Orientations sur l'élaboration de plans de gestion de la sécurité pour mettre en œuvre les normes internationales de sécurité et les Principes Volontaires

14 février 2019
Version 1,0

Introduction

Ce document fournit des orientations pour l'élaboration d'un plan de gestion de la sécurité (SMP) qui appuie la mise en œuvre des principes volontaires sur la sécurité et les droits de l'homme (VPSHR), et l'application d'autres meilleures pratiques internationales. Ces informations représentent les meilleures pratiques et l'expérience pratique des membres du MSWG qui ont obtenu l'application de ces mesures dans le monde entier.

Le groupe de travail sur la sécurité minière (MSWG) a été créé en 2015 en tant que forum pour les experts et les praticiens de la sécurité au sein de l'industrie de l'extraction pour collaborer et partager les connaissances et les enseignements des défis continus, des progrès technologiques, les meilleures pratiques et des initiatives de l'industrie telles que les principes volontaires sur la sécurité et les droits de l'homme et la déclaration des droits de l'homme des Nations Unies.

Il existe de nombreux documents, disponibles à partir de diverses sources, qui traitent de la mise en œuvre du VPSHR. Ils discutent tous de la nécessité de politiques et de procédures qui appuient ces principes, mais une organisation doit avoir une solide base de sécurité pour assurer le succès du processus de mise en œuvre.

Le MSWG est fier d'appuyer les initiatives du gouvernement du Canada, de l'Association minière du Canada et des chefs de file de l'industrie de l'extraction dans la promotion du respect des droits de l'homme. Nous nous félicitons de l'occasion qui nous est offerte de partager notre expérience de gestion collective de la sécurité avec les praticiens et les responsables de la supervision de la sécurité.

Portée

La mise en œuvre et l'application du VPSHR exigent qu'une organisation effectue des évaluations des menaces et des risques, élabore des normes de service pour la sécurité propriétaire et contractuelle, et examine attentivement leur relation avec, et leur support, de la sécurité publique. Pour ce faire, un plan de gestion de la sécurité bien considéré qui suit les meilleures pratiques de l'industrie est nécessaire.

Le plan de gestion de la sécurité (SMP) est un document qui décrit la philosophie, les stratégies, les objectifs, les programmes et les processus de sécurité de l'organisation. Il fournit des orientations stratégiques pour

le développement et la direction du service de sécurité d'une manière qui soit conforme au plan d'affaires global de l'entreprise. Il devrait également exposer les plans d'évaluation et d'atténuation des risques.

Le SMP guide les actions de l'entreprise en matière d'atténuation et de protection contre les risques de sécurité ou de nature des droits de l'homme qui pourraient menacer les communautés, les employés, les installations, les opérations, la production, la réputation de l'entreprise et ses opérations globales.

Une considération importante du développement de SMP est d'aligner la mission et les stratégies du programme de sécurité avec celles de l'organisation. Cela garantit que la fonction de sécurité n'est pas perçue comme une dépense, mais fait partie intégrante de l'entreprise et contribue à un environnement de réussite.

Le SMP est un outil qui aide le chef de la sécurité à obtenir un accord et un buy-in d'autres divisions. Il articule la façon dont le service de sécurité est interrelié et soutient tous les domaines de l'organisation. Un plan bien écrit fournit la direction, l'organisation, l'intégration et la continuité du programme de sécurité. Il démontre la connaissance des risques et une planification de réponse pensée.

Le SMP est un document stratégique. Tandis qu'un plan de sécurité du site (SSP) est un document tactique et est l'extension logique d'un SMP. Le SSP articule les spécificités de la sécurité physique, des responsabilités de la force de garde, des relations avec la sécurité publique et d'autres composantes de la prestation des services de sécurité. Des conseils supplémentaires sur le développement du SSP figurent à l'annexe A du présent document.

Développement du plan de gestion de la sécurité

1. Principes de gestion de la sécurité

Unité de l'effort : les efforts de gestion de la sécurité devraient être un effort collectif au sein de l'organisation et devraient inclure les contributions de tous les partenaires et parties prenantes tant internes qu'externes.

Transparence : les informations sur la façon dont les décisions d'atténuation des risques sont prises doivent être partagées avec ceux qui ont un besoin valide de savoir.

Adaptabilité : les stratégies et les processus doivent être conçus pour permettre des changements constants.

Praticité : les responsables de la sécurité ne peuvent pas prédire l'avenir, ni éliminer toutes les menaces. Ils doivent être maniable dans ce qu'ils choisissent de protéger et d'évaluer le coût/avantage des contre-mesures.

Personnalisation : les solutions doivent répondre aux besoins et respecter la culture de l'organisation.

2. Élaboration d'un plan directeur

Les contributions de la direction sur l'établissement des objectifs de sécurité sont impératives et devraient inclure les attentes du service et les tâches fondamentales.

Le cadre de gestion de la sécurité devrait améliorer la préparation, la réponse, la résilience et le soutien de la continuité des activités. Le développement d'un SMP devrait inclure :

- Engagement envers le politique
- Alignement sur les objectifs stratégiques de l'Organisation
- Les standards en termes de normes juridiques et internationales
- Profil organisationnel (mission, production, stratégies)
- Évaluation des risques - Contexte interne et externe
- Préoccupations des intervenants
- Élaboration de plans et de budgets
- Personnel de sécurité, exigences en matière d'infrastructure et interdépendances
- Options de sécurité (analyse de contre-mesure)
- Analyse coûts-avantages
- Assignation de responsabilité et d'autorité

3. Gestion de la sécurité

Le service de sécurité devrait s'approcher de sa mission, étant entendu que la bonne sécurité et le respect des droits de l'homme, des employés et des communautés sont pleinement compatibles. Cela devrait être énoncé dans une politique de gestion globale et un plan qui comprend :

- Un engagement de politique de gestion à la conformité avec les meilleures pratiques internationales pour la gestion de la sécurité et les normes volontaires telles que le VPSHR.
- Un engagement à prévenir et à réduire la probabilité et les conséquences des violations des droits de l'homme.
- Responsabilité et responsabilisation des meilleures pratiques internationales, telles que les principes volontaires sur la sécurité et les droits de l'homme (VPSHR) délégués au gestionnaire de la sécurité.
- Communication du plan à tous les employés et à la disposition de toutes les parties prenantes.
- Alignement avec d'autres politiques (comme l'éthique, le code de conduite, les droits de l'homme)
- Cadre de mise en œuvre et d'examen des objectifs, des cibles et des programmes.
- Engagement à respecter les exigences légales et réglementaires applicables.
- Mécanisme de réponse aux allégations reçues par le biais d'un Grief ou d'une ligne confidentielle pour dénonciateur.

4. Gestion des risques

L'analyse des risques est utilisée pour élaborer des plans de sécurité proactifs et proportionnés qui réduisent la probabilité, les chances et les conséquences des événements perturbateurs. Les évaluations de risque et de menace à la sécurité sont des prérequis pour déterminer le déploiement de forces de sécurité armées ou non armées à l'appui de l'organisation.

L'objectif est de mettre au point un processus complet et systématique pour la gestion préventive des risques associés aux opérations commerciales et de sécurité. Il faut également tenir compte de l'impact des activités de l'organisation sur les communautés dans la zone d'influence. Un enjeu clé est de savoir comment gérer de manière proactive les risques identifiés, en particulier dans les zones de faible gouvernance, où les événements humains ou les causes naturelles ont dégradés L’autorité de la loi.

La planification et les tests de la réponse aux incidents doivent être alignés sur ce processus et inclure le développement d'exercices de formation, l'évaluation des protections en place, les protocoles de réponse, les exigences d'atténuation, les capacités de rétablissement et les procédures opérationnelles actuelles.

5. Évaluation des risques

Une évaluation des risques est un exercice destiné à identifier les menaces à la sécurité, à évaluer la nature et l'étendue des risques posés par ces menaces et les vulnérabilités potentielles. L'évaluation des risques aide la direction à sélectionner et prioriser des mesures de contrôle efficaces. Les objectifs de l'évaluation des risques sont d'empêcher toute activité non autorisée et la perte d'actifs, d'équipements, de biens et de réputation.

a. Établir le contexte externe

Il est essentiel de comprendre le contexte externe de l'Organisation pour s'assurer que les objectifs et les préoccupations des parties prenantes externes sont pris en compte lors de l'évaluation des risques. L'évaluation devrait englober un contexte à l'échelle de l'organisation, tenir compte des exigences légales et réglementaires et des perceptions des intervenants.

Le risque de conflit est inhérent à l'exploitation minière et devrait être reconnu et évalué dans le cadre du processus d'évaluation des risques. Le conflit est souvent le résultat des interactions entre plusieurs facteurs, y compris les entreprises, tous les paliers du gouvernement, les communautés, les organisations non-gouvernementales (ONG), les insurgés et les criminels. Les causes profondes des conflits sont complexes et peuvent avoir des origines historiques.

L'évaluation du contexte externe devrait inclure l'évaluation des conflits créée par des organismes autoritaires et indépendants, tels que l'Institut de recherche internationale sur les conflits de Heidelberg. Les opérations dans des environnements difficiles doivent déterminer si elles ont les bonnes politiques et les systèmes en place pour remplir les obligations et les responsabilités de l'entreprise. L'objectif est d'éviter de causer, de soutenir ou de bénéficier de conflits armés illégaux, de contribuer à l'atteinte aux droits de l'homme et des violations des droits internationaux humanitaires.

Le contexte externe devrait inclure, sans s'y limiter :

- Les actions des personnes extérieures au projet qui cherchent à tirer profit des opportunités offertes par le développement et le fonctionnement de l'entreprise.
- Les activités criminelles courantes.
- Perturbation du projet pour des objectifs économiques, politiques ou sociaux ; actions délibérées qui ont un impact négatif sur le fonctionnement efficace et sûr de l'entreprise.
- Risques associés à la présence de forces et d'opérations de sécurité privée et publique.
- Social, culturel, politique, juridique, réglementaire, financier, technologique, économique, naturel et environnement concurrentiel, qu'ils soient internationaux, nationaux, régionaux ou locaux.
- Les principaux facteurs et tendances qui pourraient influencer les objectifs de l'organisation.
- Relations, perceptions et valeurs des intervenants externes.
- Dans les cas extrêmes - le terrorisme, l'insurrection armée, les coups, la guerre et les risques qu'une réaction de sécurité pourrait produire.

b. Établissement du contexte interne

Le contexte interne tient compte de l'environnement d'exploitation dans lequel l'organisation cherche à atteindre ses objectifs. Le processus de gestion des risques doit être aligné sur la culture, les processus, la structure et la stratégie de l'organisation. Le contexte interne est quelque chose au sein de l'organisation qui influence sur la façon dont une organisation gérera les risques et devrait envisager :

• Les objectifs et la mission de l'organisation.
• Le risque de comportement illégal, contraire à l'éthique ou inapproprié du personnel de projet ou de ceux qui y sont directement affiliés.
• Risques communs tels que le vol par des employés, la violence au travail, les troubles du travail et le sabotage.
• Risques pour les employés ou d'autres personnes associées à la réponse de la sécurité.

c. Analyse des écarts de risque

Avant de commencer le processus de gestion des risques, une compréhension des différents éléments contextuels interconnectés qui affectent l'organisation doit être développée. L'analyse des écarts de risque aide à établir le contexte et devrait inclure :

• Identification des exigences légales applicables et des normes internationales.
• Évaluation des pratiques et procédures de gestion des risques existants, y compris celles associées aux sous-traitants et de la chaîne d'approvisionnement.
• Évaluation des urgences et incidents antérieurs, ainsi que des mesures prises pour prévenir et réagir.
• Identification des risques, mesures préventives, mesures correctives et recommandations d'amélioration.

6. Politique et procédures

Une organisation ne doit pas supposer qu'un entrepreneur en sécurité développera les politiques, les objectifs et les procédures nécessaires pour protéger son entreprise, son personnel, ses biens et sa réputation. La direction doit assumer la responsabilité de déterminer le niveau de sécurité requis, d'identifier les actifs à protéger, et soutenir la mise en œuvre des contre-mesures de sécurité. Cette responsabilité doit être documentée et revue régulièrement, ainsi que le rendement de l'entrepreneur.

La gouvernance du SMP devrait prendre en compte :

• La responsabilisation de la haute direction.
• Les rôles et responsabilités pour tous les aspects du SMP, y compris les exigences, développement, l'examen, la formation, l'amélioration continue et l'approbation.
• La responsabilité et ressourcement pour la gestion du SMP.
• Une politique de sécurité qui articule la direction, la responsabilisation, l'autorité et surveillance du SMP.
• Une formation de mise en œuvre et de sensibilisation pour tous les employés sur l'utilisation efficace du SMP.

Une politique de sécurité est un document de haut niveau, signé par le PDG ou les cadres qui décrivent la vision de l'entreprise pour sécuriser le personnel, les actifs et la réputation. Le document démontre l'engagement de la direction en matière de sécurité et est une directive sur le « quoi » que la société veut être accompli.

La politique de sécurité couvre tous les bureaux de l'entreprise, les opérations et informe tous les responsables de leurs responsabilités. Il s'agit d'un bref document qui articule de larges concepts. C'est la responsabilité des gestionnaires de la sécurité d'élaborer des lignes directrices et procédures qui expliquent « comment » la politique sera remplie.

Les directives et procédures définissent et expliquent les actions nécessaires pour être conforme à la politique. Idéalement, ils éliminent tout point de défaillance unique, ou interprétation subjective. Ils définissent la conformité obligatoire et formeront la base d'admission et de formation récurrente pour le personnel de sécurité et les employés.

a. Dossiers

Un élément clé de la gestion de la sécurité est le maintien des registres administratifs qui comprend :

- Les contrats avec des prestataires de sécurité privés
- La documentation du MOU et de l'appui matériel avec la sécurité publique
- Évaluation et analyse des risques
- Examens de conformité interne
- Responsabilisation de l'équipement
- Autorisations d'armes
- Les licences
- Formation professionnelle
- Contrôles d'accès
- Stockage sécurisé des informations sensibles
- Code de conduite et attestations éthiques
- Lois internationales, nationales et locales applicables
- Tous les engagements publics formels ou informels pris par l'Organisation

b. Responsabilité, autorité et descriptions d'emploi

Les responsabilités, l'autorité et les descriptions de poste doivent être clairement énoncés dans le SMP. Le SMP doit être revu et signé par le responsable exécutif ou un gestionnaire supérieur à qui le gestionnaire de sécurité signale. Ces documents devraient inclure la responsabilité de documenter et de signaler toute interaction avec la sécurité publique, les entrepreneurs, les représentants des collectivités.

L'organisation doit s'efforcer d'attirer et de retenir le personnel de sécurité avec les compétences, connaissances et la capacité de mettre en œuvre le niveau de sécurité désiré. Comme le plus grand faible performance est un manque de formation, l'Organisation devrait s'engager au perfectionnement professionnel du personnel de sécurité pour améliorer la performance de l'emploi, la prestation de services, réduire les plaintes et augmenter la rétention.

7. Surveillance et contrôle de la sécurité

Le SMP doit exposer la structure et la responsabilité du ministère et articuler :

- Les lignes de contrôle, de responsabilisation et de supervision pour le service de sécurité.
- La surveillance de la force de protection de la ligne de front.
- La responsabilité du partage et de la communication des informations de sécurité.

Le SMP devrait exposer les activités de planification et de coordination entre la sécurité et d'autres ministères (relations communautaires, ressources humaines et gouvernement Relations) et les divisions commerciales, qui peuvent impliquer la participation aux réunions régulières. Il est important de veiller à ce que toutes les activités de sécurité soient coordonnées et supervisées à travers un point de contrôle et commandement, et fonctionner avec des directives et procédures consistante. La sécurité ne peut pas être efficace si elle sert deux maîtres.

Voir l'annexe A, gestion de la sécurité de transition et plans de sécurité du site, le plan de gestion stratégique avec les opérations des départements des meilleures pratiques.

Documents de référence clés

Référence 1

Principes volontaires relatifs à la sécurité et aux droits de l'homme. Protocole d'audit pour évaluer la conformité aux indicateurs de performance clés (juin 2013)
https://www.Business-humanrights.org/sites/default/files/Media/documents/Voluntary-Principles-audit-Protocol-Jun-2013.pdf

Nécessite une organisation pour préparer :
• Déclaration d'engagement ou d'approbation du VPSHR.
• Les politiques, procédures et/ou directives pertinentes (ou toute modification apportée l'année précédente) pour la mise en œuvre des principes volontaires.
• Évaluation des risques en matière de sécurité et de droits humains.
• Procédure et mécanisme de signalement des incidents liés à la sécurité des forces de sécurité publiques/privées relatives aux activités de l'entreprise.
• Inclure le VPSHR lors de la conclusion de relations ou de contrats avec les fournisseurs de sécurité.
• Traiter les incidents liés à la sécurité avec les implications des droits de l'homme par les forces de sécurité publiques/privées concernant les activités de l'entreprise.
• Appliquer les normes VPSHR dans la sélection des prestataires de sécurité privés, formulation d'un accord contractuel avec des prestataires de sécurité privés, et arrangements avec les forces de sécurité publiques.

Référence 2

La norme de performance 4 de la société financière internationale (Communauté, Santé, Sûreté et Sécurité)
https://www.ifc.org/wps/wcm/connect/a40bc60049a78f49b80efaa8c6a8312a/PS4_English_2012.pdf?MOD=AJPERES

Oblige les entreprises à :
• Évaluer le risque de sécurité que leurs opérations peuvent créer sur les communautés.
• Développer des moyens de gérer et d'atténuer ces risques.
• Gérer la sécurité privée de manière responsable.
• S'engager dans la sécurité publique.
• Examiner et enquêter sur les allégations d'actes illicites commis par le personnel de sécurité.

Également :
• Comprendre les exigences de l'organisation en matière de risque, de sécurité et de protection des droits de la personne.
• Établir des politiques et des objectifs pour gérer les risques.
• Mettre en œuvre des contrôles opérationnels pour gérer les risques, les mesures de sécurité et le respect pour les droits de l'homme.
• Surveiller et examiner la performance et l'efficacité des plans de sécurité (administration et opérations).
• Promouvoir une amélioration continue basée sur la mesure des objets.

Référence 3
Guide des bonnes pratiques de l'IFC, utilisation des forces de sécurité : évaluation et gestion des risques et impacts, orientations pour le secteur privé dans les marchés émergents
https://www.IFC.org/WPS/WCM/Connect/topics_ext_content/ifc_external_corporate_site/Sustainability-at-IFC/publications/publications_handbook_securityforces

• Gestion de la sécurité privée
Décisions concernant le type, le nombre, les responsabilités et l'armement de la sécurité privée devraient découler d'une évaluation des risques de sécurité et des réponses appropriées.
• Équiper
Les gardes ont-ils ce dont ils ont besoin pour faire leur travail correctement et en toute sécurité ? Cela signifie habituellement un uniforme, pièces d'identité et un dispositif de communication (généralement une radio). Dans certains cas, il comprend des armes non létales, comme du poivre de cayenne. La décision d'armer les gardes avec des armes de force létale, comme une arme à feu est grave, ce qui devrait dériver de l'évaluation du risque et être accompagnée d'un programme de formation spécifique.
• Contrôle
Qui assure la sécurité ? Est-ce que quelque chose dans le passé des gardes est préoccupant ? Les entreprises doivent faire des enquêtes raisonnables pour s'assurer qu'aucun antécédent d'abus ou de malhonnêteté n'est présent. Cela peut nécessiter des vérifications des antécédents ou des vérifications croisées auprès d'autres entreprises, de représentants de gouvernements nationaux ou étrangers, de missions de l'ONU, etc., selon le contexte du pays.
• Assurer l'utilisation appropriée de la force
Les gardes savent-ils ce qu'on s'attend d'eux ? Sont-ils disposés à réagir avec une force appropriée et proportionnelle dans n'importe quelle situation ? Les entreprises devraient utiliser leurs politiques et procédures, renforcées par la formation, pour fournir des instructions claires aux gardes directement employés. Cela peut être aussi simple que d'inclure une clause dans le contrat de travail fixant les attentes et le suivi de la formation.
• Formation professionnelle
La formation devrait se concentrer sur le comportement et l'utilisation de la force appropriés. Dans des contextes à faible risque Cela peut impliquer seulement un bref examen des politiques et des procédures, enregistrées dans un journal, pour veiller à ce que les gardes comprennent comment réagir aux interactions et aux scénarios communs.
• Surveillance
Les gardiens sont-ils professionnellement et adéquatement performants ? Les entreprises doivent vérifier que les politiques et procédures demeurent pertinentes et que les gardes en sont conscients et qu'ils les suivent. Les entreprises qui contractent des services de sécurité conservent toujours la responsabilité des prestataires de services de sécurité tiers pour assurer un contrôle approprié, l'utilisation de la force, la formation, l'équipement et le suivi des gardes.
• Gérer la relation avec la sécurité publique
Dans les contextes à faible risque, les entreprises peuvent avoir des interactions minimes avec les forces de sécurité publique— c'est particulièrement vrai en ce qui concerne les forces nationales, comme les forces armées. Les entreprises ont probablement besoin du soutien d'au moins la police locale en cas d'incident, et il est important de comprendre qui va intervenir, et comment. L'accent est mis sur l'évaluation et l'engagement, en s'appuyant sur des questions clés, telles que : les forces de sécurité publique susceptibles d'être impliquées ? (Par exemple, seulement lorsqu'il est appelé, ou potentiellement dans d'autres cas également ?) Quel type d'individu ou d'unité est susceptible de répondre? Comment sont-ils susceptibles de

réagir ? (Ex., quel type de capacité, de mandat, de réputation, etc., qu'ils ont, et comment cela pourrait-il s'appliquer à des scénarios probables impliquant l'entreprise ?).

• L'engagement

Existe-t-il des occasions d'établir une relation avec la police ou d'autres autorités de forces de sécurité ? Les entreprises sont encouragées à contacter les autorités, de préférence en l'avancement de toute question — pour comprendre les déploiements potentiels et, possible, de promouvoir l'utilisation appropriée et proportionnelle de la force. Dans un contexte à faible risque, cela peut impliquer simplement de faire des introductions au commandant de police local et initier une discussion sur le moment et la façon dont les autorités sont susceptibles de répondre à l'entreprise ou impliquant du personnel de l'entreprise.

• La documentation

Les entreprises doivent documenter leurs efforts d'engagement, s'ils réussissent ou non (par exemple, dans un journal de réunion de base avec les dates, les participants et les sujets clés).

• Évaluation des menaces et des risques

Recherche et analyse du contexte national : prise en compte des risques potentiels un environnement d'exploitation plus large peut inclure le risque inhérent au pays, l'état de droit, criminalité, l'environnement physique, le contexte socio-économique, la gouvernance, informations spécifiques à l'industrie qui pourraient influencer sur la situation sécuritaire. Outre le risque propre à chaque pays, il est également recommandé de revoir la solidité et la réputation des forces de sécurité publique existantes. Recherche et analyse de la situation de sécurité nationale et/ou locale : analyse des situations de sécurité considère souvent la disponibilité et la réputation professionnelle la sécurité privée, les antécédents et la réputation des forces de sécurité publique en matière de droits humains (comme la police ou l'armée), et tout autre élément significatif dans des circonstances particulières.

• Mesures de prévention et d'atténuation

L'élaboration et le raffinage de mesures de prévention et d'atténuation exigent souvent l'examen de la manière d'aborder un éventail plus large des impacts potentiels qui les scénarios, y compris un processus de priorisation. Le tableau de réponse aux risques et la carte thermique peut aider une entreprise à déterminer les risques et impacts à traiter comme étant le plus Priorité. L'inclusion du personnel des relations communautaires dans la conception des mesures d'atténuation peut accroître leur efficacité globale. Le chapitre V du présent document (préparation d'un plan de gestion de la sécurité) fournit un aperçu général des plans de gestion de la sécurité.

Référence 4

Autres documents de référence

• Norme ANSI/ASIS RA 1.2015 évaluation des risques :
https://webstore.ansi.org/Standards/ASIS/ANSIASISRIMSRA2015

• Système de gestion ANSI/ASIS pour la qualité de la société de sécurité privée Opérations :
http://www.acq.osd.mil/log/ps/.psc.html/7_Management_System_for_Quality.pdf

• ASIS orientation générale de l'évaluation des risques :

• https://www.asisonline.org/publications/SG-ASIS-General-Security-riskassessment-Guideline/

• Sélection et formation de l'agent de sécurité privée ASIS:
https://www.asisonline.org/publications/SG-ASIS-Private-Security-officerselection-and-Training-Guideline-2010-Ed/

• Vérification de la mise en œuvre du VPSHR, Global Compact Network Canada:
http://www.GlobalCompact.ca/Auditing-Implementation-of-the-voluntaryprinciples-on-Security-and-Human-Rights/

• Gestion de la sécurité contemporaine (John Fay, Elsevier):
https://www.Elsevier.com/books/Contemporary-Security-Management/Fay/978-0-12-381549-1
• ICMM
https://www.ICMM.com/en-GB/publications/Mining-and-Communities/Voluntary-Principles-on-Security-and-Human-Rights-Implementation-guidancetools
• Trousse de la sécurité et des droits de l'homme du CICR et du DCAF:
http://www.securityhumanrightshub.org/content/Toolkit
• Rapport de l'Association internationale des producteurs de pétrole et de gaz sur les armes à feu et le recours à la force :
http://www.OGP.org.uk/pubs/320.pdf
• Code de conduite international pour les prestataires de services de sécurité privée :
www.ICOCA.ch/
• Boîte à outils de mise en œuvre de la MIGA pour les grands projets :
https://www.miga.org/documents/vpshr_toolkit_v3.pdf
• Diligence raisonnable de l'OCDE pour des chaînes d'approvisionnement responsables de minéraux provenant de zones de conflit et à risque élevé :
http://www.oecd.org/Corporate/MNE/Mining.htm
• Analyse des risques et sélection des mesures de sécurité (Thomas Norman, CRC Appuyez sur):
https://www.crcpress.com/Risk-Analysis-and-Security-Countermeasure-Selection-Second-Edition/Norman-CPPPSPCSC/p/book/9781482244199
• Analyse des risques et enquête sur la sécurité (James broder, Elsevier):
https://www.Elsevier.com/books/Risk-Analysis-and-the-Security-Survey/broder/978-0-12-382233-8
• Principes fondamentaux de l'ONU sur le recours à la force et aux armes à feu par les responsables de l'application de la loi:
www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx
• Code de conduite des agents d'application de la loi des Nations Unies :
www.ohchr.org/EN/ProfessionalInterest/Pages/LawEnforcementOfficials.aspx
• Principes volontaires sur la sécurité et les droits de l'homme :
http://www.voluntaryprinciples.org/resources/
• Outil de Conseils de Mise en œuvre de Principes Volontaire :
http://www.voluntaryprinciples.org/wp-content/uploads/2013/03/VPs_IGT_Final_13-09-11.pdf Anglais
http://www.voluntaryprinciples.org/wp-content/uploads/2013/03/IGTSPANISH1.pdf Espagnol
• World Gold Council Conflict-free Gold Standard
https://www.Gold.org/who-Weare/Our-members/Responsible-Gold/Conflict-Free-Gold-standard

ANNEXE A

Transition de la gestion de la sécurité et des plans de sécurité du site

1. Gestion des forces de sécurité privées

Le rôle de la sécurité privée est de fournir des services préventifs et défensifs, de protéger les employés, les installations, l'équipement et les opérations de l'entreprise. Personnel de sécurité privé n'ont pas d'autorité de répression et ne doivent pas empiéter sur les devoirs et responsabilités réservées aux forces de sécurité publiques.

a. Sécurité contractuelle

Un contrat constitue la base juridique de la relation entre l'organisation et les l'entrepreneur en sécurité. L'organisation est responsable de toutes les activités externalisées Autre entité, et exige une surveillance et une supervision constantes. Responsabilité de respect des droits de l'homme et se conformer à la loi ne peut être sous-traitée à un tiers Parti. L'organisation est en fin de compte responsable des actions d'un entrepreneur. Le contrat doit préciser les responsabilités, les conditions et les conditions dans l'entrepreneur est de fournir des services de sécurité.

Le contrat doit clairement définir :

- Un engagement à respecter les mêmes obligations que celles détenues par la société.
- Confidentialité et exigences en matière de conflits d'intérêts.
- Un processus d'évaluation des risques et de signalement des événements indésirables et perturbateurs.
- Description des services à effectuer par l'entrepreneur.
- L'exigence de formation aux droits de l'homme avant entrer en Service.
- Les mécanismes en place pour s'assurer que la force physique n'est utilisée que lorsque cela est strictement nécessaire et dans une mesure proportionnelle à la menace.

b. Sélection de l'entrepreneur en sécurité privée

Lors de la sélection d'un fournisseur de sécurité, l'organisation doit effectuer des vérifications qui comprend le dépistage de la réputation institutionnelle, les normes de formation, les des antécédents d'allégations de violations des droits de l'homme ou d'autres comportement criminel.

Ne conserver que les services des contractants de sécurité compétents et engagés à opérer conformément aux normes en matière de droits de l'homme, telles que le VPSHR. L'organisation est responsable du travail et du personnel de l'entrepreneur. Vous ne pouvez pas sous-traiter la responsabilité de respecter les droits de la personne. L'organisation devrait établir et documenter les critères de contrôle et de sélection de la sécurité contractuelle. Il incombe à l'organisation de veiller à ce que les contrats soient conformes aux lois applicables et à toutes les autres obligations contractuelles.

Les fournisseurs potentiels de services de sécurité contractuels doivent faire l'objet d'une enquête :

- Un historique démontré de l'exécution des activités de sécurité dans le respect des lois pertinentes.
- Leur capacité à protéger les personnes, les biens et la réputation du client.
- Des ressources adéquates et du personnel qualifié sont fournis pour répondre aux objectifs.
- Transparence, responsabilisation et supervision adéquate de leur personnel.
- Tous les avantages financiers, législatifs et rémunérateurs de leur personnel sont respectés.
- Les enregistrements, licences et permis requis sont à jour.
- Des registres précis du personnel et de l'équipement sont conservés.

c. Surveillance active de la performance de l'entrepreneur

Pour assurer une bonne performance, l'organisation doit effectuer des contrôles réguliers, la formation, enquêter sur toute allégation crédible d'abus ou d'actes répréhensibles, et surveiller les performances de manière continue.

d. Sélection, dépistage des antécédents et vérification du personnel de sécurité

Le personnel de sécurité occupe des postes de confiance. L'entreprise devrait établir des procédures documentées pour les vérifications préalables à l'embauche et la vérification des antécédents. Des normes minimales doivent être établies et des procédures doivent être mises en œuvre pour éliminer les candidats qui ne possèdent pas les qualifications en fonction de leurs connaissances, de leurs compétences, de leurs aptitudes et de leur expérience. Ce processus de sélection doit faire partie de tous les contrats afin d'assurer qu'aucune personne n'est impliquée de manière crédible dans les abus des droits de l'homme.

De plus, des vérifications des antécédents valides doivent être effectuées auprès de fournisseurs de services de sécurité potentiels pour détecter les allégations d'abus passés, d'utilisation inappropriée de la force ou d'autres activités criminelles et actes répréhensibles. Le processus de dépistage et de vérification doit être fondé sur la nature du travail, le candidat est considéré, le niveau d'autorité de la personne et la zone de spécialisation. Le dépistage doit avoir lieu avant qu'un candidat ne soit offert un poste et ne commence à travailler. Les candidats doivent signer les autorisations et les consentements appropriés avant de procéder à l'examen préalable.

Le personnel de sécurité ayant accès à des informations et à des opérations sensibles doivent être soumis à des vérifications plus strictes. La vie privée et la confidentialité de tous les renseignements personnels doivent être protégées.

e. Contrôle de fond de la garde de sécurité

La vérification de l'identité et des antécédents personnels devrait comprendre :

- Vérification de l'adresse à domicile
- Dossiers d'emploi
- Médias électroniques
- Antécédents de casiers judiciaires et civils
- Violations des droits de la personne
- Registre des véhicules à moteur
- Rapport de crédit
- Base de données sur les délinquants sexuels
- Sanction du gouvernement et de l'industrie
- Dossiers de permis de l'industrie

f. Vérification de l'expérience et des qualifications

La vérification de l'expérience et des qualifications devrait tenir compte, sans toutefois s'y limiter, des éléments suivants :

- Éducation
- Antécédents professionnels
- Autorisation / Attestation / Inscription
- Références personnelles
- Entrevues avec les superviseurs et les collègues de travail
- Service militaire/de police

Les exclusions, les renseignements non disponibles, peu fiables ou inappropriés doivent être documentées.

g. Dépistage et Vérification
Établir des critères claires et définis pour évaluer :
• Les abus de substances.
• Aptitude physique et mentale.
• Aptitude à transporter des armes.
• Résilience aux conditions stressantes et défavorables.
• Association criminelle et susceptibilité à la corruption.

h. Compétence, formation et adéquation
Le plus grand contributeur à une mauvaise performance est le manque de formation. Le service de sécurité devrait identifier les connaissances et les compétences requises par le personnel propriétaire et contractuel pour accomplir les tâches assignées. Le département devrait établir sa propre norme de formation minimale à d'admission en tant qu'échelon des normes pouvant ne pas répondre aux compétences requises. La formation à d'admission doit toujours être complété avant l'entrer en service. Les contractants doivent démontrer que leurs employés ont reçu et complétés de manière satisfaisante la formation. La surveillance et la formation périodique devraient être menées de façon continue afin de cerner les possibilités d'amélioration et de faire preuve de diligence raisonnable.

Le MMN devrait engager l'organisation à maintenir les normes les plus élevées de compétence technique et professionnelle de la force de garde au moyen d'un programme de formation exhaustif. Les SSP devraient décrire les responsabilités en matière de formation du prestataire de services de sécurité et de l'entreprise, ainsi que le calendrier annuel.

La formation doit inclure le respect des droits de l'homme, des mécanismes de grief, la conduite éthique, l'emploi de la force, et la compétence avec les armes offensives et de défense émises. Une formation pratique et basée sur des scénarios qui renforce la prise de décision dans des conditions qui reflètent l'environnement d'exploitation est recommandé. La formation devrait inclure les procédures de prévention et d'atténuation, les réponses, la documentation d'incidents, la communication et la responsabilisation. L'entreprise devrait examiner les programmes de formation des entrepreneurs et, en cas échéant, augmenter la formation grâce à l'utilisation de tiers qualifiés ou des instructions directes.

Au minimum, le personnel de sécurité devrait recevoir une formation d'admission et récurrente dans :
• Compétences de garde de base
• Les commandes et procédures de poste de garde
• Code de conduite, d'éthique et de droits de l'homme
• Utilisation de la force
• Santé, sécurité et environnement
• Utilisation d'armes défensives et offensives (selon le cas)
Tous les exercices d'armement doivent être effectués selon une norme écrite appropriée pour les armes délivrées. La formation devrait comprendre une formation axée sur des scénarios, une formation en mécanique et en exploitation qui comprend des défaillances et une qualification en tir réel. La formation devrait être donnée au moins une fois par année, et plus fréquemment si la loi l'exige.

2. Utilisation de la force

Le recours à la force par la sécurité privée n'est sanctionné que pour des mesures préventives et fonction de la nature et de l'étendue de la menace. Lorsque nécessaire pour armer la force de garde, l'organisation assurera des niveaux élevés de compétences techniques et professionnelles et une compréhension claire des règles recours à la force. Cela nécessite une formation récurrente sur les lignes directrices sur l'utilisation des forces, et le respect des droits de l'homme.

L'autorisation de transporter des armes ne doit être accordée qu'au personnel qualifié conformément aux conditions d'un contrat. Les armes devraient être émises seulement après que les antécédents et les qualifications du personnel ont été établis, et qu'une formation sur l'arme spécifique soit délivrée et complétée de manière satisfaisante. Cela devrait seulement être autorisé lorsqu'il y a une attente raisonnable de menace à la vie fondée sur l'évaluation des risques. La formation, le déploiement et la nécessité de porter des armes doivent être conformes au droit du pays d'accueil. L'évaluation de la nécessité de déployer des armes tient compte des conséquences possibles de l'utilisation accidentelle ou aveugle d'armes.

L'utilisation de la force doit toujours être raisonnable et nécessaire, proportionnelle et licite. Les règles pour l'usage de la force doivent être revues pour s'assurer qu'ils satisfont aux mesures nationales ou les normes juridiques régionales. Les options pour les forces non létales, moins létales et létales doivent être dans le contexte local et les exigences légales. L'utilisation des règles de force devrait être décrite dans tous les contrats conclus avec des prestataires de sécurité privés.

Les dispositions contractuelles devraient comprendre :

- Paramètres pour l'utilisation de la force physique.
- Les circonstances dans lesquelles les personnes sont autorisées à transporter des armes ; armes et munitions permises.
- Un engagement à s'assurer que les armes ne sont utilisées que dans des circonstances appropriées et d'une manière susceptible de diminuer le risque de préjudice inutile.
- Interdiction de l'utilisation d'armes et de munitions non autorisées.
- Réglementation pour le contrôle, le stockage et la responsabilisation des armes émises.
- Directives de réponse graduée sur l'utilisation de la force.
- Mettre l'accent sur l'utilisation des techniques de désescalade.
- Un mécanisme de signalement pour toute utilisation de l'incident de la force.

a. Formation sur l'usage de la force

Les règles relatives à l'utilisation de la force doivent être incorporées à la fois à l'admission des programmes de formation. Les dossiers de formation et les compétences démontrées doivent être maintenues. L'utilisation de la formation sur l'usage de la force doit souligner :

- L'utilisation de la force létale uniquement en cas de légitime défense ou de défense autres contre la menace imminente de mort ou de blessure grave, ne jamais être utilisé en défense de biens ;
- La force devrait être raisonnablement nécessaire et utilisée en dernier recours ;
- La force doit être proportionnée à la menace et déployée uniquement en fonction de l'ensemble des circonstances pour contrer une menace ;
- L'utilisation de la force n'est utilisée que pour atteindre des objectifs légitimes.

La formation sur l'utilisation du continuum de la force devrait décrire, mais ne se limite pas à :
• Présence de sécurité ;
• Commandes verbales ;
• Commandes à main ouverte ;
• Les armes non létales ;
• La menace de la force létale ;
• Utilisation de la force létale.
La formation sur le recours à la force doit renforcer la prémisse selon laquelle la sécurité privée ne remplace pas la sécurité publique et renforcer les limites de leur autorité. Les programmes de formation doivent insister sur le fait que la force létale n'est justifiée que dans des conditions d'extrême nécessité et en dernier recours lorsque tous les moyens inférieurs ont échoué ou ne peuvent raisonnablement être employés. La force létale ne doit servir qu'à la légitime défense à la défense d'autrui ou lorsqu'il semble raisonnablement nécessaire d'empêcher la perpétration d'une infraction grave comportant une menace grave à la vie ou des lésions corporelles graves.

La défense d'autrui peut inclure l'utilisation de la force létale lorsqu'il est raisonnablement nécessaire pour empêcher le vol ou le sabotage de biens intrinsèquement dangereux, la perte ou la destruction de ce qui présenterait une menace imminente de mort ou de lésions corporelles graves. L'autorité juridique peut également autoriser l'utilisation de la force létale si elle s'avère nécessaire pour empêcher le sabotage ou la destruction des infrastructures, les dommages qui créeraient une menace imminente de mort ou de blessures corporelles graves.

b. Gestion des armes et des munitions
Le département de sécurité est chargé d'établir, de maintenir et de documenter les procédures qui garantissent :
• Toutes les armes et munitions sont acquises légalement ;
• Responsabilisation constante de toutes les armes et munitions émises et retournées ;
• Les armes et munitions émises sont proportionnées aux risques identifiés et aux tâches à exécuter et à respecter toutes les normes légales ;
• Des dispositions appropriées sont prises pour le stockage, l'émission et l'entretien ;
• Les entrepreneurs ne déploient que des armes et des munitions approuvées par l'organisation ;
Toutes les personnes autorisées à porter une arme ont une licence valide et une formation en cours.

c. Appréhension et détention des criminels
Dans le cadre de l'instruction sur le recours à la force, le personnel de sécurité doit être formé sur la façon de traiter avec les personnes appréhendées ou détenues dans l'exercice de leurs fonctions. Ils doivent comprendre les limites de leur pouvoir et que cela n'inclura généralement que les personnes interdites pendant une attaque contre le personnel et les biens sous leur protection légitime. La formation devrait insister sur la nécessité de traiter le personnel appréhendé avec humanité et de respecter ses droits humains et constitutionnels.

La formation comprendra des mesures pour protéger la personne appréhendée contre la violence, des rapports et des transferts immédiats aux autorités compétentes. Les rapports d'incidents doivent être préparés incluant l'identité de la personne, l'infraction présumée, à laquelle ont été transférés, les premiers secours ou l'assistance fournie, et leur état au moment du transfert.

Les personnes détenues peuvent être fouillées par le personnel de sécurité afin d'assurer leur sécurité contre les armes et de protéger les preuves. Les procédures de perquisition doivent garantir la dignité et le traitement humain du détenu et faire la distinction entre les perquisitions minimalement invasives et les perquisitions complètes. Toutes les personnes détenues devraient recevoir immédiatement les premiers soins nécessaires.

3. Les uniformes

Tous les membres de l'équipe de sécurité devraient utiliser des uniformes indiquant leur appartenance à un service. Les uniformes et le matériel de sécurité privés, comme les véhicules de patrouille, doivent être d'un modèle, d'une couleur et de marques qui les distinguent de la sécurité publique. Le personnel de sécurité et les véhicules devraient avoir des numéros d'insigne uniques qui facilitent l'identification et la transparence des rapports.

Les uniformes projettent une image positive de l'organisation et encouragent la conduite professionnelle et responsable. Il peut y avoir des circonstances où une évaluation des risques indique qu'il est conseillé d'utiliser la sécurité non en uniforme. Lorsqu'une approche discrète est requise, le personnel de sécurité ne devrait pas porter ouvertement des armes à feu et conserver sur ses personnes des pièces d'identité non transférables.

La présence d'agents de sécurité en uniforme est la première option pour chaque continuum de recours à la force. Les uniformes et les véhicules marqués indiquent aux employés, au public et à la sécurité publique que les membres de l'équipe ont l'autorisation et la responsabilité de protéger le personnel et les biens de l'entreprise.

4. La communication

Une communication efficace est la composante la plus importante pour prévenir, gérer, et la déclaration des événements de sécurité. Les plans de communication garantissent un contrôle adéquat, la coordination et la fonctionnalité pour les opérations de sécurité. Le SMP devrait décrire les procédures et les processus de communication considérant :

- Communications internes au sein des départements, des entrepreneurs, des clients et parties prenantes ;
- La réception, la documentation et la réponse aux communications des sources externes ;
- Communication structurée avec la sécurité publique et les intervenants d'urgence ;
- Communication dédiée et sécurisée lors de perturbations et d'urgences Événements.

L'organisation devrait établir et communiquer ses procédures internes et externes de traitement des plaintes et des griefs. Le personnel de sécurité doit être formé pour recevoir et signaler les plaintes et les griefs et assurer la confidentialité. Les plaintes non signalées et non résolues de la collectivité peuvent rapidement devenir des événements perturbateurs.

5. Santé et sécurité au travail

Un SMP devrait s'engager à fournir au personnel de sécurité un milieu de travail sain et sécuritaire, en reconnaissant les dangers inhérents à l'environnement et aux tâches. Il devrait mettre l'accent sur les précautions raisonnables à prendre pour protéger toutes les personnes qui travaillent pour le compte de l'organisation, particulièrement celles qui occupent des postes à risque élevé, comme la sécurité.

6. Gestion de la réponse aux incidents

Une structure administrative appropriée devrait être mise en œuvre pour gérer efficacement les incidents et les interventions. Le SMP doit préciser la structure de gestion du ministère, le pouvoir décisionnel, la responsabilité de la mise en œuvre et les rapports. L'organisation devrait avoir une équipe de gestion des incidents (EGI) pour diriger l'intervention en cas d'incident sous la direction claire de la direction ou de ses délégués. Le SMP devrait décrire le rôle de la sécurité au sein de l'EGI et inclure ce qui suit :

- La planification
- Gestion de la réponse aux incidents
- Gestion des ressources humaines
- Santé, sécurité et réponse médicale
- Gestion de l'information
- Communications internes et externes
- Fonctions de support critiques

7. Réponse aux incidents

Le service de sécurité est chargé de développer la réponse aux incidents et dans le cadre du processus d'évaluation des risques de l'entreprise. La réponse et la gestion des incidents doit tenir compte:

- Protéger la vie, la propriété et la réputation de l'organisation.
- Respect des droits de l'homme et de la dignité humaine.
- Identification et signalement d'événements potentiellement perturbateurs, d'atténuation et plans de rétablissement.
- Procédures de notification et de mobilisation pour la direction, les intervenants et les autorités.

L'organisation devrait élaborer des procédures pour déclarer et enquêter sur les incidents qui comprend :

- L'heure et l'emplacement.
- L'identité des personnes impliquées, y compris les coordonnées.
- Blessures et dommages subis.
- Les circonstances menant à l'événement.
- Mesures de riposte déployées.
- Cause de toutes les blessures et dommages internes et externes.
- Analyse des causes profondes.
- Actions correctives et préventives.

Le SMP et le SSP devraient décrire les responsabilités et les échéanciers pour mener des enquêtes sur les allégations et incidents, y compris :

- Un engagement à une enquête expéditive sur toute allégation d'abus ou de méfaits.
- Entrepreneur de sécurité privé qui mène des enquêtes sur des incidents ou des allégations, et le droit réservé de l'organisation de mener une enquête indépendante.
- Les conclusions de l'enquête comprendront une recommandation de mesures, l'action et les changements de politique ou de procédure.

8. Évaluation des performances et amélioration continue

L'évaluation du rendement comprend la mesure, la surveillance et l'évaluation de la prestation de services par le ministère et l'entrepreneur, l'assurance de la qualité, la conformité à la loi et le respect des droits de la personne. Les paramètres comprennent le respect des politiques, des objectifs et des cibles de rendement.

Des indicateurs de performance devraient être élaborés pour mesurer à la fois le système de gérance et la conformité opérationnelle. Les indicateurs devraient fournir des informations utiles qui identifie à la fois les réussites et les domaines nécessitant une amélioration. Ils devraient également identifier comment les risques significatifs sont gérés.
L'évaluation devrait prendre en compte :
• Validation des plans de gestion et des stratégies de sécurité physique.
• Compétence du personnel de sécurité.
• Capacités de réponse.
• Conformité des contrats.
• Formation et préparation.

Le SMP et le SSP devraient indiquer que les mesures correctives seront identifiées et communiquées en temps opportun et qu'elles devraient s'attaquer aux causes profondes de l'échec. La responsabilité des mesures correctives et une date d'achèvement devraient être attribuées. Les constatations qui dépassent les attentes devraient être notées comme des pratiques exemplaires et communiquées de l'organisation. L'amélioration continue devrait tenir compte des changements dans les risques, les activités et les opérations qui influent sur la prestation des services. Les procédures, les systèmes et la formation doivent être adaptés pour tenir compte :
• Changements de politique.
• Changements aux dangers, risques et menaces.
• Changements de personnel et de contrat.
• Changements de processus et de technologie.
• Enseignements tirés des exercices et de la formation.
• Enseignements tirés des événements perturbateurs.
• Changements dans l'environnement extérieur (tels que politique, social, juridique).

9. Gestion des relations avec la sécurité publique
Les forces de sécurité publique ont la seule responsabilité de répondre et d'enquêter l'activité criminelle, en particulier les incidents d'intérêt général. Ils ont aussi la responsabilité première de l'ordre publique, y compris les protestations, les manifestations et résistances passives. Dans le cas d'incidents impliquant des infractions criminelles, des confrontations potentiellement violentes ou des manifestations, on peut leur demander d'intervenir pour protéger le personnel et les biens de l'entreprise. Il est important que la sécurité publique soit informée des politiques et des engagements de l'organisation avant qu'ils ne soient déployés en cas d'incident.

L'entreprise doit entretenir des relations constructives et une bonne communication avec forces de sécurité publique. Si les forces de sécurité publiques sont affectées au projet, il est important qu'un MOU d'accord soit établi pour assurer la transparence. Le MOU devrait décrire les dispositions relatives aux transferts d'équipement, au soutien matériel et au rôle de la force de sécurité publique dans la protection des biens de la compagnie. Il faudrait élaborer une planification d'urgence conjointe et des mécanismes de coordination.