Segurança

Por que este Padrão do Grupo é importante?	Esta norma define os requisitos mínimos para identificar e gerenciar riscos de segurança, proteger as pessoas, ativos e instalações da AGA e garantir que nossas pessoas se sintam seguras e protegidas ao realizar tarefas em nome da empresa.
Audiência	Qualquer pessoa responsável por gerenciar, implementar e monitorar a segurança das pessoas, ativos e instalações da AGA.
Legenda	Os *Termos do Glossário* estão em itálico As ***Aprovações*** são definidas no *Delegação de Autoridade do Grupo* Hyperlink para um outro documento, ou para um site da intranet ou website *Referência* a outro documento da AGA sem hyperlink.

Você deve cumprir ao Padrõesdo Grupo AGA na medida em que eles entram em vigor

Gerenciamento de Riscos de Segurança

Antecipamos, identificamos, interpretamos e monitoramos os riscos de segurança em todos os nossos locais, implementamos controles para mitigar os riscos e nos comunicamos para informar a tomada de decisões.

- Identificar, avaliar, mitigar e relatar potenciais riscos de segurança usando uma metodologia de risco bowtie para informar se os riscos são Terminados, Tratados, Transferidos ou Tolerados.
- Monitorar continuamente os riscos de segurança e atualizar a ameaça à segurança e a avaliação de risco anualmente, ou quando ocorrer uma mudança substancial no risco.
- Comunicar mudanças substanciais (por exemplo, aumento da ameaça a pessoas, ativos e/ou instalações) em riscos de segurança imediatamente ao relevante entre:
  - Diretor Administrativo ou Gerente-Geral (para uma Operação)
  - Diretor de Projeto (para um grande projeto / exploração) ou Gerente Nacional
  - Chefe da Unidade de Negócios de Segurança e
  - Chefe do Grupo de Segurança e Direitos Humanos.

Avaliação de ameaças e riscos

- Usar o processo de avaliação de ameaças para identificar e avaliar as fontes de risco potencial de segurança. Quantificar as fontes de risco de segurança e examinar suas características, capacidade e intenções em relação aos interesses da empresa (pessoas, ativos e reputação).
- Usar o iSIMS para avaliar as ameaças à segurança do local e revisar anualmente, ou se houver uma mudança material no risco.
- Realizar um processo de identificação de riscos usado para identificar a natureza e as fontes de risco que podem impactar pessoas, ativos e reputação, devendo considerar eventos naturais, intencionais e não intencionais, como eventos malévolos, criminais, sociais/políticos, etc. Atualizar anualmente ou no caso de uma mudança substancial no risco.
- Registrar os 15 principais riscos de segurança, medidas de controle e eficácia de controle no iSIMS usando a metodologia de risco bowtie e revisar anualmente ou se houver uma mudança substancial no risco.
- Enviar, uma vez por semana, os eventos e/ou crimes internacionais, regionais, nacionais ou locais significativos que poderiam potencialmente impactar (negativos ou positivos) a operação de uma perspectiva de segurança são enviados através do Centro de Relatórios de Segurança (SRC) online uma vez por semana?
- Revisar e atualizar os Scorecards de Risco de Segurança (Security Risk Scorecards) trimestralmente para verificar a precisão das classificações de risco (probabilidade e impacto) para os 15 principais riscos de segurança.
- As avaliações do Barômetro de Risco de Conflito (CRB) devem ser gerenciadas usando a Ferramenta CRB online e atualizadas mensalmente ou quando há uma mudança substancial no risco.
- Realizar uma avaliação do Plano de 5 Pontos de Segurança anualmente ou se houver uma mudança substancial no risco.

- Fornecer informações à Segurança do Grupo (Group Security) a pedido para sustentar os requisitos de conformidade externa com relação ao risco de segurança, como o Padrão de Ouro Livre de Conflitos, os Princípios Responsáveis de Mineração de Ouro Responsável do Conselho Mundial de Ouro e as Expectativas de Desempenho do Conselho Internacional de Mineração e Metais.

Mitigação de Riscos de Segurança

- Providenciar recursos da Segurança para mitigar efetivamente o risco (remover as pessoas do risco e o risco das pessoas) e maximizar eficiências por meio da otimização e integração de pessoas e sistemas técnicos.
- Implementar medidas mitigadoras usando os princípios de gerenciamento de projetos da AGA.
- Realizar verificações de vulnerabilidade frequentes (diariamente/semanalmente/mensalmente), dependendo do tipo de medidas de controle, usando o iSIMS para testar e verificar se as medidas de controle de segurança necessárias estão em vigor e funcionam em um nível ideal para mitigar o risco.

Gerenciamento de incidentes

- Análise completa de todas as informações de segurança que influenciam o risco (por exemplo, incidentes criminais) para determinar tendências e permitir a identificação da resposta de segurança necessária e medidas de mitigação a serem implementadas.
- Registrar todos os incidentes relacionados a crimes e incidentes não criminais identificados no iSIMS.
- Usar os critérios de classificação de tipo e gravidade de incidentes no iSIMS para notificação de incidentes ou eventos.
- Realizar uma análise/investigação (utilizando a metodologia do Programa de Investigação de Incidentes (IIP)) em todos os Incidentes significativos classificados como “Alto”, “Maior” ou “Extremo” nos Critérios de Classificação de Incidentes de Segurança para:
  - determinar a(s) causa(s) básica(s), incluindo, sem limitação, a disciplina de Segurança
  - identificar e implementar medidas mitigadoras e/ou ações corretivas para evitar que um incidente semelhante aconteça ou para minimizar o impacto que tal incidente possa afetar
  - obter o endosso do relatório e das ações propostas da Segurança do Grupo (Group Security) antes da finalização.
- Realizar uma autoavaliação anual em relação a todos os procedimentos de Segurança do grupo.

Princípios Voluntários de Segurança e Direitos Humanos (VPSHR)

Nosso compromisso com os Princípios Voluntários de Segurança e Direitos Humanos (VPSHR) e o respeito aos direitos humanos são os principais impulsionadores de nossas práticas de gestão de segurança e regem a forma como identificamos o potencial de

conflito, regras de engajamento, uso da força e transparência nos acordos com as forças de segurança.

- Avaliar o risco de conflito e gerenciar a interação com a segurança privada e a segurança pública de acordo com o *Procedimento de Princípios Voluntários (VPSHR) da Segurança do Grupo*.
- Completar e documentar avaliações de ameaças e riscos para a proteção de pessoas e ativos, detalhando o potencial de conflito, riscos associados e nível de segurança necessário para mitigar o risco.
- Obter ***aprovação*** (Anexo 1 ***ID#1***) para o uso de armas letais e/ou menos letais por qualquer prestador de serviços de segurança, incluindo departamentos de segurança da AGA, serviços de segurança privada ou pública, e fornecer a avaliação completa de ameaças e riscos que demonstre um requisito para o uso de armas e que a jurisdição operacional permita a posse de armas de fogo e armas menos letais.
- Estabelecer e implementar procedimentos operacionais padrão para garantir que o pessoal de segurança cumpra as leis e regulamentos aplicáveis da jurisdição operacional e dos VPSHR.
- Verificar o treinamento e as qualificações do pessoal de segurança designado para funções de proteção e/ou realização de atividades de segurança de alto risco.
- Fornecer treinamento de pré-implantação e atualização anual, usando um provedor de treinamento credenciado, para todas as unidades de segurança. Certificar-se de que o treinamento abrange:
  - uso de armamento aplicável
  - uso mínimo de força
  - regras de engajamento
  - sua obrigação de agir de acordo com os VPSHR.
- Estabelecer memorandos de entendimento (MOUs) transparentes com as forças de segurança, obtendo o endosso da Segurança do Grupo (Group Security) e da Conformidade do Grupo (Group Compliance) e gerenciando relacionamentos por meio de acordos de nível de serviço.
- Documentar e reter uma cópia de todos os acordos com as forças de segurança e manter uma trilha de auditoria das transferências de equipamentos (propriedade; autorização; uso; rastreamento e monitoramento de equipamentos; relatórios de exceção) de acordo com os MOUs acordados.
- Exigir que os agentes de segurança notifiquem imediatamente, por meio de sua cadeia de comando, a aplicação de qualquer uso da força, quaisquer lesões associadas ou responsabilidade potencial.
- Realizar uma investigação de incidente de acordo com a *Norma de Investigações do Grupo*, assim que possível, para investigar:
  - não conformidade com os procedimentos de segurança estabelecidos
  - lesões e/ou fatalidades resultantes de intervenção de segurança e/ou atividade ilegal
  - potenciais violações de direitos humanos devido a intervenções de segurança e/ou atividades ilegais.
- Registrar todas as possíveis violações de direitos humanos no Registro de VPSHR no iSIMS assim que possível.

Medidas de Segurança

Implementamos medidas de segurança para garantir que nosso pessoal esteja sempre protegido e se sinta seguro, protegemos nossos ativos e instalações e minimizamos possíveis perdas resultantes de violações de segurança.

- Desenvolver, implementar e revisar anualmente ou uma mudança material no risco de um Plano de Gerenciamento de Segurança para cada local, incluindo:
  - planos para responder a possíveis violações de segurança
  - planos de contingência para abordar questões regionais e locais que afetam a segurança de nossos funcionários e ativos
  - contingências de segurança, proporcionais ao ambiente de risco específico, para evacuação do local, isolamento, lock-down ou lock-out.
- Gerenciar a segurança do perímetro, controle de acesso, detecção e vigilância de intrusão, movimentação e saída de pessoas e veículos, monitoramento e controle de ativos que saem da propriedade da empresa de forma temporária ou permanente, e a proteção de ativos e produtos de acordo com os *Procedimentos de Segurança de Metalurgia* e *Segurança de Mineração do Grupo*.
- Implementar e monitorar continuamente os protocolos de segurança no *Procedimento de Segurança Técnica do Grupo* em relação ao uso de tecnologia para proteger pessoas e ativos, incluindo vigilância por vídeo e áudio, sensores, salas de controle e software, equipamentos de monitoramento e outras tecnologias de segurança disponíveis comercialmente. Alocar recursos de segurança (incluindo humanos, técnicos, veículos, equipamentos de segurança) com base nas ameaças e riscos identificados na avaliação de risco de segurança e de acordo com o *Procedimento de Integridade da Disciplina de Segurança do Grupo*. Usar a tecnologia, sempre que possível, para remover as pessoas do risco e o risco das pessoas.
- Estabelecer e implementar procedimentos operacionais padrão para monitorar, rastrear e gerenciar a segurança de nosso pessoal.
- Fornecer instruções de conscientização de segurança e gerenciar a segurança de escritórios, residências e viagens de acordo com os protocolos de segurança documentados no *Procedimento de Dever de cuidado da Segurança do Grupo* (DoC).

Apêndice 1: Autoridades

Título da Autoridade		Endossar	Aprovar	Informar
ID#1 Uso de armas letais e/ou menos letais por qualquer prestador de serviços de segurança				
	Vice-Presidente, Segurança do Grupo e Direitos Humanos		✓	

Observações: *As autoridades não devem estar dentro da mesma linha de subordinação. Ou seja, uma função não endossa as decisões de sua gerência de linha.*

E ***Endossar:*** *Analisa as propostas e fornece conselhos antes que o aprovador tome a decisão. Esta função é responsável pelo conselho dado (em oposição a uma "revisão" ou "ponto de verificação" em um processo). O endosso não é um direito de veto. Se um endossante discordar de uma decisão de aprovação, ele deve escalar conforme necessário.*

A ***Aprovar:*** *Responsável pela decisão, considerando a contribuição do endossante. A maioria deve ter apenas um aprovador (responsabilidade de ponto único).*

I ***Informar:*** *Necessário para agir com base na decisão tomada. Deve excluir informações de 'processo / cortesia'.*