par le CCRIC à la lumière du niveau de tolérance au risque, de l'environnement actuel du GC et formulera sa recommandation.

2.4.4.3 L'**équipe de gestion** dressera le plan de communication. Le DG, Communications de SPC coordonnera et dirigera cette activité et pourrait faire participer en parallèle le Groupe de travail du DG, Communications de SPC.

2.4.4.4 Selon les circonstances, l'**équipe de gestion** pourra décider de porter la situation à un niveau supérieur :

2.4.4.4.1 au niveau d'intervention 2 ou 3 du PFIU à cause de la gravité de l'incident, telle que mentionnée dans la Matrice de la gravité de l'impact (annexe C);

2.4.4.4.2 à l'attention des comités exécutifs, dont :

2.4.4.4.2.1 ACF,

2.4.4.4.2.2 CGU-SMA,

2.4.4.4.2.3 CSMASN,

2.4.4.4.2.4 Comité des opérations.

2.4.4.5 L'**équipe de gestion** approuvera des documents d'information en vue d'une décision (s'il y a lieu) et des rapports de situation préparés par le COG pour conseiller les comités exécutifs à propos des répercussions possibles sur les services à la population canadienne, sur les opérations gouvernementales ou sur la confiance envers le gouvernement.

2.4.4.6 L'**équipe de gestion** approuvera le plan d'intervention (voir 2.4.3.7) en consultation avec les comités exécutifs.

2.4.4.7 L'**équipe de gestion** demandera au CCRIC, par l'intermédiaire du COG, de coordonner la mise en œuvre du plan d'intervention à l'échelle pangouvernementale. Cela pourra inclure, sans toutefois s'y limiter, la signification d'un avis aux ministères à propos des mesures d'intervention précises et de l'obligation de soumettre au CCRIC, par l'intermédiaire du COG, un rapport d'étape ou un rapport de situation.

2.4.5 Mise en œuvre du plan d'intervention du GC

2.4.5.1 Tel que demandé par l'équipe de gestion, le **CCRIC**, par l'intermédiaire du COG, coordonnera la mise en œuvre du plan d'intervention à l'échelle pangouvernementale et collaborera avec les ministères pour s'assurer que tout le GC est au fait de la situation et qu'il est prêt à prendre des mesures d'intervention s'il y lieu.

2.4.5.2 Au besoin, le **CCRIC**, par l'intermédiaire du COG, informera les ministères de certaines mesures d'intervention et de tout rapport d'étape ou rapport de situation qu'ils doivent lui soumettre par l'intermédiaire du COG.

2.4.5.3 Les **ministères touchés** (et s'il y a lieu tous les ministères) collaboreront pour mettre en œuvre dans leur organisation respective toute mesure d'intervention pertinente au GC.

2.4.5.4 S'il y a lieu, les **ministères** soumettront des rapports au CCRIC par l'intermédiaire du COG (voir 2.2.3.2.5).

2.4.5.5 Le **CCRIC** évaluera le risque résiduel en se servant des rapports ministériels sur la situation et informera l'équipe de gestion du risque, de la situation ou des changements à la lumière de cette évaluation.

2.4.5.6 Le **CCRIC** analysera de manière permanente la situation et les risques pour déterminer si l'incident est contenu dans les ministères touchés désignés et soumettra un rapport d'étape ou de situation à cet égard à l'équipe de gestion.

2.4.5.6.1 Dans l'évaluation des risques et dans le rapport de situation qu'il a soumis à l'équipe de gestion, le **CCRIC** l'informera si l'incident a été contenu avec succès. Le CCRIC précisera également si des dommages ont été causés ou si les opérations normales n'ont pas été rétablies et, le cas échéant, informera l'équipe de gestion de passer au rétablissement (voir 2.5.1), en parallèle avec l'étape d'intervention.

2.4.6 Points de décision relatifs à la confirmation du confinement

2.4.6.1 **L'équipe de gestion** examinera l'évaluation des risques et le rapport de situation du COG à la lumière de l'analyse menée et coordonnée en consultation avec les ministères touchés ou d'autres ministères (s'il y a lieu).

2.4.6.2 L'**équipe de gestion** informera ensuite les comités exécutifs, selon leur degré de participation.

2.4.6.3 Les **comités exécutifs** participants (mis au courant par l'équipe de gestion) décideront si l'incident a été contenu à la lumière de l'évaluation des risques et du rapport de situation.

2.4.6.4.1 L'**équipe de gestion** décidera s'il y a lieu ou non de clore le volet intervention ou de continuer à assurer un suivi relativement à des menaces ou à des vulnérabilités particulières ou connexes.

2.4.6.4.1 S'il est décidé de continuer à assurer le suivi relativement à des incidents particuliers ou connexes, tout renseignement additionnel sera validé et analysé (voir 2.4.3.2).

2.4.6.4.2 Si l'équipe de gestion décide de clore le volet, elle devra passer à l'analyse postérieure à l'incident (voir 2.6.1) et revenir à l'ensemble des vastes processus continus de l'étape de la préparation.

Intrants	Extrants
• Rapports ministériels d'incidents et rapports de situation • Renseignements sur le renseignement de sécurité (s'il y a lieu) • Rapports de surveillance criminelle (s'il y a lieu) • Information sur un événement d'envergure (s'il y a lieu) • Vulnérabilités et menaces connues du public • Journaux du système (s'il y a lieu) • Répertoire des systèmes essentiels et des services du GC • Ressources techniques • Aspects politiques à prendre en compte • Aspects juridiques à prendre en compte • Objectifs opérationnels	• Analyse détaillée de l'incident • Rapports de connaissance de la situation (bidirectionnels, des ministères au CCRIC et du CCRIC aux ministères) • Plan d'intervention • Signification d'un avis à la haute direction et aux comités du PGI • Mise en place du COG élargi en faisant appel à des représentants des ministères primaires et des ministères d'appui • Confinement de l'incident et intervention • Produits et demandes d'information • S'il y a lieu, confirmation que la menace, la vulnérabilité ou l'incident a été éliminé

2.5 Rétablissement

But

Ramener le système, le réseau ou le service touché à son fonctionnement normal. Dans certains cas, les services essentiels peuvent être rétablis temporairement à un état moindre, défini dans les plans de continuité des opérations (PCO). Cette étape a trait aux problèmes à régler et aux décisions à prendre une fois que la menace immédiate de l'incident a disparu et que l'incident a été contenu.

Activités

2.5.1 Prise de mesures de rétablissement

2.5.1.1 L'étape du rétablissement est activée après le confinement de l'incident qui a entraîné des dommages ou une perturbation des opérations normales.

2.5.1.2 S'il n'y a ni dommage ni perturbation des opérations normales, la **coordination horizontale au GC (CCRIC)** retournera à l'ensemble des vastes processus continus de l'étape de la préparation.

2.5.2 Signification d'avis à l'équipe de gestion

2.5.2.1 Le **CCRIC** communiquera à l'équipe de gestion l'information disponible au sujet des dommages ou de la perturbation des opérations normales de même que des résultats des mesures d'intervention que les ministères ont déclarés dans leurs rapports de situation soumis pendant l'étape de l'intervention (voir 2.4.5.4).

2.5.2.1.1 Le **chef de l'équipe de gestion (directeur général, Direction des opérations de SPC)** fera le point pour les membres de l'équipe de gestion (voir 2.4.2.2).

2.5.3 Connaissance de la situation

2.5.3.1 Les **ministères touchés** rétabliront les niveaux de services normaux en ligne, ralligneront les processus de prestation provisoires aux opérations normales.

2.5.3.2 Le **CCRIC**, par l'intermédiaire du COG, agit comme point de coordination du rétablissement du GC.

2.5.3.3 Les **ministères touchés** transmettront les mises à jour des rapports de situation et confirmeront au COG que les opérations sont revenues à la normale.

2.5.3.4 En se servant des mises à jour des rapports de situation ministériels, le **CCRIC** :

2.5.3.4.1 En collaboration avec les ministères touchés, les ministères primaires et les ministères d'appui participant à l'étape de l'intervention (voir 2.4.3.4), élaborera des recommandations et les mesures possibles (s'il y a lieu) nécessaires pour coordonner les mesures de rétablissement à l'échelle pangouvernementale.

2.5.3.4.2 Collaborera avec l'agent de liaison en communications (au besoin).

2.5.3.4.3 Recommandera les mesures de rétablissement les plus appropriées (plan de rétablissement) à l'équipe de gestion aux fins d'examen et d'approbation.

2.5.4 Points de décision relatifs aux mesures de rétablissement

2.5.4.1 L'**équipe de gestion** dressera le plan de communication. Le DG, Communications de SPC coordonnera et dirigera cet effort de communications et pourrait faire participer en parallèle le Groupe de travail du DG, Communications de SPC.

2.5.4.2 Selon les circonstances, l'**équipe de gestion** pourra décider de porter la situation à l'attention des comités exécutifs du PGI.

2.5.4.3 L'**équipe de gestion** approuvera des documents d'information en vue d'une décision (s'il y a lieu) et des rapports de situation préparés par le COG pour conseiller les comités exécutifs à propos des répercussions possibles sur les services à la population canadienne, sur les opérations gouvernementales ou sur la confiance envers le gouvernement et proposera des recommandations relatives au rétablissement à l'échelle pangouvernementale.

2.5.4.4 L'**équipe de gestion** approuvera le plan de rétablissement (voir 2.5.3.4.3) en consultation avec les comités exécutifs participants.

2.5.4.5 L'**équipe de gestion** demandera au CCRIC, par l'intermédiaire du COG, de coordonner la mise en œuvre du plan de rétablissement pangouvernemental.

2.5.5 Mise en œuvre du plan de rétablissement du GC

2.5.5.1 Tel que demandé par l'équipe de gestion, le **CCRIC**, par l'intermédiaire du COG, coordonnera la mise en œuvre du plan de rétablissement pangouvernemental et collaborera avec les ministères touchés.

2.5.5.2 Au besoin, le **CCRIC**, par l'intermédiaire du COG, informera les ministères des mesures de rétablissement applicables au GC et de tout rapport d'étape ou rapport de situation qu'ils doivent lui soumettre.

2.5.5.3 Les **ministères touchés** (et s'il y a lieu tous les ministères) mettront en œuvre dans leur organisation respective toute mesure de rétablissement pertinente au GC.

2.5.5.4 Les **ministères** soumettront au CCRIC, par l'intermédiaire du COG, des rapports sur leurs efforts de rétablissement (s'il y a lieu).

2.5.5.5 Le **CCRIC** évaluera le plan de rétablissement pangouvernemental à la lumière des rapports de situation ministériels et transmettra ses constatations à l'équipe de gestion.

2.5.6 Points de décision relatifs à la confirmation du rétablissement

2.5.6.1 L'**équipe de gestion** examinera l'évaluation du rétablissement et le rapport de situation fournis par le CCRIC.

2.5.6.2 L'**équipe de gestion** informera ensuite les comités exécutifs participants.

2.5.6.3 Les **comités exécutifs** participants détermineront si les opérations ont été rétablies à l'échelle du GC.

2.5.6.4 L'**équipe de gestion** décidera s'il y a lieu ou non de clore le volet rétablissement ou de continuer à assurer un suivi relativement aux efforts de rétablissement du GC.

2.5.6.4.1 S'il est décidé de continuer à assurer le suivi relativement au rétablissement, d'autres rapports de situation ministériels seront alors évalués et la connaissance de la situation sera mise à jour en conséquence (voir 2.5.3.4).

2.5.6.4.2 Si l'équipe de gestion décide de clore le volet, elle devra passer à l'analyse postérieure à l'incident (voir 2.6) et revenir à l'ensemble des vastes processus continus de l'étape de la préparation.

Intrants	Extrants
• Rapports de situation actualisés du (des) ministère(s) touché(s) • Ébauche des produits d'information	• Plan de rétablissement pangouvernemental • Produits d'information (comme des documents d'information en vue d'une décision, des rapports de connaissance de la situation) • Rétablissement des services du GC

2.6 Analyse postérieure à l'incident

But

Tirer parti des connaissances acquises par le GC de chaque incident afin d'améliorer la confidentialité, l'intégrité et la disponibilité de l'infrastructure de TI du GC. En examinant les résultats des activités d'atténuation, d'intervention et de rétablissement, le GC cernera les domaines susceptibles d'amélioration en ce qui a trait aux mesures de sécurité, aux processus ou aux instruments stratégiques.

Activités

2.6.1 Observations et mesures recommandées

2.6.1.1 S'il y a lieu, les **ministères touchés** participeront à la rédaction du rapport postérieur à l'incident produit par le COG.

2.6.1.2 Le **CCRIC** évaluera l'efficacité des processus et des mesures de sécurité.

2.6.1.3 Le **CCRIC**, en consultation avec l'UTC, les ministères touchés et les ministères d'appui, recommandera les domaines susceptibles d'amélioration et les mesures qui s'imposent pour atténuer le risque que de futurs incidents ne se produisent.

2.6.2 Rapport postérieur à l'incident

2.6.2.1 Le **COG** produira un rapport postérieur à l'incident.

2.6.2.2 Les **ministères touchés** examineront le rapport postérieur à l'incident produit par le COG s'il y a lieu.

2.6.2.3 Le **DG, Communications de SPC** coordonnera et dirigera les activités de communication connexes.

2.6.2.4 L'**équipe de gestion et ses comités exécutifs** (s'il y a lieu) :

2.6.2.4.1 Veilleront à ce que le rapport postérieur à l'incident soit rédigé.

2.6.2.4.2 Approuveront le rapport postérieur à l'incident.

2.6.3 Plan d'action du GC reposant sur les leçons apprises

2.6.3.1 À la lumière du rapport postérieur à l'incident, la **DDPI du SCT**, en consultation avec **SPC**, dressera le plan d'action global du GC sur les leçons apprises, dont des directives et des recommandations à l'intention des ministères. Ce document pourrait inclure :

2.6.3.1.1 la mise en œuvre d'instruments stratégiques et de processus du GC,

2.6.3.1.2 la mise en œuvre de mesures d'atténuation pour améliorer la sécurité de la TI du GC et la disponibilité de mécanismes de protection de la TI.

2.6.3.2 La **DDPI du SCT**, en collaboration avec **SPC**, veillera à ce que les leçons apprises soient prises en compte.

2.6.3.3 La **DDPI du SCT** sera le référentiel des rapports postérieurs d'incident.

2.6.3.4 La **DDPI du SCT** se chargera de clore le volet d'analyse postérieure à l'incident du PGI du GC en se fondant sur les mesures d'atténuation et autres qui auront été mises en œuvre.

2.6.4 Mise en œuvre

2.6.4.1 Les **ministères touchés** mettront en pratique les leçons apprises s'il y a lieu.

2.6.4.2 Tous les **ministères** mettront en pratique les leçons apprises s'il y a lieu.

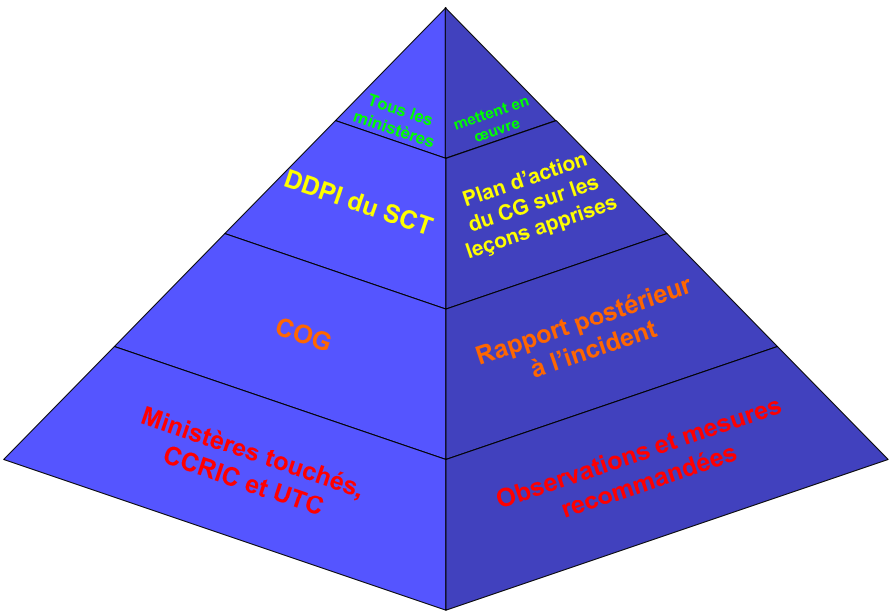

Figure 7 : Activités d'analyse postérieure à un incident

Intrants	Extrants
• Déterminer ce qui n'a pas fonctionné et ce qui a marché tel que prévu dans le plan. • Examiner la chronologie de l'incident. • Examiner la vitesse à laquelle les avis ont été signifiés et les communications faites pendant l'étape de l'intervention et cerner les domaines qui suscitent des préoccupations. • Examiner l'origine (ou les origines) du problème. • Déterminer l'efficacité du processus de confinement de l'incident. • Examiner les mesures d'atténuation relatives à la sécurité afin d'empêcher que d'autres incidents ne se produisent. • Déterminer comment l'incident aurait pu être évité. • Déterminer toutes les répercussions (dont les coûts, le niveau d'effort, l'atteinte possible à la réputation) de l'incident pour le GC et le(s) ministère(s) touché(s). • Relever les améliorations et les révisions à apporter aux politiques, aux procédures et aux processus du GC.	• Analyse postérieure à l'incident • Rapport postérieur à l'incident • Plan d'action du GC reposant sur les leçons apprises

Annexe A: Acronymes et sigles

ACF	Agent de coordination fédéral
CCRIC	Centre canadien de réponse aux incidents cybernétiques
CDPI	Conseil des dirigeants principaux de l'information
CGU-SMA	Comité de gestion des urgences des sous-ministres adjoints
COG	Centre des opérations du gouvernement
Comité Ops	Comité du Cabinet chargé des opérations
CS	connaissance de la situation
CSMSN	Comité des sous-ministres sur la sécurité nationale
DDPI	Direction du dirigeant principal de l'information
DDPI du SCT	Direction du dirigeant principal de l'information du Secrétariat du Conseil du Trésor
DG, Comm de SPC	Directeur général, Communications de Sécurité publique Canada
DI	demande d'information
DPI du GC	Dirigeant principal de l'information pour le gouvernement du Canada
ENS	entente de niveau de service
EX	cadre
GC	Gouvernement du Canada
GT - DG, Comm	Groupe de travail du directeur général, Communications
OTAN	Organisation du Traité de l'Atlantique Nord
PCO	Plan de continuité des opérations
PFIU	Plan fédéral d'intervention d'urgence
PGI du GC	Plan de gestion des incidents du GC en matière de TI
PGI	Plan de gestion des incidents

SCT	Secrétariat du Conseil du Trésor du Canada
SFGIU	Système fédéral de gestion des interventions d’urgence
SMA	sous-ministre adjoint
SMA Sécurité	Comité des sous-ministres adjoints chargé de la sécurité
SPC	Sécurité publique Canada
STI	sécurité des technologies de l’information
TI	technologie de l’information
UTC	Unité de triage des cyberincidents

Annexe B: Glossaire

Alertes	Les alertes sont cruciales et décrivent un problème de sécurité immédiate ou actif. Il est essentiel de les diffuser le plus rapidement possible. Entre autres exemples de situations qui justifient une alerte, il y a la diffusion publique d'un accès illicite se rapportant à un avis antérieur émis par SPC, la propagation rapide d'un maliciel (code malveillant), une menace imminente pour les réseaux du GC, des problèmes éventuels découlant de multiples dénis de service.
Anomalie	Une anomalie est tout ce qui diffère de ce qui est attendu.[16] Une anomalie est un terme neutre utilisé à la place des descripteurs usuels comme bogue, faute, panne, erreur, défectuosité, problème, déviation, pépin, incident ou plantage.
Avis	Les avis ne sont pas aussi urgents que les alertes, mais ils décrivent néanmoins des menaces à la sécurité et des problèmes qui pourraient menacer la sécurité informatique de l'infrastructure essentielle du Canada (comme des virus et des vers informatiques qui évoluent lentement, de graves vulnérabilités d'un logiciel commun). Ils renferment aussi des conseils pour les atténuer.
Centre canadien de réponse aux incidents cybernétiques (CCRIC)	Le CCRIC surveille les menaces, publie des alertes et des avis et coordonne la réponse aux incidents de sécurité cybernétique à l'échelle nationale. Il fait porter ses efforts sur la protection de l'infrastructure nationale essentielle contre les incidents cybernétiques.
Centre des opérations du gouvernement (COG)	Le Centre des opérations du gouvernement est le noyau stratégique des opérations du Canada. Il est au cœur d'un réseau de centres d'opérations, dirigé par divers ministères fédéraux et s'occupe de toute menace, réelle ou perçue, imminente ou actuelle, de catastrophe naturelle ou d'activité terroriste, qui compromet la sécurité de la population canadienne ou l'intégrité de l'infrastructure essentielle du Canada.
Connaissance de la	S'entend par être au courant de son environnement et de ce qui se

16 IEEE 1044-1993: Standard Classification for Software Anomalies., page 1, The Institute of Electrical and Electronics Engineers, Inc., New York, USA, 1994, page 1

situation	passe pour comprendre comment les événements et les mesures influeront sur les objectifs opérationnels, maintenant et dans un proche avenir. Il est essentiel de bien connaître la situation, de manière précise, actualisée et complète dans tout domaine où la complexité technologique, le processus décisionnel et le bien-être du public interagissent. Comme la gestion des incidents fait intervenir des prédictions et des prévisions, il est essentiel, pour connaître la situation d'un domaine de la TI, de saisir les relations qui existent entre les services et les renseignements essentiels, les mécanismes de protection de l'infrastructure et des processus de TI, de même que l'évolution des menaces.
Cybercapsule	Les cybercapsules ont un contenu et un degré d'urgence semblables à ceux des avis, à la différence qu'elles ne sont accompagnées d'aucun conseil officiel pour parer à la vulnérabilité. Contrairement aux alertes et aux avis, elles ne sont pas affichées publiquement. C'est donc une méthode idéale pour recueillir de l'information sur les nouvelles menaces émergentes, tout en évitant le battage publicitaire indésirable. Entre autres exemples, il peut s'agir de vulnérabilités aux attaques dites du type jour zéro ou de préavis qu'une rustine (programme de correction) pour un problème particulier sera bientôt disponible.
Document d'information en vue d'une décision	Les documents d'information en vue d'une décision servent à informer les cadres supérieurs et les ministres du problème de l'heure et des options possibles pour le régler, de même qu'à leur transmettre une mesure recommandée aux fins d'approbation ou d'examen. De manière typique, ils complètent un document sur la situation, qui brosse le contexte dans lequel la décision demandée doit être prise.
Événement	Un événement est un changement observable dans le comportement normal d'un système, d'un environnement, d'un processus, du flux des documents ou d'une personne (les éléments)[17].
Gestion des incidents	Cette activité vise à rétablir le niveau de service normal le plus rapidement possible et à minimiser l'effet négatif sur les

17 http://en.wikipedia.org/wiki/Computer_security_incident_management#Events

opérations, de manière à garantir le maintien des meilleurs niveaux de service, de qualité et de disponibilité.[18] La gestion des incidents inclut tous les aspects du règlement des incidents, mais s'intéresse aussi aux composantes stratégiques liées à ces éléments, y compris les fonctions de leadership et de prise de décisions requises au cours d'un incident, et consiste à s'assurer de la prestation continue des services et des activités nécessaires pour en assurer le règlement opportun et efficace.

Incidents de TI

Un incident de TI est toute situation qui :

- perturbe le fonctionnement normal d'une organisation et qui cause ou qui peut causer une interruption ou une réduction de la qualité du service et(ou) de la productivité;[19] ou
- constitue une tentative non autorisée, réussie ou non, d'accéder à tout réseau informatique ou à toute ressource appartenant à un système informatisé, de les modifier, de les détruire, de les supprimer ou de les rendre inaccessibles.

Intervention en cas d'incident

L'intervention en cas d'incidents, habituellement de nature technique, comprend les activités de niveau tactique associées à l'analyse, au confinement et à la résolution d'un incident. L'intervention en cas d'incident est faite par occurrence, au fur et à mesure des incidents et en fonction de leurs caractéristiques.

Mise à jour

La mise à jour d'une alerte, d'un avis ou d'une cybercapsule se fait après leur diffusion. Les mises à jour servent à compléter, à corriger ou à actualiser n'importe quel produit de cyberinformation que diffuse le CCRIC pour garantir que toutes les organisations participant à la gestion des vulnérabilités, des menaces et des incidents ont accès à toute l'information disponible.

Organisme de services communs

Un organisme de services communs est un ministère ou une organisation, dont un organisme de services spécial, désigné comme fournisseur central de services précis pour seconder d'autres ministères.[20]

---

18 Détails du cadre du BIT (v2), http://en.wikipedia.org/wiki/ITIL#Incident_Management

19 http://www.knowledgetransfer.net/dictionary/ITIL/en/Incident.htm

20 Politique sur les services communs, http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/TB_93/csp-psc01_f.asp#_Toc147652595

Rapport de situation	Un rapport de situation donne de l'information actualisée sur l'incident et les mesures d'intervention qui seront prises sur-le-champ et dans le futur. Ce rapport inclut aussi une analyse des répercussions et l'identification des problèmes à régler.
Services partagés	Cette expression a trait à la prestation de services par un groupe ou un secteur d'une organisation, alors que ces services ont déjà été offerts dans plusieurs parties de l'organisation ou secteurs. Le concept clé est celui du *partage* au sein de l'organisation ou entre les secteurs.[21] Ainsi, les fonds et les ressources associés à ces services sont partagés, et le groupe, l'unité ou le secteur chargé de les offrir devient en fait un fournisseur de services internes.
Signification d'avis	Cette activité permet de faire connaître l'information initiale sur un incident, sur l'évaluation des risques, sur les mesures d'intervention en cours, de même que les conseils relatifs à la production des rapports et les communications publiques. Elle peut inclure des infocapsules déjà préparées. Selon la nature de l'incident, on signifie des avis aux membres du CDPI, aux coordonnateurs de la sécurité de TI et aux agents de la sécurité des ministères.
Traitement des incidents	Le traitement des incidents inclut des fonctions opérationnelles nécessaires pour soutenir une intervention et un rétablissement opportuns et appropriés à la suite d'un incident et comprend les activités de communication, de logistique, d'analyse et de coordination.

21. http://en.wikipedia.org/wiki/Shared_services

Annexe C: Matrice de la gravité de l'impact

Le plus haut niveau atteint dans toutes les rangées détermine la gravité de l'impact sur le GC.

Catégorie	Gravité de l'impact		
	Impact faible	**Impact moyen**	**Impact élevé**
Santé et sécurité	Aucun impact réel ou éventuel sur la santé et la sécurité	Impact réel ou éventuel limité ou moyen sur la santé et la sécurité des Canadiens ou des employés	Incidents qui mettent éventuellement la vie en danger ou susceptibles de le faire
Portée de l'incident	Un ou plusieurs ministères	Nombre limité de ministères	Grand nombre de ministères
Prestation des services	Impact réel ou éventuel limité ou nul sur les services essentiels ou sur les activités du GC	Impact réel ou éventuel important sur les services essentiels ou sur les activités du GC	Impact réel ou éventuel grave sur les services essentiels ou sur les activités du GC
Répercussions financières	Impact financier réel ou éventuel limité ou moyen (p. ex. réduction de la productivité des fonctionnaires)	Impact financier réel ou éventuel important (pour le GC ou ses partenaires)	Impact financier réel ou éventuel grave (pour le GC ou ses partenaires)
Confiance du public et réputation	Impact réel ou éventuel limité ou nul sur la confiance du public ou la réputation du GC	Impact réel ou éventuel moyen sur la confiance du public ou la réputation du CG	Impact réel ou éventuel important sur la confiance du public ou la réputation du GC

Annexe D: Formulaire de déclaration d'incident

1.0 Entité déclarante

Nom de l'organisation :	

2.0 Information sur la personne-ressource

Prénom :		Initiales :	
Nom de famille :		Poste :	
Téléphone :	( )	Cellulaire :	( )
Téléavertisseur :	( )	Télécopieur :	( )
Courrier électronique :			
Adresse au bureau :			

3.0 Description de l'incident et de son impact

Date et heure de l'incident :	(date, heure et fuseau horaire)
Emplacement du site touché par l'incident :	
(s'il y en a plus d'un, les énumérer tous)	
Impact estimé :	
Durée de l'incident :	(si l'incident est terminé, sinon mentionner « en cours »)
Nombre estimatif de systèmes touchés :	
Pourcentage de systèmes ministériels touchés :	
Courte description de l'incident :	

Mesures prises :
(inclure la date et l'heure si possible)
Documents à l'appui :
(les décrire s'ils sont joints)

4.0 État des mesures d'atténuation

Détails des mesures d'atténuation prises à ce jour :	(dresser la liste de toutes les mesures qui ont été prises pour atténuer l'incident et par qui)
Résultats des mesures :	
Aide additionnelle requise?	OUI/NON

5.0 Type d'incident

Code malveillant	ver; virus; trojan; backdoor; rootkit
Attaques connues de la vulnérabilité	(dresser la liste des numéros des vulnérabilités connues)
Système compromis	modifie les journaux, modifie l'information DNS
Données compromises	détruit des données, modifie des données, mutile des sites Web
Déni de service	DS
Access Violation	tentative d'accès non autorisé, accès non autorisé, perçage de mots de passe

Accident/Erreur	panne d'équipement, erreur de l'opérateur, erreur de l'utilisateur, causes naturelles ou accidentelles
Autre inconnu	

6.0 Systèmes touchés

Zone du réseau touchée	Internet, DMZ, Administration, interne, enclave
Type de système touché	serveur de fichiers, serveur Web, serveur de courrier, base de données, poste de travail, autre (préciser)
Système d'exploitation (préciser la version)	Windows, Linux, Unix, MacOS, OS/390, autre (préciser)
Protocoles/Services	(dresser la liste de tous ceux qui s'appliquent)
Application	(inclure les versions précises)

7.0 Origine apparente de l'incident ou de l'attaque

Source et port IP :		Protocole :	
URL :	(s'il y a lieu)	Maliciel :	(s'il y a lieu)

Nota : On peut obtenir les détails sur l'échange de données électroniques auprès du CCRIC.

Annexe E: Rapport de situation

Rapport de situation

Numéro : Événement STXXX-08 (numéro fourni par le COG)

Menace ou événement : Brève description de la menace ou de l'événement

Date : Renseignements mis à jour à XX h XX (HAE/HNE)

Description de la menace ou de l'événement en cours :

- Résumé de la menace ou de l'événement
- Information sur le contexte de l'événement ou de l'incident
- Description des conditions actuelles
- Répercussions actuelles sur la population, le gouvernement (installations, services, actifs, symboles), les organismes d'intervention d'urgence et les infrastructures connexes, les infrastructures essentielles (énergie et services publics, technologie de l'information et des communications, finances, soins de santé, alimentation, eau, transports, sécurité et secteur manufacturier), la sécurité nationale et l'application de la loi, l'économie et l'environnement.

Source(s) des rapports : Source originale du rapport et toute autre source (médias, bureaux régionaux, centres des opérations d'urgence provinciaux, autres organismes gouvernementaux)

Mesures d'intervention en cours : Mesures prises pour venir à bout de la situation. Mesures d'intervention internationales, fédérales, provinciales et territoriales, interventions d'organismes non gouvernementaux, téléconférences, réunions, demandes d'aide présentées aux provinces ou au gouvernement fédéral

Suivi : Mesures à prendre ou problèmes à régler en réponse à la situation. Ce que l'on prévoit.

Évaluation et analyse : Section sur les conséquences possibles dans le rapport de situation. Ce que l'on sait au sujet de la menace, des vulnérabilités et des autres effets possibles. Attirer l'attention sur les autres questions importantes.

Autres notifications :

Autres produits :

Produits de géomatique :

Centre des opérations du gouvernement (COG)

Courriel : GOC-COG@PS-SP.GC.CA

Téléphone : (613) 991-7000

Télécopieur : (613) 996-0995

Télécopieur sécuritaire : (613) 991-7094

Annexe F: Document d’information en vue d’une décision

Document d'information en vue d'une décision

Titre

(Titre : nom de l’événement, par exemple tempête de verglas, attentat à la bombe à Londres, ouragan Katrina)

Menace ou événement

Décrire l’événement ou la menace sous forme d’un court paragraphe ou de puces. Cette section doit donner des renseignements concis et pertinents. Donner des points de repère géographique ainsi que la date et l’heure à laquelle l’événement est survenu. Vérifier que l’heure est la bonne selon l’heure normale ou l’heure avancée de l’Est, et non l’heure dans la région touchée, et indiquer (HNE/HAE) après l’heure. Les renseignements donnés dans cette section doivent correspondre à ceux contenus dans les notifications ou rapports de situation antérieurs le cas échéant. (Pour cette partie, il est possible d’utiliser les renseignements contenus à la section « Description de la menace ou de l’événement en cours » du rapport de situation).

Contexte

Cette section doit présenter des explications au sujet de l’événement en cours. L’information (y compris les renseignements illustrés) doit être ajoutée à l’onglet 3 de la trousse d’information en vue d’une décision.

Situation Actuelle

Cette section renfermera un résumé de la situation (connaissance de la situation à l’heure actuelle), dont les conséquences connues et possibles, les renseignements pertinents liés à la menace, les vulnérabilités, l’étendue des dommages, les répercussions sur le public, sur la région géographique touchée), ainsi que les circonstances aggravantes (conditions météorologiques, répercussions sur les infrastructures essentielles, disponibilité des ressources essentielles).

Mesures en cours

Décrire les mesures prises par les administrations fédérale, provinciales, territoriales, municipales et le secteur privé.

- Notification, avis et alertes diffusés
- Effort de coordination et principales décisions
- Élaboration d’un plan d’action stratégique

- Examen des enjeux stratégiques

Évaluation et analyse

Présenter une brève évaluation et analyse de l'événement ou de la menace se rapportant précisément aux aspects suivants :

- coûts
- incidence sur les relations fédérales-provinciales et territoriales
- incidence sur les relations internationales
- détérioration possible de la situation
- confiance du public (couverture médiatique)

Démarches possibles

Cette section contient une description des différentes mesures qui peuvent être prises en réaction à la situation en cours. Il faut préciser le nombre d'options.

- Option A : (description)
- Option B : (description)
- Option C : (description)

Préparé par:

Connaissance de la situation et évaluation du risque, Direction générales des opération, Sécurité publiques Canada

Annexe G: Références et autres lectures

- Plan fédéral d'intervention d'urgence
- *Politique du gouvernement sur la sécurité*
- *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*
- www.publicsafety.gc.ca
- http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_12a/siglist-fra.asp
- www.wikipedia.ca
- Article, Best-Practice Recommendations IT Incident Management, http://www.sun.com/emrkt/sunspectrum/Incd.Mgmt_Wht_ppr_5.22.pdf
- http://www.knowledgetransfer.net/dictionary/ITIL/en/Incident.htm