

Título **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA SANEAGO**

Objetivo Definir o tratamento dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente de tecnologia da Companhia de Saneamento de Goiás S.A. – Saneago.

Aplicação Todas as Unidades Organizacionais da Saneago

1 – OBJETIVO

As orientações aqui apresentadas são os princípios fundamentais para nortear a definição de procedimentos, instruções normativas e instruções de trabalho alinhados à segurança da informação exigida pela companhia, bem como a implementação de controles e processos para seu atendimento.

2 – GLOSSÁRIO

| Termo | Definições |
|---|---|
| Ameaça | Agentes ou condições causadoras de incidentes de segurança. Exploram as vulnerabilidades em sistemas e serviços. |
| Ativo | Tudo aquilo que possui valor, monetário ou não, para a Saneago e conseqüentemente exige proteção. |
| Autenticidade | Garantia de que o dado ou informação são verdadeiros. |
| Backup | Processo de salvaguarda de dados com o objetivo de amenizar os efeitos decorrentes da perda dos originais. |
| Classificação da Informação | Processo de identificar e definir níveis e critérios de proteção adequados para as informações de forma a garantir sua confidencialidade, integridade e disponibilidade. |
| Código de Conduta | Regras e práticas internas adotadas pela Saneago, no sentido de mantê-la atualizada às legislações vigentes, buscando padrões de transparência, confiabilidade e plenitude ética em todas suas transações e relacionamentos. |
| Confidencialidade | Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados. |
| Controle de Acesso | Restrições de acesso a um ativo da Saneago. |
| Comitê Gestor de Segurança da Informação e de Privacidade e Proteção de Dados Pessoais (SIPDP) | Instância responsável pela elaboração e revisão periódica da Política de Segurança da Informação e normas relacionadas. Auxilia os departamentos da empresa na implementação das ações de segurança da informação. |
| Controle de Segurança | Práticas de gestão de risco (políticas, normas, procedimentos ou mecanismos) que podem proteger os ativos contra ameaças, reduzir ou eliminar vulnerabilidades e limitar o impacto de um incidente de segurança. |
| Disponibilidade | Propriedade de que a informação esteja acessível e utilizável quando demanda. |
| Gestor de UO | Responsável por uma Unidade Organizacional da companhia. |
| Gestor da Informação | Pessoa responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação. Cada informação deverá ter o seu Gestor que será indicado formalmente pela Superintendência responsável pelos sistemas que acessam a informação. |
| Gestão de risco | Atividade contínua de identificação, análise, tratamento, aceitação e comunicação de riscos. |
| Incidente de Segurança | Qualquer evento que resulte no descumprimento da Política de Segurança da Informação e que possa representar uma ameaça. |
| Integridade | Garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais. |
| Log | Registro de eventos ocorridos nos sistemas computacionais. Deve conter: data e hora da atividade, identificação do usuário, do computador e dos procedimentos executados. |
| Monitoramento | Acompanhamento de eventuais ameaças, incidentes de segurança ou quaisquer descumprimentos às diretrizes presentes na Política, Normas ou Procedimentos de Segurança da Informação. |
| Privacidade | Condição daquilo que é privado, pessoal, íntimo. |
| Plano de Continuidade Operacional de TI | Documento que define o processo de gestão da capacidade da Saneago manter um nível de funcionamento adequado até o retorno à situação normal, após a ocorrência de incidentes e interrupções de sistemas críticos. |

| Termo | Definições |
|--------------------------------|--|
| Plano de Resposta a Incidentes | Documento que estabelece ações que visam minimizar o impacto de um incidente e permitir o restabelecimento dos serviços o mais rápido possível. |
| Risco | Probabilidade de uma determinada ameaça se concretizar. |
| Segurança da Informação | Conjunto de medidas voltadas a salvaguardar dados e informações sigilosos gerados, armazenados e processados por intermédio da informática, bem como a própria integridade dos sistemas utilizados pela companhia. |
| Vulnerabilidade | Fragilidades associadas aos ativos que os tornam suscetíveis às ameaças. |

3 – DOCUMENTOS REFERÊNCIA

- ISO/IEC 27001:2013
- Código de Conduta e Integridade da Saneago.
- Lei Geral de Proteção de Dados – Lei 13.709/2018.

4 – PRINCÍPIOS

4.1 – A informação utilizada pela Saneago é um bem que tem valor. Ela deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, legalidade e auditabilidade, independente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

4.2 – As unidades organizacionais da Saneago deverão implantar medidas técnicas/organizacionais adequadas, visando garantir a proteção de todos os dados, estejam eles em qualquer formato.

4.3 – As ações deverão se nortear pelos seguintes princípios:

- Simplicidade:** A complexidade aumenta a chance de erros, portanto todos os controles de segurança deverão ser simples e objetivos.
- Privilegio Mínimo:** Usuários devem ter acesso apenas aos recursos de tecnologia da informação necessários para realizar as tarefas que lhe foram designadas.
- Privacidade desde a concepção:** Buscar a privacidade e garantir a proteção dos dados desde sua concepção e durante o seu ciclo de vida.
- Segregação de função:** Funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos.
- Necessidade:** Limitação do tratamento de dados ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- Auditoria:** Toda mudança ou eventos significantes de usuários e processos devem ser rastreáveis até o evento inicial por meio de registro consistente e detalhado.
- Resiliência:** Os controles de segurança devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre.
- Backup:** A utilização de backups, para promover a segurança e a disponibilidade da informação, será priorizada pela companhia, no entanto, a pesquisa dentro deles só deve ser realizada se especificamente solicitado por um indivíduo autorizado com uma Solicitação de Acesso oficial.
- Conformidade e Legalidade:** Aderência a contratos, padrões normativos e legislações vigentes e cabíveis.
- Defesa em profundidade:** Os controles de segurança devem ser concebidos em múltiplas camadas de modo a prover redundância para que, no caso de falha, outro controle possa ser aplicado.
- Criptografia:** Os controles de segurança deverão primar pelo uso de sistemas criptográficos no tratamento de dados pessoais e informações sigilosas, inclusive nos meios de comunicação móvel.

5 – DIRETRIZES

5.1 – Inventário de Ativos

5.1.1 – Todo ativo da companhia deve ser inventariado e permanentemente controlado para fins de auditoria e segurança dos mesmos.

5.1.2 – Toda pessoa que opera o ativo é responsável por assegurar que a informação relacionada a este ativo está protegida.

5.2 – Ciclo de vida da informação

5.2.1 – Medidas de proteção devem ser adotadas durante todo o ciclo de vida da informação, compreendendo as fases de coleta/criação, **tratamento**, armazenamento, transporte e descarte.

5.3 – Proteção de dados

5.3.1 – Toda informação, bem como a privacidade do seu titular deve ser protegida para que não seja alterada, acessada e destruída indevidamente.

5.3.2 – A informação, **que possua valor para companhia**, deve ser protegida contra desastre físico (fogo, água, calor, fenômenos da natureza, etc.) e desastre lógico (vírus, alteração indevida de informação, etc.).

5.4 – Classificação da Informação

5.4.1 – Toda informação que faz parte de um processo deve ser classificada de acordo com sua importância para a Saneago, ou seja, em termos de valor, sensibilidade e grau de criticidade, observadas as necessidades do negócio e a legislação em vigor, para evitar modificação e/ou divulgação não autorizada.

5.5 – Confidencialidade da Informação ou de não divulgação

5.5.1 – A confidencialidade da informação deve ser mantida durante todo o seu ciclo de vida.

5.5.2 – Todo colaborador, estagiário, prestador de serviço deve conhecer e ser signatário do Acordo de Confidencialidade da Saneago.

5.5.3 – Toda negociação ou troca de informações confidenciais em ambiente externo só poderão ser realizadas após assinatura do Acordo de Confidencialidade da Saneago pela parte envolvida.

5.6 – Acesso a sistemas

5.6.1 – O acesso aos sistemas e recursos de tecnologia é de uso individual e intransferível.

5.6.2 – A solicitação de acesso a qualquer sistema ou recurso de tecnologia deverá seguir as instruções normativas pertinentes.

5.6.2.1 – Esta solicitação **poderá passar** por análise da equipe de segurança da informação, que poderá deferir ou não o pedido, levando em conta os princípios destacados no item **4**, bem como melhores práticas de segurança.

5.6.3 – O acesso a sistemas e recursos deve ser autorizado apenas para os usuários que necessitem destes para o desempenho das atividades institucionais.

5.6.4 – A utilização dos recursos de tecnologia, com finalidade pessoal, não será permitida em nenhum aspecto.

5.6.5 – *Em caso de desligamento do empregado, a Saneago tomará imediatamente medidas de segurança para restringir o acesso aos sistemas, com o objetivo de prevenir qualquer vazamento de dados. A partir da comunicação da dispensa, o empregado perderá o acesso a todos os equipamentos e sistemas da empresa.*

5.6.6 – *Durante o período de interrupção e suspensão do contrato de trabalho, o acesso do usuário aos sistemas será bloqueado, com exceção das funções de consulta ao sistema de Administração de Pessoal a ele pertinentes (Contracheque, Consultar Rendimentos, etc).*

5.7 – Continuidade da informação

5.7.1 – Toda informação crítica para o funcionamento das atividades da Saneago deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção adequada. O Gestor da Informação é responsável pela definição da criticidade.

5.7.2 – Todos os procedimentos que possibilitam a proteção da informação e a continuidade do seu uso devem ser documentados, de tal forma que possibilite que a Saneago continue a operacionalização desses procedimentos, mesmo na ausência do técnico responsável.

5.7.2.1 – O **Plano de continuidade operacional de TI** estabelece as diretrizes prévias e decisões que devem ser tomadas para reduzir o impacto negativo que pode ser causado por uma situação desastrosa.

5.8 – Segurança Física

5.8.1 – Os locais onde se encontram os recursos tecnológicos da Saneago devem ter proteção e controle de acesso físico compatível com o seu nível de criticidade e será de responsabilidade da superintendência gestora do recurso validar a solução com a Coordenação de Segurança da Informação - G-CSG.

5.9 – Dispositivos pessoais

5.9.1 – Não será permitido sob nenhuma hipótese o uso de computadores pessoais e notebooks para o desenvolvimento de atividades corporativas nas dependências da Saneago.

5.9.2 – A proteção de dispositivos como smartphone e tablets de uso particular é de responsabilidade do proprietário do equipamento.

5.9.3 – *A instalação ou o uso de dispositivos de comunicação de dados que não sejam homologados pela Ger. de Infraestrutura e Segurança da Informação (G-GSI) ou que não possuam contrato formalizado com a Saneago é estritamente proibido em qualquer computador ou rede da companhia. Exemplos incluem, mas não se limitam a, modems, roteadores, antenas e outros equipamentos de transmissão de dados ou voz não autorizados.*

5.9.4 – *A Saneago não recomenda e nem se responsabiliza por arquivos pessoais armazenados nas estações de trabalho.*

5.10 – Política da mesa limpa e da tela limpa ou bloqueada

5.10.1 – *A Saneago adota políticas de mesa limpa para papéis e mídias de armazenamento removíveis, recomendando que nenhum documento confidencial ou que contenha dados pessoais seja deixado sobre as mesas.*

5.10.2 – *A Saneago adota uma política de tela limpa com o objetivo de proteger informações sensíveis ou confidenciais exibidas nas telas de computadores, prevenindo acessos, visualizações e alterações não autorizadas. O empregado deve bloquear sua estação de trabalho sempre que se ausentar e tomar as medidas necessárias para garantir que pessoas não autorizadas não tenham acesso visual a essas informações.*

5.11 – Utilização de e-mail e monitoramento

5.11.1 – *A utilização de e-mail corporativo deverá ser única e exclusivamente para a execução do trabalho. Não será permitido acesso a e-mails particulares e a sites pessoais dentro do ambiente de trabalho com o computador da empresa.*

5.11.2 – *A empresa utiliza ferramentas de monitoramento de acesso dos seus empregados. Este monitoramento tem a finalidade de mitigar riscos de vazamento de dados pessoais, por algum tipo de acesso a sites indevidos ou a e-mails com spam, que porventura venham a comprometer a segurança das informações da Saneago.*

6 – DOCUMENTOS COMPLEMENTARES

6.1 – A Política de Segurança da Informação tem caráter corporativo e sua estrutura prevê os seguintes documentos normativos:

- a) Procedimento de classificação das informações;
- b) Norma para acesso físico ao data center e áreas críticas;
- c) Norma para gestão de senhas e credenciais privilegiadas;
- d) Norma para acesso à rede corporativa e internet;
- e) Norma para uso seguro do correio eletrônico;
- f) Norma para acesso remoto;
- g) Norma para retenção de logs e monitoramento de utilização de serviços e ativos;
- h) Norma para uso de equipamentos corporativos e pessoais;
- i) Norma para privacidade dos dados e criptografia;
- j) Norma de controle de acesso aos sistemas;
- k) Norma para aquisição, desenvolvimento e manutenção de sistemas;
- l) Norma para gestão e resposta a incidentes de segurança;
- m) Norma para proteção à propriedade intelectual;
- n) Cartilha de segurança da informação;
- o) Plano de Continuidade **Operacional de TI**;
- p) Plano de Resposta a Incidentes de Segurança;
- q) Política de Privacidade e Proteção de Dados.

6.2 – Os empregados devem estar cientes das regras descritas no conjunto de documentos que compõem a Política de Segurança da Informação, incluindo as diretrizes, regras e procedimentos, sendo que todos eles podem ser acessados livremente através da Intranet.

7 – COMPETÊNCIAS E RESPONSABILIDADES

7.1 – Alta administração

Compete à alta administração da Saneago:

- a) Assegurar que a política de segurança da informação e os objetivos dela sejam compatíveis com a direção estratégica da companhia.
- b) Apoiar e exigir o cumprimento da política, normas e procedimentos de segurança da informação.
- c) Zelar para que contratos, convênios e outros instrumentos similares elaborados pela respectiva Área Administrativa estejam alinhados a presente política e suas normas adjacentes;
- d) Priorizar a capacitação contínua de seus colaboradores de modo a promover maior conscientização das atividades que envolvem segurança da informação;
- e) Apoiar a promoção da **Política de Segurança da Informação**, mobilizando gestores para o cumprimento da Política;
- f) Promover a cultura de segurança da informação na empresa;
- g) Instituir o Comitê Gestor de Segurança da Informação **e de Privacidade e Proteção de Dados Pessoais – SIPPDP** no âmbito da Saneago.

7.2 – Comitê Gestor de Segurança da Informação e de Privacidade e Proteção de Dados Pessoais (SIPPDP)

Compete ao Comitê Gestor de Segurança da Informação **e de Privacidade e Proteção de Dados Pessoais**:

- a) **Propor atualizações** das Instruções Normativas de Segurança da Informação e Procedimentos de Segurança da Informação, em conformidade com a **Política de Segurança da Informação**, leis e regulamentos pertinentes;
- b) Instituir grupos de trabalho específicos relacionados à segurança da informação;
- c) Estabelecer mecanismo de registro e controle de não conformidade a esta Política, Normas e Procedimentos de Segurança da Informação;
- d) Encaminhar para sindicância casos de suspeita de violação desta política;

- e) Estabelecer um Programa de Gestão de Riscos relacionado à Segurança da Informação atendendo requisitos estabelecidos pela Superintendência de Governança;
- f) Conhecer e aprovar os níveis dos riscos a que os ativos envolvidos com a segurança da informação estão expostos.
- g) Aprovar os riscos residuais.
- h) Analisar criticamente os incidentes reais e potenciais de segurança da informação e recomendar, a depender de cada caso, que o assunto seja tratado pela Superintendência de Auditoria Interna – SUAUD.

7.2.1 – O comitê deverá ser composto minimamente pelo gestor de Segurança da Informação, por um membro indicado pela Superintendência de Tecnologia da Informação – SUTEC e um membro de cada Diretoria da companhia.

7.2.2 – O gestor de segurança da informação é o responsável por presidir e coordenar as atividades do comitê

7.3 – Gestor de UO

Compete ao Gestor de Unidade Organizacional:

- a) Zelar e fazer cumprir a política de segurança da informação em sua unidade de gestão;
- b) Identificar desvios de conduta na utilização das informações obtidas durante o exercício das funções de seus subordinados e adotar as medidas preventivas e corretivas apropriadas;
- c) Aplicar medidas que visem garantir que o pessoal sob sua supervisão proteja as informações a que tem acesso;
- d) Proteger, em nível físico e lógico, os ativos de informação e **os recursos necessários para armazenamento e processamento destas informações**;
- e) Garantir que as trocas de ativos sob sua responsabilidade e outras unidades sejam controladas, observando os trâmites pertinentes;
- f) Colaborar para o levantamento de dados para o gerenciamento de riscos da área sob sua gestão e informar novos riscos ainda não mapeados na área em que atua;

7.4 – Usuários

7.4.1 – Caracterizam-se como usuário todos os colaboradores, **efetivos ou terceirizados, além dos** prestadores de serviço, estagiários e participantes do programa Menor Aprendiz, **e demais agentes envolvidos**, independente do **tipo de vínculo ou** nível hierárquico que ocupa na empresa.

7.4.2 – A segurança e proteção da informação é uma responsabilidade contínua de cada usuário da Saneago em relação às informações que acessa e gerência.

7.4.3 – Também são obrigações do usuário:

- a) Seguir rigorosamente esta política, bem como documentos normativos vinculados;
- b) Manter a confidencialidade da informação de autenticação secreta, garantindo que ela não seja divulgada para quaisquer outras partes, incluindo autoridades e lideranças;
- c) Alterar as informações de autenticação sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;
- d) Não utilizar as credenciais de autenticação da Saneago para uso com finalidade pessoal;
- e) O usuário deve acessar apenas as informações e ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerado uma violação desta política;
- f) Utilizar mecanismos e controles de segurança dos ativos, recursos ou sistemas sob sua guarda ou responsabilidade, observando sempre as orientações da Política de Segurança, suas normas e melhores práticas;

- g) Assegurar o uso racional dos recursos de tecnologia das informações colocadas à sua disposição, priorizando o interesse público e institucional;
- h) Comunicar as centrais de atendimento de informática quaisquer riscos ou incidentes de segurança que venha a tomar conhecimento;
- i) Participar de programas de treinamento online ou presencial acerca da segurança da informação, sempre que ofertados.

7.5 – Gestor de sistema

7.5.1 – O gestor do sistema é aquele colaborador que mantém sob sua tutela a administração e controle de sistemas da companhia.

7.5.2 – São obrigações do Gestor de Sistema:

- a) Identificar e relatar criticamente se os requisitos da segurança da informação estão sendo atendidos;
- b) Rever periodicamente a classificação dos ativos sob sua propriedade que requerem algum grau de sigilo, observando a legislação em vigor;
- c) Participar do processo de avaliação e aceitação de risco;
- d) Participar das decisões relacionadas a qualquer violação de segurança dos ativos sob sua responsabilidade;
- e) Autorizar e solicitar a liberação de acesso à informação sob sua responsabilidade;
- f) Participar da definição dos critérios para estabelecer perfis de acesso a informações sob sua responsabilidade;
- g) Auxiliar na investigação de incidentes de segurança em ativos sob sua responsabilidade;
- h) Participar, sempre que convocado, das reuniões do Comitê Gestor de Segurança da Informação **e de Privacidade e Proteção de Dados Pessoais e/ou outras instâncias que tratam do tema**, prestando os esclarecimentos solicitados.

8 – DIVULGAÇÃO

8.1 – A Política deverá ser publicada e amplamente divulgada nas diversas plataformas de comunicação interna e externa da companhia.

8.2 – Esta política, bem como suas normas, serão disponibilizadas e agrupadas na Intranet da Saneago através do ambiente de consulta aos documentos normativos que fazem parte do Sistema de Gestão **Integrada**, em área de fácil acesso, proporcionando ampla difusão e atualização simplificada.

9 – ATUALIZAÇÃO

Esta Política deverá ser atualizada com periodicidade mínima de um ano ou quando mudanças significativas, que afetem a base de avaliação de risco original ocorrerem.

10 – PENALIDADES

10.1 – *Caso sejam identificados indícios de descumprimento desta política, a ocorrência será formalmente encaminhada à Superintendência de Governança – SUGOV e Superintendência de Transparência, Ouvidoria e Conduta – SUTOC, para as devidas apurações de responsabilidade, em consonância ao Regulamento Disciplinar e normas pertinentes, no que se refere às suas competências.*

10.2 – *As violações às normas e às diretrizes estabelecidas nesta Política de Segurança da Informação podem ser reportadas, conforme a sua gravidade e abrangência, ao Comitê Gestor de Segurança da Informação e de Privacidade e Proteção de Dados Pessoais.*

10.3 – *A Gerência de Conduta – PR-GCO, vinculada à SUTOC, é a unidade responsável por averiguar as condutas gravíssimas, graves, medias e leves, conferindo e atuando na apuração de responsabilidade quando necessário, conforme regimento interno.*

10.4 – A Gerência de Avaliação de Ocorrência Comportamental – PR-GOC, vinculada à SUGOV, é a unidade responsável por proceder a apuração de fatos quando necessário, conforme regimento interno.

10.5 – Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Saneago devem ser dirimidos pela Coordenação de Segurança da Informação – G-CSG, com a interveniência do Comitê Gestor de Segurança da Informação e de Privacidade e Proteção de Dados Pessoais nas situações que requeiram a atuação deste.

11 – DISPOSIÇÕES FINAIS

11.1 – O não cumprimento das determinações das normas e procedimentos, sujeita o infrator às penalidades previstas em lei e nos regulamentos internos da Saneago.

11.4 – Esta Instrução Normativa entra em vigor na data da sua publicação.

12 – APROVAÇÃO

Esta Política foi aprovada pelo Conselho de Administração da Saneago, na data de **06/02/2025**, conforme registrado na Ata **546**. Toda alteração ou revisão desse documento deverá ser submetida à apreciação do Conselho de Administração da Saneago.