Seguridad

¿Por qué es importante esta Estándar del Grupo?	Este estándar establece los requisitos mínimos para la conducta ética de nuestros empleados, contratistas y consultores y refuerza nuestro compromiso de cero tolerancia frente a todas las formas de soborno y corrupción.
Destinatarios	Cualquier persona responsable de gestionar, implementar y monitorear la seguridad de las personas, activos e instalaciones de AGA.
Leyenda	*Los términos del Glosario* están en cursiva. ***Autorizaciones*** se definen en *Delegación de Autoridad del Grupo*. Hipervínculo a otro documento o a un sitio de intranet o sitio web *Referencia* a otro documento AGA sin un hipervínculo.

Usted debe cumplir con las normas para todo el Grupo de AGA en la medida en que se apliquen

Gestión de riesgos de seguridad

Anticipamos, identificamos, interpretamos y monitoreamos los riesgos de seguridad en todas nuestras ubicaciones, implementamos controles para mitigar los riesgos y nos comunicamos para informar la toma de decisiones.

- Identifique, evalúe, mitigue e informe posibles riesgos de seguridad utilizando la metodología de riesgo tipo *bowtie* para informar si los riesgos se terminan, tratan, transfieren o toleran.
- Monitoree continuamente los riesgos de seguridad y actualice la evaluación de riesgos y amenazas a la seguridad anualmente, o cuando ocurra un cambio material en el riesgo.
- Comunicar los cambios materiales (por ejemplo, una mayor amenaza a las personas, los activos o las instalaciones) en los riesgos de seguridad inmediatamente a las personas pertinentes:
  - Director General o Gerente General (para una Operación)
  - Director de Proyecto (para un proyecto/exploración importante) o Country Manager
  - Jefe de la Unidad de Negocio de Seguridad y
  - Jefe de Grupo de Seguridad y Derechos Humanos.

Evaluación de amenazas y riesgos

- Utilice el proceso de evaluación de amenazas para identificar y evaluar las fuentes de posibles riesgos de seguridad. Cuantificar las fuentes de riesgo de seguridad y examinar sus características, capacidad e intenciones hacia los intereses de la empresa (personas, activos y reputación).
- Utilice iSIMS para evaluar las amenazas a la seguridad del sitio y revisarlas anualmente o si hay un cambio material en el riesgo.
- Completar un proceso de identificación de riesgos para identificar la naturaleza y las fuentes de riesgo que podrían afectar a las personas, los activos y la reputación, y debe considerar eventos naturales, intencionales y no intencionales, como eventos malévolos, criminales, sociales/políticos, etc. Actualizar anualmente o en caso de un cambio material en el riesgo.
- Registre los 15 principales riesgos de seguridad, medidas de control y efectividad del control en iSIMS utilizando la metodología de riesgo *bowtie* y revíselos anualmente o si hay un cambio material en el riesgo.
- Envíe, una vez por semana, cualquier evento y/o delito importante a nivel internacional, regional, nacional o local que podría potencialmente afectar (negativo o positivo) la operación desde una perspectiva de seguridad a través del Centro de informes de seguridad en línea.
- Revise y actualice los cuadros de mando de riesgos de seguridad (Security Risk Scorecards) trimestralmente para verificar la exactitud de las calificaciones de riesgo (probabilidad e impacto) para los 15 principales riesgos de seguridad.
- Las evaluaciones del Barómetro de Riesgo de Conflicto (CRB) deben gestionarse mediante la herramienta CRB en línea, completarse y revisarse mensualmente o cuando haya un cambio material en el riesgo.

- Complete una evaluación del Plan de seguridad de 5 puntos anualmente o si hay un cambio importante en el riesgo.
- Proporcionar información a Seguridad del Grupo (*Group Security*) cuando lo solicite para respaldar los requisitos de cumplimiento externos relacionados con el riesgo de seguridad, como el Estándar de Oro Libre de Conflictos, los Principios de Minería de Oro Responsable del Consejo Mundial del Oro y las Expectativas de Desempeño del Consejo Internacional de Minería y Metales.

Mitigación de riesgos de seguridad

- Requisitos de seguridad de recursos para mitigar eficazmente el riesgo (eliminar a las personas del riesgo y el riesgo de las personas) y maximizar la eficiencia mediante la optimización y la integración de personas y sistemas técnicos.
- Implementar medidas de mitigación utilizando los principios de gestión de proyectos de AGA.
- Complete verificaciones de vulnerabilidad frecuentes (diarias/semanales/mensuales), según el tipo de medidas de control, utilizando iSIMS para probar y verificar si las medidas de control de seguridad requeridas están implementadas y funcionando a un nivel óptimo, para mitigar el riesgo.

Gestión de incidentes

- Análisis completo de toda la información de seguridad que influye en el riesgo (por ejemplo, incidentes delictivos) para determinar tendencias y permitir la identificación de la respuesta de seguridad requerida y las medidas de mitigación que se implementarán.
- Registre todos los incidentes relacionados con delitos y los incidentes no relacionados con delitos identificados en iSIMS.
- Utilice el tipo de incidente y los criterios de clasificación de gravedad en iSIMS para la notificación de incidentes o eventos.
- Complete una revisión/investigación (utilizando la metodología del Programa de investigación de incidentes (IIP)) de todos los incidentes importantes clasificados como Alto, Mayor o Extremo según los Criterios de clasificación de incidentes de seguridad para:
  - determinar las causas básicas, incluidas, entre otras, la disciplina de seguridad
  - identificar e implementar medidas mitigantes y/o acciones correctivas para evitar que ocurra un incidente similar o para minimizar el impacto que dicho incidente podría afectar
  - obtener el respaldo del informe y las acciones propuestas por parte de Seguridad del Grupo (*Group Security*) antes de su finalización.
- Complete una autoevaluación anual de todos los procedimientos del grupo de seguridad.

Principios Voluntarios sobre Seguridad y Derechos Humanos (VPSHR)

Nuestro compromiso con los VPSHR y el respeto de los derechos humanos es el motor clave de nuestras prácticas de gestión de la seguridad y rige la forma en que identificamos

el potencial de conflicto, las normas de intervención, el uso de la fuerza y la transparencia en los acuerdos con las fuerzas de seguridad.

- Evaluar el riesgo de conflicto y gestionar la interacción con la seguridad privada y la seguridad pública de acuerdo con el *Procedimiento sobre los Principios Voluntarios (VPSHR) de Group Security*.
- Complete y documente evaluaciones de riesgos y amenazas para la protección de personas y activos, detallando el potencial de conflicto, los riesgos asociados y el nivel de seguridad requerido para mitigar el riesgo.
- Obtenga la ***aprobación*** (Apéndice 1 ***ID#1***) para el uso de armas letales y/o menos letales por parte de cualquier proveedor de servicios de seguridad, incluidos los departamentos de seguridad de AGA y los servicios de seguridad públicos o privados, y proporcione la amenaza completa y evaluación de riesgos que demuestre un requisito para el uso de armas y que la jurisdicción operativa permita la posesión de armas de fuego y armamento menos letal.
- Establecer e implementar procedimientos operativos estándar para garantizar que el personal de seguridad cumpla con las leyes y regulaciones aplicables de la jurisdicción operativa y los VPSHR.
- Verificar la formación y cualificación del personal de seguridad asignado a funciones de protección y/o realizando actividades de seguridad de alto riesgo.
- Proporcionar capacitación previa al despliegue y de actualización anual, utilizando un proveedor de capacitación acreditado, a todas las unidades de seguridad. Asegúrese de que la capacitación cubra:
  - uso del armamento aplicable
  - uso mínimo de la fuerza
  - normas de enfrentamiento
  - su obligación de actuar de acuerdo con los VPSHR.
- Establezca memorandos de entendimiento / convenios (MOU) transparentes con las fuerzas de seguridad, obtenga el respaldo de Seguridad del Grupo (Group Security) y Cumplimiento del Grupo (Group Compliance) y gestione las relaciones a través de acuerdos de nivel de servicio.
- Documentar y conservar una copia de todos los acuerdos con las fuerzas de seguridad y mantener un registro de auditoría de las transferencias de equipos (propiedad; autorización; uso; seguimiento y monitoreo de equipos; informes de excepciones) de acuerdo con los convenios (MOUs) acordados.
- Exigir a los agentes de seguridad que notifiquen de inmediato, a través de su cadena de mando, la aplicación de cualquier uso de fuerza, cualquier lesión asociada o posible responsabilidad.
- Complete una investigación de incidente de acuerdo con el *Estándar del Grupo de Investigaciones*, tan pronto como sea posible, para investigar:
  - incumplimiento de los procedimientos de seguridad establecidos
  - lesiones y/o muertes debido a intervención de seguridad y/o actividad ilegal.
  - posibles violaciones de derechos humanos debido a intervenciones de seguridad y/o actividades ilegales.

- Registre todas las posibles violaciones de derechos humanos en el Registro de Principios Voluntarios (VPSHR) en iSIMS tan pronto como sea posible.

Medidas de seguridad

Implementamos medidas de seguridad para garantizar que nuestra gente esté siempre protegida y se sienta segura, protejamos nuestros activos e instalaciones y minimice las posibles pérdidas resultantes de violaciones de seguridad.

- Desarrollar, implementar y revisar anualmente o ante un cambio material en el riesgo un Plan de Gestión de Seguridad para cada sitio, que incluya:
  - planes para responder a posibles violaciones de seguridad
  - planes de contingencia para abordar problemas regionales y locales que afectan la seguridad de nuestra gente y nuestros activos.
  - contingencias de seguridad, proporcionales al entorno de riesgo específico, para la evacuación, aislamiento, cierre o cierre patronal del sitio.
- Gestionar la seguridad perimetral, el control de acceso, la detección y vigilancia de intrusos, el movimiento y salida de personas y vehículos, el seguimiento y control de los activos que salen de la propiedad de la empresa de forma temporal o permanente, y la protección de activos y productos de acuerdo con los procedimientos del grupo sobre *Seguridad Metalúrgica* y *Seguridad Minera*.
- Implementar y monitorear continuamente los protocolos de seguridad en el *Procedimiento Técnico de Group Security* con respecto al uso de tecnología para proteger a personas y bienes, incluyendo vigilancia por video y audio, sensores, salas de control y software, equipos de monitoreo y otras tecnologías de seguridad disponibles comercialmente. Asignar recursos de seguridad (incluidos humanos, técnicos, vehículos, equipos de seguridad) en función de las amenazas y riesgos identificados en la evaluación de riesgos de seguridad, y de acuerdo con el *Procedimiento de Group Security sobre la integridad de la disciplina*. Utilice la tecnología, cuando sea posible, para alejar a las personas del riesgo y alejar el riesgo de las personas.
- Establecer e implementar procedimientos operativos estándar para monitorear, rastrear y gestionar la seguridad de nuestra gente.
- Proporcionar sesiones informativas de concientización sobre seguridad y gestionar la seguridad de oficinas, residencias y viajes de acuerdo con los protocolos de seguridad documentados en el *Procedimiento del grupo de deber de diligencia de seguridad* (DoC).

Apéndice 1: Autoridades

Título de la autoridad		Endosar	Aprobar	Informar
ID#1 Uso de armas letales y/o menos letales por parte de cualquier proveedor de servicios de seguridad				
	Vicepresidente, Group Security y Derechos Humanos		✓	

Notas: *Las autoridades no deben estar dentro de la misma línea jerárquica. Es decir, un rol no respalda las decisiones de su línea gerencial.*

E ***Endoso:*** *Revisa las propuestas y brinda asesoramiento antes de que el aprobador tome la decisión. Este rol es responsable del asesoramiento brindado (a diferencia de una "revisión" o un "punto de control" en un proceso). El respaldo no es un derecho de veto. Si un patrocinador no está de acuerdo con una decisión de aprobación, debe escalar según sea necesario.*

A ***Aprobar:*** *Responsable de la decisión, considerando los aportes del endosante. La mayoría debe tener un solo aprobador (responsabilidad de un solo punto).*

I ***Informo:*** *Obligado a actuar en base a la decisión tomada. Debe excluir los informes de "proceso/cortesía".*