

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA SANEPAR

1. DISPOSIÇÕES GERAIS

Aprovada na 17ª Reunião Extraordinária do Conselho de Administração - RECA, realizada no dia 27 de agosto de 2020 (Versão 1).

2. OBJETIVO

O objetivo desta Política é estabelecer diretrizes, responsabilidades e conceitos a serem observados para segurança da informação da Sanepar, considerando as informações presentes no ambiente da Sanepar ou por ela utilizada, abrangendo tanto as que estiverem no meio tecnológico quanto no convencional.

A Política de Segurança da Informação (PSI) é o documento orientador da Segurança da Informação da Sanepar, tendo em vista a implementação e manutenção do Sistema de Gestão de Segurança da Informação (SGSI).

3. ABRANGÊNCIA

Esta política aplica-se aqueles que venham a ter acesso a informações da Sanepar, administradores, membros de Conselhos e Comitês, empregados, estagiários, aprendizes, fornecedores, empreiteiros, prestadores de serviços em geral, e a todos os parceiros de negócios, independente da denominação ou relação contratual com que se apresente.

A Política de Segurança da Informação da Sanepar encontra-se disponível no endereço eletrônico: <http://www.sanepar.com.br> e, uma vez aprovada pelo Conselho de Administração, deverá ser divulgada a todas as pessoas que devem cumpri-la.

4. REFERÊNCIAS

- Lei Federal nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
- Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Resolução nº 006/2015 – CGE;

-
- ISO 27.001 – Sistemas de Gestão da Segurança da Informação;
 - Política de Proteção de Dados Pessoais e Privacidade; e
 - Código de Conduta e Integridade.

Esta Política deverá ser lida e interpretada juntamente com o Código de Conduta e Integridade da Sanepar e demais políticas corporativas.

5. DEFINIÇÕES

Os termos e expressões listados a seguir, quando utilizados no âmbito da Política de Segurança da Informação da Sanepar, terão o seguinte significado:

- Ambiente convencional:** É o ambiente em que o usuário acessa diretamente a informação, que poderá estar disposto diretamente no meio físico para leitura, como o papel, ou através de meio sonoro, como a comunicação oral, ou outros por meio do qual a informação possa ser acessada diretamente pelo receptor.
- Ambiente de Tecnologia:** É o ambiente em que o usuário se relaciona com a informação através de equipamentos de tecnologia, tais como computadores, tablets e celulares. Neste ambiente, as informações encontram-se no formato digital.
- Informação:** O termo informação, para fins desta política e das demais normas relativas à Segurança da Informação, deve abranger também os próprios dados que, isoladamente ou em conjunto com outros, levarão à própria informação.
- Segurança da Informação:** são as medidas administrativas, tecnológicas e físicas adotadas com o intuito de preservar a confidencialidade, a integridade e a disponibilidade da informação considerada importante para a companhia, durante todo seu ciclo de vida.

6. DIRETRIZES

As orientações desta política deverão ser interpretadas sob o viés principiológico, representando o direcionamento sobre a forma como as informações podem ser utilizadas.

Esta política deve servir de orientação para a elaboração de demais normas sobre assuntos que venham a tangenciar o uso de informações e conseqüentemente a necessidade de observar a sua proteção, garantindo os atributos de:

- a) **Disponibilidade:** a informação deve estar acessível ao uso legítimo, pelos que possuam autorização fornecida pelo Responsável pela Informação;
- b) **Integridade:** a informação deve estar correta, ser verdadeira e não estar corrompida;
- c) **Confidencialidade:** A informação deve ser acessada e utilizada somente pelos usuários cuja permissão lhe tenha sido concedida previamente em razão de sua função, para atender às exigências do exercício de suas atividades profissionais na empresa;
- d) **Autenticidade:** a informação deve ser proveniente daquele que anuncia ser a fonte, não podendo ter sido objeto de alterações no decorrer do processo;
- e) **Legalidade:** a informação deve atender a requisitos legais, estando sempre em conformidade com a legislação vigente.

Deverão ser observadas as seguintes diretrizes:

- Assegurar que a informação seja utilizada para obter seus fins institucionais, garantindo a continuidade do negócio. O desenvolvimento de uma governança de dados deve ser incentivado, tendo como objetivo o melhor planejamento, disponibilidade, monitoramento, controle e segurança dos

dados corporativos, possibilitando melhorar a estrutura de negócios da empresa;

- Garantir que o nível de confidencialidade da informação seja classificado considerando a privacidade de dados pessoais para fins de proteção de dados pessoais e os dados que devam ser considerados públicos, conforme determinado pela Lei de Acesso à Informação (LAI). A confidencialidade da informação deve ser mantida durante todo o processo de uso da informação e pode ter níveis diferentes ao longo de seu ciclo de vida;
- Garantir que cada informação tenha um Gestor da Informação (ou Grupo de Gestores da Informação);
- Garantir que a utilização da informação esteja de acordo com a necessidade do acesso e o sigilo da informação para a realização dos objetivos da empresa;
- Garantir que o acesso a informação seja autorizado apenas aos usuários que dela necessitam para o desempenho das suas atividades profissionais para a Sanepar;
- Garantir que cada usuário acesse apenas as informações e os ambientes previamente autorizados, considerando que, os dados de acesso a informação, compostos por identificação e autenticação do usuário, em ambiente de tecnologia, são individuais e intransferíveis;
- Garantir que os dados para autenticação do usuário sejam mantidos em segredo, considerando o mais alto nível de classificação da informação;
- Assegurar que toda informação da Sanepar tenha proteção para que não seja alterada, acessada e destruída indevidamente. Os locais onde se encontram os recursos de informação devem ter proteção e controle de acesso físico compatível com o seu nível de criticidade;
- Garantir que as informações corporativas tenham cópias de segurança suficiente para a manutenção de planos de continuidade de negócio;
- Assegurar que os recursos tecnológicos de infraestrutura e os ambientes físicos onde são realizadas as atividades operacionais do negócio da Sanepar devam ser protegidos contra situações de indisponibilidade e tenham planos de continuidade de negócio;

-
- Garantir que as medidas de prevenção e recuperação de informações, para situações de desastre e contingência sejam efetuadas de forma permanente e contemplem recursos de tecnologia, humanos e de infraestrutura;
 - Assegurar que os recursos de tecnologia da informação sejam utilizados tão somente para a finalidade da atividade profissional e dentro dos limites necessários para seu exercício;
 - Garantir que todo projeto considere a segurança da informação como pilar de planejamento, desenvolvimento e revisão de processos e sistemas;
 - Garantir a gestão dos ativos associados com informação e com recursos de processamento da informação;
 - Assegurar e priorizar a mitigação das vulnerabilidades dos recursos de infraestrutura.

7. RESPONSABILIDADES

Comitê de Segurança da Informação

- Emitir orientações às diferentes áreas da empresa para o desenvolvimento e a implantação de projetos, procedimentos, ações, instruções e normativos com vistas ao desenvolvimento de um Sistema de Gestão de Segurança da Informação, suportada por esta política;
- Discutir e deliberar sobre o conteúdo relativo a segurança da informação, assim como definir diretrizes e orientações estratégicas relacionados ao tema;
- Responder a incidentes (roubos de dados corporativos).

Comitê Técnico Permanente de Segurança da Informação

- Definir e executar ações nos ambientes de Tecnologia da Informação e Comunicação, alinhadas com as orientações corporativas do Comitê de Segurança da Informação.

Ouvidoria – Agente de Transparência

- Definir o nível de sigilo e da respectiva classificação das informações, a qual servirá de orientação para aplicação da segurança da informação;
- Assegurar o cumprimento das normas relativas ao acesso à informação, de forma eficiente e adequada aos objetivos da vigente legislação de acesso à informação;
 - No exercício de suas atribuições, o Agente de Transparência terá livre acesso a todos os documentos, informações e outros elementos considerados indispensáveis ao cumprimento de suas atribuições, não lhe podendo ser sonegado, sob qualquer pretexto, nenhum processo, documento ou informação, a menos que estejam classificados sob qualquer um dos graus de sigilo, previstos na legislação de acesso a informações.

Auditoria

- Realizar auditoria de avaliação quanto a aderência da política nas áreas da Companhia, contribuindo com recomendações para a melhoria da segurança da informação, propiciando a retroalimentação de processos.

Gerências Corporativas

- Normatizar os processos afetos a sua área de atuação, observando esta e as demais políticas da companhia, com a orientação do Comitê de Segurança da Informação;
- Dar ciência da Política de Segurança da Informação da Sanepar de acordo com a abrangência;
- Promover periodicamente treinamentos e orientações acerca de conceitos, regras e procedimentos de segurança da informação, tanto em termos corporativos gerais quanto específicos de sua atividade;
- Indicar um Gestor da Informação (ou Grupo de Gestores da Informação) para cada grupo de informações relativas aos principais processos da área;

-
- Avaliar, controlar e orientar a atuação do Gestor da Informação (ou Grupo de Gestores da Informação).

Gerências Regionais

- Dar ciência da Política de Segurança da Informação da Sanepar de acordo com a abrangência;
- Promover periodicamente treinamentos e orientações acerca de conceitos, regras e procedimentos de segurança da informação, tanto em termos corporativos gerais quanto específicos de sua atividade.

Gestor da Informação

- Autorizar e permitir acesso, validação e fiscalização de uso da informação e definição dos controles;
- Classificar o nível de confidencialidade e sigilo da informação internamente, de acordo com as prerrogativas do processo.

Usuário

- Responder pela segurança das informações as quais tem acesso em meio físico ou digital;
- Evitar a exposição desnecessária de informações de que tenha posse, ainda que seja objeto de sua função, devendo zelar pelas informações classificadas, em seus períodos, de acordo com os preceitos da LAI;
- Zelar pelo recurso de tecnologia da informação disponibilizado pela Sanepar, sendo de responsabilidade pessoal aqueles recursos individualmente disponibilizados.

8. RESPONSABILIZAÇÕES

A não aderência às responsabilidades dispostas na presente Política deverão ser reportadas ao Comitê de Segurança da Informação, para providências a serem adotadas para fins de apuração de responsabilização.

O descumprimento das disposições contidas nesta política, e demais normas relativas à segurança da informação, poderá acarretar na aplicação de sanções contempladas no pilar da Gestão da Consequência do Programa de Integridade da Sanepar, independente de responsabilização administrativa, civil e criminal.

9. REVISÃO

A referente política deverá ser revisada periodicamente ou extraordinariamente quando houver fato relevante que justifique. A revisão da política necessitará de comunicação prévia às áreas responsáveis pela manutenção de normas afetas para que estas sejam revisadas, mantendo coerência àquela.

10. DISPOSIÇÕES FINAIS

Dúvidas com relação à interpretação desta Política devem ser esclarecidas com o Comitê de Segurança da Informação.

Esta política entra em vigor na data de sua aprovação pelo CA.

11. HISTÓRICO

Política de Segurança da Informação			Versão		1
			Área Gestora		DAGRC
			Sigilo		Público Externo
Versão	Data	Responsável	Aprovador	Descrição da Alteração	
1	27/08/2020	Diretoria de Governança, Riscos e Compliance	Conselho de Administração	Emissão Inicial	