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 SA – Saneago.

Aplicação Todas as Unidades Organizacionais da Saneago

1 - 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 SA – Saneago.

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 consequentemente exige proteção.
Autenticidade	Garantia de que o dado ou informação são verdadeiros.
Backup	Processo de savalguarda de dados com o objetivo de amenizar os efeitos decorrentes da perda dos originais.
Banco de Dados	Software usado para gerenciar a Base de Dados da companhia.
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 Informação (CGSI)	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.
Direito de Acesso	Privilégio associado a um usuário para ter acesso a um ativo.
Disponibilidade	Propriedade de que a informação esteja acessível e utilizável quando demanda.
Gestor da 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.

Proteção de Dados pessoais	É um meio de (medidas necessárias) garantir a privacidade.
Plano de Continuidade de Negócio (PCN)	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.
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.
Regimento Interno	Define as atribuições de todas as Unidades integrantes da Estrutura Organizacional da empresa.
Regulamento Disciplinar	Fixa critérios disciplinares da Saneago, divulgando conceitos, deveres e proibições, visando o funcionamento harmônico do comportamento funcional e estabelecendo competências para adoção de eventuais penas disciplinares.
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 susceptíveis às ameaças.

3 - ABRANGÊNCIA

Esta política se aplica a todos os usuários (colaboradores, prestadores de serviços, estagiários e menores aprendizes) que coletam, utilizam, armazenam ou transmitem informações da Saneago.

Esta Política define não apenas os requisitos de segurança lógica, mas, também, os de segurança física nos ambientes computacional e convencional.

4 - DOCUMENTOS REFERÊNCIA

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

5 - PRINCÍPIOS

5.1 - 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.

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

5.3 - As ações deverão se nortear pelos seguintes princípios:

a) Simplicidade: A complexidade aumenta a chance de erros, portanto todos os controles de segurança deverão ser simples e objetivos.
b) Privilégio Mínimo: Usuários devem ter acesso apenas aos recursos de tecnologia da informação necessários para realizar as tarefas que lhe foram designadas.
c) Privacidade desde a concepção: Buscar a privacidade e garantir a proteção dos dados desde sua concepção e durante o seu ciclo de vida.
d) 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.

e) 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;
f) Auditoria: Toda mudança ou eventos significantes de usuários e processos devem ser rastreáveis até o evento inicial por meio de registro consistente e detalhado.
g) Resiliência: Os controles de segurança devem ser projetados para que possam resistir ou se recuperarem dos efeitos de um desastre.
h) 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.
i) Conformidade e Legalidade: Aderência a contratos, padrões normativos e legislações vigentes e cabíveis.
j) 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.
k) 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.

6 - DIRETRIZES

6.1 - Inventário de Ativos

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

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

6.2 - Ciclo de vida da informação

6.2.1 - Medidas de proteção devem ser adotadas durante todo o ciclo de vida da informação, compreendendo as fases de coleta/criação, manipulação, armazenamento, transporte e descarte.

6.3 - Proteção de dados

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

6.3.2 - A informação armazenada em meio digital deve ser protegida contra desastre físico (fogo, água, calor, fenômenos da natureza, etc.) e desastre lógico (vírus, alteração indevida de informação, etc.).

6.4 - Classificação da Informação

6.4.1 - 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 ou divulgação não autorizada.

6.5 - Confidencialidade da Informação

6.5.1 - A confidencialidade da informação deve ser mantida durante todo o seu ciclo de vida.

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

6.5.3 - 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.

6.6 - Acesso a sistemas

6.6.1 - O acesso aos sistemas e recursos de tecnologia é de uso individual e intransferível.

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

6.6.2.1 - Esta solicitação passará por análise da equipe de segurança da informação, que poderá deferir ou não o pedido, levando em conta os princípios destacados no item 5, bem como melhores práticas de segurança.

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

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

6.7 - Continuidade da informação

6.7.1 - 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.

6.7.2 - 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.

6.7.2.1 - O Plano de Continuidade de Negócio estabelece as diretrizes prévias e decisões que devem ser tomadas para reduzir o impacto negativo que pode ser causado por uma situação desastrosa.

6.8 - Segurança Física

6.8.1 - 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.

6.9 - Dispositivos pessoais

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

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

6.9.3 - Não é permitida a instalação/uso de dispositivos de comunicação externa que não seja homologado pela G-CRD ou possui contrato firmado com a Saneago.

6.9.4 - A Saneago não se responsabiliza por arquivos pessoais armazenados nas estações de trabalho da empresa.

7 - DOCUMENTOS COMPLEMENTARES

7.1 - A Política de Segurança da Informação tem caráter corporativo e sua elaboração, bem como dos documentos complementares é de competência da Coordenação de Segurança da Informação. 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 gestão de dados e continuidade do negócio;
n) Norma para proteção à propriedade intelectual;
o) Cartilha de segurança da informação;
p) Plano de continuidade de negócio;
q) Plano de Resposta a Incidentes de Segurança;
r) Política de Privacidade e Proteção de Dados.

7.2 - 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.

8 - COMPETÊNCIAS E RESPONSABILIDADES

8.1 - 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 PSI, 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 - CGSI no âmbito da Saneago.
h) Aprovar revisões desta política de segurança.

8.2 - Comitê gestor da segurança da informação (CGSI)

Compete ao Comitê Gestor de Segurança da Informação:

a) Elaborar e atualizar as Instruções Normativas de Segurança da Informação e Procedimentos de Segurança da Informação, em conformidade com a PSI, leis e regulamentos pertinentes;
b) Aprovar o Plano de Continuidade de Negócios;
c) Instituir grupos de trabalho específicos relacionados à segurança da informação;
d) Estabelecer mecanismo de registro e controle de não conformidade a esta Política, Normas e Procedimentos de Segurança da Informação;
e) Encaminha para sindicância casos de suspeita de violação desta política;
f) Auxiliar os departamentos da Saneago na classificação das informações de sua custódia;
g) Revisar esta Política;
h) Estabelecer um Programa de Gestão de Riscos relacionado à Segurança da Informação atendendo requisitos estabelecidos pela Superintendência de Governança;
i) Conhecer e aprovar os níveis dos riscos a que os ativos envolvidos com a segurança da informação estão expostos.
j) Aprovar os riscos residuais.
k) 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.

8.2.1 - 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.

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

8.3 - 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 de processamento relacionados com sua área de atuação;
e) Impedir o acesso de pessoal desligado de área ou função aos ativos de informação sob sua responsabilidade;
f) Comunicar formalmente o desligamento (demissão, transferência, cessão de contrato, etc) de usuários ao RH, que por sua vez deverá notificar a SUTEC para medidas cabíveis;
g) Garantir que as trocas de ativos sob sua responsabilidade e outras unidades sejam controladas, observando os trâmites pertinentes;
h) 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;

8.4 - Usuários

8.4.1 - Caracterizam-se como usuário todos os colaboradores do quadro efetivo, prestadores de serviço, estagiários e participantes do programa Menor Aprendiz independente do nível hierárquico que ocupa na empresa.

8.4.2 - A segurança e proteção da informação é uma responsabilidade continua de cada usuário da Saneago em relação às informações que acessa e gerência.

8.4.3 - 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.

8.5 - Gestor de sistema

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

8.5.2 - São obrigações do Gestor da Informação:

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 liberarão 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 de Gestão de Segurança da Informação, prestando os esclarecimentos solicitados.

9 - DIVULGAÇÃO

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

9.2 - 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 da Qualidade, em área de fácil acesso, proporcionando ampla difusão e atualização simplificada.

9.3 - Em todos os documentos constarão a data de sua publicação e/ou revisão.

10 - 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.

11 - PENALIDADES

11.1 - A constatação de descumprimento das determinações da Política de Segurança da Informação deve ser reportada ao Comitê Gestor de Segurança da Informação conforme suas atribuições definidas no item 8.2 desta política.

11.2 - 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 nas situações que requeiram a atuação deste.

12 - APROVAÇÃO

Esta Política foi aprovada pelo Colegiado de Diretores da Saneago, na data de 26/03/2020, registrada na Ata 409. Toda alteração ou revisão desse documento deverá ser submetida à apreciação do Conselho de Administração da Saneago.