POLÍTICA DE SEGURANÇA DA

INFORMAÇÃO

2022

Diretoria Executiva

Diretor Presidente
Jorge Alberto Almeida da Silva

Diretor de Finanças e Administração
Murilo Tavares Dalia

O PREV DUAS BARRAS é o Regime de previdência estabelecido no âmbito do Município de Duas Barras, sob o regime jurídico autárquico, para assegurar aos servidores titulares de cargo efetivo, os benefícios de aposentadoria e pensão por morte previstos no art. 40 da Constituição Federal.

Criado em 1993, pela Lei Municipal n° 527/93, na então gestão do Prefeito Luiz Gonzaga Pagnuzzi Araujo, denominação a época como Instituto de Aposentadoria e Pensão de Duas Barras – IAPDB, passou a ser denominado **INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE DUAS BARRAS – PREV DUAS BARRAS**, através da reestruturação promovida pela Lei Municipal nº 918/2018, tem como objetivo receber, assegurar e administrar os recursos financeiros e outros ativos para o custeio dos benefícios previdenciários a serem concedidos os seus segurados e respectivos dependentes.

APRESENTAÇÃO

Este documento tem por objetivo divulgar, no ambiente interno do PREV DB, as Políticas de Segurança da Informação, buscando orientar os usuários para utilização segura dos recursos de tecnologia da informação assegurados pela empresa especializada em sistemas informatizados para gestão de dados de contabilidade pública, tesouraria, recursos humanos, almoxarifado e bens patrimoniais do PREV DB.

Sumário:

1. INTRODUÇÃO

A principal justificativa para existência de uma política de segurança da informação nas instituições e empresas ocorre em função de estarmos inseridos em uma realidade em que a tecnologia é um elemento indispensável em qualquer setor, independentemente do porte ou área de atuação, utilizam em suas operações e principais sistemas, os computadores, com grande dependência da conectividade, por essa razão em tempos atuais, faz-se te extrema necessidade uma política de segurança da informação.

Em conformidade com essa realidade, muitas são as abrangências das circulações de informações tanto dentro de uma organização, quanto fora dela, através da internet.

Já é questão de extrema necessidade ter políticas que, documentadas, detalhem procedimentos e diretrizes para eliminar os riscos de acesso as informações sensíveis.
Dessa forma, uma política de segurança da informação, garante por meio de controles bem definidos que ainda asseguram referências para auditorias e ações corretivas.

O termo tecnologia da informação (TI) pode ser definido como o conjunto de recursos tecnológicos e computacionais para geração e uso da informação, abrangendo todas as atividades desenvolvidas na sociedade pelos recursos da informática.

Todos os recursos relacionados à tecnologia da informação, como Internet, correio eletrônico, redes sem fio, são exemplos de ferramentas de trabalho indispensáveis para realização das mais diversas atividades. Vale considerar que esses recursos podem ser utilizados para fins ilícitos, como roubo de informações e disseminação de vírus e tantos outros.

Diante do exposto, a criação desse documento, visa orientar a todos em um contexto de ambiente de trabalho, como também aos servidores e segurados, uma utilização segura dos recursos de tecnologia da informação disponibilizada pela instituição.

2. APLICAÇÃO:

Este documento que aborda a política de segurança da informação destina-se a aplicação por todos os servidores, prestadores de serviços, parceiros e usuários que utilizam informacional do PREV DB. As ações aqui tratadas atendem ao cumprimento das normas constantes por todos, sendo que o descumprimento das normas, como fraudes e invasão e violação da integridade dos dados, ficará o sujeito submetido à legislação nacional em vigor. Ressalta-se que esta política de segurança da informação, aplica-se ao gerenciamento de quaisquer equipamentos, programas, sistemas de armazenamento digital de dados e informações, incluindo notebooks, impressoras, além dos servidores inseridos nas dependências do PREV DB.

3. OBJETIVOS DA POLÍTA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação tem como objetivo garantir a instituição, diretrizes e estratégias que garantam a disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como uma ação adequada para uso, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos armazenados, sob guarda e seguros quanto ameaças e vulnerabilidade e assim minimizar os riscos de acesso.

Dessa forma, a segurança da informação está em conformidade com as disposições constitucionais, legais e regimentais vigentes. Destaca-se ainda, que a política de segurança à informação abrange todos os servidores e prestadores de serviço que acessem informações, indicando a responsabilidade de cada um quanto à segurança da informação.

4. USUÁRIOS:

A utilização dos recursos informacionais no PREV DB deve obedecer por parte dos usuários da seguinte forma:

- Cuidar adequadamente do equipamento;
- Garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela empresa responsável pela manutenção na instituição, referentes ao trabalho de TI;
- O usuário tem a responsabilidade de transferir para o servidor designado às informações que estão no computador e que precisam possuir cópias de segurança.

4.1. RESPONSABILIDADE E FORMA DE USO

O usuário que utiliza acesso à internet:

- É responsável por todo o acesso realizado com a sua identificação/autenticação.
- Não é permitido acessar locais virtuais (sites) que:

*Possam violar direitos de autor, marcas, licenças de programa ou patentes existentes.
*Possuam conteúdos pornográficos, relacionado a sexo, exploração infantil ou ao crime de pedofilia.
*Defendam atividades ilegais.
*Menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.
*Que não tenham relação direta com atividade profissional desempenhada pelo usuário.
*Não retirar (copiar) dos endereços acessados, material que não seja para uso profissional do PREV DB.
*Não é permitido o uso de serviços de mensagem instantâneas através dos computadores do PREV DB, exceto quando autorizado pela Presidência.

5. GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Todos os mecanismos de proteção utilizados pela segurança da informação devem ser mantidos com o objetivo de garantir a continuidade dos trabalhados executados pelo Instituto de Previdência de Duas Barras.
Os requisitos de segurança da informação e comunicação do PREV DB devem ser explicitados nos termos de compromisso celebrados entre a instituição e terceiros, em que precisam ter conhecimento às diretrizes desta Política, com o intuito de um comprometimento de confidencialidade.

5.1. SENHAS

O acesso aos diversos serviços de informática, como sistemas, e-mail, rede local entre outros, ocorre mediante autenticação do usuário através de seu nome de usuário e senha. Tal processo visa garantir que o acesso a informação seja obtido apenas por pessoas autorizadas.

5.2. CERTIFICADO DIGITAL

Trata-se de um documento eletrônico que identifica pessoas e instituições, provando sua identidade e permitindo acessar serviços informatizados com a garantia de autenticidade, integridade e não repúdio, assim como assinar digitalmente documentos.

O Certificado digital destina-se a qualquer pessoa, física ou jurídica, sendo emitidos por uma autoridade certificadora, os certificados utilizados no PREV DB são emitidos pela K Link Certificação Digital.
Cada usuário é responsável pela guarda e utilização de seu certificado digital.

5.3. INTERNET

O acesso à internet no PREV DB está disponível para servidores a partir das estações conectadas à rede local da instituição, em que são regidos por normas específicas de acesso em que segue as demais orientações governamentais e legislação em vigor.

5.4. CORREIO ELETRÔNICO

O serviço de Correio Eletrônico Institucional está a disposição para servidores a partir de qualquer estação com acesso a internet, em que se precisa usar todo o protocolo de segurança, em que o usuário deverá seguir e atender as seguintes determinações:

- ✓ Ser responsável por todo acesso, conteúdo, mensagens e uso relativo ao seu email;
- ✓ Enviar mensagens necessárias para o seu desempenho profissional no instituto;
- ✓ Não encaminhar, copiar ou criar mensagens e imagens que contenham declarações difamatórias ou linguagens ofensivas, que façam parte de correntes de mensagens, independentemente de serem legais ou não e repassem propagandas ou mensagens de alerta sobre quaisquer assuntos.

5.5. ESTAÇÕES DE TRABALHO:

Constituem estações de trabalho os computadores e notebooks registrados como patrimônio do PREV DB e utilizados pelos servidores no desempenho de suas atividades funcionais.
Algumas determinações são imprescindíveis para efetiva segurança da informação como:

- ✓ **Não instale softwares sem autorização da diretoria, acessar somente a estação de trabalho com sua conta de usuário, tal procedimento visa garantir a confidencialidade das informações processadas.**
- ✓ **Ao se afastar da estação de trabalho, efetue ou bloqueia, evitando assim que outra pessoa acesse a estação de trabalho através do seu nome de usuário e senha;**
- ✓ **Utilize a estação de trabalho somente para fins profissionais;**
- ✓ **Mantenha a área de trabalho da estação com a menor quantidade possível de ícones, melhorando assim o desempenho do computador.**

5.6. REDE LOCAL

O acesso à rede local do PREV DB está disponível para os servidores a partir das estações de trabalho, em que algumas recomendações são importantes:

- ✓ Não utilizar computadores pessoais na rede local do PREV DB, ou seja, somente acesse a rede local através de computadores e notebooks registrados como patrimônio da instituição;
- ✓ No PREV DB, nunca usar redes sem fio de terceiros. Caso seja necessário acesso sem fio disponibilizado pela instituição quando assim permitido, evitando assim que informações sensíveis sejam interceptadas por terceiros.

5.7. CONSCIENTIZAÇÃO E CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO

O PREV DB promoverá continuamente a capacitação para todos os usuários da instituição, por meio de aperfeiçoamento no que tange a aplicação da segurança da informação e comunicação, com o propósito de criar uma cultura de segurança dentro da Instituição.