POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

A Política de Segurança da Informação da Copa Energia Distribuidora de Gás S.A., denominada “Copa Energia” ou “Companhia”, tem como objetivo estabelecer os princípios,as diretrizes e as atribuições de responsabilidade em relação à segurança da informação.

2. APLICAÇÃO E ABRANGÊNCIA

Esta Política deve ser observada por todos os Administradores, membros dos comitês de assessoramento ao Conselho de Administração e colaboradores da Companhia, além de fornecedores, prestadores de serviços e terceiros que eventualmente venham a ter acessoaos serviços e/ou recursos tecnológicos da Companhia.

3. DOCUMENTOS DE REFERÊNCIA E COMPLEMENTARES

- Código de Conduta Ética
- Política de Governança de Dados Pessoais
- Norma de Classificação da Informação

4. DESCRIÇÃO

A segurança da informação é essencial para a competitividade e o desempenho daCompanhia, tendo em vista sua credibilidade no mercado, a segurança na gestão e utilização dos dados sob sua guarda, bem como cumprimento da respectiva legislação aplicável.

4.1. Princípios e diretrizes

a) A Companhia é proprietária das informações geradas ou adquiridas por ela (“Informações”);

b) Todas as Informações da Companhia devem ser adequadamente preservadas quantoà confidencialidade, integridade e disponibilidade, de tal forma que:

- As informações devem estar disponíveis apenas para indivíduos, entidades e/ou processos autorizados pela Companhia, garantindo sua confidencialidade;
- O processamento de informações na Companhia deve garantir a sua exatidão e a

sua completude, garantindo sua integridade;

- As informações e os ambientes de tecnologia da Copanhia devem estar acessíveis e disponíveis aos processos do negócio e aos usuários, sempre que necessário.

c) As Informações e os respectivos recursos aplicáveis ao seu tratamento, tais como dispositivos, ferramentas, softwares, computadores, relatórios e documentos, devem ser usados, pela Companhia, para o desempenho exclusivo de atividades de interessecorporativo, de acordo com a legislação, o Código de Conduta Ética e as diretrizes internas de segurança da informação;

d) A segurança da informação é responsabilidade de todos, de modo que caberá a todos os colaboradores da Companhia o respeito e a adoção, conforme o caso, de processos e comportamentos seguros para tratar e proteger as Informações, considerando também as diretrizes estabelecidas pelos padrões corporativos estabelecidos;

e) O uso das Informações e/ou dos recursos tecnológicos disponibilizados pela Companhia para o desenvolvimento das atividades profissionais deverá observar as seguintes diretrizes:

- Não violar a legislação vigente;
- Não violar o Código de Conduta Ética da Companhia, bem como eventuais outros normativos da Companhia;
- Não comprometer a imagem da Companhia, de seus Administradores, colaboradores e/ou de Terceiros, de modo a violar os preceitos aqui estabelecidos ou conforme orientados pela Companhia;
- Não prejudicar as atividades de trabalho; e
- Não prejudicar a segurança das Informações e dos recursos corporativos disponibilizados para seu tratamento.

f) Em relação à expectativa de privacidade, a Companhia se reserva ao direito de auditare/ou monitorar a utilização de seus recursos, tecnológicos ou não, e dos acessos fornecidos aos seus usuários, de modo a salvaguardar os interesses corporativos no que diz respeito à segurança de suas Informações, respeito às normas de compliance, bem como à utilização adequada dos recursos de sua propriedade; e

g) A utilização dos serviços e/ou recursos tecnológicos da Companhia por seus colaboradores ou Terceiros deve ser autorizada ou homologada previamente pela áreade Tecnologia da Informação. O uso de dispositivos pessoais (celular, tablet, notebook, computador) para acesso ao ambiente corporativo poderá ser disponibilizado, em caráter excepcional, desde que autorizado e obedecendo aos critérios de segurança estabelecidos pela Companhia.

4.2. Processo de Segurança das Informações

De forma a assegurar que as Informações tratadas sejam adequadamente protegidas, a Companhia deve adotar como premissas nos seus processos:

a) **Gestão de Ativos da Informação:** Todos os ativos da informação, ou seja, todos os mecanismos que possam criar, processar, armazenar, transmitir ou excluir informações, sejam físicas ou digitais, devem ser protegidos de acessos indevidos, pormeio de acesso controlado e de configurações de blindagem de acesso, focando a segurança dos dados todo o tempo, de acordo com as diretrizes desta Política.

b) **Classificação da Informação:** As informações devem ser classificadas quanto ao nível de confidencialidade necessária, de acordo com sua importância para os negócios da Companhia. O nível de tratamento e proteção necessário à informação deve ser definido de acordo com o possível impacto decorrente do uso ou exposição indevidos,de acordo com as diretrizes desta Política e da norma de Classificação da Informação.

c) **Gestão de Acessos a Informação:** Quanto à segurança lógica, o acesso à informaçãoe aos recursos tecnológicos deve ser concedido conforme a necessidade real dos colaboradores para o desempenho das suas atividades profissionais dentro da Companhia e deve ser revogado sempre que tal necessidade deixar de existir, nos termos dos normativos internos. Deve ser adotado, sempre que possível, o registro pararastreio e possibilidade de identificação do usuário. Quanto à segurança física, devemser estabelecidos controles de acesso físico somente a pessoas autorizadas de acordocom a criticidade das informações e do ambiente.

d) **Gestão de Riscos Cibernéticos:** A gestão de riscos cibernéticos da Companhia deve ser realizada pela Área de Tecnologia da Informação, considerando as vulnerabilidades, ameaças e impactos e os mecanismos de mitigação adequados.

e) **Segurança dos Sistemas:** Quaisquer desenvolvimentos/contratações de sistemas, plataformas e/ou aplicativos que armazenem, modifiquem ou transmitam Informações da Companhia devem considerar as práticas de segurança definidas na Política de Governança de Dados Pessoais e normativos da Companhia.

f) **Conscientização e treinamento em Segurança da Informação e Proteção de Dados:** A Companhia promoverá, periodicamente, a disseminação dos princípios e diretrizes de segurança da informação e proteção de dados, para que todos os colaboradores estejam aptos a pensar e agir de forma segura em sua rotina, visando asegurança e proteção das informações corporativas.

g) **Gestão de Incidentes de Segurança da Informação ou de Violação de Dados Pessoais:** A gestão dos incidentes, sejam eles relacionados à segurança da informação ou à violação de dados pessoais, deverá ser realizada conforme normativos, considerando sua criticidade e os impactos causados aos negócios da Companhia.

Ao identificar ou tomar conhecimento de possível *(i)* ocorrência de incidente de segurança

da informação; *(ii)* violação de dados pessoais da Companhia; e/ou *(iii)* adoção de comportamentos que não sejam considerados seguros para a proteção das Informações da Companhia, independente do meio físico ou digital, qualquer colaborador ou Administrador deve contatar o Canal de Ética da Companhia. Situações de incidentes/vulnerabilidades em sistemas informatizados devem, também, ser informadas tempestivamente para a área de Segurança de Tecnologia da Informação, através do e-mail CIRT@copaenergia.com.br disponível nos sites institucionais da Companhia.

4.3. Proteção dos Dados Pessoais e Privacidade

A Companhia deve garantir a disponibilidade, integridade e confidencialidade dos dados pessoais aos quais tiver acesso, pelo tempo que se fizer necessário e respeitada a legislação vigente, em qualquer formato de armazenamento.

Em todos os processos da Companhia em que houver o tratamento de dados pessoais, a área gestora responsável deverá adotar medidas técnicas e/ou administrativas para protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição,perda, alteração, comunicação ou difusão, seja no todo ou em parte.

A proteção dos dados pessoais e privacidade também devem seguir as diretrizes da Políticade Governança de Dados Pessoais.

4.4. Uso de redes sociais e aplicativos de mensagens instantâneas

Toda e qualquer pessoa autorizada a acessar informações e recursos da Companhia deverá observar as seguintes diretrizes no uso de redes sociais ou aplicativos de mensagens instantâneas, sem prejuízo das previsões contidas nos demais normativos da Companhia que contemplem outras regras dessa natureza:

a) Não compartilhar, sem respectiva autorização prévia, Informações Empresariais (conforme definido no normativo de Classificação do Compliance), classificadas como confidenciais, mesmo que entre colaboradores da companhia; e

b) Não publicar, sem a respectiva autorização prévia, vídeos, áudios e/ou fotos das instalações industriais ou administrativas, bem como de mapas, plantas, projetos, pessoas, situações internas da Companhia, atas ou documentos entre outros.

5. RESPONSABILIDADES

Conforme as melhores práticas de mercado, a Companhia mantém uma estrutura organizada responsável pela aplicação desta Política, em diferentes níveis da organização,conforme detalhado abaixo.

5.1. Conselho de Administração

- Compete ao Conselho de Administração aprovar esta Política e eventuais demais políticas globais relativas à segurança da informação, e suas futuras revisões.

5.2. Comitê de Auditoria

- Compete ao Comitê de Auditoria assessorar o Conselho de Administração no estabelecimento de Políticas que envolvam a segurança da informação e controles internos, bem como supervisionar os processos de controles internos e de gerenciamento dos riscos inerentes às atividades da Companhia e de suas controladas.

5.3. Diretoria

- Compete à Diretoria acompanhar a implementação das medidas e adotar as ações necessárias para que esta Política seja observada nos processos da Companhia, por meio do engajamento dos seus liderados e na adoção de condutas exemplares.

5.4. Área de Riscos e Compliance

- Compete à Área de Riscos e Compliance:
- Realizar as tratativas aos riscos de Segurança da Informação considerando as diretrizes da Política de Gestão de Riscos Empresariais.
- Estabelecer e aplicar treinamentos, de forma coordenada com a Área de Tecnologia da Informação, relacionados à proteção de dados e privacidade (LGPD), controles internose riscos corporativos, com base nas definições desta Política; e
- Disseminar no âmbito de sua atuação, de forma efetiva e contínua, as diretrizes desta Política.

5.5. Área de Tecnologia da Informação

Compete à Área de Tecnologia da Informação:

- Coordenar a implantação e o monitoramento quanto às atividades de Tecnologia da Informação na evolução das diretrizes desta Política e mantê-la atualizada com base na legislação vigente;
- Promover, de forma efetiva e contínua, treinamentos coordenados com a Área de Riscos e Compliance, quando necessário, bem como a disseminação dos princípios e diretrizes de Segurança da Informação em Tecnologia da Informação com base nas definições desta Política;
- Realizar a gestão de riscos cibernéticos da Companhia, considerando as vulnerabilidades, ameaças e impactos e os mecanismos de mitigação adequados;

- Zelar pelo monitoramento e gestão de regras de segurança da informação adotadas para o ambiente tecnológico da Companhia;
- Disseminar, no âmbito de sua atuação, de forma efetiva e contínua, as diretrizes destaPolítica; e
- Revisar os termos desta Política periodicamente conforme estabelecido no Sistema dePadronização Normativa da Companhia sempre que se considerar necessário, a fim deaprimorar os planos de respostas a Incidentes.

5.6. Gestores

Compete aos Gestores das áreas da Companhia:

- Coordenar, promover e acompanhar as ações relativas à segurança da informação emsua área de atuação; e
- Fornecer à área de Tecnologia da Informação, sempre que solicitado, todas as informações necessárias para a avaliação de tratamento de informações, seu monitoramento e reporte para a Diretoria, Comitê de Auditoria e Conselho de Administração da Companhia.

5.7. Colaboradores

- Cumprir as disposições previstas nesta Política.

5.8. Forncedores

- Cumprir as disposições previstas nesta Política, disponível no site institucional da Companhia.

6. DÚVIDAS E VIOLAÇÕES

Qualquer dúvida relacionada aos termos desta Política deve ser esclarecida pela área de Riscos e *Compliance,* ou pela área de Segurança de Tecnologia da Informação.

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

Situações de incidentes/vulnerabilidades em sistemas informatizados devem, também, serinformadas tempestivamente para a área de Segurança de Tecnologia da Informação por meio do e-mail CIRT@copaenergia.com.br.

O descumprimento das disposições previstas nesta Política, inclusive por negligência ou

omissão, sujeita o responsável pela infração às medidas disciplinares cabíveis, conforme previsto nos normativos internos, e também às medidas legais, nos casos aplicáveis.

No descumprimento desta Política por parte de Terceiros, serão adotadas as medidas cabíveis, tais como a aplicação das penalidades contratuais, o encerramento do contrato, a busca judicial ou extrajudicial para ressarcimento, entre outras. Todos os Terceiros deverão estar expressamente cientes dos termos desta Política, conforme previsão a ser incluída nos respectivos instrumentos contratuais ou afins.

7. DEFINIÇÕES

Administradores: Membros do Conselho de Administração e da Diretoria da Companhia.

Gestores: Gerentes e Coordenadores da Companhia.

Terceiros: Toda e qualquer pessoa física ou jurídica ou ente despersonalizado não pertencente ao quadro de funcionários da Companhia, incluindo, mas não se limitando, a prestadores de serviço, parceiros de negócio, consultores, distribuidores, representantes, representantes comerciais, mandatários, procuradores, clientes, fornecedores, despachantes, entre outros.

8. ANEXOS

Não aplicável.