

# Política de Segurança Corporativa

Atualizada em 29 de maio de 2024.

O Conselho de Administração da NEOENERGIA S.A. (a “**Sociedade**”) tem atribuída a competência de desenhar, avaliar e revisar, em caráter permanente, o Sistema de Governança e Sustentabilidade e, especificamente, aprovar e atualizar as políticas corporativas que contenham as diretrizes que regem a atuação da Sociedade e das sociedades integradas no grupo, cuja entidade dominante, no sentido estabelecido pela lei, é a Sociedade (o “**Grupo**”).

No exercício de suas responsabilidades e com o objetivo de estabelecer os princípios gerais que devem reger suas atuações em matéria de segurança corporativa, o Conselho de Administração aprova, em cumprimento do *Propósito e Valores do Grupo Neoenergia*, esta *Política de Segurança Corporativa* (a “**Política**”).

## 1. Finalidade

A finalidade desta *Política* é estabelecer os princípios básicos de atuação que devem reger em matéria de segurança, dentro do perímetro das sociedades do Grupo em matéria de segurança, para garantir a efetiva proteção das pessoas, dos ativos físicos (incluindo infraestrutura crítica), da informação, do conhecimento e dos sistemas de controle e comunicações, assim como a confidencialidade dos dados tratados, a todo momento, pelas atuações em matéria de segurança, para que estejam plenamente de acordo com a lei e cumpram, escrupulosamente, o previsto na Política de Respeito aos Direitos Humanos da Sociedade.

Por meio desta política, a Sociedade manifesta seu compromisso com a excelência em matéria de segurança, a qual ostenta um papel protagonista no dia a dia das sociedades do Grupo, para que permaneçam seguras, resilientes e confiáveis em uma comunidade digital em contínua transformação, onde surgem novas ameaças cada vez mais sofisticadas, tanto físicas como de cibersegurança ou híbridas, o que provoca um aumento no grau de exigência dos reguladores, dos clientes, dos demais Grupos de Interesses com os quais as sociedades dos Grupo se relacionam, respeito ao cumprimento de cada vez mais alto nível de segurança, que permita construir e consolidar relações duradouras e de confiança.

## 2. Escopo de aplicação

Esta Política é aplicável à Sociedade e às demais empresas que integram o Grupo e às sociedades participadas não integradas no Grupo sobre as quais a Sociedade detenha influência na gestão, dentro dos limites legalmente estabelecidos.

Nas sociedades participadas onde esta Política não seja aplicável, a Sociedade promoverá, por meio de seus representantes nos órgãos de administração, o alinhamento das próprias políticas com as da Sociedade.

Além disso, esta Política também se aplica, conforme o caso, às *joint ventures*, uniões temporárias de sociedades e outras associações equivalentes, quando a Sociedade assumir sua gestão.

Esta *Política* se desenvolve e complementa por meio das seguintes políticas específicas aprovadas pelo Conselho de Administração da Sociedade: a Política de Proteção de Dados Pessoais e a Política de Riscos de Cibersegurança, que respeitam as citadas matérias.

### 3. Princípios básicos de atuação

Para materializar o compromisso indicado na sua “Finalidade”, estabelecem-se os seguintes princípios básicos de atuação que devem presidir as atividades das sociedades do Grupo em matéria de segurança corporativa:

- a) Definir uma estratégia de segurança integral, com um enfoque tanto preventivo como proativo para garantir um nível razoável de risco.
- b) Assegurar a adequada proteção dos ativos (incluindo infraestruturas críticas), para gerir proativamente os riscos.
- c) Garantir a proteção dos profissionais das sociedades do Grupo, tanto em seus postos de trabalho como em suas atividades e mobilidades por motivos profissionais, assim como a proteção de pessoas quando se encontrem nas instalações ou em qualquer evento institucional das sociedades do Grupo.
- d) Definir um modelo de gestão da segurança com uma associação clara de papéis e responsabilidades e mecanismos de coordenação efetivos, que integre a segurança e a gestão proativa dos riscos nos processos de decisão.
- e) Assegurar a adequada proteção da informação e do conhecimento , assim como dos sistemas de controle, de informação e de comunicações , para gerir proativamente os riscos em conformidade com o disposto na *Política de Riscos de Cibersegurança*.
- f) Promover a identificação de informações não públicas classificadas (ou passíveis de serem classificadas) como confidenciais ou secretas, bem como de informações consideradas (ou passíveis de serem consideradas) como segredo comercial e definir os critérios para sua adequada proteção, assegurando sua implementação.
- g) Impulsionar a luta ativa contra a fraude e contra ataques à marca, à imagem, à reputação das sociedades do Grupo e de seus profissionais..
- h) Garantir o direito de proteção dos dados pessoais das pessoas físicas que se relacionam com as sociedades que pertençam ao Grupo , em conformidade com o disposto na Política de Proteção de Dados Pessoais.

- i) Adotar as medidas necessárias para prevenir, neutralizar, minimizar ou restaurar o dano causado por ameaças de segurança, sejam elas físicas, de cibersegurança ou híbridas, para a normalização do desenvolvimento das atividades, com base em critérios de proporcionalidade aos potenciais riscos e à criticidade e ao valor dos ativos e serviços afetados.
- j) Cumprir com os princípios básicos de atuação estabelecidos na Política de Resiliência Operacional.
- k) Fomentar uma cultura inclusiva e uma conscientização em matéria de segurança dentro do Grupo, mediante a realização de ações de divulgação, conscientização e formação adequadas, adaptadas a cada destinatário e com a suficiente periodicidade para garantir a atualização dos conhecimentos neste âmbito.
- l) Impulsionar a adequada capacitação em matéria de segurança de todo o pessoal, tanto interno como externo, definindo requisitos e critérios na contratação que tenham em conta tal capacitação.
- m) Monitorar o contexto atual da organização e do ambiente, bem como a evolução dos eventos que permitem a identificação das ameaças de segurança mais relevantes, a fim de antecipar seu potencial impacto.
- n) Promover as melhores práticas e a inovação no campo da segurança.
- o) Colaborar com -os Grupos de Interesses envolvidos (incluindo a cadeia de suprimentos e clientes) nos riscos de segurança que afetam as empresas do Grupo para fortalecer a resposta coordenada a potenciais riscos e ameaças de segurança.
- p) Prestar toda a assistência e cooperação que possam ser requeridas pelas instituições e organismos competentes no domínio da segurança, incluindo, entre outros, reguladores, forças e organismos de segurança e agências governamentais, nacionais e internacionais.
- q) Assegurar o efetivo cumprimento das obrigações impostas pelo Sistema de Governança e Sustentabilidade e pelas normas aplicáveis em todos os momentos em termos de segurança, atuando sempre em conformidade com a legislação vigente e com o disposto no *Código de Ética* e demais normas do Sistema de Governança e Sustentabilidade.

### 3. Programa Estratégico de Segurança

A Diretoria de Segurança Corporativa da Sociedade (ou a gerência que futuramente assumir suas funções) identificará, implementará e avaliará as ações necessárias ao desenvolvimento de um Programa Estratégico de Segurança ("**Programa**"), de acordo com os princípios e diretrizes definidos nesta *Política* e desenvolverá as

regras, metodologias e procedimentos internos para assegurar a correta implementação do Programa pela Sociedade e pelas demais empresas do Grupo, que o adaptarão às particularidades dos territórios e negócios de cada uma delas.

Os departamentos de segurança corporativa (ou os departamentos, áreas ou funções que assumirem suas responsabilidades a qualquer momento) de cada uma das empresas do Grupo comprometem-se, em relação à empresa correspondente, que em todos os momentos um nível de maturidade da organização em termos de segurança seja garantido de acordo com os mais altos padrões existentes em todos os momentos, tendo em conta o território e os negócios desenvolvidos pela empresa correspondente.

Por sua vez, a Diretoria de Segurança Corporativa da Sociedade (ou a área que assumir as suas funções de tempos a tempos) assegurará, também, a coordenação adequada das práticas e da gestão de riscos no domínio da segurança entre as diferentes empresas do Grupo, bem como a manutenção de um nível adequado de maturidade em termos de segurança.

#### **4. Monitoramento e controle**

Compete à Diretoria de Segurança Corporativa da Sociedade (ou à área que, a qualquer tempo, assumir suas funções) fiscalizar o cumprimento das disposições desta *Política*.

O acima exposto deve ser entendido, em qualquer caso, sem prejuízo das responsabilidades que correspondem a outros órgãos, áreas, funções e gestão da Sociedade e, se for o caso, aos órgãos de administração das sociedades do Grupo.

Para verificar o cumprimento desta Política, serão realizadas avaliações e auditorias periódicas com auditores internos ou externos.

\* \* \*

Esta Política foi aprovada inicialmente pelo Conselho de Administração em 19 de julho de 2018, revisada e atualizada pela última vez em Reunião do Conselho de Administração de 29 de maio de 2024.