# Guide de Protection, Détection, Réponse, et Récupération

## GSMGC-019 (2023)

Préparé par :
La Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
Sécurité ministérielle
73, promenade Leikin Ottawa (Ontario) K1A 0R2
Publication publiée : 2023-12-15
Mise à jour :

# Avant-propos

Le Guide de protection, de détection, de réponse et de récupération est une publication NON CLASSIFIÉE, publiée sous l'autorité du Principal Organisme Responsable de la Sécurité Matérielle (PORS) de la GRC. Bien que NON CLASSIFIÉ, l'accès et l'utilisation du présent guide devraient être limités aux ministères et organismes du gouvernement du Canada (GC).

Les suggestions de modifications et d'autres renseignements peuvent être envoyés au principal organisme de la sécurité matérielle de la GRC RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

# Reproduction



# Date d'entrée en vigueur

La date d'entrée en vigueur du Guide de protection, de détection, de réponse et de récupération GSMGC-019 est 2023-12-15

# Registre des modifications

| Amendement no. | Date | Entrée par | Résumé de la modification |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

Remarque : Le pouvoir de modification ou de dérogation est conféré au principal organisme responsable de la sécurité matérielle de la GRC (PORS de la GRC).

# Contenu

# 1. Introduction

La GRC, Principal Organisme Responsable de la Sécurité Matérielle pour le gouvernement du Canada, est chargée de fournir des conseils et des directives sur toutes les questions liées à la sécurité matérielle.

## 1.1. But

Le présent guide vise à fournir aux ministères et aux organismes des renseignements sur le modèle de protection, de détection, d'intervention et de rétablissement afin de faciliter l'élaboration de systèmes, de programmes et de procédures opérationnelles normalisées en matière de sécurité matérielle. Ces mesures appuient la sécurité opérationnelle, la sécurité du personnel et les efforts de continuité des activités afin de faciliter la prestation continue des services tout au long d'un incident de sécurité.

Pour obtenir des renseignements détaillés, les employés du gouvernement du Canada devraient consulter leurs politiques, normes et lignes directrices ministérielles en matière de sécurité, la Politique sur la sécurité du gouvernement (PSG), annexe C de la Directive sur la gestion de la sécurité (DSM), et d'autres guides du PORS de la GRC pour mettre en œuvre les mesures appropriées pour contrer les menaces à l'endroit des employés du gouvernement, des biens et de la prestation des services, et pour assurer une protection uniforme pour le gouvernement du Canada.

Le guide contient à la fois les mesures de contrôle de sécurité requises, indiquées par l'utilisation du mot « doit », et les mesures de contrôle de sécurité ou les lignes directrices recommandées, indiquées par l'utilisation du mot « devrait ». L'utilisation du mot « doit » indique une référence à une politique ou à une norme établie du gouvernement du Canada, tandis que l'utilisation du mot « devrait » renvoie à des conseils, à des directives ou à une pratique exemplaire.

Certains ministères et organismes ou activités opérationnelles peuvent faire face à des menaces différentes en raison de la nature de leurs activités, de leur emplacement ou de l'attrait de leurs actifs. Par exemple, les établissements policiers ou militaires, les services de santé, les laboratoires, les installations de recherche de nature délicate, les musées, les comptoirs de services, les bureaux dans les zones à criminalité élevée et les installations situées à l'extérieur du Canada.

## 1.2. Applicabilité

Le présent guide s'applique à toutes les installations du gouvernement du Canada, puisque les ministères et organismes sont responsables de la protection des employés, des biens et de la prestation des services dans leur secteur de responsabilité. Les directives fournies dans le présent document s'adressent aux dirigeants principaux de la sécurité (ASC), aux directeurs, aux gestionnaires et au personnel de sécurité qui sont responsables de la conception, de l'exploitation et de la protection des installations et du personnel du gouvernement du Canada.

Les organisations de locataires sont responsables d'informer les ministères et organismes gardiens de leurs exigences en matière de sécurité pour le choix du site et l'aménagement des locataires.

Les ministères et organismes gardiens sont responsables de fournir et de financer les mesures de protection jugées nécessaires par le gardien pour protéger les installations en fonction d'une évaluation de la menace et des risques (EMR) effectuée par le gardien ou pour lui. Cette responsabilité comprend la mise en œuvre et l'intégration de mesures pour la sécurité de l'immeuble de base (p. ex., portes extérieures et éclairage), les systèmes de l'immeuble (ascenseurs, systèmes mécaniques et électriques) et la sécurité des personnes (escaliers de sortie, alarmes d'incendie et gicleurs). Les gardiens sont également responsables d'intégrer les exigences financées par les locataires à l'infrastructure de leur immeuble.

### 1.3. Considérations aux technologies de l'information

Suite aux menaces qui évoluent constamment et l'intégration de la sécurité matérielle et de la technologie de l'information (TI), il est essentiel d'évaluer le risque de toute application et/ou de tout logiciel connecté à un réseau pour faire fonctionner et soutenir l'équipement dans les bâtiments contrôlés par le gouvernement du Canada.

Avant de mettre en œuvre des applications et/ou des logiciels qui contrôleront et/ou automatiseront certaines fonctions de l'immeuble, votre service de sécurité ministériel exige la réalisation d'une évaluation et d'une autorisation de sécurité (SA&A). Cela permettra de s'assurer que l'intégrité et la disponibilité des composants que les applications et/ou logiciels contrôlent sont maintenues et que tout risque mis en évidence sera atténué. Il est fortement recommandé de commencer le processus SA&A tôt afin de s'assurer que les calendriers de livraison des projets ne sont pas affectés. Pour plus d'informations sur le processus SA&A, veuillez consulter votre service de sécurité ministériel.

## 2. Coordonnées

Pour plus d'informations, contacter :

Gendarmerie royale du Canada
Principale organisme responsable de la sécurité matérielle
73, promenade Leikin, arrêt postal 165
Ottawa (Ontario)
K1A 0R2
Courriel : RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

## 3. Acronymes

| Acronyme | Signifiant |
|---|---|
| **APPS** | Autre point de prestation de services |
| **CATV** | Distribution de télévision par câble |
| **COS** | Centre des Operations de Sécurité |

| | |
|---|---|
| **DGS** | Directive sur la gestion de la sécurité |
| **EMR** | Évaluation de la menace et des risques |
| **GSMGC** | Guide de sécurité matérielle du gouvernement du Canada |
| **IT** | Technologie de l'information |
| **PCCE** | Prévention du crime par la conception environnementale |
| **PCR** | Poste de commande de rechange |
| **PDRR** | Protection, détection, réponse et récupération |
| **PON** | Procédures opérationnelles normalisées |
| **PSG** | Politique sur la sécurité du gouvernement |
| **SA&A** | Évaluation et autorisation de sécurité |
| **ZHS** | Zone de haute sécurité |
| **ZS** | Zone de sécurité |
| **ZT** | Zone de travail |

# 4. Glossaire

| Terme | Définition |
|---|---|
| **Accès non autorisé** | Accès à des renseignements ou à des biens par un particulier qui n'a pas fait l'objet d'une enquête de sécurité du personnel exigée ou ne satisfait pas aux critères du « besoin de connaître », ou les deux. |
| **Actif** | Actifs matériels ou immatériels du gouvernement du Canada. Ce terme s'applique, sans toutefois s'y limiter, aux renseignements, sous toutes leurs formes et quel que soit leur support, aux réseaux, aux systèmes, au matériel, aux biens immobiliers, aux ressources financières, à la confiance des employés et du public, et à la réputation internationale. |
| **Actifs classifiés** | Actifs dont la compromission risquerait vraisemblablement de porter préjudice à l'intérêt national. |
| **Adversaire** | Une personne ou un groupe cause intentionnellement un préjudice, direct ou indirect, au personnel, aux ministères ou aux organismes du GC. Le plus souvent, il s'agit d'une intrusion ou d'une activité criminelle, mais il peut aussi s'agir d'actes allant jusqu'au terrorisme ou à la violence parrainée par l'État. |
| **Autre point de prestation de services** | Un emplacement distinct pour loger le personnel afin de continuer à fournir des services aux clients ou au grand public. Le PDSA ne devrait pas être situé au même endroit que le PVA d'un ministère ou d'un organisme afin d'éviter toute ingérence dans la structure de gestion ou de commandement en cas d'urgence ou de crise. |
| **Besoin d'accéder à** | Critère utilisé par le ou les dépositaires de renseignements, de biens ou d'installations de nature délicate pour établir, avant de fournir un accès physique ou une entrée, que le destinataire visé doit avoir accès à l'espace pour s'acquitter de ses fonctions officielles. |
| **Besoin de connaître** | Le principe selon lequel il est nécessaire pour une personne d'avoir accès à des renseignements et de les connaître afin de pouvoir |

| | |
|---|---|
| | exécuter ses tâches. |
| **Compromission** | Divulgation, destruction, suppression, modification, interruption d'accès ou utilisation de renseignements ou de biens non autorisée. |
| **Complexe Protégé** | Un complexe où les immeubles et les biens nécessitent des contrôles de sécurité supplémentaires pour protéger les personnes, les renseignements ou les biens qu'ils contiennent. |
| **Confinement** | Ensemble de mesures visant à empêcher le personnel d'entrer dans un espace ou d'en sortir en raison d'une urgence de sécurité personnelle. Le plus souvent causée par des menaces de dommages physiques au personnel à l'intérieur. |
| **Contrôle de l'accès** | Assurer l'accès autorisé aux biens à l'intérieur d'une installation ou de zones d'accès restreint, en effectuant le triage des visiteurs et du matériel aux points d'entrée par les membres du personnel, les gardes ou de façon informatisée et, lorsque requis, en surveillant leur déplacement à l'intérieur de l'installation ou des zones d'accès restreint en les escortant. |
| **Défense en profondeur** | C'est le principe selon lequel les zones de sécurité sont mises en œuvre de manière progressivement restrictive, allant de la zone la moins restrictive à la plus restrictive. |
| **Dépositaire** | Ministère ou organisme responsable de l'administration des biens immobiliers fédéraux. |
| **Détection électronique d'intrusion** | Un système composé de capteurs qui détectent un changement d'état (mouvement, courant électrique, chaleur, codes d'accès), transmet des messages à un programme de surveillance électronique ou à un équipement de notification (sonnerie d'alarme, tableau de distribution, logiciel d'accès à distance) et permet l'analyse du changement d'état signalé (alarme sonore, Centre des opérations de sécurité, arbre d'appels/avis électronique). |
| **Disponibilité** | Se dit de l'information utilisable sur demande au soutien des opérations, des programmes et des services. |
| **Dissuader** | Capacité de prévenir une attaque visant une couche de sécurité en raison de la difficulté perçue ou de la menace d'une intervention. Distance de sécurité Distance entre une menace potentielle et le bien protégé. |
| **Équipe d'intervention d'urgence** | Structure de gestion au sein d'un événement ou d'une crise de continuité des activités. Aussi appelée structure de commandement des interventions. |
| **Escorte** | Personne possédant une cote de sécurité appropriée qui est responsable de la surveillance continue de personnes n'ayant pas une cote de sécurité dans les secteurs où une cote de sécurité ou un statut seraient normalement exigés. |
| **Évaluation de la menace et des risques** | Processus d'évaluation des biens d'une installation, des menaces qui pèsent sur eux et du rendement des mesures de protection contre ces menaces, visant à définir les risques. |

| | |
|---|---|
| **Évaluation et autorisation de sécurité** | – La composante d'évaluation de la sécurité de l'ESA vise à vérifier si les exigences de sécurité établies pour un système ou un service particulier sont respectées et si les contrôles et les mesures de protection fonctionnent comme prévu. L'objectif de la composante d'autorisation de l'ESA est de signifier que la direction a accepté le risque résiduel d'exploitation du système ou du service et a autorisé son utilisation en s'appuyant sur la preuve. |
| **Installation** | Une installation peut être un bâtiment (en tout ou en partie) et peut comprendre son site ou son terrain, ou peut-être une zone ou une construction qui n'est pas un bâtiment (par exemple, champs de tir, champs agricoles). |
| **Intrus** | Toute personne non autorisée qui est entrée dans un espace contrôlé contrairement aux procédures de gestion de l'accès. |
| **Intrusion armée** | Urgence mettant la vie en danger lorsqu'une ou plusieurs personnes attaquent d'autres personnes dans l'intention de causer des lésions corporelles graves ou la mort. Initialement définie pour l'utilisation d'armes à feu par les attaquants, elle comprend également les armes à lame (couteaux, épées), les armes chimiques (acide) et d'autres armes (bâtons, véhicules). |
| **Locataire** | Un ministère qui occupe un immeuble du gouvernement fédéral administré par un autre ministère ou une société d'État. |
| **Menace interne** | Cas où le personnel autorisé à entrer ou à travailler dans une installation du GC prend délibérément des mesures contre le GC, son employeur ou ses collègues. Les actions peuvent inclure l'activité criminelle, les menaces ou actions physiques, l'espionnage, la subversion et le sabotage. |
| **Ministères et organismes** | Tout ministère, organisme, installation scientifique ou installation connexe du GC qui est responsable de la gestion des biens immobiliers, de l'information, des biens et/ou du personnel fédéraux. |
| **Périmètre** | Ligne de sécurité continue délimitant une zone protégée. |
| **Personne autorisée** | Une personne qui travaille avec le gouvernement du Canada, y compris des employés du gouvernement fédéral ainsi que des employés occasionnels, des entrepreneurs, des étudiants et d'autres personnes qui ont obtenu une autorisation de sécurité pour accéder aux renseignements, aux biens, aux installations, aux réseaux et aux appareils électroniques du gouvernement. |
| **Poste de commandement alternante** | Un emplacement distinct pour héberger et exploiter une équipe d'intervention d'urgence ou du personnel de gestion si l'espace de travail normal n'est pas disponible en raison d'une urgence ou d'une crise. |
| **Prévention du crime par la conception** | Principe qui encourage l'utilisation de la conception paysagère et/ou architecturale pour réduire ou éliminer les comportements |

| | |
|---|---|
| **environnementale** | criminels. |
| **Procédures Opérationnelles Normalisées** | Un ensemble d'instructions écrites décrivant les mesures étape par étape à prendre pour accomplir une ou des tâches ou intervenir en cas d'incident. Les PON visent à normaliser le rendement et à compenser tout manque de connaissances ou d'expérience. |
| **Résilience** | Capacité de résister ou de gérer une augmentation soudaine du risque ou du danger pour une personne, une procédure ou un bien immobilier. Exemple : une alimentation de secours capable de fournir de l'électricité pendant une période prolongée en cas de perte du réseau électrique. |
| **Retardement** | Durée nécessaire pour percer une couche de sécurité après la détection d'une tentative d'intrusion. |
| **Risque** | Incertitude que peut engendrer l'exposition à des événements ou résultats non désirés. Il s'agit de l'expression de la probabilité et de l'incidence d'un événement susceptible de nuire à la réalisation des objectifs d'une organisation. |
| **Risque interne** | Une personne ayant une connaissance ou un accès à l'infrastructure d'une organisation (réseaux physiques ou informatiques) qui, de manière malveillante, ou par une mauvaise utilisation de son accès de confiance, nuit aux employés, aux clients, aux actifs, à la réputation ou aux intérêts de l'organisation |
| **Sauvegarde** | Les actifs ou les contrôles externes qui réduisent le risque global pour les employés, les autres actifs ou la prestation de services en diminuant la probabilité d'un événement menaçant, réduisant la probabilité de compromission ou en atténuant la gravité du résultat par une interaction directe ou indirecte avec la valeur des actifs, les menaces ou les vulnérabilités. |
| **Sécurité Matérielle** | L'utilisation de contrôles physiques pour prévenir et retarder l'accès non autorisé aux biens, détecter les tentatives d'accès et les accès non autorisés et activer une intervention appropriée. |
| **Sortie** | Moyens de sortie, y compris les portes, qui mènent de la surface de plancher qu'ils desservent à un bâtiment distinct, à une voie publique ouverte ou à un espace extérieur ouvert protégé de l'exposition au feu du bâtiment et ayant accès à une voie publique ouverte. |
| **Surveillance** | Pour surveiller ou détecter une faille de sécurité. |
| **Surveillance continue** | Surveillance sur une base continue pour confirmer qu'il n'y a pas eu infraction à la sécurité. |
| **Surveillance périodique** | Surveillance périodique, mais régulière pour confirmer qu'il n'y a pas eu d'infraction à la sécurité. La fréquence et la diligence de la surveillance périodique sont fondées sur les recommandations d'une évaluation des risques. |
| **Test de Pénétration** | Exercice visant à tester l'efficacité des systèmes de sécurité en tentant de contourner physiquement les systèmes établis de |

| | |
|---|---|
| | gestion et de protection de l'accès, de détection, d'intervention et de rétablissement utilisés dans une installation. |
| **Vulnérabilité** | Insuffisance liée à la sécurité qui pourrait accroître la susceptibilité à la compromission ou au préjudice. |
| **Zone de haute sécurité** | Zone où l'accès est limité au personnel autorisé détenant la cote de sécurité du GC correspondante et aux visiteurs préapprouvés/contrôlés et escortés de façon appropriée. Exemple – zone où les renseignements et les biens classifiés plus haut que secret sont traités ou stockés. |
| **Zone de sécurité** | Zone où l'accès est limité au personnel autorisé détenant la cote de sécurité du GC correspondante et aux visiteurs dûment escortés. Exemple – zone où les renseignements classifiés jusqu'au niveau Secret inclusivement sont traités ou stockés. |
| **Zone de travail** | Zone où l'accès est limité au personnel qui travaille à l'intérieur et aux visiteurs dûment escortés. Exemple – Espace de bureau du gouvernement ou entrepôt réservé au personnel |

# 5. Protection, détection, réponse et récupération

L'approche du gouvernement du Canada en matière de sécurité matérielle complète d'autres aspects de la PSG. Il est basé sur le principe que la zone externe et interne des installations gouvernementales peut être conçue et gérée pour créer des conditions qui, avec des mesures de contrôle de sécurité matérielle spécifiques, réduiront le risque de violence envers les employés, protéger contre les accès non autorisés, détecter les tentatives ou les accès non autorisés réels et activer des activités d'intervention et de récupération efficaces. Cet objectif de sécurité matérielle, qui se trouve dans le Guide de sécurité matérielle opérationnelle GSMGC-010, comprend le concept de protection, de détection, d'intervention et de rétablissement (PDRR).

## 5.1. Approche préventive

La prévention des préjudices ou des dommages est acceptée comme étant moins coûteuse, en termes de pertes humaines et financières, que de réparer les dommages après qu'ils se produisent. Cela résume l'importance d'intégrer les éléments de la PDRR dans les systèmes de sécurité matérielle du gouvernement du Canada. La protection, la détection et l'intervention sont des éléments interdépendants qui permettent une récupération naturelle des opérations normales d'une manière rentable et rapide. Les personnes autorisées devraient effectuer des essais périodiques des procédures, des plans et de l'équipement de sécurité pour vérifier la conformité aux pratiques de sécurité de chaque ministère ou organisme afin d'atteindre un niveau de préparation plus élevé en cas de menaces potentielles à la sécurité.

### 5.1.1. Prévention du crime par la conception environnementale

Prévention du crime par la conception environnementale (PCCE) est une approche multidisciplinaire de la prévention du crime pendant la désignation, la définition et la conception de la sécurité d'un environnement. La conception des installations et la gestion des environnements naturels et artificiels peuvent permettre aux ministères et aux

organismes de dissuader les actes criminels ou accusatoires tout en gérant de façon sécuritaire le flux de personnes dans l'ensemble d'une installation. Ces modèles visent à influencer positivement le comportement et les activités tout en décourageant les actions indésirables du personnel, des visiteurs et des adversaires potentiels.

#### 5.1.2. Évaluation et gestion des risques

Une évaluation des menaces et des risques (EMR) est un processus utilisé pour déterminer, analyser et traiter les vulnérabilités observées par rapport aux menaces connues ou prévues afin d'établir l'environnement de risque et fait partie intégrante de la stratégie globale de gestion des risques d'un ministère ou d'un organisme. Une fois que le paysage des risques d'un ministère ou d'un organisme a été établi, l'application de ces concepts de DRRR et d'autres guides de sécurité matérielle, que l'on trouve dans les du PORS de la GRC, aidera à gérer les risques connus et à renforcer la résilience aux risques rares ou imprévus à l'avenir.

# 6. Protection

La protection est assurée par l'utilisation d'obstacles physiques, procéduraux et psychologiques pour retarder ou dissuader l'accès non autorisé. Les mesures de protection empêchent la survenue d'événements indésirables et sont souvent appelées barrières. Une barrière de protection doit remplir une partie ou l'ensemble des fonctions suivantes:

- Marquer le périmètre d'une zone d'accès restreint;
- Fournir un niveau de protection contre les attaques physiques ou la force;
- Dissuader une intrusion en rendant un agresseur/attaquant/intrus plus facile à identifier;
- Prévenir, retarder ou contrôler l'accès par le personnel ou les véhicules non autorisés;
- Contenir du personnel ou des biens dans une pièce, une zone ou une zone; et
- Empêcher la fuite.

Une barrière est considérée comme efficace contre l'accès non autorisé lorsqu'elle limite les voies d'accès à un bien et est capable d'arrêter ou de gêner la ou les personnes non autorisées qui s'approchent de n'importe quel côté. Une évaluation doit être effectuée contre les menaces connues et probables, l'adversaire probable et la motivation, les capacités, les compétences et les ressources de l'adversaire. La protection contre les menaces identifiées dans une EMR devrait inclure:

## 6.1. Barrières Physiques

Les barrières physiques sont passives, actives ou une combinaison des deux.

Une barrière passive, comme une borne, empêche les véhicules non autorisés de passer, mais elle ne répondra pas à une attaque. Les barrières actives réagissent ou sont modifiées en cas d'activité non autorisée; par exemple, les agents de sécurité en patrouille.

Une barrière active et passive combinée pourrait être une clôture qui restreint l'accès à la zone en créant un périmètre composé qui est ensuite utilisé pour contenir des gardes de patrouille

qui détecteraient et répondraient à un intrus.

Lorsque la détection n'active pas une réponse efficace, un système de barrière physique ne fait guère plus que fournir une barrière psychologique à un adversaire déterminé et qualifié. Sans les éléments de détection et de réponse, une barrière ne fera que dissuader le déclenchement de l'événement et limiter les adversaires opportunistes non qualifiés.

### 6.1.1. Objectifs des barrières physiques

Les obstacles physiques ont habituellement deux objectifs:

- Rendre la pénétration si complexe ou difficile que seuls quelques attaquants pourront franchir la barrière; et
- Retarder ou, si possible, arrêter une intrusion ou une attaque.

### 6.1.2. Complexité du système

Une conception bien planifiée réduit le nombre d'attaquants potentiels qui ont les connaissances, la détermination, les compétences et les ressources nécessaires pour surmonter un obstacle. La conception de barrières qui utilisent une variété de matériaux et de procédures peut aider à dissuader de nombreux attaquants potentiels qui pourraient ne pas être assez qualifiés ou ambitieux pour relever ce défi.

### 6.1.3. Prolonger et retarder l'attaque

Une barrière robuste nécessite du temps pour être exploitée ou vaincue. La conception de la barrière avec un délai temporisé devrait intégrer les caractéristiques suivantes:

- La force nécessaire pour vaincre la barrière;
- Temps nécessaire pour surmonter la barrière (délai);
- Capacité de reconnaître toute tentative de vaincre la barrière; et
- Temps d'intervention de la force de garde/police.

### 6.1.4. Superposition des obstacles

Les systèmes de sécurité sont souvent conçus à l'aide de multiples barrières entourant un bien protégé; communément appelées « défense en profondeur » ou « anneaux de protection ». Les barrières en couches sont avantageuses lorsqu'elles nécessitent des connaissances, des compétences et des talents accrus pour être contournées et, par conséquent, augmentent la probabilité d'être découvertes en raison d'une exposition prolongée des efforts d'un attaquant à chaque couche de protection. Cela permet aux systèmes de détection d'identifier rapidement l'incident et de lancer une réponse.

## 6.2. Barrières Procédurales

L'utilisation de procédures de routine, afin d'établir une norme de base de conduite ou d'activité acceptable, aidera le personnel à reconnaître les actions et les comportements qui dépassent la norme, ce qui, à son tour, appuie la détection. Le recours au personnel de sécurité, aux registres et aux procédures administratives, comme l'ouverture d'une session dans un bureau, peut avoir un effet dissuasif sur toute activité non désirée. De telles procédures peuvent être automatisées, ce qui peut activer une réponse lorsqu'elles ne sont pas

correctement suivies. Ils peuvent également dissuader les activités indésirables en créant une barrière apparente à l'entrée d'une zone, ce qui tend à empêcher la compromission du bien.

Exemple : Accès aux fichiers d'une salle de fichiers. Si les procédures administratives exigent que quelqu'un se déconnecte ou enregistre les fichiers consultés, cela peut dissuader les personnes de prendre des fichiers sans avoir le besoin de connaître le contenu du fichier. Ainsi, la protection des renseignements contenus dans les dossiers est assurée conformément aux principes du besoin de savoir et du besoin d'accès.

### 6.3. Barrières Psychologiques

Une barrière psychologique est seulement dissuasive, car elle n'entrave pas ou n'arrête pas un événement si l'adversaire décide d'attaquer. Une barrière psychologique comme la présence de caméras de vidéosurveillance ou d'un éclairage de sécurité fonctionnel qui éclaire une installation aidera à confirmer à tout intrus qu'il sera plus facile de les détecter, mais qu'elle n'empêchera physiquement personne d'entrer dans la zone. L'intrus reconnaîtra que cela augmentera son risque d'être détecté et pourrait générer une réponse du personnel de sécurité. L'étendue de l'utilité des obstacles psychologiques particuliers devrait être déterminée par le processus d'EMR.

## 7. Détection

La détection implique l'utilisation d'une conception, de dispositifs, de systèmes et de procédures appropriés pour signaler qu'une tentative ou un accès non autorisé s'est produit. Les systèmes de détection devraient être conçus et mis en œuvre dans le but de fournir la notification la plus rapide possible, de tout événement, afin de réduire le temps nécessaire pour fournir une réponse appropriée. Les éléments de détection augmentent l'efficacité des mesures de protection si elles sont utilisées de façon complémentaire dans le cadre du système de gestion de l'accès de tout ministère ou organisme. Des renseignements supplémentaires sur la gestion de l'accès se trouvent dans GSMGC-006 Guide de gestion de l'accès.

### 7.1. Détection électronique des intrusions

Les systèmes de détection électronique d'intrusion sont conçus pour assurer une surveillance continue des emplacements vitaux ou de grande valeur, des points de contrôle d'accès, des zones dans lesquelles l'accès est contrôlé et de tout autre espace dans lequel la surveillance et le contrôle humains ne sont pas possibles. Les systèmes de détection électronique d'intrusion sont souvent intégrés aux systèmes d'alarme, aux systèmes de sécurité incendie, à la vidéosurveillance, à l'éclairage de sécurité et aux systèmes de cartes de contrôle d'accès électroniques. Les systèmes de détection électronique d'intrusion doivent être surveillé par du personnel capable de coordonner une intervention en cas d'intrusion ou d'urgence. La pratique exemplaire consiste pour les ministères et organismes à établir un Centre des opérations de sécurité (COS) pour diriger cette fonction.

### 7.2. Centre des opérations de sécurité

Un COS fournit une installation pour soutenir le personnel de sécurité dans la surveillance, à

examiner, l'affichage, le contrôle, la gestion et la réponse aux événements liés à la sécurité. Un COS fournit généralement des activités de surveillance 24 heures sur 24 au moyen de systèmes de caméras vidéo, de capteurs d'alarme d'intrusion et de systèmes connexes. Le COS permet également de détecter et d'évaluer les notifications d'alarme et de dépêcher le personnel pour résoudre le problème, comme les équipes de sécurité sous contrat, les commissionnaires ou le personnel des services d'urgence. Le COS exerce un certain nombre de fonctions essentielles et la connaissance de la situation est au premier plan de l'objectif opérationnel. Opérateurs dans le COS peuvent:

- Recueillir des renseignements sur l'environnement contrôlé et surveillé;
- Analyser l'information pour déterminer l'incidence sur le personnel ou l'installation;
- Réagir adéquatement à la situation;
- Peut également servir de centre de commandement en cas d'urgence.

De plus amples renseignements sur les fonctions d'utilisation d'un COS se trouvent dans le GSMGC-003, Guide des considérations relatives à la conception du Centre des opérations de sécurité.

### 7.3. Programmes de sensibilisation à la sécurité

Conformément au DGS, Annexe H : Procédures obligatoires pour la sensibilisation à la sécurité et le contrôle de la formation, les ministères et organismes du gouvernement du Canada doivent élaborer et tenir à jour un programme de sensibilisation à la sécurité et de formation pour les employés de tous les niveaux. Il est fortement recommandé d'inclure dans tous les programmes de sensibilisation à la sécurité des directives sur les procédures que le personnel doit suivre lorsqu'il observe ou subit des incidents de sécurité. L'établissement d'une solide culture de coopération en matière de sécurité et de production de rapports renforcera les fonctions de détection au sein des ministères et organismes du gouvernement du Canada.

## 8. Réponse

L'intervention comprend la mise en œuvre de mesures pour s'assurer que les incidents de sécurité sont signalés aux responsables de la sécurité appropriés et que des mesures correctives immédiates et à long terme sont prises en temps opportun. Les priorités d'intervention, dans l'ordre, sont les suivantes:

1. Préservation de la vie et de la sécurité du personnel;
2. Protection de l'information et des biens du gouvernement du Canada; et
3. Protection des biens pour permettre un rétablissement rapide des opérations normales.

Les plans d'intervention et les PON des ministères et des organismes devraient être fondés sur une EMR qui comprend les menaces connues et prévues à l'endroit et au personnel, les capacités du personnel de sécurité sur place et le soutien disponible des premiers intervenants (police, incendie, ambulance). Ceux-ci devraient être régulièrement pratiqués (exercés) par le personnel de sécurité et le personnel non chargé de la sécurité afin de favoriser une meilleure préparation et de permettre un rétablissement agile des opérations normales. Ces exercices peuvent comprendre des scénarios fondés sur des situations d'urgence liées aux incendies, des évacuations d'installations,

des plans de destruction d'urgence, des alarmes d'intrusion, des confinements, des intrus armés, des catastrophes naturelles, des manifestations ou des démonstrations/protestations. Les méthodes disponibles pour mettre à l'essai ces plans comprennent des exercices sur table, une formation de l'équipe d'intervention d'urgence, une formation et des exercices pratiques fondés sur des scénarios et des tests de pénétration.

# 9. Récupération

La récupération fait référence au rétablissement des niveaux complets de prestation de services à la suite d'un incident. La capacité d'un ministère ou d'un organisme de se rétablir d'un incident, aussi appelé résilience, est directement rendue possible par les mesures utilisées dans les domaines de la protection, de la détection et de l'intervention. Dans un contexte de sécurité matérielle, cela peut comprendre:

- La remise d'un intrus appréhendé à la police;
- Retourner dans les bureaux après une évacuation par alarme incendie;
- La restauration des systèmes de gestion des accès endommagés ou compromis; au
- L'activation d'un autre poste de commandement ou d'un autre point de prestation des services jusqu'à ce que l'emplacement d'origine soit sécuritaire et pleinement opérationnel.

À la suite d'un incident, un examen des principaux éléments de l'événement et des mesures prises pour prévenir ou limiter les répercussions devrait être inclus dans le processus de rétablissement. Les leçons tirées de chaque incident peuvent ensuite être intégrées aux préparatifs et aux plans de PDRR d'un ministère ou d'un organisme.

# 10. Application collaborative de la PDRR

L'élaboration de dispositifs de protection robustes, de systèmes de détection complets et de services d'intervention bien formés et exercés aidera à assurer la résilience dont les ministères et organismes ont besoin pour un rétablissement rapide après un incident ou un événement de sécurité, conformément à la Gestion de la continuité des activités du gouvernement du Canada (BCM) exigences. La PSG et la Politique fédérale de gestion des urgences désignent Sécurité publique Canada (SP) comme l'organisme responsable de la sécurité de la GCA. SP peut fournir des renseignements supplémentaires sur la GCA par l'intermédiaire de son Centre de gestion de la résilience et de la continuité. De plus, à mesure que la société adopte les progrès technologiques, la PDRR pour la sécurité matérielle et la technologie de l'information (TI) et la cybersécurité deviennent de plus en plus étroitement liées. La PSG indique que le Centre de la sécurité des télécommunications (CST) est le principal responsable technique de la sécurité des TI. Le CST peut fournir des renseignements supplémentaires par l'intermédiaire de son Centre canadien pour la cybersécurité.

Lors de la conception d'un système PDRR, il est important que tous les aspects du système fonctionnent de manière complémentaire pour assurer son efficacité. Pour aider à identifier les aspects nécessaires d'un système PDRR, les éléments suivants doivent être pris en compte:

1. Qu'est-ce qui a de la valeur ou de la valeur perçue qu'un adversaire peut souhaiter:
    - Divulguer (exemple: vendre des renseignements à d'autres);
    - Interruption (exemple: arrêt du service d'alimentation électrique d'une installation);
    - Modifier (exemple: modifier l'intention des documents écrits ou des fichiers électroniques);
    - Détruire (exemple: brûlure); où
    - Supprimer (exemple: voler).

2. Qui/quelle est la menace connue ou potentielle? Le risque provient-il:
    - D'une personne ou un groupe (client, ancien employé, employé actuel/menace interne);
    - D'une organisation (crime organisé, groupe terroriste);
    - Dun autre pays (espionnage, adversaire politique ou commercial); où
    - De risques environnementaux (catastrophes naturelles, changements climatiques, régions éloignées, criminalité élevée).
3. Comment/pourquoi une menace connue ou potentielle peut avoir une incidence sur l'installation:
    - Quelle est la méthode d'intrusion ou d'attaque connue ou probable;
    - Quelles sont les capacités connues ou probables d'un adversaire;
    - Quelles sont les motivations connues ou évaluées d'un adversaire;
    - Quelles sont les intentions déclarées ou évaluées d'un adversaire; où
    - Quels sont les antécédents connus des incidents qui se sont produits dans la région et/ou contre le gouvernement du Canada, le ministère ou l'organisme?

Une fois que ces considérations sont examinées, évaluées au moyen d'une EMR et traitées avec des barrières et des mesures de protection interopérables, des systèmes de détection et du personnel d'intervention, les ministères et organismes peuvent être mieux adaptés pour atténuer le risque et permettre le rétablissement en temps le plus opportun possible des menaces pour le personnel, l'information et les biens immobiliers du gouvernement du Canada.

# 11. Références et documents connexes

- Politique sur la sécurité du gouvernement
- Directive sur la gestion de la sécurité
- Politique fédérale en matière de gestion des urgences
- Sécurité publique Canada
- Centre canadien pour la cybersécurité
- GCMGC-003 Guide des considérations relatives à la conception d'un centre des opérations de sécurité
- GCPSG-006 Guide de gestion de l'accès
- GSMGC-010 Guide opérationnel de la sécurité matérielle (rcmp-grc.gc.ca)
- L'international Prévention du crime grâce à une conception environnementale Association

# 12. Promulgation

**Examiné et recommandé aux fins d'approbation.**

J'ai examiné et recommande par la présente, GSMGC-019 (2023) Guide de Protection, Détection, Réponse, et Récupération pour approbation.

Nattress,Shawn Thomas,000302786 Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2023.12.12 14:05:43 -05'00'

Shawn Nattress, Date
Gestionnaire
Principale Organisme Responsable de la Sécurité Matérielle, GRC

**Approuvé**

J'approuve par la présente GSMGC-019 (2023) Guide de Protection, Détection, Réponse, et Récupération.

St-Pierre,Andre Vincent,000171484 Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2024.01.05 12:32:44 -05'00'

André St-Pierre, Date
Directeur, Sécurité Matérielle
Gendarmerie royale du Canada