



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

Informação é o resultado do processamento, manipulação e organização de dados. Sendo esta representante de uma modificação qualitativa e quantitativa no sistema de conhecimento que a recebe. A informação é um dos principais patrimônios da rede de negócios pública e privada, o que a torna por consequência alvo de constantes ameaças internas e externas, colocando em risco a integridade, justiça e preservação da mesma.

As informações tratadas no Regime Próprio de Previdência Social dos Servidores Públicos de Nova Esperança do Sul – NESPREV, são de fundamental importância para o núcleo político, social e cultural, sendo influenciadora direta do desenvolvimento municipal, e mesmo que sejam de acesso público, torna-se de sublime importância que um criterioso processo de segurança seja estabelecido para proteção das informações por todos aqueles os quais possuem acesso a tais elementos.

É para garantir a integridade das informações que o NESPREV administra, que criamos a Política de Segurança da Informação, sendo esta, alicerce para proteção dos dados do Setor de Previdência Municipal. Tendo como objetivo a confidencialidade, integridade e acessibilidade das informações, garantindo o sigilo e acesso exclusivo de pessoas especificamente autorizadas, e assegurando que ao gerenciar e processar os dados sejam mantidos íntegros.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2.1 PROTEÇÃO DA INFORMAÇÃO

A informação é instrumento essencial para a operação das atividades no NESPREV, devendo esta ser adequadamente manuseada e protegida, podendo estar presente em diversas formas, tais como: sistema de informação, conjunto de arquivos, banco de dados, informações em rede, diferentes tipos de mídias, como impressa, televisiva e digital, e, ainda, por meio da comunicação oral.

As informações manuseadas no NESPREV constituem influente contribuição para estabilidade e conservação da organização e de todo núcleo municipal, desta forma, independente do modo a qual for manifesta, compartilhada, processada ou armazenada, é fundamental que seja utilizada apenas para a finalidade autorizada e manipulada em concordância com as necessidades destinadas, para manter a integridade das informações e garantir que não sejam utilizadas de forma desonesta, sendo indevidamente manipuladas, divulgadas, destruídas, ou qualquer outro procedimento que cause danos ou riscos diretos ou indiretos ao setor do NESPREV, e para também assegurar a qualidade, integridade e fidelidade das informações disponibilizadas.



ESTADO DO RIO GRANDE DO SUL

MUNICÍPIO DE NOVA ESPERANÇA DO SUL

SECRETARIA DE ADMINISTRAÇÃO E GESTÃO PÚBLICA

REGIME PRÓPRIO DE PREVIDÊNCIA SOCIAL DOS SERV. PÚBL. DE NOVA ESPERANÇA DO SUL - NESPREV

2.2 RESPONSABILIDADES

Toda e qualquer pessoa deve compreender o papel e importância da segurança das informações em suas atividades diárias, garantindo o cumprimento da legislação vigente e normatização dos órgãos, entidades e instituições dirigentes. Reguladas por princípios éticos e morais que sustentem a integridade de todos os seus participantes.

É responsabilidade do Regime Próprio de Previdência Social dos Servidores Públicos de Nova Esperança do Sul, garantir a seguridade de todos os dados manuseados pelo setor, seja através de seu funcionário, estagiário, prestador de serviços, parceiro ou visitante, assegurando a realização das orientações, procedimentos, políticas e padrões estabelecidos para fazer cumprir a presente Política de Segurança de Informação.

3. PRINCÍPIOS E DIRETIVAS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

3.1 CLASSIFICAÇÃO DA INFORMAÇÃO

3.1.1 INFORMAÇÃO PÚBLICA

Está em vigor desde de 16 de maio de 2012 a Lei de Acesso a Informação (LAI) – Lei nº 12.527/11, a qual garante a transparência e a acessibilidade de dados e informações, tendo como princípio a publicidade e divulgação de informações de interesse público. Todas as informações produzidas ou custodiadas pelo poder público são de acesso aberto para todos os membros da comunidade em geral, sendo estas as informações produzidas ou controladas por órgãos públicos e entidades públicas e ainda informações pertinentes ao patrimônio público, utilização de serviços públicos, licitações e contratos administrativos.

Referente ao Regime Próprio de Previdência Social dos Servidores Públicos do município de Nova Esperança do Sul as informações de interesse público são disponibilizadas por meio do Sistema de Cadastro Previdenciário dos RPPS (Cadprev), sendo obrigatório o envio das seguintes informações:

- Demonstrativo das Aplicações e Investimentos dos Recursos – DAIR
- Demonstrativo de Informações Previdenciárias e Repasses – DIPR
- Demonstrativo da Política de Investimentos – DPIN
- Demonstrativo de Resultados de Avaliação Atuarial – DRAA
- Cadastramento/alteração do Regime de previdência e de Entes Federativos

As informações de interesse público estão também disponibilizadas no endereço online da Prefeitura municipal (<http://www.novaesperancadosul.rs.gov.br>) na seção referente ao NESPREV. Qualquer interessado pode, ainda, apresentar um pedido para acessar as informações de interesse público, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação solicitada.



ESTADO DO RIO GRANDE DO SUL

MUNICÍPIO DE NOVA ESPERANÇA DO SUL

SECRETARIA DE ADMINISTRAÇÃO E GESTÃO PÚBLICA

REGIME PRÓPRIO DE PREVIDÊNCIA SOCIAL DOS SERV. PÚB. DE NOVA ESPERANÇA DO SUL - NESPREV

3.1.2 INFORMAÇÃO CONFIDENCIAL

A Lei de nº 12.527/11 define informação como “dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato”, tratando ainda das possíveis exceções que dizem respeito a informações confidenciais, as quais não disponíveis ao público ou reservadas, consideradas imprescindíveis à segurança da sociedade ou do Estado, que possam por meio direto ou indireto pôr em risco a vida, segurança e saúde da população, prejudicar a condução de negociações ou as relações internacionais do País, causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, ou comprometer atividades de inteligência, investigação ou fiscalização em andamento, relacionadas com a correção e cautela de infrações.

Na parte tangível ao NESPREV, são consideradas informações confidenciais não disponíveis ao público ou reservadas, sistemas de informação, bancos de dados, diretórios de redes, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pelo Setor de Previdência Municipal. Nenhuma das informações consideradas confidenciais podem ser repassadas a terceiros sem a autorização do NESPREV, sendo responsáveis pela seguridade destas informações o funcionário, estagiário, prestador de serviços, parceiro ou participante do Setor, sendo protegidas de alterações não autorizadas a disponibilizadas apenas às pessoas autorizadas a manuseá-las dentro das diretrizes estabelecidas. Devendo estas informações serem tratadas em conformidade com a normatização referente aos processos de utilização ou arquivamento.

São exemplos de informações sigilosas, não disponíveis ao acesso público, informações de clientes protegidas por obrigatoriedade legal, incluindo dados cadastrais como CPF, RG, etc, situação financeira e bancária dos mesmos, todo o material estratégico do NESPREV, seja ele impresso ou armazenado em sistemas, todos os tipos de senhas, sistemas, redes, arquivos, e outras informações utilizadas na autenticação da identidade de funcionários, estagiários, prestadores de serviços, parceiros ou participantes, sendo estas informações pessoais e intransferíveis, e também qualquer informação do setor que não deve ser divulgada a meios externos antes da publicação pelas áreas competentes.

Se houver uso indevido, fraude, revelação, com o intuito de prejudicar ou causar danos ao órgão municipal, o funcionário ou cidadão o qual tiver conhecimento do mau uso das informações deve informar imediatamente o NESPREV. Podendo a falha na confidencialidade ou integridade das informações trazer grandes prejuízos ao órgão municipal, tendo potencial para trazer prejuízos financeiros, perdas de produtividade ou a imagem do NESPREV, causando danos graves ao setor e ao município.



3.2 RECURSOS DE INFORMAÇÃO

Todos os recursos de informação devem ser protegidos, sejam eles documentos em papel, mídias removíveis, bancos de dados e sistemas. Apenas os equipamentos e softwares legítimos disponibilizados pelo NESPREV podem ser instalados e conectados à rede do setor. Devendo toda informação, documento, dado, arquivo, ou sistema, serem devidamente arquivados e protegidos de acordo com os processos estabelecidos para seu manuseio.

3.3 SISTEMAS E RECURSOS DE REDE

O acesso a sistemas de informação, bancos de dados, diretórios de redes e demais recursos devem ser restritos a pessoas autorizadas, devendo as senhas e autorizações a conexão de sistemas serem disponibilizadas para o acesso mínimo necessário para o desempenho da função e cumprimento da ação solicitada. Sendo os funcionários, estagiários, prestadores de serviços, parceiros ou participantes, responsáveis pela posse e utilização das senhas e autorizações de acesso a sistemas.

3.4 LOGIN E SENHA

Todo funcionário e estagiário do NESPREV possui um login e senha próprios para utilização dos sistemas de informações e recursos tecnológicos disponíveis no setor, sendo o funcionário ou estagiários responsáveis por todos os atos executados com seu identificador. Sendo dever do funcionário ou estagiário do NESPREV:

- Manter o sigilo de sua senha e login.
- Memorizar e não registrar em papel ou mídia.
- Alterar a senha quando houver suspeita do comprometimento da mesma.
- Zelar pelo seu equipamento, impedindo acesso por outras pessoas, quando não autorizadas ou quando conectados com sua própria identificação.
- Bloquear ou desconectar o seu dispositivo quando se ausentar.

4. LEIS E REGULAMENTOS

É responsabilidade de todo funcionário, estagiário, prestador de serviços, parceiro, participante ou visitante, conhecer a legislação vigente, e cumprir todos os requisitos legais, normativas e padrões estabelecidos por esta Política de Segurança da informação.