Grupo ENERGO-PRO

POLÍTICA DE SEGURIDAD

2026

ENERGO-PRO

POLÍTICA DE SEGURIDAD (LA «POLÍTICA»)

1. Introducción

La actividad principal de ENERGO-PRO a.s. («ENERGO-PRO») y de sus filiales (conjuntamente, el «Grupo») es la generación de energía renovable. Las actividades adicionales del Grupo incluyen la distribución, el suministro y la comercialización de electricidad.

ENERGO-PRO se compromete a proteger la seguridad de la plantilla, de nuestra cadena de valor, de las personas visitantes y de las comunidades afectadas por nuestras operaciones. ENERGO-PRO respeta los principios recogidos en la Declaración Universal de Derechos Humanos de las Naciones Unidas, los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos, los Principios Voluntarios sobre Seguridad y Derechos Humanos (VPSHR) y la Declaración de la Organización Internacional del Trabajo relativa a los principios y derechos fundamentales en el trabajo.

La presente Política establece el estándar a nivel de Grupo para la gestión de la seguridad en todas las operaciones y proyectos de ENERGO-PRO, y define los requisitos para la identificación, prevención y gestión de los riesgos de seguridad de conformidad con la legislación aplicable, las Buenas Prácticas Internacionales del Sector (Good International Industry Practice, GIIP), nuestro Código de Conducta del Grupo, la Política de Derechos Humanos del Grupo y demás políticas aplicables de ENERGO-PRO. Los procedimientos, planes y controles a nivel de país podrán establecer requisitos más detallados en función de las condiciones legales, operativas y de seguridad locales, siempre que permanezcan alineados con la presente Política del Grupo. Los requisitos establecidos en esta Política se basan en los riesgos relevantes en materia de derechos humanos de ENERGO-PRO relacionados con la seguridad, incluidos el trato a trabajadores y trabajadoras y a las comunidades, la conducta del personal de seguridad y la gestión de conflictos y del uso de la fuerza.

2. Objetivos

Los objetivos de esta Política son:

- Proporcionar un entorno de trabajo seguro para todos los trabajadores y trabajadoras, la cadena de valor (contratistas, subcontratistas y otros) y las personas visitantes.
- Mantener y proteger la seguridad e integridad de las operaciones, instalaciones y activos.
- Establecer y mantener una relación basada en la confianza, el respeto mutuo y la integridad con las comunidades, las autoridades locales y otros grupos de interés.
- Proporcionar orientación y reforzar la rendición de cuentas de la dirección, la gestión y los trabajadores y trabajadoras.
- Respetar y demostrar las Buenas Prácticas Internacionales del Sector en materia de derechos humanos y seguridad.

3. Gobernanza

El Consejo de Administración del Grupo ENERGO-PRO y de sus filiales es responsable de garantizar la implementación de esta Política. La alta dirección es responsable de asegurar que la Política se integre en los procesos y operaciones empresariales pertinentes.

4. Ámbito de aplicación

La Política se aplica a todos los trabajadores y trabajadoras y a nuestra cadena de valor.

Esta Política es de aplicación a ENERGO-PRO, a sus filiales que operan en Bulgaria y Georgia, y a la filial Murat Nehri Elektrik Üretim A.Ş., que opera en Turquía.

Asimismo, se aplica a todas las demás filiales de ENERGO-PRO, que, no obstante, podrán solicitar al Consejo de Administración del Grupo la aprobación de una exclusión respecto de determinadas disposiciones de esta Política. El Consejo de Administración del Grupo podrá aprobar dicha solicitud cuando considere que la exclusión se basa en motivos objetivos y comercialmente razonables y, además, es conforme con la legislación local, el Código de Conducta del Grupo y los compromisos de financiación vinculantes. Las exclusiones aprobadas se documentarán y se comunicarán al Departamento ESG del Grupo.

Esperamos que todas las personas que trabajen con nosotros y para nosotros respeten unos estándares equivalentes, pudiendo incluso solicitarles que demuestren su adhesión a estos principios como parte de nuestros procesos empresariales.

5. Requisitos

ENERGO-PRO reconoce la necesidad de fomentar una cultura de concienciación y disciplina en materia de seguridad, especialmente cuando se trabaja en entornos remotos o complejos. Los requisitos específicos de esta Política tienen por objeto establecer un estándar mínimo a nivel de Grupo y se aplicarán, según proceda, al contexto jurídico, operativo y de seguridad de cada país, oficina, proyecto u operación.

1. Gestión de la seguridad

El Consejo de Administración de la(s) unidad(es) de negocio es responsable de garantizar que todas las oficinas y operaciones/proyectos sean seguros y de que se haya asignado personal debidamente cualificado para gestionar la seguridad. Todos los emplazamientos de construcción/operación deberán contar con medidas y controles de seguridad, incluidos, según corresponda, evaluaciones de riesgos de seguridad en construcción/operaciones, así como sistemas de notificación y gestión de incidentes de seguridad. En función del nivel de amenaza, los activos ubicados en entornos que presenten riesgos de seguridad deberán contar asimismo con Planes de Gestión de la Seguridad.[1] El Consejo de Administración de la unidad de negocio es responsable de evaluar la materialidad de los riesgos de seguridad mediante la valoración de las amenazas y riesgos pertinentes, y de determinar en consecuencia el nivel requerido de medidas de seguridad.

Las siguientes consideraciones se incluirán en la gestión de la seguridad:

I. Clasificación de activos para unidades de negocio con alto riesgo de seguridad: Antes de cualquier evaluación de riesgos, todos los activos del proyecto deberán ser identificados y clasificados en cuatro categorías principales: humanos (personal y contratistas); físicos (infraestructuras y equipos); informativos

[1] La guía en materia de gestión de la seguridad está disponible en *«Good Practice Handbook: Use of Security Forces: Assessing and Managing Risks and Impacts».* 2017, página web de la IFC.

(propiedad intelectual y datos); reputacionales (integridad de la marca). A cada categoría se le asignará un nivel de criticidad con el fin de priorizar las medidas de protección y la asignación de recursos.

II. Evaluaciones de riesgos de seguridad: Todas las unidades de negocio deberán evaluar los riesgos de seguridad; el grado de exhaustividad de la evaluación dependerá de la materialidad del riesgo de seguridad de la unidad de negocio. Las evaluaciones se realizarán para identificar los riesgos de seguridad existentes y previsibles asociados al proyecto/operaciones, e incluirán controles y medidas de mitigación para gestionar dichos riesgos. Deberán asignarse recursos financieros y humanos suficientes para implementar los controles establecidos, así como para garantizar su mantenimiento y seguimiento.

La evaluación tendrá en cuenta los requisitos internacionales, legales y de la propia Compañía. Las evaluaciones de riesgos se revisarán en función del nivel de amenaza o tras un incidente de seguridad significativo o un cambio en las operaciones. La frecuencia de las evaluaciones de riesgos se determinará en función
(i) antecedentes históricos; (ii) factores políticos; (iii) factores socioeconómicos; (iv) cuestiones étnicas; (v) consideraciones religiosas; (vi) presencia o percepción de presencia de grupos terroristas o extremistas; (vii) actividad delictiva oportunista; (viii) cumplimiento normativo y legal; (ix) localización; y (x) conflictos comunitarios significativos.

Los riesgos de seguridad a nivel de país, de carácter general o puntual, podrán ser evaluados ocasionalmente por el Consejo de Administración del Grupo en colaboración con la(s) unidad(es) de negocio.

Las evaluaciones de riesgos tendrán en cuenta las siguientes amenazas:
Amenazas a la seguridad física:

- Ataques armados (terroristas o delictivos)
- Secuestro, rescate y extorsión
- Robo y vandalismo
- Disturbios civiles a nivel nacional o local
- Inestabilidad o colapso del Gobierno del país anfitrión
- Amenazas operativas y ambientales
- Riesgos relacionados con el transporte
- Riesgos asociados al alojamiento
- Eventos geográficos y climáticos
- Aislamiento y acceso limitado a servicios de emergencia
- Tensiones socioeconómicas
- Conflictos étnicos o religiosos
- Conflictos comunitarios o reclamaciones excesivas
- Presencia o percepción de presencia de grupos terroristas o extremistas
- Amenazas sociopolíticas y relacionadas con la comunidad

Amenazas no físicas:

- Intimidación o coacción
- Amenazas por parte de trabajadores y trabajadoras, incluidos miembros sindicales
- Coacción económica, incluido el chantaje

- Daños reputacionales o a la marca
- Amenazas informáticas y tecnológicas
- Interrupciones de sistemas informáticos y paradas operativas
- Riesgos de ciberseguridad que afecten a operaciones, infraestructuras y datos personales
- Malentendidos culturales y sensibilidades locales

III. Planes de gestión de la seguridad: Las unidades de negocio ubicadas en entornos de alto riesgo de seguridad deberán contar con planes de gestión de la seguridad. Estos planes se adaptarán a las necesidades específicas de cada proyecto/operación y describirán cómo cada proyecto/operación proporcionará seguridad y mitigará los riesgos asociados. Asimismo, tendrán en cuenta la complejidad del emplazamiento, incluyendo factores culturales, geográficos y políticos. El Plan de Gestión de la Seguridad deberá establecer expresamente que el uso de la fuerza será proporcional, conforme a la ley y estrictamente limitado a situaciones en las que sea necesario para proteger la vida o evitar daños graves.

Deberán definirse funciones y responsabilidades en función de los niveles de riesgo identificados, asegurando su adecuación al nivel y complejidad de los riesgos y su aplicabilidad a la operación.

El plan incluirá una sección relativa a la gestión y notificación de incidentes, en la que se establecerá un enfoque coherente para la identificación, notificación, evaluación, gestión y respuesta ante incidentes de seguridad. Asimismo, se definirán las funciones y responsabilidades en materia de gestión y notificación de incidentes.

IV. Plan de continuidad de negocio (BCP): Las unidades de negocio de alto riesgo elaborarán un Plan de Continuidad de Negocio adaptado al entorno de amenazas específico de la unidad. Dichos planes establecerán protocolos claros para la respuesta inmediata ante amenazas materializadas (por ejemplo, ataques armados, secuestros o incidentes informáticos) y definirán las medidas de recuperación necesarias para garantizar la resiliencia de las operaciones con el menor tiempo de inactividad posible.

V. Planificación de emergencias y evacuación Las emergencias de seguridad se incluirán en el Plan de Preparación y Respuesta ante Emergencias de cada activo. Además, las unidades de negocio de alto riesgo mantendrán un Plan de Respuesta a Incidentes de Seguridad (SIRP) y procedimientos de evacuación, incluidas rutas de evacuación, diseñados para garantizar una respuesta coordinada y eficaz ante incidentes de seguridad.

VI. Revisión y mejora continuas Los planes y controles de seguridad deberán ser objeto de seguimiento periódico y actualizarse tras cualquier incidente significativo. Un proceso de revisión posterior al incidente permitirá identificar deficiencias, garantizando que las medidas de mitigación sigan siendo adaptativas, proactivas y adecuadas a su finalidad.

2. Diligencia debida respecto de contratistas de seguridad

Con carácter previo a la contratación de servicios de seguridad, ENERGO-PRO, a través de sus oficinas en cada país, llevará a cabo un proceso de diligencia debida sobre el potencial contratista de seguridad con el fin de evaluar su historial en materia de derechos humanos, sus cualificaciones pertinentes y su cumplimiento de los requisitos legales aplicables. Si lo solicita a la sede central, se le facilitará un modelo de cuestionario de la Evaluación del Cumplimiento de los Derechos Humanos (HRCA) para llevar a cabo la diligencia debida. Los contratistas de seguridad deberán proporcionar formación en materia de derechos humanos a todo su personal, incluyendo formación sobre la conducta adecuada hacia trabajadores y trabajadoras, comunidades y otros grupos de interés, en la medida en que sea pertinente para sus funciones. En caso de que no se imparta dicha formación, las oficinas nacionales de ENERGO-PRO se encargarán de proporcionarla.

3. Comunidades y autoridades locales

En el desarrollo e implementación de los planes de seguridad de los emplazamientos deberá tenerse en cuenta el impacto sobre las comunidades. El personal de seguridad deberá colaborar estrechamente con los equipos sociales correspondientes para minimizar los impactos negativos de la seguridad en las comunidades locales y apoyar una comunicación y participación adecuadas, según corresponda.

ENERGO-PRO reconoce la importancia de establecer buenas relaciones de trabajo con las comunidades y las autoridades locales. Todos los emplazamientos con personal de seguridad establecerán procesos adecuados para la gestión de cuestiones de seguridad relacionadas con la comunidad, en función del contexto específico del emplazamiento.

4. Derechos Humanos

ENERGO-PRO ha desarrollado una Política de Derechos Humanos que establece los principios relativos a nuestras expectativas en materia de derechos humanos. La Política de Derechos Humanos incluye riesgos en materia de derechos humanos relacionados con la seguridad y los conflictos.

ENERGO-PRO garantizará que trabajadores y trabajadoras, contratistas y personal de seguridad reciban la formación adecuada en materia de derechos humanos.

5. Responsabilidad

- La alta dirección, incluidos los responsables de los emplazamientos, es en última instancia responsable de la seguridad.
- La alta dirección deberá demostrar su compromiso garantizando la disponibilidad de recursos financieros y humanos adecuados para implantar y mantener un entorno seguro.
- Todos los incidentes de seguridad y las reclamaciones de las comunidades relacionadas con la seguridad deberán comunicarse de inmediato a la alta dirección, incluidos los informes de investigación y las medidas de control pertinentes.

6. Comunicación

Esta Política se comunica al menos una vez al año a todos los trabajadores y trabajadoras y a la cadena de valor a través de múltiples canales, incluidos programas de incorporación, sesiones

de formación, nuestro sitio web corporativo, comunicaciones por correo electrónico y SMS, cartelería en oficinas, contratos con proveedores y otros métodos de comunicación.

Asimismo, cada unidad de negocio deberá demostrar cómo integra y cumple esta Política, incluyendo la diligencia debida respecto de los contratistas de seguridad, la formación y la comunicación de estas expectativas a lo largo de toda nuestra cadena de valor.

7. Difusión

El presente documento está disponible en el sitio web de la Compañía, se incorpora a determinadas condiciones generales de contratación y podrá revisarse periódicamente en función de las aportaciones de nuestros grupos de interés y en respuesta a cambios regulatorios.

8. Entrada en vigor

La presente versión de la Política entra en vigor y resulta aplicable a partir de mayo de 2026.