1 PÚBLICO ALVO

1.1 Esta Política aplica-se a todas as pessoas naturais que trabalham na Companhia de Saneamento de Minas Gerais – COPASA MG e suas subsidiárias, sejam Conselheiros, Diretores, empregados, contratados, profissionais de qualquer natureza, estagiários, aprendizes e afins, bem como para qualquer pessoa física ou pessoa jurídica, de direito público ou privado, com quem a Companhia se relaciona: fornecedores, prestadores de serviços, clientes, entre outros, que possam acessar as áreas, equipamentos, informações, arquivos, redes e dados de titularidade ou propriedade da COPASA MG.

1.2 Para os efeitos desta Política, entende-se que os termos COPASA MG ou Companhia compreendem a Controladora e suas Subsidiárias.

2 OBJETIVOS

2.1 Estabelecer diretrizes e competências para uniformizar os procedimentos da COPASA MG no que concerne ao planejamento, implementação e controle de ações relacionadas à proteção e segurança das informações geradas, recebidas e tratadas no âmbito da Companhia, inclusive dados pessoais, atendendo a padrões nacionais e internacionais e aspectos legais e regulatórios relacionados ao tema.

2.2 E ainda, especificamente, objetiva:

a) preservar a confidencialidade, a integridade e a disponibilidade das informações;

b) prevenir possíveis incidentes e responsabilidade legal da Companhia e de seus empregados, prestadores de serviços, estagiários, aprendizes e afins;

c) assegurar o treinamento contínuo e atualizado na aplicabilidade das políticas, dos procedimentos e normas de segurança da informação, enfatizando as obrigações das pessoas em relação à respectiva segurança da informação;

d) garantir que todas as responsabilidades referentes à segurança da informação sejam claramente definidas e preservadas, no âmbito interno e externo da Companhia.

3 REFERÊNCIAS

Para aplicação desta Política, poderá ser necessário consultar os seguintes documentos:

a) Lei Federal n.º 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação - LAI;

b) Lei Federal n.º 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais - LGPD, em vigor desde 14/08/2020;

c) Código de Conduta e Integridade da COPASA MG.

d) ISO/IEC 27001:2022 – padrão para sistema de gestão da segurança da informação (*ISMS - Information Security Management System*) publicado em outubro de 2005 pelo *International Organization for Standardization e pelo International Electrotechnical Commission*;

e) ISO/IEC 27002:2022 – código de prática para controle de segurança da informação, publicado em 07 de julho de 2013 pelo *International Organization for Standardization e pelo International Electrotechnical Commission*;

4 DEFINIÇÕES

Para os efeitos desta Política adotam-se as seguintes definições:

a) **Ativos de informação –** todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação, incluindo seus dados e a própria informação. Exemplos: base de dados e arquivos, contratos e acordos, documentações de sistemas, pesquisas, manuais, procedimentos de operação e suporte, informações armazenadas em microcomputadores, notebooks, smartphones, tablets, pen drives e mídias em geral, impressoras e outros;

b) **Dados pessoais –** quaisquer informações que identificam ou que possam identificar uma pessoa, nos termos da LGPD;

c) **Confidencialidade –** garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meios eletrônicos ou físicos. Pressupõe manter o sigilo e a privacidade de uma informação ou dado, e requer controles implementados para tal;

d) **Disponibilidade** - as informações devem estar acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de TI;

e) **Informação –** qualquer informe, relatório, elemento, notícia, comunicação, material, instrução ou direção que seja disponibilizado em formato físico ou eletrônico, e seja utilizado nos processos e atividades da Companhia;

f) **Integridade –** indica a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados e efetuados, como também a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário;

g) **Usuários em geral –** são formados por empregados, contratados, prestadores de serviços, estagiários, aprendizes e afins que acessam informações na Companhia. O cadastro é realizado pela unidade de pessoas ou outra unidade que foi devidamente autorizada;

h) **Segurança da informação**: consiste em medidas técnicas e administrativas implementadas para resguardar as informações, de modo a mantê-las seguras e preservadas em sua confidencialidade, integridade e disponibilidade;

i) **Servidores corporativos**: computadores de alto desempenho projetados para fornecer serviços, armazenar dados e gerenciar recursos de rede de forma centralizada. Exemplo o "*V:*\" disponibilizado;

j) **Tratamento de dados pessoais**: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

5 DIRETRIZES

No atendimento ao que é recomendado pela ISO 27001 e demais padrões relacionados, a COPASA MG adotará em seus processos e atividades, as diretrizes estabelecidas a seguir:

5.1 Governança

5.1.1 Aliado ao comprometimento da alta administração (Diretoria Executiva e Conselho de Administração) com a proteção das informações, a Companhia possui uma estrutura de governança definida e estabelecida para tratar a segurança da informação, em seus níveis executivo e operacional.

5.1.2 Adicionalmente, por meio desta Política, institui-se o Comitê Executivo de Segurança da Informação, com composição multidisciplinar e com o papel de analisar e propor para os órgãos competentes diretrizes e orientações a serem adotadas sobre segurança da informação da Companhia, conforme regimento interno.

5.1.2.1 Compõem este Comitê os titulares das seguintes unidades organizacionais: Superintendência de Tecnologia da Informação (coordenador), Gerência de Infraestrutura e Cibersegurança, Superintendência de *Compliance*, Superintendência de Desenvolvimento Comercial, Superintendência de Compras e Licitações, Superintendência de Planejamento e Excelência Operacional, Auditoria Interna, Diretoria Adjunta de Pessoas, Diretoria Adjunta Jurídica e o DPO (*Data Protection Officer*), que é o encarregado pela proteção de dados pessoais da Companhia. A participação da Auditoria Interna se dá a título de consultoria, de forma a preservar sua objetividade e independência.

5.1.3 Além desta Política, normativos específicos devem ser estabelecidos para definição de padrões técnicos alinhados às melhores práticas de segurança da informação. Os normativos devem detalhar os controles operacionais, os procedimentos, a tecnologia e os processos que implementem as diretrizes aqui apresentadas. Tais documentos devem ser propostos pela Superintendência de Tecnologia da Informação - SPIN, unidade responsável pelo processo de segurança da informação, apreciados pelo Comitê Executivo de Segurança da Informação e submetidos à aprovação das instâncias superiores competentes.

5.2 Informação

5.2.1 Controle de acesso à informação

5.2.1.1 A SPIN deverá estabelecer critérios, procedimentos e responsabilidades para a gestão de acessos, observando o disposto na Norma de Procedimentos Utilização de Recursos Computacionais, Segurança e Tratamento de Informações - NP-CSMG-2011/005.

5.2.1.2 O controle e o acesso às informações são gerenciados pela SPIN e deverão observar:

a) o registro de cada usuário geral;

b) o uso de privilégio, se restrito ou controlado;

c) o gerenciamento de senha do usuário geral;

d) o uso de senhas para acesso aos sistemas, a rede de dados, aos e-mails, aos locais em que haja necessidade do uso e afins;

e) a autenticação para conexão externa dos usuários;

f) os procedimentos seguros de entrada no sistema;

g) a identificação e a autenticação de usuários;

h) o sistema de gerenciamento de senha;

i) o limite de tempo de sessão;

j) os critérios de acesso à informação;

k) os critérios e medidas de segurança para uso de dispositivos particulares.

5.2.2 Classificação da informação

5.2.2.1 Todas as informações da Companhia deverão ser classificadas a partir de sua sensibilidade para os negócios, com vistas a garantir a sua proteção, de acordo com o nível de acesso, conforme a seguir:

a) **Informações confidenciais:** informações cujo acesso é restrito somente a pessoas autorizadas e sua exposição pode violar a privacidade de pessoas ou revelar segredos da Companhia, em razão de serem caracterizadas como sigilos estratégicos, comerciais ou industriais;

b) **Informações internas:** informações de livre acesso a colaboradores e parceiros da Companhia, mas de uso exclusivo destes, não podendo ser compartilhadas com pessoas externas à COPASA MG, sem prévia autorização;

c) **Informações públicas:** informações sem restrição de divulgação ou acesso, que podem ser dispostas em *site* ou disponibilizadas a qualquer pessoa sem prejuízo para a Companhia.

5.2.2.2 As condições para se promover tal classificação - responsáveis, critérios, ferramentas e prazos, dentre outras - serão definidas em Norma de Procedimentos a ser proposta pela SPIN.

5.2.2.3 A SPIN deverá implementar tecnologias e processos de controle e monitoramento com o objetivo de garantir um nível adequado de proteção das informações. Tais medidas devem assegurar a confidencialidade, integridade e disponibilidade dos dados desde a sua concepção, adotando o princípio de segurança.

5.2.2.4 Adicionalmente, devem ser incorporados recursos que possibilitem a rastreabilidade, auditoria e investigação de eventos de não conformidade, assegurando a aderência aos padrões, normas e diretrizes estabelecidos pela Companhia.

5.2.3 Cópias de segurança

5.2.3.1 As informações digitais armazenadas nos servidores e bancos de dados da Companhia devem ser copiadas pela SPIN para um meio externo dentro de uma periodicidade e de acordo com os procedimentos de segurança existentes. As cópias devem ser completas e incrementais, além de utilizar programas modernos e atualizados.

5.2.3.2 Os critérios de cópias, guarda e recuperação de informações, bem como a periodicidade de testes a serem realizados para verificar a qualidade e completude da recuperação deverão ser definidos em Norma de Procedimentos sob a gestão da SPIN.

5.2.3.3 As informações criadas, modificadas e armazenadas na Companhia são consideradas seus ativos, e só poderão ser copiadas, reproduzidas ou compartilhadas de acordo com os critérios de classificação de informações previsto nesta norma.

5.2.3.4 As informações corporativas devem ser armazenadas nos servidores corporativos disponibilizados pela SPIN, sendo vedado o armazenamento exclusivo nos microcomputadores (C:\ da máquina) e notebooks.

5.2.3.5 O período de retenção e de descarte das informações, dentre outros aspectos, devem ser definidos em Norma de Procedimentos sob a gestão da SPIN, devendo considerar os requerimentos regulatórios envolvidos, as definições de segurança da informação e os aspectos dos distintos processos da Companhia.

5.2.3.6 A SPIN deverá implementar procedimentos seguros para o referido descarte.

5.3 Tratamento das informações pessoais

5.3.1 A aplicação desta Política deve garantir o adequado tratamento de dados pessoais, conforme disposto na LGPD e nas políticas internas correlatas, assegurando a adequação aos princípios e finalidades, enquadramento às bases legais e atendimento aos direitos dos titulares de dados pessoais.

5.4 Educação e treinamento

5.4.1 Dentro da periodicidade a ser definida em Norma de Procedimentos, capacitações e campanhas de conscientização em segurança da informação devem ser realizadas e

documentadas pela SPIN, com o objetivo de atingir todos os colaboradores da Companhia, devendo abordar, no mínimo, os temas a seguir:

a) uso e gerenciamento de senha, incluindo criação, frequência de troca e proteção;

b) proteção contra vírus, *worms*, cavalos de troia e outros códigos maliciosos;

c) políticas e normativos internos, bem como as implicações do seu não cumprimento;

d) *e-mails* e anexos desconhecidos;

e) uso da *Web* (liberação versus proibição, monitoramento das atividades de usuários);

f) *spam*, como agir em caso de recebimento, o que significa, entre outros;

g) *backup* de dados e armazenamento (abordagem centralizada ou descentralizada);

h) resposta a incidentes (A quem devo contatar? O que faço quando ocorre?);

i) mudanças no ambiente do sistema;

j) uso do trabalho remoto (teletrabalho);

k) questões de segurança em dispositivos portáteis (identificar tanto questões físicas quanto segurança do *wireless*);

l) uso de criptografia e transmissão de informações sensíveis e as confidenciais por meio da *internet* (identificar políticas, procedimentos e contato técnico para assistência);

m) segurança de *notebook* durante viagens (identificar tanto questões de segurança física quanto de segurança da informação);

n) sistemas e *software* de propriedade pessoal no trabalho (indicar se é permitido ou não);

o) licenças de *software* (identificar quando cópias são permitidas ou não);

p) controle de acesso (identificar lista de privilégios);

q) responsabilidade individual (explicar o que isso significa na Organização);

r) controle de visitantes e acesso físico aos espaços (discutir política de segurança física aplicável e procedimentos, relatórios de atividades fora do comum);

s) segurança da área de trabalho.

5.4.2 Independentemente do conteúdo e método utilizados para as capacitações e campanhas de conscientização, a SPIN deverá manter os materiais disponíveis para todas as áreas da organização.

5.5 Desligamento de colaboradores

A SPIN deverá definir, em normativo interno, os procedimentos adotados quando do desligamento de empregados da Companhia, no que diz respeito aos ativos digitais sob sua responsabilidade, bem como a eliminação das senhas de acesso e da conta corporativa de *e-mail*.

5.6 Recursos tecnológicos

5.6.1 Toda e qualquer aquisição de sistemas, de equipamentos ou de *software* de mercado deverá ser adquirida ou aprovada previamente pela SPIN e considerar os requisitos de segurança padrões da Companhia no processo de aquisição, de forma a manter os padrões mínimos definidos para proteção de suas informações.

5.6.2 Todos os recursos tecnológicos, incluindo os de rede de comunicação e telecomunicação de dados, devem ser protegidos pela SPIN contra acessos não autorizados e devem ser monitorados proativamente e reativamente para identificação de possíveis eventos adversos por parte de usuários internos ou externos. Os registros dos acessos devem permitir a investigação ativa de eventos suspeitos, a identificação de causa raiz do evento e a identificação de incidentes de segurança.

5.6.3 A SPIN adotará os procedimentos e controles necessários para garantir que os administradores de ambiente (rede de comunicação e telecomunicação de dados, banco de dados, sistemas de informática) e gestores de informação não possuam acessos que permitam alterar diretamente os registros de operações (informações de negócios) ou de eventos citados acima.

5.6.4 Alterações no ambiente (mudanças de versão de sistema, infraestrutura, entre outros), tratativa de incidentes de segurança e operacionais, planos de continuidade de negócios e de recuperação de ambiente, deverão ser disciplinados pela SPIN em normas específicas e testados periodicamente, no mínimo anualmente, objetivando minimizar riscos e consequentes impactos às operações da Companhia.

5.6.5 Para os casos definidos por entidades regulatórias como casos de incidentes de segurança, a SPIN deverá adotar processo de registro, comunicação e reporte, visando à preservação da imagem e reputação da Companhia, dos colaboradores, de clientes e demais envolvidos.

5.7 Fornecedores e prestadores de serviços

5.7.1 A SPIN deverá definir os procedimentos necessários para garantir a segurança da informação, a serem adotados pelas empresas contratadas nos casos de contratações envolvendo o trato de informações corporativas internas ou confidenciais da Companhia.

5.7.2 A Superintendência de Compras e Licitações - SPCL deverá incluir no regulamento de contratações as condições definidas pela SPIN e os casos aos quais elas serão aplicadas.

5.8 Instalações da Companhia

5.8.1 As informações da Companhia, sejam em meio físico ou digital, devem estar protegidas contra acesso físico não autorizado, danos, perdas, furtos e outros eventos de natureza interna e externa. Todas as proteções a serem implementadas devem estar alinhadas aos riscos operacionais previamente definidos e devem mitigar os impactos em caso de materialização, sendo:

a) os acessos às instalações da Companhia devem ser restritos a pessoas previamente autorizadas pelas unidades responsáveis. Níveis de autorização de acesso (alçadas) às dependências físicas também devem ser implementados, bem como a capacidade de registro e identificação, conforme definição prévia e documentada pela Copasa;

b) nos ambientes críticos, como por exemplo, Datacenter, todas as intervenções no ambiente devem ser registradas de forma a garantir a identificação do que foi realizado (trilha de auditoria) e devem ficar disponíveis para usos de investigação e análise sempre que necessário.

6 COMPETÊNCIAS

6.1 Do Conselho de Administração e da Diretoria Executiva

6.1.1 Aprovar esta Política, fornecendo diretrizes e supervisão sobre o tema e prestar o suporte necessário para seu cumprimento.

6.2 Do Comitê Executivo de Segurança da Informação

a) direcionar e acompanhar as ações e incidentes de segurança da Companhia, bem como monitorar as ações implementadas para cumprimento desta Política e julgar casos omissos para deliberação da alta administração.

b) propor soluções sobre segurança da informação, acompanhar apurações quando da suspeita de ocorrências e incidentes em segurança da informação, dirimir as dúvidas eventuais sobre esta Política, monitorar o Plano Estratégico de Segurança da Informação, bem como determinar que sejam realizados os ajustes necessários;

c) apreciar as propostas das normas necessárias à implementação desta Política, a serem elaboradas ou alteradas pela SPIN;

d) apoiar a alta administração da Companhia no planejamento de investimentos em segurança da informação com base nas exigências estratégias e legais.

6.3 Da Superintendência de Tecnologia da Informação

a) gerenciar, acompanhar e monitorar as ações de proteção da informação em todos os seus níveis, interagindo diretamente com as unidades responsáveis pelos processos (demais unidades organizacionais da Companhia), visando garantir o cumprimento de todas as determinações desta Política;

b) definir, implementar e controlar o processo de revisão periódica dos acessos e permissões dos usuários aos diversos ambientes e sistemas da Companhia;

c) coordenar as atividades de tratamento e resposta a incidentes de segurança;

d) agir de forma proativa com o objetivo de evitar que ocorram incidentes de segurança, bem como proceder à divulgação de práticas e recomendações de segurança da informação;

e) avaliar constantemente as condições de segurança de redes;

f) analisar os ataques e intrusões que a rede de dados da Companhia porventura sofrer;

g) executar ações necessárias para tratar todos os tipos de quebras de segurança;

h) manter controle documental das ações que possam violar esta Política, diretrizes e normas de segurança e suprir o Comitê Executivo de Segurança da Informação de dados relativos aos incidentes e intrusões, de forma que possam ser analisadas as possibilidades de aprimoramento e, se for o caso, aplicadas sanções penais, administrativas e civis vigentes;

i) elaborar e manter um Plano de Continuidade de Negócios (PCN) visando possuir contingência para manter a disponibilidade de infraestrutura e sistemas informatizados para a Companhia;

j) manter controle efetivo dos ciclos de vida dos ativos de informação da Companhia, realizando avaliações dos riscos e oportunidades de substituí-los, para que atendam aos requisitos técnicos e regulatórios;

k) estabelecer regras para o uso adequado das informações corporativas.

6.3.1 Dos gestores das áreas de TI

a) responsabilizar-se pelo correto funcionamento de suas unidades, e ainda garantir o monitoramento da execução das diretrizes desta Política, assim como das normas e procedimentos relacionados;

b) divulgar esta Política internamente e comunicar os casos de desvios de conduta por parte dos usuários. Devem, também, reportar para as unidades definidas pela Companhia, todo e qualquer evento adverso (interno ou externo) gerado pelo mau uso das informações que tenham sido identificados;

c) manter suas equipes informadas e treinadas sobre o assunto segurança da informação, bem como ser capaz de identificar comportamentos nocivos à base de dados da Companhia;

d) responsabilizar-se por prover e manter os padrões e diretrizes de segurança que garantem o correto funcionamento da infraestrutura de TI, trabalhando em conjunto com a área responsável pela segurança da informação da Companhia;

e) garantir que os equipamentos da Companhia estejam configurados de acordo com as normas, procedimentos e padrões estabelecidos dentro das melhores práticas de segurança;

f) garantir que os acessos concedidos aos usuários sejam os mínimos necessários para execução de suas atividades, seguindo a determinação dos gestores das informações sob sua responsabilidade;

g) monitorar os incidentes de natureza física e lógica e que este monitoramento resulte em indicadores que possam ser utilizados para melhoria e prevenção dos riscos.

6.4 Dos gestores das informações

a) responsabilizar-se pelas informações dos sistemas utilizados pelas unidades, possuir pleno conhecimento das políticas e normas referentes à segurança da informação para o manuseio corporativo das informações, assim como do uso das ferramentas disponibilizadas pela Companhia para realização das tarefas das unidades usuárias (sistemas de informática, infraestruturas de telecomunicações e de comunicação, equipamentos e assemelhados);

b) zelar pela segurança das informações geridas ou não, definindo os requisitos de confidencialidade, integridade e disponibilidade delas, em conjunto com as áreas responsáveis pela segurança da informação e pela TI, para os controles de segurança a serem aplicados às informações geridas;

c) promover a classificação das informações das quais sejam proprietários, visando o acesso e utilização adequada pelos usuários, em conformidade com esta Política e normas complementares.

6.5 Dos usuários

a) atuar como agentes de proteção das informações da Companhia, bem como custodiantes dos ativos de informação cumprindo o disposto nesta Política em sua totalidade, incluindo as normas, regulamentos e procedimentos relacionados;

b) agir com zelo para que não haja exposição indevida dos dados e informações que tenham acesso;

c) não compartilhar com terceiros não autorizados informações consideradas sigilosas ou internas da Companhia;

d) cuidar dos recursos de tecnologia à sua disposição, agindo com responsabilidade e respeito às diretrizes estabelecidas pela Companhia;

e) comunicar tempestivamente ao seu superior imediato e demais unidades definidas pela Companhia (*Compliance*, Riscos, Auditoria, entre outras), qualquer violação ou descumprimento desta Política, das normas de segurança da informação, dos regulamentos ou dos procedimentos técnicos das unidades;

f) participar dos treinamentos/capacitações referentes à segurança da informação promovidos pela Companhia;

g) zelar pelos ativos de informações sob sua utilização;

h) classificar as informações que gerar.

7 DISPOSIÇÕES FINAIS

7.1 Esta Política deverá ser revisada anualmente, para atualização de regras e procedimentos relacionados no documento.

7.2 A violação a qualquer dispositivo desta Política sujeitará o responsável às penalidades cabíveis, de acordo com as normas e políticas da COPASA MG, sem prejuízo das demais penalidades previstas na legislação e regulamentação aplicáveis.

7.3 Esta Política, aprovada pelo Conselho de Administração em reunião realizada em 24/06/2026, entra em vigor a partir desta data, revogadas as demais disposições em contrário.

Informações de Controle:

Versão 0 (Instituição): aprovada pelo Conselho de Administração, em reunião de 23/05/2024.

Versão 1: revisão, sem alteração de conteúdo, conforme relatório *Compliance* nº 070/25 de 20/05/2025.

Versão 2: revisão, sem alteração de conteúdo, em razão das reestruturações organizacionais, ondas 1 e 2, aprovadas pelo Conselho de Administração em 12/12/2024 e 28/08/2025, respectivamente.

Versão 3: revisão aprovada pelo Conselho de Administração em 24/06/2026.

Unidade gestora do documento: Superintendência de Tecnologia da Informação.

Instância de revisão: Diretoria Executiva.

Instância de aprovação: Conselho de Administração.