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 elas 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 OBJETIVO

Garantir a continuidade dos serviços prestados à população de uma forma geral ao estabelecer princípios, conceitos, diretrizes e responsabilidades por meio de um planejamento de atividades que, sob a coordenação da Superintendência de Telecomunicações e Informática, tem a finalidade de orientar o restabelecimento funcional da base de dados, arquivos, serviços ou atividades da Companhia, provocado por qualquer incidente de segurança cibernética e da informação, de forma que estes sejam tratados adequadamente, bem como reduzido, ao máximo, os impactos provocados para o negócio da Companhia.

3 REFERÊNCIAS

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

a) ABNT NBR ISO 22301:2020 – Segurança e Resiliência – Sistema de gestão de continuidade de negócios – Requisitos, traduzida pela Associação Brasileira de Normas Técnicas (ABNT);

b) ABNT NBR ISO/IEC 27001:2013 – Norma internacional de segurança da informação (2005) traduzida pela Associação Brasileira de Normas Técnicas (ABNT);

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

d) Guia de Resposta a Incidentes de Segurança – Programa de Privacidade e Segurança da Informação do Governo Federal, Versão 3.2, maio de 2024;

e) NIST (National Institute of Standards and Technology) SP (Special Publication) 800-30 – Risk Managemente Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology;

f) NIST (National Institute of Standards and Technology) SP (Special Publication) 800-

39 – Managing Information Security Risk - Organization, Mission, and Information System View;

g) Política Segurança da Informação da COPASA MG**;**

h) Código de Conduta e Integridade da COPASA MG.

4 DEFINIÇÕES

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

a) **Agentes de tratamento -** correspondem ao Controlador e Operador. Não são considerados controladores ou operadores os indivíduos subordinados, tais como os empregados ou as equipes de trabalho de uma organização, uma vez que atuam sob o poder diretivo do agente de tratamento;

b) **Anonimização -** é a utilização de meios técnicos razoáveis e disponíveis por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

c) **Ataque -** evento de exploração de vulnerabilidades, que ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

d) **Autoridade Nacional de Proteção de Dados (ANPD) -** é o órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados Pessoais em todo o território brasileiro;

e) **Bot -** código malicioso o qual permite que o invasor controle remotamente o computador ou dispositivo que hospeda;

f) **Colaborador -** entende-se como colaborador qualquer pessoa que trabalhe para a COPASA MG, seja na condição de: administradores, membros de comitês, conselheiros fiscais, empregados, terceirizados, estagiários, aprendizes e aqueles que exercem mandato, cargo, emprego ou função, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, convênio, contratação ou qualquer outra forma de investidura ou vínculo;

g) **Controlador -** toda pessoa física ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais;

h) **Dados pessoais sensíveis -** são dados pessoais que dizem respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

i) **Dados pessoais -** qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente, por conta própria ou quando combinada com outras informações;

j) **Encarregado ou *Data Protection Officer* (DPO) -** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

k) **Gestor -** Colaborador que exerce cargo de liderança, tal como presidente, vice-presidente, diretor, superintendente, gerente, coordenador, líder ou supervisor;

l) **Incidente -** evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

m) **Incidente de segurança -** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

n) **Incidente de segurança com dados pessoais -** de acordo com a ANPD, incidente de segurança à proteção de dados pessoais é qualquer evento adverso, confirmado, que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados;

o) **Incidentes de Segurança da Informação -** são considerados quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais princípios básicos de segurança da informação: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio e seus objetivos em risco;

p) **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;

q) **IP:** Protocolo da Internet (*Internet Protocol*), número utilizado para identificar um dispositivo de tecnologia da informação em uma rede, ou Internet;

r) **Log -** processo de registro de eventos relevantes de um determinado sistema computacional;

s) **Malware -** é um termo genérico para qualquer tipo de "*malicious software*" ("software malicioso") projetado para se infiltrar em dispositivos eletrônicos sem o devido conhecimento do usuário. Existem muitos tipos de malware, e cada um funciona de maneira diferente na busca de seus objetivos;

t) **Operador -** é toda pessoa física ou jurídica, de direito público ou privado, que

realiza o tratamento de dados pessoais em nome do Controlador;

u) **Plano de Resposta a Incidentes Cibernéticos:** é um documento estratégico e detalhado que descreve o conjunto de medidas/ações ou deveres a serem executados pelos atores envolvidos em: identificar incidentes cibernéticos e suas causas, executar medidas de contenção, retomada do(s) ambiente(s) paralisado(s), correção das vulnerabilidades identificadas e registro do(s) evento(s) ocorrido(s);

v) **Porta -** uma porta de conexão está sempre associada a um endereço IP de um host e ao tipo de protocolo de transporte utilizado para a comunicação. Exemplo: o servidor de e-mail que executa um serviço de SMTP usa a porta 25 do protocolo TCP;

w) **Recurso -** Qualquer ativo, tangível ou intangível, pertencente a serviço ou sob responsabilidade da COPASA MG, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados em nuvem, sistemas e processos;

x) **Sistemas -** *hardware, software*, rede de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pela COPASA MG para dar suporte na execução de suas atividades;

y) **Tratamento -** qualquer operação ou conjunto de operações efetuadas sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização.

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:

a) todos os sistemas corporativos devem possuir Acordo de Nível de Serviço – ANS (SLA – *Service Level Agreement*) previamente convencionado entre as partes de usuários proprietários do sistema e a Superintendência de Telecomunicações e Informática que disponibiliza a aplicação ou o serviço;

b) o SLA de cada sistema corporativo deve contemplar, de forma clara e objetiva, o tempo máximo tolerável em que o serviço pode ficar indisponível, de acordo com a sua criticidade;

c) todos os colaboradores devem estar devidamente treinados para identificar incidentes de segurança da informação quando for testemunhado;

d) todos os colaboradores devem notificar qualquer evento que possa colocar em risco de segurança ou fragilidade, podendo causar: prejuízos, interrupções, maus

funcionamentos, imprecisão ou vazamento de informação nos sistemas da COPASA MG;

e) as vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos colaboradores, sob o risco de violar a Política de Segurança da Informação, bem como provocar danos aos serviços ou recursos tecnológicos da Companhia;

f) o rol a seguir exemplifica, mas não esgota, os possíveis incidentes de segurança da informação tratados nesta política:

f.1) todo evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, bem como estruturas físicas e lógicas associadas, que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

f.2) indisponibilidade do ambiente tecnológico em virtude de ataques maliciosos internos e/ou externos;

f.3) vazamento de informações confidenciais (informações de clientes/colaboradores/terceiros, informações estratégicas, outros);

f.4) tentativas internas ou externas de ganhar acesso não autorizado a sistemas, a dados ou até mesmo comprometer o ambiente de TI;

f.5) ato de violar uma política de segurança, explícita ou implícita;

f.6) uso ou acesso não autorizado a um sistema de informações;

f.7) modificações em um sistema de informações, sem o conhecimento, instruções ou consentimento prévio do proprietário do sistema;

f.8) compartilhamento de senhas;

g) o conteúdo da notificação precisa ser claro, em formato simples e deve incluir as informações necessárias para a rápida e correta identificação do problema e da ação requerida;

h) os eventos de incidente de segurança da informação devem ser categorizados e classificados por meio de uma matriz de severidade, que deverá constar no Plano de Resposta a Incidentes Cibernéticos, com intuito de se ter uma melhor visibilidade, tratamento e prioridade quanto a sua gestão. Este Plano deverá ser elaborado pela Superintendência de Telecomunicações e Informática;

i) os eventos abaixo não são considerados eventos de segurança da informação:

i.1) eventos acidentais (falhas de *hardware* ou sistêmicas), não intencionais;

i.2) eventos não maliciosos (erro humano ou descuido que não infrinja as regras de segurança da informação).

j) todo e qualquer incidente que se caracterize como uma crise (extrema severidade) deve seguir o Plano de Resposta a Incidentes Cibernéticos da COPASA MG;

k) todos os eventos de incidente de segurança da informação devem ser registrados nos controles e/ou ferramentas para a devida triagem e tratamento;

l) a gestão de incidentes de segurança da informação deve contemplar processos que atendam aos seguintes atributos:

l.1) detecção: identificação de incidentes por meio de monitoração, relatórios, denúncias, informações obtidas de unidades parceiras ou qualquer outra análise de eventos adversos;

l.2) registro e análise: registro dos incidentes, análise, classificação quanto ao tipo, severidade e priorização;

l.3) comunicação: comunicação do incidente às partes envolvidas e, caso necessário, entidades externas;

l.4) resposta: contenção do incidente, análises forenses (se necessário), custódia de evidências, tratamento do incidente e da causa raiz;

l.5) finalização: encerramento formal e análise "*pós mortem*" para identificação de possíveis melhorias em processos, controles e na própria Gestão de Incidentes.

m) é de extrema importância que o horário de servidores e equipamentos de redes estejam sincronizados com uma fonte confiável de tempo (ex: via protocolo NTP que pode ser baseado em uma fonte precisa de tempo, como os relógios atômicos do Observatório Nacional, que definem a Hora Legal Brasileira), para que não haja disparidades na correlação de eventos, logs e outros dados;

n) violações ou tentativas de violação de diretrizes da Política de Segurança da Informação, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança da informação;

o) incidentes de segurança podem ser identificados por processos de monitoração da área de infraestrutura por colaboradores que observem fragilidades, anomalias e violações que coloquem a segurança da Companhia em risco;

p) todos os incidentes de segurança da informação devem ser documentados, classificados, priorizados de acordo com a criticidade da COPASA MG e comunicados aos gestores responsáveis.

q) deve ser definido um plano de comunicação de incidentes de segurança da informação que esteja de acordo com a classificação e o nível de criticidade do incidente. Em casos mais simples e de baixa criticidade, apenas o gestor responsável pelo recurso ou informação deve ser comunicado. Em casos mais graves a Diretoria Executiva, a unidade Jurídica, Auditoria ou outras unidades organizacionais pertinentes devem ser comunicadas;

r) a investigação de incidentes de Segurança da Informação deve ser realizada exclusivamente pela Superintendência de Telecomunicações e Informática e pelo DPO, quando envolverem dados pessoais, de forma a garantir a privacidade e o sigilo das informações obtidas;

s) sendo necessárias informações ou levantamentos, para os quais devam ser analisadas trilhas de auditoria (logs), acessos à *Internet*, fluxo de mensagens ou conteúdo de caixas de correio, ou outras informações que coloquem em risco a privacidade de colaboradores e o sigilo das informações da COPASA MG, deve ser aberto um incidente junto a Superintendência de Telecomunicações e Informática e ao DPO, para que estes realizem as investigações, observando sempre a legislação afeta;

t) as informações obtidas e arquivadas oriundas do processo de gestão de incidentes de segurança da informação devem ser protegidas de forma a garantir a privacidade de colaboradores e o sigilo das informações do grupo, não podendo ser fornecidas a outras unidades organizacionais ou auditorias;

u) a identificação de incidentes de segurança pode ocasionar o corte imediato dos acessos de colaboradores envolvidos ou a desconexão de sistemas, de forma preventiva, até que sejam concluídas as investigações necessárias e tomadas as medidas corretivas necessárias;

v) o acesso às evidências e relatório de incidentes de segurança da informação é permitido apenas a Superintendência de Telecomunicações e Informática, ao DPO e aos Gestores diretamente envolvidos nos incidentes;

w) a documentação de incidentes, resultados de investigações, evidências e suas soluções devem ser atualizadas logo após a conclusão do tratamento do incidente;

x) o contato para a notificação de incidentes de segurança da informação deve ser feito diretamente a Superintendência de Telecomunicações e Informática e ao DPO por meio de canais previamente definidos;

w) a gestão de incidentes, deverá possuir um escopo ou limites de atuação bem definidos por meio dos grupos e equipes de trabalhos descritos nesta Política, os quais terão atribuições e responsabilidades delimitadas.

z) as atividades inerentes ao escopo da gestão de Incidentes, deverão ser documentadas por meio de um plano desenvolvido pelos grupos de trabalho e equipes envolvidas, o qual deverá contemplar, ao menos, os seguintes itens:

z.1) detectar e registrar incidentes;

z.2) diagnosticar e investigar incidentes;

z.3) restaurar os serviços afetados e seus itens de configuração para a qualidade acordada;

z.4) gerenciar e documentar registros de incidente;

z.5) comunicar com as partes interessadas relevantes de acordo com o ciclo de vida do incidente;

z.6) revisar incidentes e iniciar melhorias nos serviços e na prática de gerenciamento de incidentes depois da resolução.

aa) as atividades descritas no Plano de Gestão de Incidentes que serão executadas pelas equipes envolvidas, poderão impactar toda a Companhia, objetivando uma maior eficiência e produtividade na resolução dos eventos. Consequências adversas poderão ser evidenciadas, como por exemplo, a paralisação ou interrupção do funcionamento dos serviços, aplicativos ou sistemas, até que a solução definitiva seja encontrada e todos os serviços restabelecidos;

bb) as equipes envolvidas trabalharão em busca da solução dos problemas de forma a buscar o melhor nível de atendimento de serviço (SLA) programado, mantendo todos os integrantes envolvidos sempre atualizados periodicamente sobre o andamento dos trabalhos, com o objetivo de apresentar melhor visibilidade e transparência aos fatos.

6 COMPETÊNCIAS

6.1 Do Conselho de Administração e da Diretoria Executiva: 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: instituído por meio da Política de Segurança da Informação, é responsável pelo direcionamento e acompanhamento das ações e incidentes de segurança na Companhia, deverá também respaldar as ações da Equipe de Tratamento e Resposta a Incidentes Cibernéticos, atuar como porta-voz aos órgãos externos referente ao tratamento de crises cibernéticas, gerenciar e propor alterações desta Política.

6.3 Do Grupo de Trabalho de Segurança da Informação:

a) deverá ser definido pela Superintendência de Telecomunicações e Informática com no mínimo um representante de cada unidade organizacional subordinada a ela. O grupo será responsável por recomendar e disseminar as práticas de segurança propostas no âmbito da Companhia, bem como discutir sobre os assuntos relacionados às novas implementações e avaliação dos novos incidentes que tenham ocorrido, propondo ações para mitigar os riscos de segurança e ataques cibernéticos;

b) manter, gerenciar e acompanhar os processos de segurança da informação, das bases de dados, dos sistemas de informação e de proteção de dados.

6.4 Da Equipe de Tratamento e Resposta a Incidentes Cibernéticos: deverá ser definida pela Superintendência de Telecomunicações e Informática para manter e gerenciar os processos de segurança da informação, as bases de dados, os serviços e sistemas de informação em perfeito funcionamento, bem como receber, analisar, documentar e responder as notificações e atividades relacionadas a incidentes de segurança da informação em todo o ambiente tecnológico.

6.5 Da Superintendência de Telecomunicações e Informática e do DPO (*Data Protection Officer*), efetuar:

a) condução do processo de Gestão de Incidentes de Segurança da Informação;

b) investigação de incidentes, levantamento, cadeia de custódia e segurança das evidências;

c) acompanhamentos dos planos de tratamento junto aos responsáveis pelos incidentes e criação de indicadores e relatórios;

d) comunicação aos Gestores responsáveis;

e) realização de análises pós-incidentes (*post mortem*) para identificação e tratamento de causas raiz e aprimoramento de processos da empresa e do próprio processo de gestão de incidentes de segurança da informação.

6.6.1 Das unidades subordinadas a Superintendência de Telecomunicações e Informática efetuar:

a) provimento dos acessos necessários para que a Superintendência de Telecomunicações e Informática e o DPO possam realizar a identificação e investigação de incidentes de segurança;

b) provimento de trilhas de auditoria e evidências para a investigação de incidentes;

c) suporte às investigações por meio do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da unidade.

6.7 Dos Gestores das demais Unidades Organizacionais: ao serem notificados sobre incidentes que envolvam recursos ou informações sob sua responsabilidade, devem colaborar com eventuais investigações e tratar os incidentes com a devida urgência e SLAs pré-definidos pela Superintendência de Telecomunicações e Informática e pelo DPO.

6.8 Da Diretoria Adjunta Jurídica: prestar o apoio às questões legais relacionados a incidentes de segurança da informação, levando sempre em consideração os prazos e cronogramas previamente definidos, priorizando os fatos com a devida urgência.

6.9 Da Superintendência de *Compliance:* prestar o apoio às questões pertinentes a conformidade dos fatos com as normas e Leis vigentes, relacionadas a incidentes de segurança da informação, levando sempre em consideração os prazos e cronogramas previamente definidos, priorizando os fatos com a devida urgência.

6.10 Da Superintendência de Comunicação Institucional: realizar todo o processo de comunicação dos fatos relacionados a incidentes de segurança da informação, junto aos órgãos reguladores, agência de fiscalização, bem como todos os interessados e a sociedade de um modo geral, utilizando os devidos meios de comunicação disponíveis, sempre em consonância com o que determina a lei e, sobretudo, levando sempre em consideração os prazos e cronogramas previamente definidos, priorizando os fatos com a devida urgência

6.11 Da Superintendência de Pessoas: prestar o apoio necessário às questões pertinentes a incidentes de segurança da informação que afetem diretamente os colaboradores ou a base de dados de informação.

6.12 Dos usuários: informar imediatamente à Superintendência de Telecomunicações e Informática e ao DPO todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

7 DISPOSIÇÕES FINAIS

7.1 Esta Política deverá ser revisada anualmente, para alteração de normas 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 24/07/2024, 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 24/07/2024.

Versão 1: revisão, sem alteração de conteúdo, conforme relatório do *Compliance* n.º 069 de 20/05/2025.

Unidade gestora do documento: Superintendência de Telecomunicações e Informática.

Instância de revisão: Diretoria Executiva.

Instância de aprovação: Conselho de Administração.