# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

## 1. OBJETIVO

A presente política é uma declaração formal acerca do compromisso da Copa Energia S.A. (“Copa Energia” ou “Companhia”) com a proteção dos seus ativos de informação.

## 2. APLICAÇÃO E ABRANGÊNCIA

Esta política é informativa aos clientes, fornecedores, parceiros e demais partes externas interessadas.
Esta política deve ser observada por todos os fornecedores, prestadores de serviços e terceiros que tenham acesso aos serviços e/ou recursos tecnológicos da Companhia.

## 3. DESCRIÇÃO

### 3.1. Introdução

O Sistema de Gestão da Segurança da Informação (“SGSI”) da Copa Energia é baseado na norma ABNT NBR ISO/IEC 27001, garantindo medidas alinhadas às estratégias, requisitos de segurança, leis e regulamentações. Para manter os controles e recursos que suportam o SGSI, constituiu-se o Comitê de Gestão de Segurança da Informação e Privacidade de Dados, que adotam um conjunto de políticas e procedimentos de segurança da informação.

A Alta Direção da Companhia se compromete a apoiar e garantir a melhoria contínua do SGSI, disponibilizando recursos, promovendo engajamento e assegurando que os processos sejam constantemente avaliados e aprimorados.

Todas as informações devem ser protegidas quanto à confidencialidade, integridade e disponibilidade, garantindo que sejam acessadas apenas por pessoas autorizadas e utilizadas exclusivamente para fins corporativos.

Terceiros, parceiros e prestadores de serviço devem conhecer e cumprir as disposições previstas nesta Política, disponível no site institucional da Companhia.

### 3.2. Diretrizes

a) Garantir a proteção adequada, utilizando um SGSI) robusto e alinhado com os requisitos da ISO/IEC 27.001;

b) Realizar a gestão diária de eventos e incidentes de segurança da informação, com objetivo principal de prevenir, monitorar, responder e recuperar o ambiente da Companhia contra ataques cibernéticos;

c) Possuir uma política interna de segurança da informação que contemple as diretrizes e orientações sobre a proteção das informações de nossos clientes e funcionários, com atualizações periódicas;

d) Garantir a correta atribuição do grau de sensibilidade das informações armazenadas, através de uma Norma de Classificação da Informação, estabelecida e implementada;

e) Assegurar, através de controles de acesso lógico, destinados a evitar acessos não autorizados ou indevidos que sejam capazes de prejudicar a confidencialidade, disponibilidade ou a integridade das informações;

f) Garantir o uso de técnicas de criptografia em repouso e em transferência, além da adoção de métodos seguros de comunicação com parceiros;

g) Adotar medidas físicas, visando assegurar que todas as instalações onde houver recursos e ativos de informação disponham de controle de acesso adequado e monitorado, capaz de protegê-los de acessos não autorizados e/ou de riscos ambientais;

h) Manter cópias de segurança ("*backups*") para fins de recuperação em caso de desastres, com testes de restauração periódicos visando garantir a confidencialidade, integridade e a disponibilidade no caso do uso emergencial;

i) Utilizar controles de segurança de máquinas e estações de trabalho, com limitações para alterações de configurações administrativas, exportação de arquivos e dados, instalações de softwares não homologados e injeção de mídias removíveis (como pen-drive);

j) Utilizar ferramentas robustas e qualificadas para a varredura de vulnerabilidades, detecção de ameaças e exfiltração de informações;

k) Celebrar Acordos de Confidencialidade ("*NDAs*") com colaboradores, prestadores de serviços e parceiros, visando evitar a divulgação e/ou transmissão não autorizada de dados ou informações, ainda que por meio de cláusula de confidencialidade nos contratos firmados com os mesmos;

l) Garantir o mapeamento, o monitoramento e o *report* de riscos relacionados à privacidade e à segurança da informação, com participação da Alta Direção;

m) Implementar a gestão de ativos, classificação da informação e controles de acesso físico e lógico conforme criticidade;

n) Promover conscientização e treinamento periódico sobre segurança da informação e proteção de dados; e

o) Estabelecer processo formal para gestão de incidentes e vulnerabilidades, com comunicação imediata ao canal designado.

Na Copa Energia, a proteção das informações é de extrema importância. O respeito à privacidade e a transparência das atividades fazem parte do compromisso que a Companhia mantém com terceiros, por isso, é fundamental que os terceiros sejam encorajados a conhecer as políticas da Copa Energia, disponíveis no site corporativo www.copaenergia.com.br.

Situações de incidentes/vulnerabilidades em sistemas informatizados devem, também, ser informadas tempestivamente para a área de Segurança da Informação, através do e-mail CIRT@copaenergia.com.br, disponível nos sites institucionais da Companhia.

## 4. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A documentação gerada no presente processo pode conter dados pessoais de titulares de dados, devendo ser tratados, portanto, com restrição e cuidados necessários, garantindo a proteção e a privacidade dos dados pessoais, em observância à LGPD.

A coleta, a guarda e o tratamento da eventual documentação deve ser realizada de forma restrita, segura e confidencial, com acesso apenas das pessoas designadas para a atividade, sendo proibida a divulgação dessas informações fora da sua finalidade específica.

O armazenamento dos documentos digitais gerados no processo, devem ser feitos somente em pasta de rede, com acesso restrito. Se gerados em meio físico, eles devem ser arquivados em armário com chave, e com acesso restrito à equipe responsável.

## 5. DÚVIDAS E DENÚNCIAS

Qualquer dúvida relacionada aos termos desta Política, entre em contato com a Gerência da Segurança da Informação.

Todos têm o dever de reportar prontamente qualquer violação ou suspeita de violação da presente Política ao Canal de Denúncias da Companhia, por meio do link **https://aloetica.com.br/copaenergia** ou pelo telefone 0800-795-1509.

Administradores, colaboradores ou terceiros devem se recusar a participar de quaisquer processos que envolvam violação à legislação ou as diretrizes da Companhia, e não devem sofrer retaliações em razão disso.

O descumprimento das disposições previstas nesta Política, seja por negligência ou omissão, sujeita o responsável pela infração às medidas disciplinares cabíveis, conforme previsto nas normas internas, e também às medidas legais, nos casos aplicáveis.

Em caso de descumprimento desta Política por parte de terceiros, serão adotadas as medidas legais cabíveis, tais como a aplicação das penalidades contratuais, o encerramento do contrato, a busca judicial ou extrajudicial para ressarcimento, entre outras.