POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. DISPOSIÇÕES GERAIS

Revisado na 10ª Reunião Ordinária do Conselho de Administração - RECA, realizada no dia 19 de outubro de 2023 (Versão 3).

2. OBJETIVO

O objetivo desta Política de Segurança da Informação (PSI) é o de estabelecer princípios, diretrizes, responsabilidades e conceitos a serem observados para a Segurança da Informação da Sanepar no âmbito do Sistema de Gestão de Segurança da Informação (SGSI) e do Programa de Integridade.

Esta Política tem por escopo a proteção dos dados, documentos e informações da Companhia, a fim de resguardá-los, visando a escorreita condução dos negócios por meio das melhores práticas, buscando a sustentabilidade econômica, social e ambiental, a proteção contra concorrência desleal, práticas colusivas ou fraudulentas, visando sempre a eficiência dos processos e a absorção de inovações, estejam os referidos dados, documentos ou informações armazenados em meio convencional ou tecnológico, interno ou externo à área física da empresa e disponibilizados em plataformas de compartilhamento de arquivos.

3. ABRANGÊNCIA

Esta política aplica-se àqueles 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

4.1 Constituição da República Federativa do Brasil;
4.2 Lei Federal n° 12.527/2011 (Lei de Acesso à Informação);
4.3 Decreto do Estado do Paraná n° 10.285/2014 (Dispõe sobre procedimentos a serem observados pela Administração Direta e Indireta, com vista a garantir o acesso à informação);
4.4 Lei Federal n° 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
4.5 Lei Federal n° 12.965/2014 (Marco Civil da Internet);
4.6 Lei Federal n° 6.404/1976 (Dispõe sobre as Sociedades por Ações);

4.7 Lei Federal n° 13.303/2016 (Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios);

4.8 Lei Federal n° 12.846/2013 (Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências);

4.9 Resolução n° 55/2021 – CGE - Paraná;

4.10 ISO 27.001 – Sistemas de Gestão da Segurança da Informação;

4.11 Política de Proteção de Dados Pessoais e Privacidade da Sanepar;

4.12 Código de Conduta e Integridade da Sanepar;

4.13 Código De Conduta e Integridade Para Terceiros da Sanepar; e

4.14 CAVOUKIAN, Ann et al. Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada, v. 5, 2009.

Esta Política deverá ser lida e interpretada juntamente com o Estatuto Social, demais políticas corporativas, principalmente o Regulamento de Proteção à Informação, o Código de Conduta e Integridade da Sanepar.

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:

5.1 **Ambiente convencional**: É o ambiente em que o usuário acessa diretamente ao dado ou a informação, que poderá estar disposto diretamente no suporte (meio) físico para leitura, como o papel, ou através de meio sonoro, visual, como a comunicação oral, ou outros por meio do qual tanto os dados quanto a informação possa ser acessada diretamente pelo receptor.

5.2 **Ambiente de Tecnologia**: É o ambiente em que o usuário se relaciona com os dados e a informação através de suporte físico, utilizando equipamentos de tecnologia, tais como computadores, tablets e celulares. Neste ambiente, as informações encontram-se em suporte físico, no formato digital.

5.3 **Dados**: Estrutura elementar da cadeia informacional, que poderá ser transformada em informação. Precisa de contexto para ser entendido.

5.4 **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.

5.5 **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 consideradas importantes para a companhia, durante todo seu ciclo de vida.

6. PRINCÍPIOS

As orientações desta política deverão ser interpretadas sob o viés principiológico, representando o direcionamento sobre a forma como os dados e 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 e o fornecimento de dados e de informações e consequentemente a necessidade de observar a sua proteção, garantindo os atributos de:

6.1 **Disponibilidade:** a informação deve estar acessível ao uso legítimo, pelos que possuam autorização fornecida pelo Responsável pela Informação;

6.2 **Integridade**: a informação deve estar correta, ser verdadeira e não estar corrompida;

6.3 **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;

6.4 **Autenticidade:** a informação deve ser proveniente daquele que anuncia ser a fonte, não podendo ter sido objeto de alterações no decorrer do processo; e

6.5 **Legalidade**: a informação deve atender a requisitos legais, estando sempre em conformidade com a legislação vigente.

7. DIRETRIZES

A presente Política de Segurança da Informação possui diretrizes gerais e diretrizes referentes a segurança desde a concepção, descritas a seguir:

7.1. DIRETRIZES GERAIS

I. Assegurar que tanto os dados quanto as informações sejam utilizados para obter seus fins institucionais, garantindo a continuidade do negócio.

II. 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;

III. Garantir que o nível de confidencialidade da informação seja classificado considerando o nível de sigilo da informação, a privacidade de dados pessoais para fins de proteção de dados pessoais e os dados que devam ser considerados públicos, conforme classificação estabelecida em legislação específica e o Regulamento de Proteção a Informação da Sanepar. 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;

IV. Garantir que cada informação tenha um Gestor da Informação (ou Grupo de Gestores da Informação);

V. 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;

VI. Garantir que o acesso a informação seja autorizado apenas aos usuários que dela necessitam para o desempenho das suas atividades profissionais para a Sanepar;

VII. 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;

VIII. Realizar a gestão e revisão das identidades e dos acessos aos recursos computacionais da Sanepar, garantindo a definição de privilégios mínimos e rastreabilidade de acessos realizados.

IX. Garantir que os dados para autenticação do usuário sejam mantidos em segredo, considerando o mais alto nível de classificação da informação;

X. 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;

XI. Garantir que as informações corporativas tenham cópias de segurança suficientes para a manutenção de planos de continuidade de negócio;

XII. 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;

XIII. 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;

XIV. 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;

XV. Garantir que todo projeto considere a segurança da informação como pilar de planejamento, desenvolvimento e revisão de processos e sistemas;

XVI. Garantir a gestão dos ativos associados com informação e com recursos de processamento da informação; e

XVII. Assegurar e priorizar a mitigação das vulnerabilidades dos recursos de infraestrutura.

7.2. SEGURANÇA DESDE A CONCEPÇÃO

Segurança desde a concepção (*Security By Design)*" significa que os produtos de tecnologia são construídos de forma a proteger razoavelmente contra atividades mal-intencionadas que possam obter acesso com sucesso a dispositivos, dados e infraestrutura tecnológica. Os envolvidos com a gestão, desenvolvimento, projeto e manutenção de tecnologia, devem realizar uma avaliação de risco para identificar e enumerar as ameaças cibernéticas predominantes as tecnologias críticas e, em seguida, incluir proteções nos projetos de produtos que levem em consideração o cenário de ameaças cibernéticas em evolução.

Todos os projetos, produtos e processos a serem desenvolvidos para a Sanepar devem passar pela análise de Segurança da Informação desde sua iniciação, tendo como objetivo viabilizar e assegurar os pilares fundamentais de segurança a fim de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, representadas pelos princípios abaixo elencados:

Princípios do Security by Design

I. Minimizar superfícies de ataque

Corresponde a identificação de vulnerabilidades e vetores de ataque no aspecto digital (sites, softwares, servidores e etc.) ou físico (dispositivos, armazenamento, sensores, controladores e etc.) que um agente mal-intencionado poderia utilizar.

Devem ser elaborados meios e técnicas para reduzir essas superfícies, como: mecanismos de controle de acesso, restrições de perfil, utilização de softwares e componentes homologados, protocolos de segurança para acesso remoto, entre outros.

II. Estabelecer Padrões de Segurança

Atribuir padrões elevados de segurança em projetos de tecnologia. A padronização é um importante fator para elaborar segurança de forma inteligente, pois ela possibilita que sejam criadas soluções mais eficientes, confiáveis e até econômicas.

Adotar padrões mais rígidos de segurança, como a utilização de um framework de projeto seguro de tecnologia, garantem ativos de tecnologia mais seguros e suscetíveis a melhorias contínuas.

III. Adotar o princípio do mínimo privilégio

Ao fornecer acesso às pessoas usuárias, apenas os privilégios estritamente necessários devem ser concedidos. A ideia é receber autorização para dispor de privilégios somente para executar determinada atividade, pertinente às atribuições do operador.

É importante dar atenção às permissões solicitadas para acessar um serviço. Não compartilhar informações sensíveis e configurar protocolos de gestão de privacidade são exemplos de ações relacionadas a este princípio.

Sempre que for identificada a disponibilidade de acesso a recursos que extrapole a necessidade, para o exercício de suas atividades diárias, tal fato deve ser reportado para o seu Gestor, com o objetivo de remover os acessos desnecessários.

IV. Defesa em profundidade

É um conjunto de práticas que se concentram na proteção, detecção e reação de invasões. Para isso, são usados processos, softwares de segurança e ferramentas para a construção de uma estratégia contra possíveis ataques.

Acrescentar camadas de segurança em todos os níveis de um ativo tecnológico, ao invés de criar apenas camadas primárias de validação de inputs ou regras de negócio é uma boa prática.

V. Falhar com segurança

As falhas não devem comprometer a segurança ou expor informações críticas. Seguindo a ideia de falhar seguro e falhar rápido, as mensagens de falhas e erros devem ser apresentadas o mais cedo possível e evitar que isso ocorra em momentos cruciais, além de filtrar com cuidado as informações expostas em um log de erro, por exemplo.

A manipulação segura de erros é um aspecto importante para um software seguro. Existem dois tipos de erros que merecem destaque:

a) O primeiro são as exceções que ocorrem no processamento de um controle de segurança.
b) O outro tipo de exceção relevante à segurança está no código que não faz parte de um controle de segurança.

É importante que essas exceções não permitam comportamentos que o sistema normalmente não permitiria. Um software desenvolvido com segurança deve considerar a existência de três resultados possíveis de um mecanismo de segurança: proibir a operação, permitir a operação ou lançar uma exceção.

VI. Não confiar em serviços

Serviços e componentes de terceiros devem ser considerados ameaças em potencial, até uma validação profunda. Todo serviço terceirizado deve ser considerado inseguro como regra, uma vez que pode conter vetores de ataque ou mesmo propósitos maléficos em si, comprometendo a segurança da aplicação.

Dessa forma, todo serviço deve ser validado e monitorado conforme rígidos padrões de segurança.

VII. Segregação de funções e responsabilidades

É o controle de acesso baseado no papel, na atividade ou na função de um usuário dentro de um sistema. A utilização de um perfil por função (ou *RBAC – Role Based Access Control*) providencia um modelo para administrar privilégios de acessos aos sistemas e infraestrutura de uma empresa. O perfil por função consegue agrupar os acessos, possibilitando uma visão geral dos privilégios e controlando os acessos de uma forma segura.

VIII. Evitar segurança por obscuridade

A segurança por obscuridade ocorre quando os desenvolvedores codificam os sistemas de forma secreta, acreditando que ninguém será capaz de encontrar as vulnerabilidades do software. O problema com essa técnica é a dependência em relação ao sigilo da implementação do projeto como forma principal de prover segurança para o sistema. Geralmente, as pessoas que fazem uso dessa técnica assumem que o não conhecimento das vulnerabilidades de um software é um indicativo de segurança.

Para evitar a segurança por obscuridade é preciso investir em práticas comprovadas para a segurança de sistemas.

IX. Mantenha segurança simples

Arquiteturas muito complexas podem deixar as aplicações muito mais suscetíveis a erros. Quanto maior é a complexidade de um ativo tecnológico, mais detalhes e falhas de segurança poderão passar despercebidos, ou seja, a complexidade excessiva resulta em uma aplicação muito menos segura.

A existência de muitas ferramentas pode aumentar as brechas de segurança em vez de extingui-las, assim como procedimentos pouco documentados ou falta de automações que podem deixar usuários esperando demais por um acesso.

É necessário refletir sobre a relevância e a complexidade dos controles, se eles acrescentam mais segurança ou burocracia aos sistemas.

X. Manutenção e correção segura de problemas

A gestão de vulnerabilidades deve ser aplicada como forma de identificar e mapear as vulnerabilidades, bem como seus riscos e formas de mitigação. Além disso, adotar estratégias de melhoria contínua são práticas recomendadas para um projeto de tecnologia mais seguro.

É preciso entender o comportamento da vulnerabilidade de forma estrutural no ativo tecnológico e verificar se existem outros componentes que podem ser afetados pela mesma vulnerabilidade.

A falta de um processo ou controle para realizar as correções de problemas pode causar o surgimento de novos problemas e brechas de segurança nos ativos tecnológicos. Um processo contínuo de gestão de vulnerabilidades é visto como um

aliado para as equipes de projetos e produtos, atuando na identificação, análise, classificação e tratamento das vulnerabilidades. Esse processo busca medir o progresso e avaliar os riscos aos quais os sistemas estão submetidos, colaborando com uma estratégia adequada.

8. RESPONSABILIDADES

Esta Política prevê responsabilidades para o Comitê de Segurança da Informação, Comitê Técnico Permanente de Segurança da Informação, Agente de Transparência, Auditoria, Gerências Corporativas, Gerências Regionais, Gestor da Informação e Usuário, elencadas a seguir:

8.1 Comitê de Segurança da Informação

I. 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;
II. Discutir e deliberar sobre o conteúdo relativo a segurança da informação, assim como definir diretrizes e orientações estratégicas relacionadas ao tema;
III. Responder a incidentes (por exemplo: furto e roubos de dados e informações corporativas).

8.2 Comitê Técnico Permanente de Segurança da Informação

I. Apoiar na definição de ações nos ambientes de Tecnologia da Informação e Comunicação, alinhadas com as orientações corporativas do Comitê de Segurança da Informação;
II. Estabelecer padrões de tecnologia e controles apropriados;

8.3 Agente de Transparência

I. Apoiar os gestores da informação na definição do nível de sigilo e da respectiva classificação das informações, a qual servirá de orientação para aplicação da segurança da informação;
II. Assegurar o cumprimento das normas relativas ao acesso à informação, de forma eficiente e adequada aos objetivos da vigente legislação de acesso à informação;
III. No exercício de suas atribuições, o Agente de Transparência terá livre acesso a todos os documentos, dados, informações e outros elementos considerados indispensáveis ao cumprimento de suas atribuições, não 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 à informação.

8.4 Auditoria

I. 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.

8.5 Gerências Corporativas

I. 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;
II. Dar ciência da Política de Segurança da Informação da Sanepar de acordo com a abrangência;
III. 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;
IV. Indicar um Agente da Informação (ou Grupo de Agentes da Informação) para cada grupo de informações relativas aos principais processos da área.

8.6 Gerências Regionais

I. Dar ciência da Política de Segurança da Informação da Sanepar de acordo com a abrangência;
II. 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.

8.7 Gestor da Informação

I. Autorizar e permitir acesso, validação e fiscalização de uso de dados e de informações, bem como a definição dos controles;
II. Auxiliar o Agente de transparência no processo de revisão do rol de informações protegidas da Companhia;
III. Classificar o nível de confidencialidade e sigilo da informação internamente, de acordo com a norma interna e as prerrogativas do processo.

8.8 Usuário

I. Responder pela segurança das informações as quais tem acesso em qualquer meio;
II. Evitar a exposição desnecessária de dados e informações de que tenha posse, ainda que seja objeto de seu cargo ou sua função, devendo zelar pelas informações classificadas tanto pela normativa interna, quanto em seus períodos;

III. Zelar pelo recurso de tecnologia da informação disponibilizado pela Sanepar, sendo de responsabilidade pessoal aqueles recursos individualmente disponibilizados.

9. RESPONSABILIZAÇÕES

9.1 A não aderência às responsabilidades dispostas na presente Política deverá ser reportada tanto ao Comitê de Segurança da Informação quanto para a Gerência de Governança, Riscos e Compliance e serão tratadas nos moldes do previsto no Código de Conduta e no Regulamento Disciplinar da Sanepar, sem prejuízo de incidência de outras normas que regulam as questões de segurança da informação e relações de trabalho.

9.2 O descumprimento das disposições contidas nesta política, e demais normas relativas à Segurança da Informação, poderá acarretar na aplicação de medidas disciplinares conforme o Programa de Integridade da Sanepar, independente de responsabilização administrativa, civil e criminal.

10. REVISÃO

Esta 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.

11. DISPOSIÇÕES FINAIS

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

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

12. HISTÓRICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO			**Versão**	**3ª**
			Área Gestora	**DAGRC**
			Sigilo	**Público Externo**
Versão	**Data**	**Responsável**	**Aprovador**	**Descrição da Alteração**
1ª	27/08/2020	Diretoria de Governança, Riscos e Compliance	Conselho de Administração	Emissão Inicial
2ª	17/11/2022	Diretoria de Governança, Riscos e Compliance	Conselho de Administração	Primeira Revisão
3ª	19/10/2023	Diretoria de Governança, Riscos e Compliance	Conselho de Administração	Segunda Revisão, inserção da segurança desde a concepção