POLÍTICA DE SEGURANÇA

Atualizada em 18 de junho de 2026.

O Conselho de Administração da NEOENERGIA S.A. (a "**Sociedade**") tem o poder de elaborar, avaliar e revisar constantemente, o Sistema de Governança e Sustentabilidade da Sociedade, bem como aprovar e atualizar as políticas que contêm as diretrizes que regem a atuação da Sociedade, e informam, ainda, no que for aplicável, as políticas que, no exercício da sua autonomia societária, resolvam aprovar as sociedade que integram o grupo, cuja entidade controladora é, no sentido estabelecido pela lei, é a Sociedade (as "**Controladas**" e o "**Grupo Neoenergia**").

No exercício destas competências e no âmbito da legislação, do *Estatuto Social* da Sociedade e do *Propósito e Valores do Grupo Iberdrola* (o "***Propósito e Valores***"), o Conselho de Administração aprova esta *Política de Segurança* (a "***Política***"), que respeita, desenvolve e adapta, em relação à Sociedade, os *Princípios Éticos e Básicos de Governança e de Sustentabilidade do Grupo Iberdrola* (os "***Princípios Éticos e Básicos de Governança e de Sustentabilidade***" e o "**Grupo**", respectivamente).
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 da Sociedade e de suas Controladas, 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 Interesse com os quais as sociedades do Grupo Neoenergia se relacionam, respeito ao cumprimento de um nível cada vez mais alto de segurança, que permita construir e consolidar relações duradouras e de confiança.

1. Âmbito de aplicação

Esta Política é aplicável à Sociedade. Não obstante, inclui princípios que complementam, no âmbito da segurança, os *Princípios Éticos e Básicos de Governança e de Sustentabilidade*. Nessa medida, os princípios desta *Política* informam as ações e os normativos específicos das Controladas, observadas suas competências e sua autonomia nesta matéria.

Estes princípios deverão informar também, quando aplicável, a atuação do Instituto Neoenergia, vinculado ao Grupo Neoenergia.

A Sociedade promoverá o alinhamento dos normativos das sociedades nas quais participe, mas que não façam parte do Grupo Neoenergia, bem como das *joint ventures*, associações

temporárias e outras entidades nas quais assuma a gestão, com os princípios contidos nesta *Política*.

2. Finalidade

A finalidade desta Política *é* estabelecer os princípios de atuação que devem reger em matéria de segurança da Sociedade, como *subholding* do Grupo no Brasil, e suas Controladas, para zelar a efetiva proteção das pessoas, dos ativos físicos e de cibersegurança (incluindo infraestrutura crítica), da informação, do conhecimento e dos sistemas de controle e das 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.

3. Princípios de atuação

A Sociedade adota e promove os seguintes princípios de atuação que devem nortear suas atividades em matéria de segurança:

a) Zelar pela proteção dos profissionais da Sociedade e das Controladas, tanto em seu local de trabalho quanto durante deslocamentos por motivos profissionais, bem como pela proteção das pessoas que se encontrem nas instalações ou em qualquer evento institucional da Sociedade.

b) Assegurar a proteção adequada dos ativos, tanto físicos quanto cibernéticos, para gerenciar proativamente os riscos em todas as fases de seu ciclo de vida, garantindo que possuam um nível apropriado de segurança, cibersegurança e resiliência, aplicando os padrões mais avançados para aqueles que sustentam a operação de infraestruturas críticas, em conformidade com as *Bases Gerais de Controle e Gestão de Riscos do Grupo Iberdrola* e com as *Diretrizes e Limites de Risco de Cibersegurança* adotadas pelo Conselho de Administração.

c) Definir um modelo de gestão da segurança com atribuição clara de papéis, responsabilidades e mecanismos de coordenação eficazes, que integre a segurança e a gestão proativa de riscos nos processos decisórios, e zele pelo cumprimento da normativa aplicável em matéria de segurança, reforçando especialmente a cibersegurança e a proteção dos serviços essenciais como elementos prioritários.

d) Promover a identificação de informações não públicas consideradas (ou passíveis de serem consideradas) como segredo empresarial, bem como aquelas cuja divulgação

ou alteração não autorizada possa causar sérios prejuízos aos interesses da Sociedade.

e) Definir os critérios para a proteção adequada da informação e do conhecimento, bem como dos sistemas de controle, informação e comunicações, supervisionando e assegurando sua implementação.

f) Impulsionar o combate ativo à fraude e a ataques à marca, à imagem e à reputação da Sociedade e de seus profissionais.

g) Garantir o direito à proteção dos dados pessoais das pessoas físicas com as quais se relaciona, em conformidade com o disposto na *Política de Proteção de Dados Pessoais*.

h) Adotar as medidas necessárias para prevenir, mitigar, minimizar ou restaurar os danos causados por ameaças à segurança, sejam físicas, de cibersegurança ou híbridas, para o desenvolvimento normal das atividades, com base em critérios de proporcionalidade aos riscos potenciais, à criticidade e ao valor dos ativos e serviços afetados.

i) Cumprir com os princípios de atuação estabelecidos na *Política de Resiliência Operacional*, contribuindo para a definição, planejamento e execução de testes e simulações voltados à gestão de incidentes e crises decorrentes de riscos de segurança; bem como para a análise e avaliação sistemática das causas e impactos dos incidentes, identificando lições aprendidas e promovendo as correspondentes ações corretivas.

j) Fomentar uma cultura inclusiva e de conscientização em matéria de segurança, em toda a sua dimensão (física, cibersegurança e resiliência), tanto internamente quanto externamente, junto a terceiros e colaboradores, por meio da realização de ações de divulgação, conscientização e formação adequadas, adaptadas a cada público e com periodicidade suficiente para garantir que possuam os conhecimentos, habilidades, experiência e capacidades necessárias.

k) Promover a capacitação adequada em segurança de todo o seu pessoal, interno e externo, definindo requisitos e critérios na contratação que considerem tal capacitação.

l) Promover a integração da segurança na gestão dos projetos da Sociedade que possam implicar algum risco potencial de segurança, de forma a garantir a identificação e o tratamento adequados desse risco desde o design e as fases iniciais

do projeto, bem como o estabelecimento dos controles necessários durante sua vigência.

m) Impulsionar o uso seguro dos ativos que fortaleça as capacidades de detecção, prevenção, defesa, resposta e recuperação frente a ataques ou incidentes de segurança, zelando por sua eficácia e dando especial atenção às ameaças de cibersegurança.

n) Impulsionar a adequada gestão de incidentes de segurança, zelando por sua detecção, análise, contenção, recuperação e notificação de incidentes significativos às autoridades competentes e, quando aplicável, aos Grupos de interesse da Sociedade afetados.

o) Definir os critérios para o uso seguro das capacidades de inteligência artificial, supervisionando e zelando por sua implementação.

p) Estabelecer requisitos e padrões de segurança exigíveis aos fornecedores e parceiros da cadeia de suprimentos da Sociedade, para gerenciar os riscos de segurança associados à cadeia de suprimentos, equivalentes e coerentes com o estabelecido nesta Política, supervisionando e zelando por sua implementação.

q) Monitorar o contexto atual da organização e do ambiente, bem como a evolução de eventos que permitam identificar as ameaças de segurança mais relevantes, com o objetivo de antecipar seu potencial impacto.

r) Promover as melhores práticas, a melhoria contínua e a inovação no âmbito da segurança.

s) Colaborar com os grupos de interesse envolvidos (entre outros, a cadeia de suprimentos e os clientes) em riscos de segurança que afetem a organização, a fim de reforçar a resposta coordenada diante de potenciais riscos e ameaças em matéria de segurança.

4. Coordenação em nível de Grupo

No que diz respeito ao escopo de atuação específico de cada sociedade do Grupo Neoenergia, a Superintendência de Segurança e Resiliência Corporativa (ou a área que, a qualquer momento, assuma suas competências), por meio da Comissão de Segurança, Resiliência e Tecnologias Digitais (ou da comissão que, a cada momento, assuma suas competências), atuará em coordenação com a Diretoria de Segurança e Resiliência da Iberdrola, S.A. (ou a

diretoria que, a qualquer momento, assume seus poderes) e com a Comissão de Segurança, Resiliência e Tecnologias Digitais da Iberdrola, S.A. (ou a comissão que, a qualquer momento, assuma suas competências) e estabelecerá o marco para relações de coordenação com suas Controladas, de forma a assegurar um nível consolidado adequado de maturidade e riscos em termos de segurança ao nível do Grupo.

Além disso, a Superintendência de Segurança e Resiliência Corporativa (ou a área que, a cada momento, assuma suas competências), por meio da Comissão de Segurança, Resiliência e Tecnologias Digitais (ou da comissão que, a cada momento, assuma suas competências), identificará, implantará e avaliará as ações necessárias para a elaboração e supervisão de um Programa estratégico de segurança, conforme os princípios e diretrizes definidos nesta *Política*, e desenvolverá as normas, metodologias e procedimentos internos para assegurar sua adequada implementação.

5. Implementação e acompanhamento

Para a implementação e o acompanhamento do previsto nesta Política, o Conselho de Administração conta com a Diretoria Executiva de Recursos (ou a diretoria que, a cada momento, assuma suas competências), que desenvolverá os procedimentos necessários para tal.

* * *

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 18 de junho de 2026.