

RESOLUÇÃO Nº 02/2019

Institui a Política de Segurança da Informação do Fundo de Previdência Social do Município de Aratiba – FPSA e normatiza os procedimentos para o uso e segurança dos equipamentos de informática.

O Conselho de Administração do Fundo de Previdência Social de Aratiba, no uso de suas atribuições legais contidas na Lei Municipal de nº 3.844/2016, resolve:

Art. 1º - Aprovar, nos termos do Anexo Único desta Resolução, a **Política de Segurança da Informação** do Fundo de Previdência Social de Aratiba - FPSA

Art. 2º - Esta Resolução entra vigor na data de sua publicação.

Aratiba - RS, 08 de agosto de 2019.

ROSMARI ANGONEZE

Presidente do Conselho de Administração do RPPS

NILTON ANTÔNIO MOCELLIN

Gestor do RPPS

GIANCARLOS BIANCHI

Conselheiro

JOÃO PAULO MUSTIFAGA

Conselheiro

MAURO LUIS MENTZ

Conselheiro

MENGELE F.W. DALPONTE

Conselheira

VANDERLEI CÉSAR CASASOLA

Conselheiro

ANEXO ÚNICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
FUNDO DE PREVIDÊNCIA SOCIAL DE ARATIBA - FPSA

1.0 – DO OBJETIVO E FINALIDADE

A Política de Segurança da Informação do Fundo de Previdência Social do Município de Aratiba - FPSA busca normatizar os procedimentos para o uso com segurança dos equipamentos de informática, visando levar em consideração o uso apropriado, a proteção e a privacidade efetiva aos usuários e ao FPSA.

A Política da Segurança da Informação do FPSA tem por finalidade:

- a) Estabelecer as políticas de adoção de softwares livres e outras boas práticas de gestão da informação;
- b) Definir as responsabilidades dos servidores públicos e contratados do FPSA no que concerne à administração, proteção e uso dos recursos informacionais do FPSA;
- c) Descrever a política de proteção das informações contra o acesso não autorizado, manutenção da confidencialidade, integridade e disponibilidade das informações armazenadas e assegurar que as medidas legislativas e regulamentares e outros requisitos sejam cumpridos;
- d) Otimizar o gerenciamento de riscos, prevenir e minimizar o impacto dos incidentes de segurança da informação de modo a preservar a segurança do patrimônio intangível do FPSA.

Os objetivos da normatização dos procedimentos para o uso e segurança dos equipamentos de informática são:

- a) Orientar os usuários para a melhor utilização dos recursos computacionais;
- b) Definir responsabilidades e obrigações visando a ética de utilização;
- c) Manter a confidencialidade, integridade e disponibilidade da informação;
- d) Aplicar as devidas penalidades em caso de infração ou uso inadequado dos recursos.

2.0 – DAS CONTAS DE ACESSO

As contas de acesso ao sistema informatizado do FPSA serão fornecidas pela Administração Municipal de Aratiba, onde o usuário terá acesso a microcomputadores, correio eletrônico, internet da rede corporativa do Município, software, aplicativos e pastas em geral.

Toda conta de acesso é atribuída a uma única pessoa e será de responsabilidade e uso exclusivo de seu titular, não podendo essa permitir ou colaborar com o acesso aos recursos computacionais por parte de pessoas não autorizadas e nem compartilhar com outros usuários.

O usuário será responsável pela segurança de sua conta de acesso e senha, pelas informações armazenadas nos equipamentos dos quais faz uso e por qualquer atividade neles desenvolvida.

Em caso de demissão, exoneração, licença ou transferência, a Administração Municipal providenciará o bloqueio imediato das cotas de acesso do usuário.

3.0 – DAS ESTAÇÕES DE TRABALHO E COMPONENTES

O usuário deverá executar as tarefas e aplicações que estejam dentro do escopo de trabalho de seu setor, utilizando os programas e equipamentos com zelo e responsabilidade.

Caberá aos usuários comunicar imediatamente a Administração Municipal, quaisquer problemas que venham a ocorrer, bem como relatar qualquer suspeita de uso inadequado dos recursos computacionais.

Os usuários deverão manter os equipamentos nas suas perfeitas condições de uso na forma como lhes foram entregues.

O usuário deverá encerrar sua sessão na estação de trabalho ao término de suas atividades. Ao final do expediente, a estação de trabalho deverá ser desligada.

4.0 – DO AMBIENTE DE REDE

A Administração Municipal disponibilizará os pontos de rede necessários ao desenvolvimento das atividades dentro de seus prédios. Qualquer alteração ou criação de um ponto novo deverá ser comunicado em tempo hábil.

É proibido o uso de meios ilícitos de acesso aos computadores, sistemas e arquivos do ambiente de rede computacional do FPSA.

Não deverá utilizar quaisquer materiais, informações, incluindo arquivos, textos, planilhas ou imagens disponíveis na rede corporativa do FPSA, que não respeitem os direitos autorais, marcas registradas, patentes, sigilos comerciais ou outros direitos de propriedade intelectual de terceiros.

5.0 – DO CORREIO ELETRÔNICO

O acesso ao sistema de correio eletrônico será disponibilizado aos usuários com necessidade manifesta de usá-la como ferramenta de apoio às atividades profissionais, podendo ocasionalmente ser utilizado para mensagens pessoais curtas e pouco frequentes.

Não será permitido participar, criar, ou distribuir voluntariamente mensagens indesejáveis, como circulares, manifestos políticos, correntes de cartas ou similares que possam prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar os sistemas computacionais desnecessariamente.

Ficará proibido utilizar os serviços para o envio de SPAM. Considera-se SPAM o envio em massa de e-mails para usuários que não os solicitaram de forma explícita e com os quais o remetente não mantenha qualquer vínculo de relacionamento profissional e cuja quantidade comprometa o bom funcionamento dos servidores de e-mail.

Não será permitido o uso de endereços de e-mail para troca de informações ligadas a práticas que infringem qualquer lei nacional ou internacional.

O usuário não deverá abrir e-mails com arquivos anexados, quando não conhecer o remetente, sob o risco infectar com vírus seu equipamento.

6.0 – DA INTERNET

O uso da internet deverá ser controlado e restrito às atividades profissionais, no sentido de manter os mais altos níveis de qualificação em prol da atualização da informação.

Ficará proibido visualizar, criar, postar, carregar ou encaminhar quaisquer arquivos ou mensagens de conteúdos abusivos, obscenos, insultuosos, sexualmente tendenciosos, pornográficos, ofensivos, difamatórios, agressivos, ameaçadores, vulgares, racistas, de apologia ao uso de drogas, de incentivo à violência ou outro material que possa violar qualquer lei aplicável.

Ficará proibido utilizar ferramentas que burlam a segurança para usufruir serviços que não lhes são concebidos.

Não será permitida a manutenção não autorizada de páginas pessoais ou de serviços particulares envolvendo comercialização pela internet, utilizando os recursos computacionais do FPSA.

7.0 – DO ARMAZENAMENTO DE DOCUMENTOS E INFORMAÇÕES

O usuário deverá manter sigilo sobre os documentos e informações considerados estratégicos, confidenciais ou de interesse particular do FPSA.

Os documentos e informações considerados estratégicos ou confidenciais deverão ser armazenados nos diretórios pessoais em pasta devidamente identificada.

O diretório C:\ não deverá ser utilizado pelo usuário para guardar documentos importantes ou confidenciais, sob risco de perdê-los a qualquer tempo.

Os documentos e informações geradas pelos usuários referentes às rotinas de trabalho, no que diz respeito a: alterações, gravações e leituras, são de inteira responsabilidade do usuário do arquivo.

Os arquivos do diretório C:\ poderão ser removidos sempre que não condizer com assuntos importantes do FPSA, independentemente de seu conteúdo.

8.0 – DAS ADVERTÊNCIAS E PENALIDADES

Os usuários deverão estar cientes das regras e normas de uso dos recursos computacionais, evitando, desse modo, os procedimentos que prejudicam ou impedem outras pessoas de terem acesso a esses recursos ou de usá-los de acordo com que é determinado.

Todo servidor que tiver conhecimento de ato ilícito praticado no uso dos recursos computacionais, assim como qualquer comportamento considerado inaceitável ou suspeito de violação dessas normas, deverá comunicar o fato imediatamente ao FPSA e/ou a Administração Municipal.

Sempre que julgar necessário para a preservação da integridade dos recursos computacionais e segurança da informação ou em caso de constatação e identificação de não conformidade às normas, a Administração Municipal fará imediatamente o bloqueio temporário da conta de acesso e comunicará o superior imediato o teor da infração e o nome do responsável, para que sejam tomadas as medidas cabíveis para a apuração dos fatos.

Caso a violação de alguma norma for passível de aplicação de penalidade além das aqui determinadas, incluindo as situações determinadas graves ou reincidentes, o caso será apurado mediante a instauração de Processo de Sindicância, podendo derivar para Processo

Administrativo Disciplinar, considerando que, sempre que tiver ciência de irregularidade no Serviço Público, acha-se obrigada a autoridade competente de promover a sua apuração imediata.

9.0 – DISPOSIÇÕES GERAIS

A organização e os servidores devem cumprir rigorosamente esta Política de Segurança da Informação e todas as leis aplicáveis referentes aos assuntos dispostos. A presente Política de Segurança da Informação tem validade indeterminada, entretanto poderá haver revisões periódicas, quando necessário. O FPSA será responsável pelo monitoramento e esclarecimento de eventuais infrações. A inobservância do disposto nesta política implicará na adoção de providências necessárias, com vistas à aplicação das sanções previstas na Lei Municipal nº 2.298/2005 e suas alterações posteriores.

Para denúncias, questionamentos, reclamações, elogios, sugestões ou algo que esteja em desacordo com a Política de Segurança da Informação, dirigir-se diretamente ao FPSA pelo e-mail rpps@pmaratiba.com.br ou formulário disponível no site do FPSA <https://www.fpsaratiba.com.br/faleconosco>.

Aratiba - RS, 08 de agosto de 2019.

ROSMARI ANGONESE

Presidente do Fundo de Previdência Social de Aratiba