1 PÚBLICO ALVO

1.1 Esta Política aplica-se à 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: contratados, 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, atendendo a padrões nacionais e internacionais e aspectos 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) ABNT NBR ISO/IEC 27001:2013 – Norma internacional de segurança da informação (2005) traduzida pela Associação Brasileira de Normas Técnicas (ABNT);

d) ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação (TI) – Técnicas de segurança – Código de prática para controles de segurança da informação, traduzida pela Associação Brasileira de Normas Técnicas (ABNT);

e) Código de Conduta e Integridade da COPASA MG.

4 DEFINIÇÕES

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

a) **Ativos de informação** – microcomputador, *notebook*, aparelho celular, *tablet*, *switch*, roteador, equipamentos de controle automatizado, câmera IP e todos os demais aparelhos que tenham capacidade de qualquer tipo de processamento e que sejam capazes de se conectarem a outros dispositivos, ou não, inclusive na rede de dados;

b) **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;

c) **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;

d) **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;

e) **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;

f) **ISO 27001** – 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*;

g) **ISO 27002** – 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*;

h) **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;

i) **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.

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 Para 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 responsabilidades sobre as ações de segurança da informação da Companhia para com seus usuários em geral (internos e externos), clientes, acionistas e demais envolvidos.

5.1.2.1 Compõem este Comitê os titulares das seguintes unidades organizacionais: Superintendência de Telecomunicações e Informática (coordenador), Unidade de Serviços de Produção e Suporte, Superintendência de *Compliance*, Superintendência de Relacionamento com Cliente, Superintendência de Aquisições e Logística, Superintendência de Pessoas e Diretoria Adjunta Jurídica. Também compõe o comitê o DPO (Data *Protection Office*), que é o encarregado de proteção de dados pessoais da Companhia, conforme exige a LGPD.

5.1.4 Além desta Política, normativos específicos devem ser estabelecidas para definição de padrões técnicos alinhados com as 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 apreciados pelo Comitê Executivo de Segurança da Informação e aprovados pela Diretoria Executiva. Isto posto, devem ser observados e cumpridos pelos que aqui se aplicam.

5.2 Para Informação

5.2.1 Controle de acesso à informação

5.2.1.1 A Companhia deverá estabelecer critérios, procedimentos e responsabilidades para a gestão de acessos, compreendendo regras sobre: quem pode acessar dados, as permissões de cada usuário geral e o controle das ações.

5.2.1.2 Basicamente, o controle e acesso à informação deverá 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) a restrição de acesso à informação;

k) o uso de dispositivos particulares (*smartphones, notebooks e e-mail*).

5.2.1.3 As informações necessárias para as fases de teste e homologação devem ser distintas daquelas do ambiente de produção. Técnicas de mascaramento, anonimização e outras que venham a oferecer resultados semelhantes, devem ser implementadas em todas as fases de testes e homologações.

5.2.2 Para gestão de ativos de informação

5.2.2.1 A responsabilidade pela gestão de ativos de informação é de todos os usuários em geral da Companhia. Recomenda-se que se tenha um controle efetivo de seus ciclos de vida, que sejam realizadas avaliações dos riscos e oportunidades, que atendam aos requisitos regulatórios e apresentem soluções inovadoras e sustentáveis que visem contribuir para a realização dos resultados almejados, em consonância com o planejamento estratégico da Companhia.

5.2.2.2 Ressalta-se que as informações e os contatos que fazem parte dos *e-mails* corporativos também são ativos da empresa, e como tal, merecem o mesmo tratamento relativo à segurança, sendo recomendado que se tenha normas e regras para o uso.

5.2.3 Para classificação da informação

5.2.3.1 Qualquer informação sob responsabilidade da Companhia deve estar classificada conforme o nível de sensibilidade para os seus negócios e controles de acessos específicos devem estar aplicados para garantir os níveis adequados de proteção. As informações de outras partes que estejam em custódia pela COPASA MG devem estar protegidas com o mesmo grau de atenção.

5.2.3.2 A classificação da informação é um procedimento de responsabilidade de todos na Companhia e deve respeitar as diretrizes aqui estabelecidas e os requerimentos da LGPD, na proteção da privacidade das pessoas naturais, com a implementação de controles de segurança adicionais quando necessário.

5.2.3.3 As informações podem ser classificadas conforme o nível de acesso em: confidenciais, privadas, públicas e restritas, sendo:

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 privadas:** serão acessadas mediante autorização de quem as detém;

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;

d) **Informações restritas:** devem ser acessadas por pessoas devidamente identificadas, normalmente são de cunho estratégico e restritas à Direção ou a funções corporativas específicas.

5.2.3.4 As tecnologias e processos de controle e monitoramento a serem implementados, devem garantir o nível adequado de proteção para a informação, de modo que, a confidencialidade, a integridade e a disponibilidade das informações estejam asseguradas, e devem incluir recursos para investigação de eventos de não conformidade de acordo com os padrões implementados pela Companhia.

5.2.4 Para cópias de segurança

5.2.4.1 As informações digitais devem ser copiadas 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.

5.2.4.2 Os critérios de recuperação deverão estar descritos em procedimentos, bem como testes de recuperação devem ser realizados dentro de uma periodicidade de, pelo menos, uma vez por ano, a ser determinada pelo Comitê Executivo de Segurança da Informação.

5.2.4.3 As informações e os sistemas criados, modificados e/ou armazenados na Companhia são considerados ativos pertencentes a ela, e não podem ser copiados, reproduzidos ou enviados externamente sem o prévio conhecimento da Superintendência de Telecomunicações e Informática e o consentimento das Diretorias responsáveis envolvidas, de acordo com as normas e procedimentos específicos.

5.2.4.4 É recomendado que as informações sejam armazenadas em ambiente definido pela Companhia evitando-se, ao máximo possível, o armazenamento nos equipamentos dos usuários, sejam aqueles instalados nas unidades para uso dos empregados e os móveis (*notebooks*) disponibilizados para alguns usuários. Estes direcionamentos são de responsabilidade da Superintendência de Telecomunicações e Informática, e devem considerar os aspectos e características das demais Unidades Organizacionais quanto ao tratamento e armazenamento das informações.

5.2.4.5 Aspectos específicos para período de retenção e de descarte das informações devem considerar os requerimentos regulatórios envolvidos, as definições de segurança da informação e os aspectos dos distintos segmentos de negócios da Companhia.

5.2.4.6 Procedimentos seguros devem ser implementados e monitorados para garantir que o descarte seja efetivo e não permita a recuperação das informações.

5.3 Para o tratamento das informações pessoais

5.3.1 A aplicação desta Política deve garantir o cumprimento do tratamento das informações pessoais, conforme art. 6º e 7º da Lei nº 13.709/18, que dispõe sobre o assunto.

5.4 Para educação e treinamento

5.4.1 Dentro de uma periodicidade a ser definida e documentada, campanhas de conscientização em segurança da informação devem ser realizadas com o objetivo de atingir o máximo dos empregados da Companhia. Para tal, devem ser utilizados os canais de comunicação institucionais existentes.

5.4.2 Segundo a ISO 27002, todos os empregados da Companhia devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções. A conscientização de segurança é obrigatória para todos os empregados, incluindo estagiários, aprendizes, contratados e afins que estejam, de alguma forma, inseridos com os sistemas de TI.

5.4.3 Recomenda-se que haja sinergia entre as unidades de TI, de treinamento e comunicação da Companhia de forma a produzirem material com diversos conteúdos, tais como:

a) uso e gerenciamento de senha, incluindo criação, frequência de troca e proteção; proteção contra vírus, *worms*, cavalos de troia e outros códigos maliciosos;

b) políticas (implicações do não cumprimento);

c) *e-mails* e anexos desconhecidos;

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

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

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

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

h) mudanças no ambiente do sistema;

i) Uso do trabalho em casa;

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

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

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

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

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

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

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

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

r) segurança da área de trabalho.

5.4.4 Independente do conteúdo e método utilizado, os materiais de treinamento devem estar disponíveis para todas as áreas da organização.

5.5 Para encerramento das atividades

A Companhia deve manter uma normatização quanto ao desligamento dos empregados da Companhia no que diz respeito aos ativos digitais que estão sob sua responsabilidade, tais como: *notebook, smartphone, tablet,* celular, *token, pendrive*, disco rígido ou *flash* externo, entre outros, bem como validade das senhas de acesso e a conta corporativa de *e-mail*.

5.6 Para trabalho remoto

5.6.1 A Companhia, caso venha a adotar, deve normatizar o trabalho remoto e para tal deve balizar-se nos requisitos que estão dispostos no Acordo Coletivo vigente, na Consolidação das Leis Trabalhistas e no Código Civil.

5.6.2 A normatização deve esclarecer, além de outros pontos, os pormenores sobre o uso ou não de IP exclusivos, compartilhamento ou não de senhas por usuários terceiros, questões sobre monitoramento dos acessos e os perfis de acesso, bem como a abrangência de cada um dos acessos.

5.7 Para recursos tecnológicos

5.7.1 Toda e qualquer aquisição de sistemas, de equipamentos ou de *software* de mercado, deve 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. Os mesmos procedimentos devem ser utilizados nos casos de desenvolvimento interno de novas tecnologias ou de sistemas de informática.

5.7.2 Todos os recursos tecnológicos, incluindo os de rede de comunicação e telecomunicação de dados, devem ser protegidos 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: investigação ativa de eventos suspeitos, identificação de causa raiz do evento e identificação de incidentes de segurança.

5.7.3 Os administradores de ambiente (rede de comunicação e telecomunicação de dados, banco de dados, sistemas de informática) e gestores de informação não devem ter acessos que permitam alterar diretamente os registros de operações (informações de negócios) ou de eventos citados acima.

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

5.7.5 Para os casos definidos por entidades regulatórias como casos de incidentes de segurança, devem ser adotados processo de registro, de comunicação e de reporte, garantindo a preservação da imagem e reputação da Companhia, dos empregados, de clientes e demais envolvidos.

5.8 Do Plano de Continuidade de Negócios (PCN) e Plano de Contingência

5.8.1 Os planos de continuidade de negócios das unidades e de contingência da Companhia, incluindo aspectos de recuperação de desastre, devem ser elaborados com base na mitigação do risco de indisponibilidade do ambiente produtivo com impacto nas atividades das unidades e consequente impacto para os clientes da Companhia.

5.8.2 Estes planos devem trazer a correta identificação dos ativos críticos da Companhia, os pontos de falhas específicas, e devem estabelecer os processos emergenciais que serão ativados a fim de minimizar os impactos devidos aos eventos pontuais e inesperados.

5.8.3 Todas as ações tomadas e executadas durante os períodos em que estiveram ativos devem ser registradas para fins de investigação da causa raiz e de ações de melhorias na sequência. Estas informações de log deverão estar à disposição para consulta por período a ser definido em norma de procedimento.

5.8.4 Com foco na prestação de serviços, o plano de continuidade das unidades deve indicar as ações emergenciais que serão acionadas para permitir que a Companhia possa garantir os compromissos firmados com seus clientes e, quando aplicável, com os órgãos reguladores relacionados com o tipo de serviço prestado.

5.8.5 Para a elaboração do Plano de Continuidade de Negócios – PCN, as unidades devem levantar os eventos que, em ocorrendo isoladamente ou combinados, impactam nas atividades e devem indicar as ações emergenciais que são necessárias para permitir seu trabalho de forma limitada ou integral. São exemplos de eventos: falhas em equipamentos, na rede, nos sistemas de informática, as ameaças internas ou externas ou aos ambientes estruturais ou cibernéticos. Um mapa de risco, bem como um Plano de Resposta ao Risco devem ser implementados e atualizados constantemente.

5.8.6 Com foco em tecnologia, o Plano de Contingência deve ser definido e implementado para garantir a continuidade das operações da Companhia, ou seja, suportar os planos de continuidade das unidades previamente documentado, e deve ter procedimentos claros e efetivos para a recuperação do ambiente em casos de desastres (diversas naturezas e distintos graus de severidade), e também deve garantir o retorno ao estado operacional regular.

5.8.7 As simulações ou testes monitorados devem ser realizados periodicamente para garantir a eficácia das contingências, em periodicidade a ser determinada pelo Comitê Executivo de Segurança da Informação, que deverá considerar o risco do negócio.

5.9 Fornecedores e prestadores de serviços

5.9.1 O processo de gestão de fornecedores e de prestação de serviço deve incluir as diretrizes de segurança da informação para garantir que as informações da Companhia estejam protegidas de acordo com os parâmetros de segurança e privacidade por ela indicados.

5.9.2 Os contratos, em geral, estão relacionados com prestação de serviços e/ou mão-de-obra, fornecimento de sistemas de informática, de infraestrutura de tecnologia, de processamento e armazenamento de informações. As cláusulas são elaboradas com foco em segurança e proteção da informação e da privacidade, e devem incluir:

a) a indicação de que mecanismos e controles de segurança serão implementados e controlados pelos fornecedores ou prestadores de serviços, para preservação da confidencialidade, da disponibilidade e da integridade das informações da Companhia durante os serviços contratados e também durante um período definido entre as partes após o encerramento do contrato, denominado período de quarentena;

b) a indicação de que são adotadas medidas técnicas e administrativas, visando garantir a privacidade e proteção dos dados pessoais que sejam tratados em virtude da relação contratual, seguindo todos os requisitos previstos na legislação vigente;

c) a indicação de que toda criação, invenção e desenvolvimento de aplicativos, de processos, de sistemas, de produtos e de serviços realizados durante a prestação de serviço serão transferidos para a Companhia. As exceções devem ser definidas em acordos especiais e formais, bem como fazer constar em documento contratual ou similar;

d) a garantia de que a Companhia possa acessar o ambiente do fornecedor ou prestador de serviços para realização de avaliação anual ou eventual, para validar os controles de segurança e privacidade requeridos. Esta avaliação pode ser realizada pela própria Companhia ou por quem ela designar como sua representante para este fim.

5.10 Para acesso físico às instalações da Companhia

5.10.1 Assim como as informações, os ativos físicos da Companhia devem estar protegidos contra acesso físico não autorizado, danos, perdas, furtos e outros eventos de natureza interna e externa que possam trazer impacto às operações da empresa. 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 aos empregados e aos terceiros formal e previamente autorizados 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. Recomenda-se o uso de biometria para o controle de acesso e câmeras com registro das movimentações;

c) as salas técnicas onde são instalados os equipamentos de conectividade também devem merecer atenção quanto à segurança e devem ser, de alguma forma, monitoradas, uma vez que constitui ponto nevrálgico, onde o acesso indevido pode ocasionar intrusão.

6 COMPETÊNCIAS

6.1 Do Conselho de Administração e da Diretoria Executiva

6.1.1 Por padrão, a alta administração (Conselho de Administração e Diretoria Executiva) representa o primeiro nível de comprometimento com esta Política e deve apoiar suas metas e princípios, de forma a patrocinar sua comunicação, aplicabilidade e efetividade em todos os níveis da Companhia que tratam informações.

6.2 Do Comitê Executivo de Segurança da Informação

6.2.1 O Comitê Executivo de Segurança da Informação é responsável pelo direcionamento e acompanhamento das ações e incidentes de segurança da Companhia, do monitoramento das ações implementadas para cumprimento desta Política e também por aprovar situações que, por ventura, não foram previstas no presente documento, uma vez que possui a alçada necessária para tal procedimento.

6.2.2 Este Comitê deve propor soluções específicas sobre segurança da informação, conduzir 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.

6.2.3 Compete, ainda, ao Comitê elaborar ou delegar a elaboração de normas específicas e necessárias à implementação desta Política.

6.2.4 É responsabilidade do Comitê Executivo de Segurança da Informação apoiar a alta administração da Companhia no planejamento de investimentos em segurança da informação com base nas exigências estratégias e legais.

6.3 Da segurança da informação

6.3.1 Caso a Companhia opte por ter uma unidade ou equipe de Segurança da Informação ou entender que as atribuições a seguir possam ser atribuídas a empregado ou a um grupo constituído de empregados, juntamente com o Grupo de Segurança da Informação, estes deverão:

a) responsabilizar-se pelo direcionamento, pelo acompanhamento e pelo monitoramento das ações de proteção da informação em todos os seus níveis, interagindo diretamente com as unidades responsáveis pelos processos (TI e demais unidades organizacionais da Companhia) para 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 divulgação de práticas e recomendações de segurança da informação;

e) avaliar constantemente as condições de segurança de redes por meio de reuniões semanais e verificação das conformidades;

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

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, se identificados, aplicadas sanções penais, administrativas e civil vigentes.

6.4 Dos gestores das informações

a) responsabilizar-se pelas informações dos sistemas utilizados pelas unidades, e ainda ter conhecimento completo das práticas de segurança da informação durante 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.

6.5 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) recomendar que haja um monitoramento sobre os incidentes de natureza física e lógica e que este monitoramento resulte em indicadores que possam ser utilizados para melhoria e prevenção dos riscos.

6.6 Dos gestores de riscos e incidentes

a) estabelecer processos de Gestão de Riscos de Segurança da Informação que possibilitem a identificação das ameaças e redução das vulnerabilidades dos ativos da informação e dos eventuais impactos provocados por incidentes;

b) estabelecer o mapeamento dos riscos, seus fatores, causas e possíveis consequências, com intuito de mitigar as possíveis ameaças;

c) elaborar o Plano de Resposta ao Risco para cada um dos riscos apontados nas matrizes de risco. Estes planos devem conter indicadores, estratégias, bem como as medidas necessárias para o tratamento do risco.

6.7 Dos usuários

a) representar os principais agentes de proteção das informações da Companhia. Atuam como custodiantes dos ativos de informação e, consequentemente, devem observar o cumprimento desta 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) cuidar dos recursos de tecnologia à sua disposição, agindo com responsabilidade e respeito às diretrizes estabelecidas pela Companhia;

d) 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.

7 DISPOSIÇÕES FINAIS

7.1 Esta Política deverá ser revisada anualmente, para alteração 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 23/05/2024, 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.

Unidade gestora do documento: Superintendência de Telecomunicações e Informática.

Instância de revisão: Diretoria Executiva.

Instância de aprovação: Conselho de Administração.