



FUNDO MUNICIPAL DE APOSENTADORIAS E PENSÕES - FMAP

Política de Segurança da Informação

Fevereiro de 2022

RESOLUÇÃO N.º 02, DE 14 DE FEVEREIRO DE 2022

Aprova a Política de Segurança da Informação no âmbito do FMAP - Fundo Municipal de Aposentadorias e Pensões de Itapira.

O **PRESIDENTE DO CONSELHO MUNICIPAL DE PREVIDÊNCIA** de Itapira, 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 RPPS;

CONSIDERANDO que a adoção de procedimentos que garantam a segurança das informações deve ser prioridade constante do RPPS, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer seus objetivos;

CONSIDERANDO o disposto no Manual do PRÓ-GESTÃO, aprovado pela Secretaria da Previdência;

CONSIDERANDO a deliberação do Conselho Municipal de Previdência na reunião ordinária realizada em 14 de fevereiro de 2022;

R E S O L V E:

Art. 1º. Fica aprovada a **Política de Segurança da Informação** no âmbito do FMAP - Fundo Municipal de Aposentadorias e Pensões de Itapira, na forma do Anexo Único desta Resolução.

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

Itapira, 14 de fevereiro de 2022.

Henrique Mariano Bortolotto
Presidente do Conselho Municipal de Previdência



FUNDO MUNICIPAL DE APOSENTADORIAS E PENSÕES - FMAP

Política de Segurança da Informação

CAPÍTULO I - OBJETIVOS DA PSI

Art. 1º. A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas do RPPS para a proteção dos ativos de informação e a responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas do Fundo Municipal de Aposentadorias e Pensões, e por todos os colaboradores e prestadores de serviços que tenham acesso às informações de propriedade do RPPS.

Art. 2º. Constitui objetivo da PSI:

I - estabelecer diretrizes que permitam aos colaboradores e fornecedores do RPPS seguirem padrões de comportamentos relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal do FMAP 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 - preservar as informações do RPPS quanto à:

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.

CAPÍTULO II - APLICAÇÕES DA PSI

Art. 3º. As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviços, e se aplicam à informação em qualquer meio ou suporte.

Parágrafo único. É obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

CAPÍTULO III - DAS RESPONSABILIDADES ESPECÍFICAS

Art. 4º. Entende-se por colaborador toda e qualquer pessoa física, contratada no regime estatutário, CLT ou temporário, e os prestadores de serviços, contratados por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora do RPPS.

§ 1º. Os colaboradores deverão:

I - manter sigilo das informações do RPPS;

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

III - seguir as diretrizes e recomendações do FMAP 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 RPPS e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

CAPÍTULO IV - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Art. 5º. Para garantir as regras mencionadas nesta PSI, o FMAP poderá:

I - implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, 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 física nos equipamentos de sua propriedade; e

IV - instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

CAPÍTULO V - CORREIO ELETRÔNICO

Art. 6º. O uso do correio eletrônico do RPPS é para fins corporativos e relacionados às atividades do colaborador usuário do Fundo Municipal de Aposentadorias e Pensões, sendo terminantemente proibido:

I - enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo do FMAP;

II - enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

III - enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o RPPS vulneráveis a ações civis ou criminais;

IV - divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

V - falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

VI - apagar mensagens pertinentes de correio eletrônico quando o RPPS estiver sujeito a algum tipo de investigação;

VII - produzir, transmitir ou divulgar mensagem que:

a) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do RPPS;

b) contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;

c) contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

d) vise obter acesso não autorizado a outro computador, servidor ou rede;

e) vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

f) vise burlar qualquer sistema de segurança;

g) vise vigiar secretamente ou assediar outro usuário;

h) vise acessar informações confidenciais sem explícita autorização do proprietário;

i) vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

j) inclua imagens criptografadas ou de qualquer forma mascaradas;

k) tenha conteúdo considerado impróprio, obsceno ou ilegal;

l) seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, entre outros;

m) contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

n) tenha fins políticos locais ou do país (propaganda política);

o) inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

Art. 7º. As mensagens de correio eletrônico sempre deverão incluir assinatura com os seguintes dados formato:

I - Nome do colaborador;

II - Cargo/Departamento;

III - Nome do RPPS;

IV - Telefone(s); e

V - Site do RPPS na Internet.

Parágrafo único. O Presidente ou outro servidor designado, poderá definir o formato da assinatura de que trata este artigo, obrigando sua utilização por todos os usuários do correio eletrônico.

CAPÍTULO VI - INTERNET

Art. 8º. Exige-se dos colaboradores usuários comportamento eminentemente ético e profissional do uso da internet.

Art. 9º. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do FMAP, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

§ 1º. Qualquer informação acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria, tendo o RPPS, em total conformidade legal, o direito de monitorar e registrar todos os acessos a ela.

§ 2º. Qualquer alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo superior hierárquico.

§ 3º. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos o RPPS cooperará ativamente com as autoridades competentes.

§ 4º. O uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Art. 10º. Somente os colaboradores que estão devidamente autorizados a falar em nome do RPPS para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Art. 11º. Apenas os colaboradores autorizados pelo FMAP poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

Parágrafo único. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Art. 12º. Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no RPPS e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pelo responsável da área de TI.

§ 1º. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

§ 2º. Os colaboradores não poderão, em hipótese alguma, utilizar os recursos do RPPS para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Art. 13º. É proibido o acesso, exposição, armazenamento, distribuição, edição, impressão ou gravação por meio de qualquer recurso, de materiais de cunho sexual.

Art. 14º. Os colaboradores não poderão utilizar os recursos do RPPS para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

Art. 15º. As regras expostas neste capítulo se aplicam ao uso de computadores e outros dispositivos de propriedade do RPPS, bem como a dispositivos particulares dos usuários que estiverem conectados à internet do RPPS (cabeados ou sem fio).

CAPÍTULO VII - COMPUTADORES E OUTROS DISPOSITIVOS

Art. 16º. Os computadores disponibilizados pelo FMAP aos colaboradores, constituem instrumento de trabalho para execução das atividades do RPPS.

§ 1º. Cada colaborador deve zelar para segurança e bom uso dos equipamentos, reportando à área competente qualquer incidente que tenha conhecimento.

§ 2º. Em caso de mau uso, ou uso em desacordo com as instruções desta norma, o colaborador poderá ser responsabilizado.

CAPÍTULO VIII - IDENTIFICAÇÃO E CONTROLE DE ACESSO

Art. 17º. Para o acesso aos recursos tecnológicos do FMAP será exigido, sempre que possível, identificação e senha exclusiva de cada colaborador, permitindo assim o controle de acesso.

§ 1º. É proibido o compartilhamento de login entre os colaboradores.

§2º. Recomenda-se como boa prática de segurança que, ao realizar o primeiro acesso ao ambiente de rede local, o usuário seja direcionado a trocar imediatamente a sua senha.

§ 3º. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

§ 4º. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.