

RESOLUÇÃO N.º 327, DE 12 DE DEZEMBRO DE 2019

Aprova a Política de Segurança da Informação do SEPREV.

O CONSELHO ADMINISTRATIVO DO SEPREV – Serviço de Previdência e Assistência à Saúde dos Servidores Municipais de Indaiatuba, usando das atribuições que lhe são conferidas por lei, e

CONSIDERANDO que a informação é um ativo essencial da organização e precisa ser protegida quanto a eventuais ameaças, preservando e minimizando os riscos para a continuidade dos serviços prestados pelo SEPREV;

CONSIDERANDO que a adoção de procedimentos que garantam a segurança das informações deve ser prioridade constante das organizações públicas e privadas, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da instituição;

CONSIDERANDO o disposto no Manual do Programa de Certificação Institucional e de Modernização da Gestão dos Regimes de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios – “PRÓ-GESTÃO RPPS”, aprovado pela Portaria nº 3, de 31 de janeiro de 2018, da Secretaria da Previdência;

CONSIDERANDO a deliberação do Conselho Administrativo na reunião ordinária realizada em 12 de dezembro de 2019.

R E S O L V E:

Art. 1º. Estabelecer a **Política de Segurança da Informação (PSI)** no âmbito do SEPREV, da qual são parte integrante todas as normas e procedimentos complementares e afins editados pelo SEPREV.

Parágrafo único. A Política de Segurança da Informação deverá ser revista no mínimo a cada 2 (dois) anos.

Art. 2º. A Política de Segurança da Informação é o documento que orienta e estabelece as diretrizes corporativas do SEPREV para a segurança do manuseio,

tratamento e controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio, pelos sistemas de informação no âmbito do SEPREV.

Art. 3º. Constituem objetivos desta PSI:

I – Estabelecer diretrizes que permitam aos colaboradores do SEPREV seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da Autarquia e do indivíduo;

II – Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento; e

III – Estabelecer mecanismos de controle para garantir a efetiva proteção dos dados, informações e conhecimentos gerados, preservando a:

a) 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;

b) Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas; e

c) Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Art. 4º. As diretrizes estabelecidas nesta Resolução se aplicam aos colaboradores do SEPREV, assim definidos os membros de órgãos colegiados (Conselhos e Comitês), os servidores, os estagiários e demais agentes públicos ou particulares que executem atividades vinculadas à atuação institucional da Autarquia.

Parágrafo único. Esta Resolução e as normas complementares são divulgadas a todos os colaboradores, não os eximindo da responsabilidade de se manterem atualizados quanto a estas normas, devendo buscar orientação sempre que não estiverem absolutamente seguros quanto à aquisição, uso e/ou descarte de informações.

Art. 5º. Os colaboradores deverão:

I - Manter sigilo dos dados e informações que tiverem acesso;

II - Zelar pelos ativos de informação do SEPREV, sejam eles físicos (processos, documentos, etc) ou digitais (arquivos lógicos, sistemas, etc); e

III - Seguir as diretrizes e recomendações da Superintendência quanto ao uso, divulgação e descarte de dados e informações.

§ 2º. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao SEPREV e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Art. 6º. Para garantir as regras mencionadas nesta PSI, o SEPREV poderá:

I - Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, sistema de telefonia, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

II - Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação do superior hierárquico;

III - Realizar, a qualquer tempo, inspeção nos equipamentos de sua propriedade; e

IV - Instalar sistemas de proteção e de monitoramento para garantir a segurança das informações e dos perímetros de acesso – físicos e lógicos.

Art. 7º. A Superintendência do SEPREV editará Normas Complementares de Segurança (NCS) com o objetivo de atender ao disposto nesta Resolução, devendo normatizar no mínimo:

I – Uso do Serviço de Correio Eletrônico;

II – Uso do Serviço de Internet;

III – Uso de Computadores e outros Dispositivos; e

IV – Procedimentos de Contingência que determinem a existência de cópias de segurança dos sistemas informatizados e dos bancos de dados e o controle de acesso (físico e lógico) aos sistemas.

Art. 8º. A aplicação de penalidades decorrentes do descumprimento das regras estabelecidas por esta Resolução e pelas Normas Complementares de Segurança respeitará o disposto no Estatuto dos Servidores Públicos Municipais de Indaiatuba ou no contrato firmado com o SEPREV, conforme o caso.

Art. 9º. Caberá a Superintendência do SEPREV apresentar relatório e eventuais normativas para a adequação desta Política, na forma, critério e prazo

estabelecidos na Lei Federal nº 13.709, de 14 de agosto de 2018, que dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD).

Art. 10. Esta Resolução entrará em vigor na data de sua publicação.

Indaiatuba, 12 de dezembro de 2019

Vani Rosa Moreira Rieder
Presidente do Conselho Administrativo