Grupo ENERGO-PRO

POLÍTICA DE SEGURANÇA

2026

ENERGO-PRO

POLÍTICA DE SEGURANÇA (“POLÍTICA”)

1. Introdução

O principal negócio da ENERGO-PRO a.s. ("ENERGO-PRO") e suas subsidiárias (coletivamente "o Grupo") é a geração de energia renovável. As atividades adicionais do Grupo incluem distribuição, fornecimento e comercialização de eletricidade.

A ENERGO-PRO está comprometida em proteger a segurança da força de trabalho, da nossa cadeia de valor, dos visitantes e das comunidades impactadas por nossas operações. A ENERGO-PRO respeita os princípios da Declaração Universal dos Direitos Humanos das Nações Unidas, os Princípios Orientadores da ONU sobre Empresas e Direitos Humanos, os Princípios Voluntários sobre Segurança e Direitos Humanos (VPSHR) e a Declaração da Organização Internacional do Trabalho sobre Princípios e Direitos Fundamentais no Trabalho.

Esta Política estabelece o padrão a nível do Grupo para a gestão de segurança em todas as operações e projetos da ENERGO-PRO e define os requisitos para identificar, prevenir e gerenciar riscos de segurança de forma consistente com as leis aplicáveis, as Boas Práticas Internacionais da Indústria (GIIP), nosso Código de Conduta do Grupo, a Política de Direitos Humanos do Grupo e outras políticas aplicáveis da ENERGO-PRO.

2. Objetivos

Os objetivos desta política são:

- Proporcionar um ambiente de trabalho seguro para todos os colaboradores, cadeia de valor (contratados, subcontratados e outros) e visitantes.
- Manter e proteger a segurança e integridade das operações, instalações e ativos.
- Estabelecer e manter um relacionamento baseado em confiança, respeito mútuo e integridade com comunidades, autoridades locais e outras partes interessadas.
- Fornecer direção e construir responsabilidade da liderança, da gestão e dos colaboradores.
- Respeitar e demonstrar Boas Práticas Internacionais da Indústria em relação a direitos humanos e segurança.

3. Governança

O Conselho de Administração do Grupo e das Subsidiárias da ENERGO-PRO é responsável por garantir a implementação desta política. A alta direção é responsável por assegurar que a Política seja integrada nos processos e operações relevantes do negócio.

4. Escopo

A Política aplica-se a todos os empregados e à nossa Cadeia de Valor.

Também se aplica à ENERGO-PRO, e suas subsidiárias que operam na Bulgária e na Geórgia e à subsidiária Murat Nehri Elektrik Üretim A.Ş., que opera na Turquia.

Também se aplica a todas as demais subsidiárias da ENERGO-PRO que podem solicitar ao Conselho de Administração do Grupo a aprovação de uma dispensa de disposições específicas desta Política. O Conselho poderá aprovar tal solicitação quando estiver satisfeito de que a dispensa se baseia em fundamentos objetivos e comercialmente razoáveis e, além disso, é consistente com a legislação local, o Código de Conduta do Grupo e compromissos financeiros vinculativos.

Esperamos que aqueles que trabalham conosco ou para nós mantenham padrões equivalentes e podemos buscar avaliar o alinhamento com esses princípios como parte de nossos processos de negócios.

5. Requisitos e Gestão de Segurança

A ENERGO-PRO reconhece a necessidade de cultivar uma cultura de conscientização e disciplina em segurança, especialmente ao trabalhar em ambientes remotos ou complexos. Os requisitos específicos desta política têm como objetivo estabelecer um padrão mínimo em nível de Grupo e devem ser aplicados, conforme relevante, ao contexto legal, operacional e de segurança de cada país, escritório, projeto ou operação.

1. Gestão de Segurança

O Conselho de Administração das unidades de negócios é responsável por garantir que todos os escritórios e operações/projetos estejam seguros e que pessoal devidamente qualificado tenha sido designado para gerenciar a segurança. Todos os locais de construção/operação devem possuir medidas e controles de segurança, incluindo, conforme apropriado, avaliações de risco de segurança de construção/operação e relatórios e gestão de incidentes de segurança. Dependendo do nível de ameaça, ativos localizados em ambientes que representem risco de segurança também deverão ter Planos de Gestão de Segurança. O Conselho de Administração da unidade de negócios é responsável por avaliar a materialidade da segurança, analisando as ameaças e riscos relevantes e determinando, de acordo, o nível necessário de medidas de segurança.

As seguintes considerações serão incluídas na gestão de segurança:

I. Classificação de Ativos para unidades de negócios de alto risco de segurança**:** Antes de qualquer avaliação de risco, todos os ativos do projeto devem ser identificados e categorizados em quatro categorias principais:

Humanos (pessoal e contratados), Físicos (infraestrutura e equipamentos), Informações (propriedade intelectual e dados) e Reputacionais (integridade da marca). Cada categoria deverá receber um nível de criticidade para priorizar medidas de proteção e alocação de recursos.

II. Avaliações de Risco de Segurança: Todas as unidades de negócios devem avaliar os riscos de segurança, sendo a robustez da avaliação dependente da materialidade da segurança da unidade. As avaliações serão conduzidas para identificar os riscos de segurança existentes e previsíveis associados ao projeto/operação e incluirão controles e medidas de mitigação para gerenciar os riscos. Recursos financeiros e humanos suficientes devem ser alocados para implementar os controles estabelecidos, bem como para garantir sua manutenção e monitoramento.

---

1 Orientações sobre gestão de segurança estão disponíveis no "Good Practice Handbook: Use of Security Forces: Assessing and Managing Risks and Impacts", publicado no site da IFC em 2017.

A avaliação deve considerar requisitos internacionais, legais e da própria empresa. As avaliações de risco serão revisadas de acordo com o nível de ameaça ou após um evento significativo de segurança ou mudança nas operações. A frequência das avaliações de risco será orientada por: (i) fatores históricos; (ii) fatores políticos; (iii) questões socioeconômicas; (iv) questões étnicas; (v) considerações religiosas; (vi) presença ou percepção de presença de grupos terroristas ou extremistas; (vii) atividade criminosa oportunista; (viii) requisitos legais e de conformidade; (ix) localização; e (x) conflitos comunitários significativos.

Riscos de segurança em nível nacional, de caráter ad hoc e de alto impacto, poderão ser avaliados periodicamente pelo Conselho de Administração do Grupo em colaboração

As avaliações de risco considerarão as seguintes ameaças:
Ameaças de segurança física:

- ✓ Ataque armado (terrorista ou criminoso)
- ✓ Sequestro, pedido de resgate e extorsão
- ✓ Roubo e vandalismo
- ✓ Agitação civil nacional ou local
- ✓ Instabilidade ou colapso do governo do país anfitrião
- ✓ Ameaças operacionais e ambientais
- ✓ Ameaças relacionadas ao transporte
- ✓ Exposições relacionadas à acomodação
- ✓ Eventos geográficos e climáticos
- ✓ Isolamento e acesso limitado a suporte de emergência
- ✓ Tensões socioeconômicas
- ✓ Conflitos étnicos ou religiosos
- ✓ Conflitos comunitários ou excesso de reclamações
- ✓ Presença ou percepção de presença de grupos terroristas ou extremistas

- ✓ Ameaças sociopolíticas e relacionadas à comunidade

Ameaças não físicas:

- ✓ Intimidação ou coerção
- ✓ Ameaça por colaboradores, incluindo membros de sindicatos
- ✓ Coerção econômica, incluindo chantagem
- ✓ Danos à reputação ou à marca
- ✓ Ameaças de informação e tecnologia
- ✓ Interrupção de TI e paralisação operacional
- ✓ Riscos de cibersegurança que afetam operações, infraestrutura e dados pessoais
- ✓ Mal-entendidos culturais e sensibilidades locais

III. Planos de Gestão de Segurança: As unidades de negócios localizadas em ambientes de alto risco de segurança devem possuir planos de gestão de segurança. Esses planos serão adaptados aos requisitos específicos do projeto/operação e deverão ser adequados ao propósito. Os planos explicarão como cada projeto/operação fornecerá segurança e mitigará os riscos associados. Devem levar em consideração as complexidades do local, incluindo aspectos culturais, geográficos e políticos. O Plano de Gestão de Segurança mencionará explicitamente que o uso da força deve ser proporcional, legal e estritamente limitado a situações em que seja necessário proteger a vida ou evitar danos graves.

Os papéis e responsabilidades devem ser definidos para lidar com os níveis de risco identificados, garantindo que estejam alinhados ao grau e à complexidade dos riscos e aplicáveis à operação.

O plano de gestão de segurança incluirá uma seção sobre gestão e reporte de incidentes. Essa seção estabelecerá uma abordagem consistente para identificar, relatar, avaliar, gerenciar e responder a incidentes de segurança. Também definirá os papéis e responsabilidades relacionados à gestão e ao reporte de incidentes.

IV. Plano de Continuidade de Negócios (BCP): As unidades de negócios de alto risco devem preparar um BCP adaptado ao ambiente específico de ameaças da unidade. Esses planos devem estabelecer protocolos claros para resposta imediata a ameaças materializadas (por exemplo, ataques armados, sequestros ou falhas de TI) e definir as etapas de recuperação para garantir a resiliência das operações com o mínimo de tempo de inatividade.

V. Planejamento de Emergência e Evacuação: As emergências de segurança serão incluídas no Plano de Preparação e Resposta a Emergências de cada ativo individual. Além disso, as unidades de negócios de alto risco manterão um Plano de Resposta a Incidentes de Segurança (SIRP) e procedimentos de evacuação, incluindo rotas de evacuação, projetados para assegurar uma resposta coordenada e eficaz a incidentes de segurança.

VI. Revisão e Melhoria Contínua: Os planos e controles de segurança devem ser monitorados regularmente e atualizados após qualquer incidente significativo. Um processo de revisão pós-evento identificará lacunas para garantir que as medidas de mitigação permaneçam adaptativas, proativas e adequadas ao propósito.

2. Due Diligence de Contratados de Segurança

Antes da contratação, a ENERGO-PRO realiza *due diligence* para avaliar o histórico de direitos humanos, qualificações e conformidade legal dos contratados de segurança. Estes devem fornecer treinamento de conscientização em direitos humanos a seus funcionários. Na ausência desse treinamento, a ENERGO-PRO o fornecerá.

3. Comunidades e Autoridades Locais

Ao desenvolver e implementar planos de segurança nas localidades, deve haver consciência sobre os impactos nas comunidades. A equipe de segurança deve trabalhar em estreita colaboração com as equipes sociais relevantes para minimizar os impactos negativos da segurança nas comunidades locais e apoiar uma comunicação e engajamento adequados, conforme necessário.

A ENERGO-PRO reconhece a importância de estabelecer boas relações de trabalho com comunidades e autoridades locais. Todos os locais que possuam equipes de segurança deverão estabelecer processos apropriados para a gestão de questões de segurança relacionadas às comunidades, de acordo com o contexto específico de cada site.

4. Direitos Humanos

A ENERGO-PRO possui uma Política de Direitos Humanos que estabelece expectativas claras. Todos os colaboradores, contratados e pessoal de segurança devem receber treinamento de conscientização em direitos humanos.

5. Responsabilidade

- A alta liderança, incluindo os gerentes de site, é responsável em última instância pela segurança.
- A alta liderança deve demonstrar comprometimento, garantindo que recursos financeiros e humanos adequados estejam disponíveis para implementar e manter um ambiente seguro.
- Todos os incidentes de segurança e reclamações comunitárias relacionadas à segurança devem ser comunicados imediatamente à alta liderança, incluindo relatórios de investigação e medidas de controle relevantes

6. Comunicação

Esta política é comunicada pelo menos uma vez por ano a todos os empregados e à cadeia de valor por meio de programas de integração, treinamentos, site corporativo, e-mails, SMS, cartazes, contratos e outros canais.

Cada unidade de negócios deve demonstrar como integra e cumpre esta política, incluindo *due diligence* de contratados de segurança, treinamentos e comunicação de expectativas em toda a cadeia de valor.

7. Distribuição

Este documento está disponível no site da empresa, incorporado em termos e condições padrão de negócios e pode ser revisado regularmente com base no feedback das partes interessadas e em resposta a mudanças regulatórias.

8. Vigência

Esta versão da Política entra em vigor e é efetiva a partir de **maio de 2026**.