Guía para el Desarrollo de Planes de Gestión de Seguridad a fin de Implementar Normas Internacionales de Seguridad y Principios Voluntarios

14 de febrero de 2019
Versión 1.0

Introducción

Este documento proporciona orientación para desarrollar un Plan de Gestión de Seguridad (PGS) que apoye la implementación de Principios Voluntarios sobre Seguridad y Derechos Humanos (VPSHR), y la aplicación de otras mejores prácticas internacionales. Esta información representa las mejores prácticas y experiencia práctica de los miembros del MSWG obtenidas de la aplicación de estas medidas en todo el mundo.

El Grupo de Trabajo sobre Seguridad Minera (MSWG) fue establecido en 2015 como un foro para expertos en la materia y profesionales de seguridad dentro de la industria extractiva para colaborar y compartir ideas y aprendizajes de desafíos constantes, avances tecnológicos, mejores prácticas y promover los objetivos de las iniciativas de la industria, tales como los Principios Voluntarios sobre Seguridad y Derechos Humanos y la Declaración de Derechos Humanos de la ONU.

Hay muchos documentos, a partir de una variedad de fuentes, que abordan la implementación de los VPSHR. Todos ellos discuten la necesidad de políticas y procedimientos que apoyen los principios, pero una organización debe tener una base de seguridad sólida para asegurar el éxito del proceso de implementación.

El MSWG se enorgullece en apoyar las iniciativas del Gobierno de Canadá, la Asociación Minera de Canadá y de líderes de la industria extractiva en promover el respeto a los derechos humanos. Acogemos con beneplácito la oportunidad de compartir nuestra experiencia colectiva de gestión de seguridad tanto con profesionales como con aquellos responsables de la supervisión de la seguridad.

Alcance

La implementación y aplicación de los VPSHR requiere que una organización realice Evaluaciones de Amenazas y Riesgos, desarrolle estándares de departamento para la seguridad

propietaria y de contratos, y considere cuidadosamente su relación con, y en apoyo de, la seguridad pública. Para lograrlo, se requiere un plan de gestión de seguridad bien pensado que cumpla con las mejores prácticas de la industria.

Un Plan de Gestión de Seguridad (SMP) es un documento que describe la filosofía, estrategias, objetivos, programas y procesos de la seguridad de una organización. Proporciona orientación estratégica para el desarrollo y dirección del departamento de seguridad, de una manera coherente con el plan de negocios general de la compañía. También debe esbozar los planes de evaluación de riesgos y mitigación.

El SMP guía las acciones de la empresa en la mitigación y protección contra riesgos de índole de seguridad y derechos humanos que pudieran amenazar a comunidades, empleados, instalaciones, operaciones, producción, la reputación de la empresa y sus operaciones globales.

Una consideración importante del desarrollo de SMP es alinear la misión y las estrategias del programa de seguridad con los de la organización. Esto garantiza que la función de seguridad no se vea solo como un gasto, sino como una parte integral del negocio que contribuye a un entorno de éxito.

El SMP es una herramienta que ayuda al gerente de seguridad a lograr acuerdo y convencer a otras unidades de negocio. Articula cómo se interrelaciona y apoya el departamento de seguridad a todas las áreas de la organización.

Un plan bien redactado proporciona dirección, organización, integración y continuidad al programa de seguridad. Demuestra conocimiento de los riesgos y planificación de reacción reflexiva.

El SMP es un documento estratégico. Mientras que un Plan de Seguridad de Sitio (SSP) es un documento táctico y la extensión lógica de un SMP. El SSP indica los detalles de la seguridad física, las responsabilidades de la fuerza de guardia, las relaciones con la seguridad pública y otros componentes de la prestación de servicios de seguridad. En el Apéndice A de este documento se pueden encontrar orientación adicional sobre el desarrollo del SSP.

Desarrollo del Plan de Gestión de Seguridad

1. Principios de Gestión de Seguridad

Unidad de esfuerzo: los esfuerzos de gestión de seguridad deben ser un esfuerzo colaborativo dentro de la organización y deben incluir aportaciones de todos los socios y partes interesadas, tanto internas como externas.

Transparencia: la información sobre cómo se toman las decisiones de mitigación de riesgo debe compartirse con aquellos que tengan una necesidad válida de conocerla.

Adaptabilidad: las estrategias y los procesos deben diseñarse para permitir cambios constantes.

Practicidad: los gerentes de seguridad no pueden predecir el futuro, ni pueden eliminar todas las amenazas. Deben ser prácticos en lo que elijan para proteger y evaluar el costo/beneficio de las contramedidas.

Personalización: las soluciones deben satisfacer las necesidades y respetar la cultura de la organización.

2. Desarrollo de un esquema

El aporte de gerencia para establecer metas de seguridad es imperativo y debe incluir las expectativas de entrega de servicios y tareas básicas.

El marco de gestión de seguridad debe mejorar la preparación, respuesta, resiliencia y apoyar la continuidad del negocio. El desarrollo de un SMP debe incluir:

- Compromiso de políticas
- Alineación con los objetivos estratégicos de la organización
- Requisitos legales y normas internacionales
- Perfil Organizacional (misión, producción, estrategias)
- Evaluación de riesgos – contexto interno y externo
- Inquietudes de partes interesadas
- Desarrollo de planes y presupuestos
- Personal de seguridad, requisitos de infraestructura e interdependencias
- Opciones de seguridad (análisis de contramedidas)
- Análisis costo/beneficio
- Asignación de responsabilidad y autoridad

3. Gestión de Seguridad

El departamento de seguridad debe enfrentar su misión entendiendo que una buena seguridad y el respeto a los derechos humanos de los trabajadores y de las comunidades son plenamente compatibles. Esto debe ser expresado en una política y plan de gestión integral que incluya:

- Un compromiso de política de gestión que conforme con las mejores prácticas internacionales para la gestión de seguridad y normas voluntarias tales como las VPSHR.
- Un compromiso para prevenir y reducir la probabilidad y consecuencias de violaciones a los derechos humanos.

- Responsabilidad y rendición de cuentas de las mejores prácticas internacionales, tales como los Principios Voluntario sobre Seguridad y Derechos Humanos (VPSHR) delegados al gerente de seguridad.
- Comunicación del plan a todos los empleados, y disponible a todas las partes interesadas.
- Alineación con otras políticas (como ética, código de conducta, derechos humanos)
- Implementación y marco de revisión de objetivos, metas y programas.
- Compromiso de cumplimiento de los requisitos legal and regulatorios de aplicación.
- Mecanismos de respuesta a acusaciones recibidas a través de la Línea de Quejas o de Informantes.

4. Gestión de Riesgos

El análisis de riesgos se utiliza para desarrollar planes de seguridad proactivos y equilibrados que reduzcan la probabilidad y consecuencias de eventos disruptivos. Las evaluaciones de riesgos y amenazas de seguridad son requisitos previos para determinar el despliegue de fuerzas de seguridad armadas o desarmadas en apoyo de la organización.

El objetivo es desarrollar un proceso integral y sistemático para prevenir de manera preventiva el riesgo asociado con operaciones comerciales y de seguridad. También debe tenerse en cuenta el impacto de las actividades de la organización en las comunidades del área de influencia. Un desafío clave es cómo gestionar proactivamente los riesgos identificados, particularmente en áreas de gobernanza débil, donde eventos humanos o causados por la naturaleza han socavado el estado de derecho.

La planificación y pruebas de respuesta a incidentes deben estar alineadas con este proceso e incluir el desarrollo de ejercicios de capacitación, evaluación de las protecciones implementadas, protocolos de respuesta, requisitos de atenuación, capacidades de recuperación y procedimientos operativos actuales.

5. Evaluación de Riesgos

Una evaluación del riesgo es un ejercicio destinado a identificar las amenazas de seguridad, evaluar la naturaleza y el alcance del riesgo que plantean esas amenazas y las posibles vulnerabilidades. La evaluación de riesgos ayuda a la gerencia a seleccionar y priorizar medidas de control eficaces. Los objetivos de la evaluación de riesgos son evitar la actividad no autorizada y la pérdida de activos, equipos, bienes y reputación.

a. Establecimiento del Contexto Externo

La comprensión del contexto externo de la organización es esencial para garantizar que los objetivos e inquietudes de las partes interesadas externas se consideren al realizar una evaluación de riesgos. La evaluación debe abarcar un contexto de toda la organización, considerar los requisitos legales y reglamentarios y los puntos de vista de las partes interesadas.

El potencial de conflicto es inherente a la minería y debe ser reconocido y evaluado como parte del proceso de evaluación de riesgos. El conflicto es a menudo el resultado de las interacciones entre múltiples actores, incluyendo empresas, todos los niveles de gobierno, comunidades, organizaciones no gubernamentales (ONG), insurgentes y delincuentes. Las causas profundas del conflicto son complejas y pueden tener orígenes históricos.

La evaluación del contexto externo debe incluir la evaluación de conflictos causados por organizaciones autoritarias e independientes, tales como el Instituto de Investigación de Conflictos Internacionales de Heidelberg. Las operaciones en entornos difíciles deben considerar si tienen las políticas y los sistemas adecuados para cumplir las obligaciones y responsabilidades corporativas. El objetivo es evitar causar, apoyar o beneficiar a conflictos armados ilegales, contribuir al abuso de derechos humanos y violaciones al derecho internacional humanitario.

El contexto externo debe incluir, sin tener que limitarse a:

- Las acciones de personas ajenas al proyecto que tratan de tomar ventaja de las oportunidades presentadas por el desarrollo y operación de la empresa.
- Actividad delictiva común.
- Interrupción del proyecto de metas económicas, políticas o sociales; acciones deliberadas que tienen un impacto negativo en la operación eficiente y segura de la empresa.
- Los riesgos asociados con la presencia de fuerzas de seguridad privadas y públicas y operaciones.
- Entorno social, cultural, político, legal, regulatorio, financiero, tecnológico, económico, natural y
  competitivo, ya sea internacional, nacional, regional o local.
- Impulsores clave y tendencias que puedan impactar en los objetivos de la organización.
- Relaciones, percepciones y valores de las partes interesadas externas.
- En casos extremos- terrorismo, insurgencia armada, golpes de estado o guerra y los riesgos que una respuesta de seguridad pueda causar.

b. Establecimiento del Contexto Interno

El contexto interno considera el entorno operativo en el cual la organización trata de alcanzar sus objetivos. El proceso de gestión de riesgos debe alinearse con la cultura, los procesos, la estructura y la estrategia de la organización.

El contexto interno es aquello dentro de la organización que influye en la manera en que la organización administra el riesgo, y debe considerar:

- Los objetivos y misión de la organización.
- La posibilidad de conductas ilegal, inmorales o inadecuadas de parte de personal de proyecto o de aquellos directamente asociados al mismo.
- Riesgos comunes tales como hurto por parte de empleados, violencia en el lugar de trabajo, agitación laboral y sabotaje.
- Riesgos a empleados u otros asociados con respuesta de seguridad.

c. Análisis de Brecha de Riesgos

Antes de comenzar el proceso de gestión de riesgos, se debe desarrollar la comprensión de los diversos elementos contextuales interconectados que afectan a la organización. El análisis de brecha de riesgos ayuda a establecer el contexto y debe incluir:

- Identificación de los requisitos legales y normas internacionales de aplicación.
- Evaluación de las prácticas y procedimientos existentes de gestión de riesgos, incluyendo aquellas relacionadas con subcontratistas y la cadena de suministro.
- Evaluación de las emergencias e incidentes previos y las medidas tomadas para prevenir y responder.
- Identificación de riesgos, medidas preventivas, correctivas y recomendaciones para mejorar.

6. Políticas y Procedimientos

Una organización no debe asumir que un contratista de seguridad desarrollará las políticas, objetivos y procedimientos necesarios para proteger su negocio, las personas, activos y reputación. La gerencia debe asumir la responsabilidad de determinar el nivel de seguridad requerido, identificar los activos a proteger y apoyar la implementación de las contramedidas de seguridad. Esta responsabilidad debe ser documentada y revisada periódicamente, junto con el desempeño del contratista.

La gobernanza del SMP debe considerar:

- Responsabilidad de la gerencia ejecutiva.
- Roles y responsabilidades de todos los aspectos del SMP, incluyendo los requisitos, desarrollo, revisión, capacitación, mejora continua y aprobación.
- Responsabilidad y recursos para la gestión del SMP.
- Una política de seguridad que articule dirección, responsabilidad, autoridad y control del SMP.

- Implementación y capacitación para todos los empleados a fin de asegurar el máximo uso eficaz del SMP.

Una Política de Seguridad es un documento de alto nivel, firmado por el CEO u otros altos ejecutivos que delinea la visión de la compañía para proteger a su personal, activos y reputación. El documento demuestra el compromiso de gerencia con la seguridad y es una directiva sobre 'qué' desea lograr la compañía.

La política de seguridad cubre todas las oficinas y operaciones de la compañía e informa a todos los gerentes sobre sus responsabilidades. Es un breve documento que expresa conceptos amplios. Es responsabilidad del gerente de seguridad de desarrollar pautas y procedimientos que expliquen "cómo" se cumplirá la política.

Las pautas y procedimientos definen y explican las acciones requeridas para asegurar cumplir con la póliza. En forma ideal, eliminan todo punto único de fracaso o interpretación subjetiva. Definen el cumplimiento obligatorio y conforman la base de inducción y formación recurrente del personal de seguridad y de los empleados.

a. Registros

Una parte clave de la gestión de seguridad es llevar registros administrativos que incluyan:

- Contratos con proveedores privados de seguridad
- MOU y documentación de apoyo importante de seguridad pública
- Evaluación y análisis de riesgos
- Revisiones internas de cumplimiento
- Responsabilidad de equipo
- Autorizaciones de armas
- Licencias
- Capacitación
- Controles de acceso
- Almacenamiento seguro de información sensible
- Declaraciones de cumplimiento del Código de Conducta y Ética
- Leyes de aplicación internacionales, nacionales y locales
- Todos los compromisos públicos formales o informales asumidos por la organización

b. Responsabilidad, autoridad y tareas laborales

Las responsabilidades, autoridad y descripciones de tareas laborales deben quedar claramente expresadas en el SMP. El SMP debe ser revisado y firmado por el ejecutivo responsable o gerente senior a quien reporta el gerente de seguridad. Estos documentos deben incluir la responsabilidad de documentar e informar toda interacción con la seguridad pública, contratistas, autoridades públicas y representantes de la comunidad.

La organización debe esforzarse por atraer y retener personal de seguridad con habilidades, conocimiento y capacidad de implementar el nivel de seguridad deseado. Como el mayor contribuyente a un rendimiento deficiente es la falta de capacitación, la organización debe comprometerse con el desarrollo profesional del personal de seguridad para mejorar el desempeño laboral, la prestación de servicios, reducir las quejas y aumentar la retención.

7. Supervisión y Control de Seguridad

El SMP debe reseñar la estructura y responsabilidad del departamento, e indicar :

- Líneas de control, responsabilidad y supervisión del departamento de seguridad.
- Supervisión de la fuerza de guardias en primera línea.
- Responsabilidad de la diseminación y comunicación de información de seguridad.

El SMP debe esbozar las actividades de planificación y coordinación entre seguridad y otros departamentos (Relaciones Comunitarias, Recursos Humanos y Relaciones Gubernamentales) y las unidades comerciales, lo cual puede requerir la participación en evaluaciones de riesgos de seguridad en reuniones periódicas.

Es importante garantizar que todas las actividades de seguridad se coordinen y supervisen a través de un único punto de control y mando y que funcionen dentro de directrices y procedimientos coherentes. La seguridad no puede ser eficaz si pretende quedar bien con todos.

Ver el **Apéndice A**, Tendiendo un Puente entre la Gestión de Seguridad y los Planes de Seguridad de Sitios para conectar el plan de gestión estratégica con las mejores prácticas en operaciones de departamento.

Documentos de Referencias Claves

<u>Referencia 1</u>

Principios Voluntarios sobre Seguridad y Derechos Humanos. Protocolo de Auditoría para Evaluar el Cumplimiento de Indicadores Clave de Rendimiento (Junio 2013)

https://www.business-humanrights.org/sites/default/files/media/documents/voluntary-principles-audit-protocol-jun-2013.pdf

Requiere una organización que prepare:

- Declaración de compromiso o respaldo a las VPSHR.
- Políticas, procedimientos y/o directrices relevantes (o todo cambio a las mismas del ejercicio anterior) para la implementación de los Principios Voluntarios.
- Evaluaciones de riesgos de seguridad y derechos humanos.
- Procedimiento y mecanismo para informar incidentes relacionados con seguridad con implicaciones de derechos humanos por fuerzas de seguridad públicas/privadas relacionados con actividades de la compañía.
- Incluir los VPSHR al suscribir relaciones o contratos con proveedores públicos/privados de seguridad.
- Abordar incidentes relacionados con la seguridad con implicaciones de derechos humanos por fuerzas de seguridad públicas/privadas relacionados con actividades de la compañía.
- Aplicar las normas VPSHR en la selección de proveedores privados de seguridad, formular acuerdos contractuales con proveedores privados de seguridad, y todos los arreglos con las fuerzas de seguridad públicas.

Referencia 2

Norma de Desempeño 4 de la Corporación Financiera Internacional (Comunidad, Salud, Seguridad y Seguridad)

https://www.ifc.org/wps/wcm/connect/a40bc60049a78f49b80efaa8c6a8312a/PS4_English_2012.pdf?MOD=AJPERES

Requiere que las compañías:

- Evaluar el riesgo de seguridad que sus operaciones puedan tener o puedan crear a las comunidades.
- Desarrollar formas de gestionar y atenuar dichos riesgos.
- Gestionar responsablemente la seguridad privada.
- Involucrarse con la seguridad pública.
- Considerar e investigar acusaciones de actos ilegales por parte de personal de seguridad.

Asimismo:

- Entender los requisitos de riesgo, seguridad y protección de derechos humanos de la organización.
- Establecer políticas y objetivos para gestionar los riesgos.
- Implementar controles operativos para gestionar los riesgos, las medidas de seguridad y el respeto a los derechos humanos.
- Monitorear y revisar el desempeño y eficacia de los planes de seguridad (administración y operaciones).
- Promover una mejora continua en base a una medición objetiva.

Referencia 3

Manual de Buenas Prácticas de la IFC, Uso de las Fuerzas de Seguridad: Evaluación y Gestión de Riesgos e Impactos, Guía para el Sector Privado en Mercados Emergentes

https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/publications/publications_handbook_securityforces

- **Gestión de Seguridad Privada**

Las decisiones relativas al tipo, número, responsabilidades y armado de las fuerzas de seguridad privadas deben fluir de una evaluación de los riesgos de seguridad y las respuestas apropiadas.

- **Equipamiento**

¿Tienen los guardias lo que necesitan para hacer su trabajo de manera adecuada y segura? Esto generalmente se traduce en uniforme, identificación y un dispositivo de comunicaciones (normalmente una radio). En algunos casos, se incluyen armas no letales, como aerosol irritante. La decisión de armar guardias con fuerza letal, tal como un arma de fuego, es una seria que debe provenir de la evaluación del riesgo y estar acompañada de un programa de entrenamiento específico.

- **Investigación**

¿Quién está brindando seguridad? ¿Hay algo en los antecedentes de los guardias que sea motivo de preocupación? Las empresas deben realizar averiguaciones razonables para asegurarse de que ningún guardia tenga antecedentes de abuso o deshonestidad en el pasado. Esto puede requerir verificaciones de antecedentes o verificación cruzada con otras empresas, funcionarios gubernamentales nacionales o extranjeros, misiones de las Naciones Unidas, etc., según corresponda al contexto del país.

- **Asegurar el uso adecuado de fuerza**

¿Saben los guardias lo que se espera de ellos? ¿Están preparados para reaccionar con fuerza apropiada y proporcional en cualquier situación? Las empresas deben utilizar sus políticas y procedimientos, reforzados por la capacitación para brindar instrucciones claras a los guardias empleados directamente. Esto puede ser tan simple como incluir una cláusula en el contrato de trabajo que establezca las expectativas y el seguimiento de la capacitación.

- **Capacitación**

La formación debe centrarse en el comportamiento y en el uso adecuado de la fuerza. En contextos de bajo riesgo esto puede requerir sólo una breve revisión de las políticas y procedimientos, registrados en un registro, a fin de asegurar que los guardias entiendan cómo responder a las interacciones y situaciones comunes.

- **Monitoreo**

¿Los guardias se desempeñan de manera profesional y apropiada? Las empresas deben verificar y confirmar que las políticas y procedimientos siguen siendo relevantes y que los guardias son conscientes de ellos y los siguen. Las empresas que contratan servicios de seguridad aún conservan la responsabilidad de supervisión de los proveedores de seguridad externos para garantizar una adecuada investigación, uso de la fuerza, capacitación, equipamiento y supervisión de los guardias.

- **Gestionar la Relación con la Seguridad Pública**

Particularmente en contextos de bajo riesgo, las empresas pueden tener interacciones limitadas con las fuerzas de seguridad pública, esto es especialmente cierto en lo que respecta a fuerzas nacionales, tales como las fuerzas armadas. Es probable que las empresas necesiten apoyo de al menos la policía local en caso de incidentes, y es importante entender quién va a responder y cómo. El enfoque se centra en la evaluación y compromiso, basándose en cuestiones clave, tales como: ¿Cuándo es probable que participen las fuerzas de seguridad pública? (Por ejemplo, sólo cuando se les llama, o potencialmente, ¿en otros casos también?) ¿Qué tipo de persona o unidad es probable que responda? ¿Cómo es probable que respondan? (Por ejemplo, ¿qué tipo de capacidad, mandato, reputación, etc., tienen, y cómo podría aplicarse eso a situaciones probables que involucren a la empresa?).

- **Participación**

¿Hay oportunidades para establecer una relación con la policía u otras fuerzas pertinentes de seguridad pública? Se alienta a las empresas a que lleguen a las autoridades, preferiblemente antes de cualquier problema, a entender posibles despliegues y, en la medida de lo posible, a promover el uso adecuado y proporcional de la fuerza. En contextos de bajo riesgo, esto puede implicar simplemente hacer presentaciones al comandante de la policía local e iniciar un diálogo sobre cuándo y cómo responden probablemente las autoridades a incidentes en la empresa o que involucren al personal de la compañía.

- **Documentación**

Las empresas deben documentar sus esfuerzos de compromiso, sean o no exitosos (por ejemplo, en un registro básico de reuniones con fechas, asistentes y temas clave).

- **Amenaza y evaluación de riesgo**

Investigación y análisis del contexto del país: las consideraciones de riesgo potencial en el entorno operativo más amplio pueden incluir el riesgo inherente al país, el estado de derecho, la criminalidad, el entorno físico, el contexto socioeconómico, la gobernanza, la situación de los conflictos, y la información específica de la industria que podría afectar a la situación de seguridad. Además del riesgo específico de cada país, también es aconsejable revisar la solidez y reputación de las fuerzas de seguridad pública existentes.

Investigación y análisis de la situación de seguridad nacional y/o local: el análisis de la situación de seguridad a menudo considera la disponibilidad y la reputación profesional de la seguridad privada, el historial y reputación de derechos humanos de las fuerzas de seguridad pública (tales como la policía o las fuerzas armadas), y cualquier otro elemento significativo en las circunstancias particulares de una empresa.

- **Prevención y Medidas de Mitigación**

El desarrollo y la refinación de medidas de prevención y mitigación a menudo requieren considerar cómo abordar la gama más amplia de impactos potenciales que surgen de las situaciones, incluido un proceso de priorización. La gráfica de respuesta a riesgos y el mapa de temperatura pueden ayudar a una empresa a determinar qué riesgos e impactos abordar como máxima prioridad. El incluir personal de relaciones comunitarias en el diseño de medidas de mitigación puede aumentar la efectividad general.

El capítulo V del presente documento (*Preparación de un Plan de Gestión de Seguridad*) proporciona un esquema amplio para los planes de gestión de seguridad.

Referencia 4

Otros documentos de referencia

- ANSI/ ASIS RA1.2015 Norma de Evaluación de Riesgos:

  https://webstore.ansi.org/Standards/ASIS/ANSIASISRIMSRA2015

- ANSI/ ASIS Sistema de Gestión para la Calidad de las Operaciones de Compañías Privadas de Seguridad: http://www.acq.osd.mil/log/ps/.psc.html/7_Management_System_for_Quality.pdf

- ASIS Guía General de Evaluación de Riesgos:

- https://www.asisonline.org/publications/sg-asis-general-security-risk-assessment-guideline/

- ASIS Selección y Capacitación de Oficiales de Seguridad Privada:

  https://www.asisonline.org/publications/sg-asis-private-security-officer-selection-and-training-guideline-2010-ed/

- Implementación de Auditoría de los VPSHR, Red Global Compact Canadá: http://www.globalcompact.ca/auditing-implementation-of-the-voluntary-principles-on-security-and-human-rights/

- Gestión de Seguridad Contemporánea (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-guidance-tools

- ICRC y Herramientas de Seguridad y Derechos Humanos de DCAF: http://www.securityhumanrightshub.org/content/toolkit

- Informe de la Asociación Internacional de Productores de Petróleo y Gas sobre Armas de Fuego y Uso de la Fuerza: http://www.ogp.org.uk/pubs/320.pdf

- Código de Conducta Internacional para Proveedores de Seguridad Privada:

  www.icoca.ch/

- Herramientas de Implementación de MIGA para Sitios de Grandes Proyectos: https://www.miga.org/documents/vpshr_toolkit_v3.pdf

- Guía de Diligencia Debida de OECD para Cadenas de Suministro de Minerales Responsables provenientes de áreas de conflicto y alto riesgo:

  http://www.oecd.org/corporate/mne/mining.htm

- Análisis de Riesgo y Selección de Contramedidas de Seguridad (Thomas Norman, CRC Press):

  https://www.crcpress.com/Risk-Analysis-and-Security-Countermeasure-Selection-Second-Edition/Norman-CPPPSPCSC/p/book/9781482244199

- Análisis de Riesgo y Encuesta de Seguridad (James Broder, Elsevier):

  https://www.elsevier.com/books/risk-analysis-and-the-security-survey/broder/978-0-12-382233-8

- Principios Básicos de la ONU sobre el Uso de la Fuerza y Armas de Fuego por parte de Oficiales de Seguridad: www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx
- Código de Conducta de la ONU para Oficiales de Seguridad: www.ohchr.org/EN/ProfessionalInterest/Pages/LawEnforcementOfficials.aspx
- Principios Voluntarios sobre Seguridad y Derechos Humanos: http://www.voluntaryprinciples.org/resources/
- Herramienta de Guía de Implementación de Principios Voluntarios:

  http://www.voluntaryprinciples.org/wp-content/uploads/2013/03/VPs_IGT_Final_13-09-11.pdf (Inglés)

  http://www.voluntaryprinciples.org/wp-content/uploads/2013/03/IGT-SPANISH1.pdf (Español)
- Estándar de Oro de Ausencia de Conflicto del Consejo Mundial del Oro https://www.gold.org/who-we-are/our-members/responsible-gold/conflict-free-gold-standard

APÉNDICE A

Vínculo entre Gestión de Seguridad y Planes de Seguridad de Faenas

1. Gestión de Fuerzas de Seguridad Privadas

El papel de la seguridad privada es brindar servicios preventivos y defensivos, protegiendo a los empleados de la compañía, las instalaciones, equipos y operaciones. El personal de seguridad privada no tiene autoridad para hacer cumplir la ley y no debe traspasar los deberes y responsabilidades reservados a las fuerzas de seguridad pública.

a. Seguridad contractual

Un contrato brinda una base legal para la relación entre la organización y el contratista de seguridad. La organización es responsable de todas las actividades externalizadas a otra entidad y requiere un control y supervisión constantes. La responsabilidad de respetar los derechos humanos y cumplir con la ley no puede ser subcontratada a un tercero. La organización es en última instancia responsable de las acciones de un contratista.

El contrato deberá especificar las responsabilidades, términos y condiciones según los cuales el contratista debe proporcionar los servicios de seguridad. El contrato debe definir claramente:

- Un compromiso de cumplir con las mismas obligaciones que tiene la compañía.

- Requisitos de confidencialidad y conflicto de intereses.
- Proceso para la evaluación de riesgos e informe sobre hechos no deseados y perturbadores.
- Descripción de los servicios a ser brindados por el contratista.
- El requisito de capacitación en derechos humanos antes de entrar en servicio.
- Implementación de mecanismos a fin de asegurar que la fuerza física sea usada solamente cuando sea estrictamente necesaria y proporcional a la amenaza.

b. **Selección de un Contratista Privado de Seguridad**

Al seleccionar un proveedor de seguridad, la organización debe realizar la debida diligencia adecuada que incluya la revisión de la reputación institucional, los estándares de capacitación, los procedimientos para la selección de empleados y cualquier historia de denuncias de abusos de derechos humanos u otro comportamiento delictivo.

Contratar únicamente los servicios de contratistas de seguridad competentes comprometidos a operar de manera coherente con las normas de derechos humanos, tales como los VPSHR. La organización es responsable del trabajo y del personal del contratista. No se puede subcontratar la responsabilidad de respetar los derechos humanos.

La organización debe establecer y documentar los criterios de revisión y selección de contratistas de seguridad. Es responsabilidad de la organización garantizar que los contratistas cumplan con las leyes aplicables y todas las demás obligaciones contractuales. Se deben investigar a los posibles proveedores de seguridad por contrato a fin de garantizar:

- Una historia demostrada de realización de actividades de seguridad en cumplimiento de las leyes pertinentes.
- Su capacidad de proteger el personal, bienes y reputación del cliente.
- Se provean adecuados recursos y personal calificado para alcanzar los objetivos operativos.
- Transparencia, responsabilidad y supervisión adecuada de su personal.
- Se cumpla todo beneficio financiero, estatutario y remunerativo de su personal.
- Los registros, licencias y permisos requeridos estén al día.
- Se lleven registros precisos de personal y equipo.

c. Control active del desempeño del contratista

A fin de garantizar un desempeño adecuado, la organización debe realizar auditorías periódicas, ayudar con capacitación, investigar toda acusación creíble de abuso o delito y monitorear el desempeño de forma continua.

d. Selección, Revisión de Antecedentes e Investigación de Personal de Seguridad

El personal de seguridad ocupa puestos de confianza. La empresa debe establecer procedimientos documentados para verificación de antecedentes e investigación previos al empleo. Se deben establecer normas mínimas y procedimientos para descartar solicitantes que no cumplan con las calificaciones en base a sus conocimientos, habilidades, capacidades y experiencia. Este proceso de selección debe formar parte de todas las contrataciones para garantizar que ninguna persona implicada de manera creíble en abuso de derechos humanos sea contratada.

Además, se deben realizar verificaciones de antecedentes de los posibles proveedores de seguridad para detectar denuncias de abusos en el pasado, uso inadecuado de la fuerza u otra actividad delictiva y actos ilícitos.

El proceso de selección y de investigación debe basarse en la naturaleza del trabajo para el cual se está considerando al candidato, el nivel de autoridad de la persona y el área de especialización. La selección se debe llevar a cabo antes de ofrecerle un puesto a un candidato y que empiece a trabajar. Los candidatos deben firmar las autorizaciones y consentimientos apropiados antes de realizar la investigación de antecedentes.

El personal de seguridad que tenga acceso a información y operaciones sensibles debe someterse a verificaciones de antecedentes más estrictas.

La privacidad y confidencialidad de toda la información personal debe estar protegida.

e. Verificación de Antecedentes de Guardias de Seguridad

La verificación de la identidad e historia personal debe incluir:

- Verificación de domicilio
- Registros de empleo
- Medios electrónicos
- Historia de registros penales y civiles
- Violaciones de los derechos humanos
- Registros de vehículos automotores
- Informes de crédito

- Base de datos de agresores sexuales
- Sanciones de gobierno y de la industria
- Registros de licencias de la industria

f. Verificación de experiencia y calificaciones

La verificación de experiencia y calificación debe considerar, sin que se limite, lo siguiente:

- Educación
- Historia laboral
- Licencias / Certificación / Registros
- Referencias personales
- Entrevistas con el supervisor y compañeros de trabajo
- Servicio militar/policial

Las exclusiones, falta de disponibilidad, de confiabilidad o información no adecuada debe ser documentada.

g. Revisión e Investigación

Establecer criterios claramente definidos para evaluar:

- Abuso de sustancias.
- Aptitud física y mental.
- Aptitud para llevar armas.
- Resiliencia a condiciones estresantes y adversas.
- Asociación delictiva y susceptibilidad a la corrupción.

h. Competencia, Capacitación y Aptitud

EL mayor contribuyente al desempeño mediocre es la falta de capacitación.

El Departamento de Seguridad debe identificar los conocimientos y habilidades que requieren el personal propio y contratado para realizar las tareas asignadas. El Departamento debe establecer su propia norma de formación de inducción mínima, ya que las normas nacionales o regionales pueden no cumplir con las competencias requeridas. La formación de inducción debe completarse siempre antes de entrar al servicio. Los contratistas deben demostrar que sus empleados han recibido y completado satisfactoriamente la capacitación. La supervisión y la formación periódica deben llevarse a cabo de manera continua para identificar oportunidades de mejora y demostrar debida diligencia.

El SMP debe comprometer a la organización a mantener los más altos estándares de competencia técnica y profesional de la fuerza de seguridad a través de un programa de capacitación integral. Los SSP deben delinear las responsabilidades de capacitación tanto del proveedor de seguridad como de la compañía y del calendario anual.

La capacitación debe incluir respeto a los derechos humanos, mecanismos de quejas, conducta ética, uso de la fuerza y competencia con armas ofensivas y defensivas autorizadas. Se recomienda una formación práctica y basada en situaciones que refuerce la toma de decisiones en condiciones que reflejen el entorno operativo. La capacitación debe incluir procedimientos para la prevención y mitigación, respuesta, documentación de incidentes, comunicaciones y rendición de cuentas.

La compañía debe revisar los programas de capacitación de contratistas y, cuando sea necesario, aumentar la capacitación mediante el uso de terceros calificados o instrucción directa. Como mínimo, el personal de seguridad debe recibir formación de inducción y capacitación recurrente en:

- Habilidades básicas de protección
- Post-órdenes y procedimientos de protección
- Código de Conducta, Ética y Derechos Humanos
- Uso de la Fuerza
- Salud, Seguridad y Ambiente
- Uso de armas defensivas y ofensivas (según corresponda)

Todos los entrenamientos de armas deben llevarse a cabo según una norma escrita adecuada para las armas autorizadas. La capacitación debe incluir capacitación en base a situaciones, entrenamiento mecánico y de operación que incluya fallas de funcionamiento y calificación con munición real. La capacitación debe llevarse a cabo no menos que una vez al año y con mayor frecuencia, si lo requiere la ley.

2. Uso de la fuerza

El uso de la fuerza por parte de seguridad privada se autorizará sólo con fines preventivos y defensivos en proporción a la naturaleza y magnitud de la amenaza.

Cuando sea necesario armar la fuerza de protección, la organización garantizará altos niveles de competencia técnica y profesional y una clara comprensión de las reglas para el uso de la fuerza. Esto requiere una formación periódica sobre las directrices del Uso de la Fuerza, proporcionalmente, y respeto a los derechos humanos.

La autorización para portar armas sólo debe ser dada a personal calificado de acuerdo con los términos y condiciones de un contrato. Las armas deben autorizarse sólo después de haber establecido los antecedentes y calificaciones del personal, y se haya completado satisfactoriamente la capacitación en el arma específica autorizada. Esto sólo debe autorizarse cuando exista una expectativa razonable de amenaza a la vida en base a la evaluación de riesgos. La capacitación, despliegue y necesidad de portar armas debe cumplir con la legislación del país de acogida. La evaluación de la necesidad de desplegar armas tiene en cuenta las posibles consecuencias del uso accidental o indiscriminado de las armas.

El uso de la fuerza siempre debe ser razonablemente necesario, proporcional y legal. Las normas para el uso de la fuerza deben revisarse para garantizar que cumplan con el estándar jurídico nacional o regional apropiado. Las opciones de fuerza no letal, menos letal y letal deben considerarse en el contexto local y según los requisitos legales.

Las reglas del uso de la fuerza deben estar delineadas en todos los contratos con proveedores de seguridad privada. Las disposiciones contractuales deben incluir:

- Parámetros para el uso de fuerza física.
- Las circunstancias en las cuales se autoriza al personal a portar armas, y las armas y munición permitidas.
- Un compromiso para garantizar que las armas se usen solamente en circunstancias apropiadas y de manera tal que disminuya el riesgo de daño innecesario.
- Prohibición del uso de armas y munición no autorizadas.
- Regulaciones para el control, almacenamiento y responsabilidad de armas autorizadas.
- Directrices de respuesta gradual sobre el uso de la fuerza.
- Énfasis en el uso de técnicas de disminución de escalada.
- Mecanismo de informe para todos los incidentes de uso de fuerza.

a. Capacitación en el Uso de la Fuerza

Las normas sobre el uso de la fuerza deben incorporarse en los programas de inducción y de formación recurrente. Se deben llevar registros de formación y de la capacidad demostrada. El entrenamiento en uso de la fuerza debe acentuar:

- El uso de fuerza letal únicamente en circunstancias de autodefensa o en defensa de otros contra amenaza inminente de muerte o lesiones serias, nunca debe ser usada en defensa de bienes;
- La fuerza debe ser razonablemente necesaria y ser usada como último recurso;

- La fuerza debe ser proporcional a la amenaza y desplegada solamente en base a la totalidad de las circunstancias para contrarrestar una amenaza;
- El uso de la fuerza se usa solamente para alcanzar objetivos legales.

La capacitación constante en el uso de la fuerza debe señalar, sin restringirse a:

- Presencia de seguridad;
- Ordenes verbales;
- Controles manos abiertas;
- Armas no-letales;
- La amenaza de fuerza letal;
- Uso de la fuerza letal.

La capacitación en el uso de la fuerza debe reforzar la premisa de que la seguridad privada no es un sustituto de la seguridad pública y refuerza las limitaciones de su autoridad.

Los programas de capacitación deben enfatizar que la fuerza letal está justificada sólo en condiciones de extrema necesidad, y como último recurso cuando todos los medios menores han fallado o no pueden ser empleados razonablemente. La fuerza letal sólo se utilizará en defensa propia en defensa de otros, o cuando parezca razonablemente necesario para impedir la comisión de un delito grave que implique una grave amenaza a la vida o un daño corporal grave.

La defensa de otros puede incluir el uso de la fuerza letal cuando sea razonablemente necesario para prevenir el robo o sabotaje de bienes inherentemente peligrosos, cuya pérdida o destrucción podría constituir una amenaza inminente de muerte o daño corporal grave. La autoridad jurídica también podrá autorizar el uso de la fuerza letal si resulta razonablemente necesario para impedir el sabotaje o la destrucción de infraestructuras críticas, cuyos daños causarían una amenaza inminente de muerte o daños corporales graves o lesiones.

b. Gestión de Armas y Municiones

El Departamento Seguridad es responsable de establecer, mantener y documentar procedimientos que garanticen:

- Que todas las armas y municiones se adquieran legalmente;
- Constante rendición de cuentas de todas las armas y municiones entregadas y devueltas;
- Las armas y municiones entregadas sean proporcionales a los riesgos identificados y las tareas a ser ejecutadas y cumplir con todas las normas legales;

- Se establezcan disposiciones apropiadas para el almacenamiento, entrega y mantenimiento;
- Los contratistas desplieguen armas y munición solamente aprobadas por la organización;

Todas las personas autorizadas a portar armas tengan una licencia válida y capacitación al día.

c. Aprehensión y Detención de Delincuentes

Como parte de la capacitación sobre el uso de la fuerza, el personal de seguridad debe estar capacitado en cómo tratar con personas detenidas o recluidas en el transcurso de sus funciones. Deben entender los límites de su autoridad y que esto normalmente sólo incluirá a la persona interceptada durante un ataque contra el personal y bienes bajo su protección legal. La formación debe enfatizar el requisito de tratar al personal detenido humanamente y respetar sus derechos humanos y constitucionales.

La capacitación incluirá medidas para proteger a las personas aprehendidas contra la violencia, e informar y transferirlas inmediatamente a las autoridades competentes. Se deben preparar informes de incidentes que incluyan la identidad de la persona, el presunto delito, a quien fueron transferidos, primeros auxilios o asistencia proporcionada y su situación en el momento de la transferencia.

Las personas detenidas pueden ser chequeadas por el personal de seguridad para garantizar su seguridad con relación a armas y salvaguardar pruebas. Los procedimientos de chequeo deben garantizar la dignidad y el trato humano del detenido y se diferenciarán entre búsquedas mínimamente invasivas y exhaustivas.

Todas las personas detenidas deben recibir primeros auxilios inmediatos si son necesarios.

3. Uniformes

Todos los miembros del equipo de seguridad deben adoptar el uso de uniformes que indiquen su afiliación al Departamento. Los uniformes y equipos de seguridad privada, tales como vehículos de patrulla, deben tener patrones, colores y marcas que los diferencien de los de seguridad pública. El personal de seguridad y los vehículos deben tener números de distintivo únicos que faciliten la identificación y permitan la presentación de informes transparentes.

Los uniformes proyectan una imagen positiva sobre la organización y fomentan una conducta profesional y responsable. Puede haber circunstancias en las que una evaluación de riesgos indique que sea aconsejable utilizar seguridad no uniformada. Cuando se requiera un enfoque discreto, el personal de seguridad no debe portar abiertamente armas de fuego ni mantener sobre sí identificación intransferible.

La presencia de seguridad uniformada es la primera opción en todo uso continuo de fuerza. Los uniformes y los vehículos con marcas indican a los empleados, al público y a la seguridad

pública que los integrantes del equipo tienen autorización y responsabilidad de proteger al personal y los bienes de la empresa.

4. Comunicaciones

La comunicación eficaz es el componente más importante en la prevención, administración y notificación de hechos de seguridad. Los planes de comunicaciones garantizan un control, coordinación y funcionalidad adecuados para las operaciones de seguridad.

El SMP debe reseñar procedimientos y procesos de comunicaciones que tomen en cuenta:

- Comunicaciones internas de los departamentos, contratistas, clientes y partes interesadas;
- Recibir, documentar y responder a comunicaciones de fuentes externas;
- Comunicaciones estructuradas con la seguridad pública y agencias de emergencia;
- Comunicaciones separadas y seguras durante hechos perturbadores y emergencias.

La organización debe establecer y comunicar sus procedimientos de quejas internas y externas. El personal de seguridad debe estar capacitado para recibir y reportar quejas y asegurar la confidencialidad. Las quejas de la comunidad no denunciadas y no resueltas pueden convertirse rápidamente en eventos disruptivos.

5. Salud y Seguridad Ocupacional

El SMP debe comprometerse en proporcionar al personal de seguridad un ambiente de trabajo seguro y saludable, reconociendo los peligros inherentes que presentan el medio ambiente y las tareas. Debe recalcar las precauciones razonables que deben tomarse para proteger a todas las personas que trabajan en nombre de la organización, en particular las que están en puestos de alto riesgo, como la seguridad.

6. Gestión de Respuesta a Incidentes

Se debe implementar una estructura administrativa adecuada para hacer frente eficazmente a la gestión y respuesta de incidentes. El SMP debe indicar la estructura de administración del departamento, la autoridad para las decisiones, la responsabilidad de la implementación y la presentación de informes. La organización debe tener un Equipo de Gestión de Incidentes (EGI) para liderar la respuesta a incidentes bajo la dirección clara de gerencia o sus representantes. El SMP debe delinear el papel de la seguridad dentro del EGI e incluir:

- Planificación
- Gestión de respuesta a incidentes
- Gestión de recursos humanos

- Salud, seguridad y respuesta médica
- Gestión de la información
- Comunicaciones internas y externas
- Funciones de apoyo crítico

7. Respuesta a incidentes

El Departamento de Seguridad es responsable de desarrollar protocolos de respuesta y gestión de incidentes como parte del proceso de evaluación de riesgos de la empresa. La respuesta y la gestión de incidentes deben considerar:

- Salvaguardar la vida, los bienes y la reputación de la organización.
- Respetar los derechos humanos y la dignidad humana.
- Identificar e informar hechos potencialmente disruptivos, planes de mitigación y recuperación.
- Procesos de notificación y de movilización para gerencia, partes interesadas y autoridades.

La organización debe desarrollar procedimientos para informar e investigar incidentes que incluyan:

- Hora y lugar.
- Identidad de las personas involucradas, incluyendo información de contacto.
- Lesiones y daños sufridos.
- Circunstancias que llevaron a desencadenar el incidente.
- Medidas de respuesta desplegadas.
- Causa de todas las lesiones y daños internos y externos.
- Análisis de las causas profundas.
- Acciones correctivas y preventivas.

El SMP y el SSP deben delinear responsabilidades y plazos para realizar consultas sobre denuncias e incidentes, incluyendo:

- El compromiso a realizar una investigación expeditiva de todas las acusaciones de abusos o delitos.

- Contratistas privados de seguridad que realicen investigaciones de incidentes o acusaciones, y el derecho de la organización a realizar una averiguación independiente.
- Los resultados de las averiguaciones incluirán una recomendación sobre la acción disciplinaria adecuada y los cambios a las políticas o procedimientos.

8. Evaluación de Desempeño y Mejora Continua

La evaluación de desempeño implica la medición, monitoreo y evaluación de la prestación de servicios del departamento y del contratista, aseguramiento de la calidad, cumplimiento legal y respeto a los derechos humanos. La métrica incluye el cumplimiento de políticas, objetivos y metas de rendimiento.

Se deben desarrollar indicadores de rendimiento para medir tanto el sistema de gestión como el cumplimiento operativo. Los indicadores deben proporcionar información útil que identifique los éxitos y las áreas que requieran mejoras. También deben identificar cómo se gestionan los riesgos significativos.

La evaluación debe considerar:

- Convalidación de los planes de gestión y las estrategias de seguridad física.
- Competencia del personal de seguridad.
- Capacidades de respuesta.
- Cumplimiento contractual.
- Capacitación y preparación.

El SMP y el SSP deben indicar que la acción correctiva será identificada y comunicada de manera oportuna y debe abordar la falla raíz. Se debe asignar la responsabilidad de la acción correctiva y la fecha de finalización. Las conclusiones que excedan las expectativas deben ser observadas como mejores prácticas y compartidas en toda la organización.

La mejora continua debe considerar cambios en los riesgos, actividades y operaciones que afecten la prestación de servicios. Los procedimientos, sistemas y formación deben adaptarse para abordar:

- Cambios de políticas.
- Cambios en peligros, riesgos y amenazas.
- Cambios en el personal y en contratistas.
- Cambios de procesos y tecnología.
- Lecciones aprendidas de ejercicios y entrenamiento.

- Lecciones aprendidas de hechos disruptivos.
- Cambios en el entorno externo (político, social, legal).

9. Gestionando las Relaciones con la Seguridad Pública

Las fuerzas públicas de seguridad tienen la responsabilidad exclusiva de responder e investigar actividades delictivas, en particular incidentes de interés público. También tienen la responsabilidad primordial del orden público, incluidas las protestas, manifestaciones y desobediencia civil. Para incidentes que involucren violaciones criminales, confrontaciones potencialmente violentas o manifestaciones, se les puede solicitar que respondan para proteger al personal y bienes de la compañía. Es importante que la seguridad pública sea informada sobre las políticas y compromisos de la organización antes que se desplieguen a un incidente.

La empresa debe mantener relaciones constructivas y buenas comunicaciones con las fuerzas de seguridad pública. Si se asignan fuerzas de seguridad públicas al proyecto, es importante que se establezca un memorando de entendimiento para garantizar la transparencia. El MOU debe describir las disposiciones relativas a las transferencias de equipos, apoyo material y el papel de la fuerza de seguridad pública en la protección de bienes de la empresa. Se deben desarrollar mecanismos de planificación de contingencia y coordinación conjunta.