Título	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**
Objetivo	**Definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente de tecnologia da Saneamento de Goiás SA Saneago.**

1 – PREÂMBULO

As orientações aqui apresentadas são os princípios fundamentais para nortear a definição de procedimentos, instruções normativas e instruções de trabalho alinhados a 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.
Análise de Risco	Processo de identificação de ameaças e vulnerabilidades associadas a um ativo de modo a estimar o impacto na ocorrência de um incidente.
Ativo	Tudo aquilo que tenha valor para a Saneago e consequentemente exige proteção.
Autenticidade	Garantia de que o dado ou informação são verdadeiros.
Backup	Processo de cópia de dados com o objetivo de proporcionar a proteção contra a perda dos originais.
Banco de Dados	Software usado para gerenciar a Base de Dados da companhia.
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, além de auxiliar os departamentos na implementação das ações de segurança da informação.
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.
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 por uma entidade autorizada.
Firewall	Solução de segurança que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.
Forense Computacional	Técnicas para o tratamento de ativos computacionais que possam ter sido utilizados como apoio para execução de crimes de diversas naturezas.

TERMO	DEFINIÇÕES
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 continua de identificação, análise, tratamento, aceitação e comunicação de riscos.
Gestor de Segurança da Informação	Coordenador de Segurança da Informação da Saneago (PR-CIN)
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.
Não-repúdio	Garantia que uma entidade não possa negar ter participado de uma dada operação.
Proxy Web	Software que age como um intermediário para requisições de usuários solicitando recursos de páginas na Internet. Realiza filtro de conteúdo e fornece controle de acesso, para garantir que o uso da Internet está de acordo com a política de uso definida.
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 utilizam as informações da Saneago.

Esta Política engloba não apenas os requisitos de segurança lógica, mas, também, os de segurança física e de pessoal nos ambientes computacionais.

4 – PRINCÍPIOS

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.

O conjunto de documentos que compõe esta PSI deverá se nortear pelos seguintes princípios:

Simplicidade: A complexidade aumenta a chance de erros, portanto todos os controles de segurança deverão ser simples e objetivos;

Privilégio Mínimo: Usuários devem ter acesso apenas aos recursos de tecnologia da informação necessários para realizar as tarefas que lhe foram designadas;

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, bem como permitir maior eficácia dos controles de segurança;

Auditabilidade: Todos os 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 recuperarem dos efeitos de um desastre;

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 e recursos modernos: Os controles de segurança deverão primar pela utilização de tecnologias modernas e o uso de sistemas criptográficos na transmissão de dados e informações sigilosas, inclusive nos meios de comunicação móvel.

Salvaguarda das informações: A utilização de backups, para promover a segurança e a disponibilidade da informação, serão priorizados pela companhia.

Melhoria contínua: Princípio que busca o aperfeiçoamento contínuo de qualquer processo, sistema de processos ou procedimento, de forma a implementar um ciclo virtuoso de melhoria crescente;

Conformidade e Legalidade: Aderência a contratos, padrões normativos e legislação vigentes e cabíveis

5 – ESTRUTURA NORMATIVA

A política de segurança da informação tem caráter corporativo e sua elaboração é de competência da Coordenação de Segurança da Informação – PR-CIN.

A estrutura normativa da segurança da informação da Saneago, é estabelecida e implementada minimamente como segue:

a) Política de Segurança da Informação (PSI)

b) Instruções Normativas (IN): normas que estabelecem regras para a utilização de ativos e recursos de tecnologia da informação com o intuito de atingir os objetivos desta PSI;

c) Instruções de Trabalho (IT): descrevem, detalhadamente, as medidas operacionais necessárias para atingir os resultados estabelecidos nas Normas e na Política, abordando aspectos técnicos e práticos, adaptados à realidade do ambiente.

A PSI e seus documentos normativos complementares devem se mantidos/atualizados permanentemente e ter forte aderência tanto com as mudanças e necessidades de segurança dos ativos de informação, quanto da missão ou organização interna da Saneago. Assim, todos documentos devem ser periodicamente reavaliados e eventualmente revistos sempre que ocorram eventos ou fatos relevantes que os demandem ou justifiquem.

Os documentos normativos complementares e suas decorrências deverão, como regra, recomendar ou implementar apenas normas técnicas, boas práticas e outros procedimentos de segurança já normatizados por legislação vigente cabível hierarquicamente superior ou, caso inexistente, oriundas ou recomendadas por órgão ou entidade normativa técnica nacional ou internacional, de competência e aceitação amplamente reconhecidas

5.1 – Documentos complementares

Fica a Coordenação de Segurança da Informação e demais UOs vinculadas a Superintendência de Tecnologia da Informação, expedir normas complementares, visando abordar os seguintes aspectos:

a) Procedimento de classificação das informações;

b) Norma para acesso físico ao CPD e áreas críticas;

c) Norma para gestão de senhas e credenciais privilegiadas;

d) Norma para acesso à rede, internet e correio eletrônico;

e) Norma para acesso remoto;

f) Norma para retenção de logs e monitoramento de utilização de serviços e ativos;

g) Norma para uso de equipamentos corporativos e pessoais;

h) Norma para privacidade dos dados e criptografia;

i) Norma de controle de acesso aos sistemas em ambiente de desenvolvimento, homologação e produção;

j) Norma para aquisição, desenvolvimento e manutenção de sistemas;

k) Norma para acesso a redes sem fio e do uso dispositivos móveis;

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.

Complementando o arcabouço de normas complementares, as seguintes ações devem ser constantemente implementadas e monitoradas por todas Unidades Organizacionais pertencentes a Superintendência de Tecnologia da Informação – SUTEC:

a) assegurar que qualquer alteração em dados contidos nos Sistemas de Gerenciamento de Banco de Dados, em produção, seja feita por meio de sistemas adequados, evitando intervenções diretas;

b) elaborar e manter planos de contingência e recuperação de informações e serviços considerados críticos;

c) agregar cotidianamente ao processo de desenvolvimento de software as melhores práticas de segurança, estabelecendo trilhas de auditoria ou logs;

d) criar ações que visem controlar e conhecer a estrutura de rede física, a fim de permitir a rápida identificação e localização de quaisquer ativos existentes, no menor espaço de tempo possível;

e) monitorar o tráfego de rede;

f) analisar vulnerabilidades em serviços, aplicações e firmwares;

g) planejar ações ou projetos que tenham como produto o incremento da segurança da informação, além de participar do planejamento de outros projetos, onde se faz necessária a observância de aspectos de segurança;

h) executar atividades ou administrar recursos que sejam relacionados à segurança da informação;

i) auxiliar os responsáveis técnicos a identificar e definir as informações críticas e os requerimentos de confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio dos ativos de informação sob controle ou custódia da Saneago;

j) participar das decisões relacionadas a qualquer violação de segurança dos ativos sob controle ou custódia da Saneago;

k) encaminhar solicitação dos recursos tecnológicos necessários para implantação da Política de Segurança da Informação;

l) apurar incidentes de segurança e, em caso de comprovada omissão ou desrespeito a esta Política, encaminhar os fatos à chefia do infrator e ao Comitê Gestor da Segurança da Informação.

6 – COMPETÊNCIAS E RESPONSABILIDADES

6.1 – 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 Saneago;

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 à presente política e suas normas adjacentes;

d) Priorizar a capacitação contínua de seus recursos humanos de modo a promover maior independência na gestão e execução das atividades de 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.

6.2 – 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) Estabelecer um Programa de Gestão de Riscos relacionado a Segurança da Informação atendendo requisitos estabelecidos pela Superintendência de Controle Interno;

c) Desenvolver um Plano de Continuidade de Negócios, que deverá ser testado periodicamente;

d) Instituir grupos de trabalho específicos relacionados à segurança da informação;

e) Estabelecer mecanismo de registro e controle de não conformidade a esta Política, Normas e Procedimentos de Segurança da Informação;

f) Estabelecer sindicância para apuração de fatos que estão em desacordo com este documento;

g) Auxiliar os departamentos da Saneago na classificação das informações de sua custódia;

h) Revisar esta Política;

O CGSI será composto minimamente pela seguinte formação:

a) gestor de Segurança da Informação, que coordenará as atividades do comitê;

b) um membro indicado Superintendência de Tecnologia da Informação - SUTEC

c) um membro indicado pela Superintendência Jurídica - SUJUR

d) um membro indicado pela Superintendência de Recursos Humanos - SUREH

e) um membro indicado pela Superintencia de Controle Interno - SUCOI

f) um membro indicado pela Diretoria Corporativa – DICOR

6.3 – Gestor da segurança da informação

Compete ao Gestor da Segurança da Informação:

a) presidir o Comitê Gestor da Segurança da Informação (CGSI);

b) conduzir avaliações e auditorias para assegurar a aderência à Política de Segurança da Informação;

c) monitorar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

d) cobrar dos respectivos proprietários a classificação das informações na Área sob sua gerência;

e) propor recursos necessários às ações de segurança da informação;

f) realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação;

g) propor Normas e procedimentos relativos à segurança da informação e comunicações;

h) definir métricas que permitam aferir a eficiência e eficácia dos controles de segurança.

A gestão de segurança da informação deverá somente ser realizada por Colaboradores da Saneago.

6.4 – Gestor da UO

Compete ao Gestor da Unidade Organizacional:

a) zelar e fazer cumprir a psi;

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, utilizando-se dos mecanismos previstos no plano de desligamento da empresa;

f) comunicar formalmente o desligamento (demissão, transferência, cessão) de usuários aos gestores da área de RH, os quais deverão notificar a área de tecnologia da informação 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.

6.5 – Usuários

Caracteriza-se como usuário todos os colaboradores do quadro efetivo, prestadores de serviço, estagiários e menores aprendizes independente do nível hierárquico que ocupa na empresa.

São obrigações do usuário:

a) utilizar mecanismos e controles de segurança dos ativos, recursos ou sistemas sob sua guarda ou responsabilidade, observando as orientações da Política de Segurança, suas normas ou as melhores práticas;

b) assegurar que as senhas de acesso aos serviços sob sua responsabilidade estejam em conformidade com a norma gestão de senhas e credenciais privilegiadas;

c) seguir rigorosamente esta política, bem como as Normas e Procedimentos a ela vinculados;

d) assegurar o uso racional dos recursos de Tecnologia da Informação colocados à sua disposição, priorizando o interesse público e institucional;

e) comunicar a área competente quaisquer riscos ou incidentes de segurança que venha a tomar conhecimento;

f) participar de programas de treinamento online ou presencial acerca da segurança da informação, sempre que ofertados;

g) manter, obrigatoriamente, os dados críticos da sua área de atuação em compartilhamentos de rede disponibilizados pela Saneago;

h) não utilizar serviços de e-mail gratuitos para atividades institucionais, visto que tais serviços não possuem garantia de autenticidade, disponibilidade e confidencialidade das informações;

i) utilizar sua conta de e-mail corporativo apenas para fins institucionais e de forma a não cometer qualquer ato que possa prejudicar o trabalho, a imagem de terceiros ou da própria Saneago;

j) acessar a Internet apenas para navegação em sítios cujo conteúdo esteja adequado aos dispositivos legais, às determinações da Saneago e às suas atribuições institucionais.

6.6 – Gestor da informação

São obrigações do Gestor da Informação:

a) identificar e relatar criticamente se os requisitos da segurança da informação estabelecidos na política, procedimentos, normas e outras regulamentações aplicáveis, 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 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 de Gestão de Segurança da Informação, prestando os esclarecimentos solicitados.

7 – DIRETRIZES GERAIS

7.1 – Os ativos de informação

a) são inventariados e permanentemente controlados para os seus diversos fins;

b) possuem gestor responsável;

7.2 – Ciclo de vida da informação

As medidas de proteção devem ser adotadas durante todo o ciclo de vida da informação, compreendendo as fases de criação, manipulação, armazenamento, transporte e descarte.

7.3 – Proteção da informação

Toda informação deve ser protegida para que não seja alterada, acessada e destruída indevidamente. 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.).

7.4 – Confidencialidade da informação

O Gestor da Informação deverá classificar o nível de confidencialidade e sigilo da informação baseando-se nos critérios predefinidos pela Coordenação de Segurança da Informação. A confidencialidade da informação deve ser mantida durante todo o processo de uso da informação e pode ter níveis diferentes ao longo da vida dessa informação.

7.5 – Classificação da Informação

Classificar a informação assegura que ela receba um nível adequado de proteção, de acordo com a sua importância para a Saneago.

A informação deve ser classificada de acordo com sua importância para Saneago, ou seja, em termos de valor, sensibilidade e grau de criticidade em relação aos pilares de confidencialidade, integridade e disponibilidade, observadas as necessidades do negócio e a legislação em vigor, para evitar modificação ou divulgação não autorizada[1].

Os Níveis de Classificação possíveis são:

a) pública: Indica que informações corporativas devem ser divulgadas publicamente por força e na forma da lei, ou que possa ou precise ser divulgada, sem implicar em riscos, por interesse ou necessidade da Saneago no cumprimento de suas atividades;

b) interna: Indica que a informação, por sua natureza, conteúdo ou exigência legal, caso divulgada publicamente, possam representar risco ou inconveniência operacional;

c) restrito: Indica que a informação, se divulgada trará impacto significativo nas operações, o uso é restrito e o nível de confidencialidade maior e somente pode ser acessada por usuários da Saneago.

d) confidencial: Indica que a informação, se divulgada, trará um sério impacto sobre os objetivos estratégicos da companhia e sua imagem perante a sociedade. Somente pode ser acessada por usuário da Saneago explicitamente indicado pelo gestor da informação. É obrigatório a indicação do grupo ou pessoas que podem acessar essa informação.

Todos os relatórios de sistemas, relatórios elaborados no ambiente de escritório e todas as telas de sistema deverão indicar o nível de classificação da informação referente a ela.

Essa indicação do nível de classificação deve ser colocada no rodapé ou no cabeçalho de cada página do relatório ou na tela.

O Gestor da Informação é o responsável pela classificação da informação de sua custódia, seguindo o documento normativo de Classificação da informação.

Toda e qualquer outra forma de exposição da informação da Saneago deve ser classificada e ter explícito o seu nível de confidencialidade.

As informações classificadas devem ser atualizadas de acordo com as mudanças do seu valor, sensibilidade e criticidade ao longo do seu ciclo de vida.

1 Seguindo boas práticas NBR ISO/IEC 27002:2013

7.6 – Definições para classificação da informação

a) quais as pessoas, áreas da companhia e/ou organizações clientes que deverão ter acesso à informação;

b) que procedimentos de proteção da informação devem ser seguidos;

7.7 – Segurança Física dos ambientes

Os ativos críticos devem ser mantidos em área segura, protegidos por um perímetro de segurança definido e acesso controlado, com obediência as normas de acesso físico ao CPD.

Somente os responsáveis pelos ativos devem possuir credenciais de acesso administrativo ao mesmo.

7.8 – Uso dos equipamentos no ambiente corporativo

Devem ser precedidos de autorização ou licença da SUTEC, mediante a solicitação formal do superior via memorando:

a) o uso de microcomputadores portáteis pertencentes a Saneago, bem como a retirada de equipamentos de sua propriedade para fora de suas dependências;

b) o uso, nas dependências da Saneago de equipamentos de informática que não sejam de responsabilidade desta;

c) no caso de utilização de equipamentos portáteis da Saneago no desenvolvimento das atividades fora das dependências da companhia, o usuário fica responsável pela guarda, conservação e utilização do respectivo equipamento, além de assegurar que as informações da empresa não sejam comprometidas;

7.8.1 – Dispositivos móveis pessoal

A proteção de recurso computacional de uso individual é de responsabilidade do usuário que o utiliza.

7.9 – Aquisição, Desenvolvimento e Manutenção de sistemas de informação

Deverão ser desenvolvidas ações que garantam que a segurança seja parte integrante dos sistemas de informação existentes, e também os que forem desenvolvidos e adquiridos.

Todos os requisitos de segurança deverão ser identificados na fase de definição de requisitos de um projeto e justificados, acordados e documentados como parte do caso geral de negócios do sistema de informação.

a) os ativos de rede, em suas configurações, devem possuir política do tipo restritiva como opção padrão;

b) os procedimentos operacionais devem ser documentados, executados e estar sob a responsabilidade da coordenação ou gerência;

c) os ativos considerados críticos devem ser redundantes e possuir plano de continuidade elaborado pela equipe responsável pelo ativo, para manutenção dos serviços.

7.10 – Ambiente real dos sistemas

O ambiente do sistema computacional destinado à execução dos sistemas e dados reais (ambiente de produção) não deve ser utilizado para testes e outras atividades semelhantes

A passagem de programas e dados para o ambiente de produção deve ser controlada de maneira a garantir a integridade e disponibilidade desse ambiente para continuidade do negócio.

7.11 – Acesso a informação e recursos

A liberação do acesso da informação para os usuários será autorizada pelo Gestor da UO, que levará em conta a confidencialidade da informação e a necessidade de acesso do usuário.

O acesso da informação deve ser autorizado apenas para os usuários que necessitem da mesma para o desempenho das suas atividades profissionais na Saneago. Esse conhecimento do usuário deve ser utilizado apenas para o desenvolvimento e operacionalização do negócio.

Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerado uma violação desta política.

O acesso a informação armazenada e processada no ambiente de tecnologia é individual e intransferível. Esse acesso acontece através da identificação e autenticação do usuário. Quando a autenticação for feita através de senha, o usuário deve manter em segredo e não utilizar senhas óbvias, de forma que somente ele seja capaz de reproduzi-la.

Os recursos de tecnologia da Saneago, disponibilizados para os usuários têm como objetivo a realização de atividades profissionais. A utilização dos recursos de tecnologia, com finalidade pessoal, não será permitida em nenhum aspecto.

7.12 – Correio eletrônico

As mensagens de correio eletrônico são instrumentos de comunicação interna e externa para a realização dos negócios da Saneago. Elas devem ser escritas em linguagem profissional, que não comprometa a imagem da empresa, que não vá de encontro à legislação vigente e nem ao Código de Conduta da Saneago. Mensagens fora desse contexto não devem ser enviadas.

O conteúdo do correio eletrônico de cada usuário pode ser acessado pela Saneago quando de situações que ponham em risco a imagem e o negócio da empresa. Este acesso será feito a critério da Saneago, mediante comunicação ao superior imediato do usuário, à Coordenação de Segurança da Informação deve ser registrado formalmente permitindo uma auditoria desse procedimento.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. Mensagens recebidas não coerentes com esta política devem ser eliminadas.

7.13 – Ambiente de internet

O acesso à Internet deve ser usado para o desempenho das atividades profissionais do colaborador. Sites que não contenham informações que agreguem conhecimento profissional e para o negócio não

devem ser acessados. Os acessos são monitorados pela Saneago com objetivo de garantir o cumprimento dessa política.

7.14 – Continuidade do uso da informação

Toda informação crítica para o funcionamento as 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 dessa criticidade.

Para a criação das cópias de segurança devem ser considerados os aspectos legais, históricos, de auditoria e de recuperação do ambiente, bem como uma política de descarte.

Os recursos tecnológicos, de infraestrutura e os ambientes físicos onde os usuários realizam o negócio da Saneago devem ter contingência e ser protegidos contra desastres.

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.

A definição e implementação das medidas de prevenção e recuperação, para situações de desastre e contingência, devem ser efetuadas de forma permanente e devem contemplar recursos de tecnologia, humanos e de infraestrutura. Elas são de responsabilidade da SUTEC, contando com o apoio e validação da Coordenação de Segurança da Informação.

7.15 – Treinamento dos usuários

Para uma efetiva proteção das informações, as Unidades Organizacionais deverão elaborar um plano contínuo de capacitação de recursos humanos em segurança da informação, de modo a promover maior consciência da responsabilidade individual dos usuários e maior independência da Saneago na contratação de serviços de segurança.

7.16 – Documentação

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.

8 – DIVULGAÇÃO

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, a área é de fácil acesso, proporcionando ampla difusão e atualização simplificada.

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

9 – ATUALIZAÇÃO

Esta Política, Normas e Procedimentos que dela se originaram deverão ser atualizadas com periodicidade mínima anual ou quando mudanças significativas, que afetem a base de avaliação de risco original, ocorrerem.

10 – PENALIDADES

A constatação de descumprimento das determinações da Política de Segurança da Informação, deve ser reportada à chefia imediata do infrator, e ao Comitê Gestor da Segurança da Informação, tendo em vista que este grupo é responsável pelos processos de sindicância e administrativos disciplinares da Saneago que embasarão as penalidades administrativas/contratuais a serem aplicadas, sem qualquer prejuízo de outras.

11 – CONCLUSÃO

A utilização das informações corporativas pelos usuários da Saneago devem estar de acordo com os documentos institucionais “Código de Conduta”, “Regimento interno” e o “regulamento disciplinar de pessoal”. Todos os usuários devem conhecer e entender esses documentos.

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

Todos os usuários devem utilizar a informação da empresa, de acordo com as determinações desta Política de Segurança da Informação.

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 – PR-CIN, com a interveniência do Comitê Gestor de Segurança da Informação nas situações que requeiram a atuação desta.

ITEM	TÍTULO DO DOCUMENTO
01	Definir padrões e boa práticas para proteção da informação

12 – APROVAÇÃO

Esta Política foi aprovada pelo Conselho de Administração da Saneago, na data de 15/12/2017, registrada na Ata 353. Toda alteração ou revisão desse documento deverá ser submetida à apreciação do Conselho de Administração da Saneago.