INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MUNICIPAIS DE SÃO VICENTE FERRER – IPSESVI

RESOLUÇÃO Nº 02/2024.

Institui a Política de Segurança da Informação no Instituto de Previdência dos Servidores Municipais de São Vicente Férrer – IPSESVI, e dá outras providências.

O Diretor Presidente do Instituto de Previdência dos Servidores Municipais de São Vicente Férrer – IPSESVI, no uso de suas atribuições legais e,

Considerando a necessidade de proteção dos dados e informações dos segurados em posse do Instituto, garantindo a integridade, confidencialidade e disponibilidade dos dados;

Considerando o disposto na Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e as exigências do Programa Pró-Gestão RPPS;

Considerando a importância da capacitação contínua dos servidores e colaboradores do Instituto para garantir o adequado manuseio e proteção das informações;

RESOLVE:

Art. 1º – Fica instituída a Política de Segurança da Informação - PSI do Instituto de Previdência dos Servidores Municipais de São Vicente Férrer – IPSESVI, conforme os termos estabelecidos no Anexo I desta Resolução.

Art. 2º – Todos os servidores, conselheiros, estagiários e prestadores de serviços que acessem informações do Instituto deverão aderir à PSI, sendo esta adesão obrigatória.

Art. 3º – Esta Resolução entra em vigor na data de sua publicação.

São Vicente Férrer, 08 de outubro de 2024.

ELDELITA DE FÁTIMA BORBA MOURA
Presidente

ANEXO I – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

CAPÍTULO I – OBJETIVOS

Art. 1º – A Política de Segurança da Informação do Instituto de Previdência dos Servidores Municipais de São Vicente Férrer – IPSESVI tem como objetivos:

I – Proteger as informações dos segurados e demais dados sob guarda do Instituto;
II – Atender aos princípios da LGPD e às diretrizes do Pró-Gestão RPPS;
III – Estabelecer normas e diretrizes de proteção de dados, garantindo a confidencialidade, integridade e disponibilidade das informações;
IV – Garantir a transparência na gestão de dados e informações;
V – Assegurar que todos os envolvidos com o Instituto compreendam suas responsabilidades no que se refere à segurança da informação;
VI – Promover a capacitação contínua dos servidores para garantir a correta aplicação da PSI e o cumprimento das normas de proteção de dados.

CAPÍTULO II – TERMINOLOGIAS

Art. 2º – Para os fins desta Política, aplicam-se as seguintes definições:

I – Confidencialidade: Garantia de que as informações são acessadas apenas por pessoas autorizadas;
II – Integridade: Garantia de que as informações não sejam alteradas indevidamente, preservando sua exatidão e completude;
III – Disponibilidade: Garantia de que as informações estejam acessíveis às pessoas autorizadas sempre que necessário;
IV – Dados Sensíveis: Informações pessoais relativas à origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, ou outros dados previstos na LGPD.

CAPÍTULO III – DIREITOS E DEVERES DOS SERVIDORES

Art. 3º – São direitos dos servidores, conselheiros, estagiários e prestadores de serviço:

I – Receber orientações e treinamentos sobre boas práticas de segurança da informação;
II – Ter acesso a informações sobre os procedimentos adotados pelo Instituto para proteger seus dados;
III – Denunciar, de forma segura, qualquer violação à PSI.

Art. 4º – São deveres dos servidores, conselheiros, estagiários e prestadores de serviço:

I – Manter a confidencialidade das informações acessadas no exercício de suas funções;
II – Respeitar as normas e diretrizes estabelecidas pela PSI no uso dos sistemas e ferramentas do Instituto;
III – Comunicar imediatamente qualquer incidente de segurança ou suspeita de violação ao

superior imediato ou à Comissão de Acompanhamento da PSI;
IV – Adotar boas práticas de segurança no manuseio de dados e documentos, físicos ou eletrônicos;
V – Atender às previsões do Código de Ética e Conduta do IPSESVI no que tange à integridade e confidencialidade das informações.

CAPÍTULO IV – FORMAS DE PROTEÇÃO DOS DADOS

Art. 5º – O Instituto deverá implementar as seguintes medidas de proteção dos dados e informações:

I – **Controle de Acesso**: Restringir o acesso a informações confidenciais apenas a usuários autorizados mediante autenticação segura;
II – **Senhas Fortes**: Exigir a utilização de senhas robustas, com combinações de letras, números e caracteres especiais;
III – **Autenticação de Dois Fatores**: Implementar autenticação de dois fatores para o acesso a sistemas que contenham dados sensíveis, quando possível;
IV – **Compartilhamento Seguro de Dados**: Garantir que o compartilhamento de informações com terceiros seja feito apenas de forma segura.
V – **Backup Regular**: Realizar backups periódicos das informações em servidores seguros para garantir a recuperação em caso de perda de dados;
VI – **Monitoramento:** Monitorar o acesso a sistemas e dados para identificar e registrar atividades suspeitas ou não autorizadas;
VII – **Bloqueio Automático de Tela:** Implementar bloqueio automático de estações de trabalho após período de inatividade;
VIII – **Segurança Física de Documentos**: Armazenar documentos físicos em locais seguros com controle de acesso e registro de entrada e saída;
IX – **Descarte Seguro**: Proceder ao descarte seguro de documentos físicos e digitais, utilizando métodos que garantam a destruição completa das informações;
X – **Proteção contra Malware**: Utilizar softwares de proteção contra vírus, malwares e outras ameaças digitais em todas as máquinas e servidores;
XI – **Atualizações Regulares:** Manter sistemas e softwares sempre atualizados com as últimas versões e patches de segurança;
XII – **Treinamento Contínuo**: Promover treinamento periódico aos servidores e prestadores de serviços sobre a importância da segurança da informação e as práticas adequadas;
XIII – Restrição de Dispositivos Externos: Controlar o uso de dispositivos de armazenamento externo (pendrives, HDs externos) nos computadores do Instituto;

CAPÍTULO V – CAPACITAÇÃO E TRANSPARÊNCIA

Art. 6º – O Instituto deverá promover capacitações periódicas sobre segurança da informação, garantindo que servidores, conselheiros, estagiários e prestadores de serviços estejam sempre atualizados sobre as melhores práticas de proteção de dados.

Art. 7º – A Política de Segurança da Informação deverá ser amplamente divulgada e publicada no site institucional do IPSESVI, assegurando a transparência para todos os segurados e demais interessados.

CAPÍTULO VI – ACOMPANHAMENTO E FISCALIZAÇÃO

Art. 8º – A Presidente do Instituto será responsável por monitorar o cumprimento desta Política e sugerir melhorias contínuas.

CAPÍTULO VII – DISPOSIÇÕES FINAIS

Art. 9º – O não cumprimento das disposições da Política de Segurança da Informação resultará em sanções administrativas.

Art. 10 – Esta Política será revisada periodicamente, a fim de garantir sua constante adequação às normas legais e melhores práticas de segurança da informação.

São Vicente Férrer, 08 de outubro de 2024.

ELDELITA DE FÁTIMA BORBA MOURA
Presidente