PORTARIA N.º 89, DE 7 DE DEZEMBRO DE 2020

Institui a Política de Segurança da Informação no Instituto de Previdência do Município de Mafra - IPMM.

O Diretor Presidente do Instituto de Previdência do Município de Mafra – IPMM, CARLOS OTÁVIO SENFF, no uso das atribuições que lhe são conferidas pela Lei 2.571/01,

RESOLVE

Art. 1º. Instituir a Política de Segurança da Informação no âmbito do Instituto de Previdência do Município de Mafra – IPMM, constante do Anexo Único desta Portaria.

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

CARLOS OTÁVIO SENFF
Diretor Presidente do Instituto de Previdência do Município de Mafra - IPMM

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO DE PREVIDÊNCIA DO MUNICÍPIO DE MAFRA - IPMM

SUMÁRIO

1. INTRODUÇÃO

As normas descritas neste documento têm como objetivo orientar os servidores e os prestadores de serviços que acessem informações do Instituto de Previdência do Município de Mafra (IPMM) sobre o correto uso dos recursos disponibilizados, bem como apontar práticas proibidas e passíveis de sanções.

Após a leitura deste documento, caso ainda haja dúvida sobre situações e atos considerados violações das normas aqui expostas, o usuário deve entrar em contato com seus superiores ou com o responsável pela segurança da informação no IPMM.

Os recursos de Tecnologia da Informação englobam todos os equipamentos, periféricos, suprimentos e qualquer outro serviço e/ou dispositivo correlato disponibilizado pelo IPMM aos usuários para a realização de atividades diversas, dentre os quais estão incluídos impressoras e suprimentos (papel, tôner, cartuchos de tinta, etc), dispositivos de armazenamento (pendrive, memory card, disquete, CD, DVD, etc), computadores, tablets, celulares, smartphones, contas de acesso (internet, correio eletrônico e demais sistemas), escâneres, rede local, câmeras digitais, etc.

O uso dos recursos de Tecnologia da Informação e de telecomunicação do IPMM restringem-se exclusivamente a fins de interesse público, sendo vedada a utilização para finalidades particulares ou maliciosas como:

1. Efetuar download e/ou armazenar músicas, vídeos, fotos, entre outros para uso ou interesse pessoal;

2. Utilizar computadores, impressoras ou outro dispositivo ou recurso do IPMM para desenvolver trabalhos particulares de qualquer finalidade que não sejam em benefício do IPMM;

3. Acessar contas de e-mail particulares utilizando computadores ou a conexão de acesso à internet do IPMM quando a conexão não for disponibilizada para este fim ou quando não houver autorização expressa do responsável pela segurança da informação do IPMM;

4. Usar as contas de e-mail disponibilizadas pelo IPMM para enviar correntes, mensagens de meditação, autoajuda ou spams, com ou sem anexos ou contendo qualquer assunto que não se refira a suas atividades laborais;

5. Acessar, por meio de computadores ou da conexão de acesso à internet do IPMM, páginas com conteúdo impróprio para o ambiente de trabalho, como blogs, fotologs, páginas de relacionamentos (exceto páginas oficiais do IPMM e para usuários expressamente autorizados pela chefia), conteúdos

pornográficos, horóscopo, etc;

6. Acessar, alterar, adulterar ou remover indevidamente pastas, arquivos, sistemas ou qualquer recurso disponibilizado.

A política de uso dos recursos de Tecnologia da Informação visa oferecer maior segurança e comodidade aos usuários. Uma rede não controlada é totalmente suscetível a ataques que, entre outros, ocasionam a destruição ou furto de informações, congestionamento da rede e impossibilidade de manutenção dos serviços.

Estas normas podem ser atualizadas a qualquer momento, conforme sejam notadas mudanças ou necessidades de adequação no cenário atual, bem como alterações na legislação vigente. Qualquer prática não mencionada ou não explicitamente permitida é considerada proibida e caracteriza violação a esta Política, sendo passível das punições previstas neste documento.

Nos itens descritos a seguir apresentam-se as normas para a utilização dos recursos de tecnologia da informação.

2. DAS CONTAS DE ACESSO

- Cada usuário possui uma conta de e-mail específica para cada recurso e/ou serviço a ele autorizado. É do proprietário da conta a responsabilidade por manter o sigilo de suas senhas e a responsabilidade administrativa, civil e/ou penal por qualquer dano causado ao IPMM ou a terceiros por meio de suas contas de acesso. Usuários flagrados utilizando contas de acesso de terceiros responderão pelo ato e a conta em questão será imediatamente bloqueada;

- Somente os superiores diretos ou pessoas por ele designadas estão autorizadas a solicitar criação de contas de acesso aos usuários. Os superiores têm responsabilidade direta sobre a criação de contas de acesso para os seus subordinados e serão cobrados sobre solicitações de criação de contas de acesso indevidas, para fins particulares ou que não sejam para uso profissional no IPMM;

- Solicitações de criação de contas que sejam identificadas como sendo de acesso indevido, não autorizado, para uso particular ou que não tenha relação com as atividades laborais do usuário não serão atendidas e o superior direto do funcionário será notificado. Caso a conta já exista, mas

se encaixe em uma ou mais situações descritas acima, o IPMM reserva-se o direito de cancelar o acesso;

- Qualquer tentativa, por parte do usuário, de obtenção de acesso não autorizado ou de interferir na qualidade e/ou confiabilidade de equipamentos informáticos ou sistemas, rede interna, conexões de acesso, dados ou serviços mantidos e disponibilizados, seja qual for a finalidade, será considerada como falta grave e acarretará os procedimentos administrativos e legais cabíveis ao caso;

- O IPMM reserva-se o direito de monitorar e gravar todos os acessos e conexões a seus links de acesso à internet independentemente da origem da conexão, bem como monitorar o acesso a seus sistemas e equipamentos, incluindo capturas de tela dos computadores do IPMM. Os conteúdos classificados como impróprios ou não autorizados serão bloqueados. O IPMM poderá usar os dados de acessos gravados e informações coletadas para comprovar desvios de conduta ou violações das normas previstas neste documento e no Estatuto dos Servidores de Mafra.

3. DO ACESSO À INTERNET

Todos os acessos à internet são gravados em um banco de dados de auditoria, estando disponíveis para possível verificação da Diretoria e dos Supervisores de cada área, contendo a hora, tempo de acesso, páginas acessadas e o tráfego consumido da conexão. Os acessos indevidos, quando detectados, serão coibidos e o usuário responderá perante seus superiores.

Em relação aos acessos à internet, o controle de acesso bloqueia por padrão as seguintes situações (exceto para usuários devidamente autorizados pela chefia):

- Sites já catalogados como impróprios;
  - Blogs, Fotologs e jogos online;
  - Sites de relacionamento (Facebook, Twitter, LinkedIn, etc);
  - Conteúdos pornográficos;
  - Horóscopos, numerologia e outros conteúdos místicos;

- Serviços de streaming de áudio ou vídeo como TVs ou rádios online;
- Sites ou conteúdos suspeitos ou que exponham o computador ou a rede interna a riscos de segurança (malware, spyware, rootkit, phishing, etc).

- Downloads de arquivos executáveis, scripts ou qualquer arquivo com risco potencial de transmitir vírus ou explorar falhas de segurança e combater pirataria;
- Acesso a webmail de contas de e-mail que não sejam as oficiais do IPMM;
- Uso de softwares de troca de arquivos, mais conhecidos como P2P (kazaa, Morpheus, Emule, Bittorrent e afins).

Obs.: Haverá casos em que conteúdos legítimos poderão ser bloqueados. Caso isso ocorra, o usuário deve solicitar o desbloqueio, pois assim estará ajudando a refinar o sistema de segurança.

- É proibido o upload de softwares licenciados pelo IPMM, arquivos ou informações confidenciais do IPMM;
- O uso de softwares de mensagens instantâneas é autorizado com restrições e somente para fins laborais, sendo liberado mediante solicitação de serviços, justificativa plausível do superior imediato;
- É vedado o uso das conexões do IPMM para postar ou inserir na internet conteúdo ou comentários ofensivos, preconceituosos, discriminatórios ou que caracterizem assédio moral ou sexual, assim como propaganda política, publicidade comercial e anúncios que não sejam de interesse do IPMM;
- O uso da internet durante o horário de expediente é exclusivamente para fins de interesse do IPMM. É permitido ao usuário utilizar a Internet para atividades não relacionadas ao trabalho durante o horário de almoço ou fora do expediente, desde que dentro das regras de uso definidas neste regulamento.

4. DO USO DE E-MAILS

- Cada usuário é responsável por sua conta de e-mail. Caso desconfie

que alguém está enviando e-mails utilizando a sua conta, deve alterar a senha.

- Não é permitida a configuração e uso de contas de e-mails que não sejam do Instituto nos computadores pertencentes ao IPMM;
- É veementemente vedada a utilização de contas de e-mail de terceiros, assim como o ato de forjar qualquer informação do código fonte do e-mail ou de configuração de conta a fim de se passar por outra pessoa. Essa atitude será enquadrada como crime de falsidade ideológica, passível de processo penal e sanções administrativas;
- Não é permitido usar as contas de e-mail disponibilizadas pelo IPMM para enviar, encaminhar ou propagar correntes, mensagens de meditação, pirâmides, autoajuda, spams, propaganda política, publicidade comercial, anúncios, conteúdo ofensivo, preconceituoso, discriminatório ou que caracterize assédio moral ou sexual, com ou sem anexos;
- É proibido enviar e-mails mal intencionados, com intuito de sobrecarregar links de acesso, servidores de e-mails, sites ou caixas de e-mail de usuários;
- Assim como no acesso à Internet, o serviço de e-mails também possui um filtro que impede que mensagens com conteúdos e/ou anexos impróprios sejam enviados e recebidos. O sistema verifica nas mensagens a presença de algum dos itens abaixo:
- Arquivos que possam conter código malicioso embutido, trazendo risco de infecção por vírus ou outras pragas virtuais como, por exemplo:
  - **Executáveis:** .com, .exe, .pif, .scr, .bat, .cmd, .cpl, .dll, .lnk, .src, .vbs, .vbx, .sh, .bin, etc;
  - **Arquivos compactados**: .zip, .tgz, .gz, .rar, .arj, .tar, etc;
  - **Apresentações:** .pps, .ppt, .ppsx, .pptx, etc.
  - **Vídeo ou música:** .avi, .mpg, .mpeg, .mov, .asf, .asx, .mp2, .mp3, .mpe, .mpeg, .wma, .wmv, etc;
  - **Palavras de baixo calão/ofensivas:** termos desrespeitosos, preconceituosos, palavrões, palavras impróprias e não cabíveis num ambiente de trabalho e de uso coloquial;

- **Conteúdo pornográfico:** qualquer termo ou condição que possa evidenciar a propagação de material erótico, pornográfico ou impróprio;
- **Cartões virtuais:** mensagens do tipo "Você recebeu um cartão virtual" na maioria das vezes fazem com que o usuário clique em um link em que pode ser executado um vírus;
- **Tentativas de fraude:** um exemplo muito comum são os e-mails de bancos solicitando a atualização de dados da conta clicando em um link. Essas páginas são cópias da página original e os dados ali inseridos são capturados por pessoas mal intencionadas;
- **Links:** assim como nos dois últimos casos, os links podem direcionar para tentativas de fraudes, vírus e outras ameaças;
- **Spam:** mensagens enviadas para uma grande quantidade de destinatários sem que estes a tenham solicitado, normalmente contendo propagandas e/ou conteúdos não interessantes a um ambiente de trabalho;
- **Imagens:** existe uma limitação na quantidade de arquivos de imagens anexadas para evitar a propagação de conteúdo impróprio;
- **Tamanho:** o servidor bloqueia automaticamente mensagens que excedam o limite de 10 megabytes, independentemente de seu conteúdo ser ou não permitido.

- E-mails que se enquadrem em alguma das regras acima serão bloqueados. Para solicitar o desbloqueio basta seguir o procedimento conforme explicado no e-mail de bloqueio. Antes de entrar em contato com o setor de TI solicitando o desbloqueio, o usuário deve verificar algumas informações na mensagem de bloqueio para se certificar de que o e-mail realmente é esperado e seu conteúdo é pertinente ao trabalho:
  - Verificar se o remetente é conhecido ou a mensagem é esperada. Caso não seja, a chance de a mensagem ser um Spam, tentativa de fraude ou disseminação de vírus é maior;
  - Verificar se o remetente é conhecido ou a mensagem é esperada. Caso não seja, a chance de a mensagem ser um Spam, tentativa

de fraude ou disseminação de vírus é maior;

- Verificar se o assunto é legível, de seu interesse e referente a assuntos de trabalho. Se, ao ler o assunto, houver dúvidas sobre o que se trata ou desconhecimento a respeito, provavelmente esta mensagem não tenha algo relevante ou não seja algo seguro;
- Verificar o motivo do bloqueio. Assim saberá a razão pela qual a mensagem foi bloqueada.

- Recomenda-se a realização da manutenção periódica da caixa de e-mail, removendo conteúdo desatualizado ou não pertinente e evitando acúmulo de e-mails com conteúdo inútil. Existem meios de se realizar backup dos e-mails para consulta posterior;
- Com o intuito de tornar a ferramenta de e-mails mais profissional e facilitar a identificação do remetente por parte dos destinatários, sugere-se a criação de assinaturas no rodapé das mensagens conforme o modelo abaixo:

Nome do funcionário
Função | Setor
Telefone comercial | e-mail@ipmm.sc.gov.br
http://ipmm.sc.gov.br/

5. DA UTILIZAÇÃO DE IMPRESSORAS

- É proibido imprimir documentos particulares utilizando as impressoras e suprimentos fornecidos pelo IPMM;
- Todas as impressoras instaladas nos computadores são configuradas por padrão para imprimir no modo monocromático (preto e branco), mesmo as impressoras que dispõem de opção de impressão em cores. Os usuários devem ser conscientes e imprimir no modo colorido somente a versão final dos trabalhos e quando realmente houver essa necessidade;
- Caso a folha impressa possa ser reaproveitada para outra impressão, o papel deve ser colocado no local destinado a rascunhos. Se o mesmo não tiver mais serventia, deve ser corretamente descartado na lixeira

destinada a material reciclável;

- Caso se perceba que o papel na bandeja da impressora está acabando, deve ser feita a gentileza de reabastecê-la, evitando que pedidos de impressão sejam prejudicados, gerando acúmulo de trabalhos ou o bloqueio da fila de impressão.

6. DA INSTALAÇÃO DE SISTEMAS OPERACIONAIS E SOFTWARES

Nos procedimentos de formatação e reinstalação do sistema operacional dos computadores, a equipe técnica realizará cópia de segurança (backup) de documentos do usuário, em que serão copiados os arquivos da pasta de documentos ("Meus documentos" no Windows ou "Documentos" no Linux), da "Área de trabalho" e da pasta compartilhada "Trânsito". Se o usuário mantiver arquivos em outros locais que não sejam os citados acima, os mesmos serão perdidos acaso não informe à equipe técnica. Não serão realizados backup de músicas, vídeos, fotos, apresentações, e-mails e outros formatos de arquivos que não sejam relacionados ao trabalho do usuário. Exceções deverão ser informadas à equipe técnica.

Em relação à instalação de programas nos computadores do IPMM, cabe ressaltar:

- Todo software a ser adquirido ou instalado deverá ter a aprovação, homologação e consentimento do responsável pela segurança da informação. Nenhum software, mesmo que atrelado a algum equipamento, poderá ser adquirido, seja por compra direta, licitação, com recursos próprios ou vinculados sem o conhecimento e aprovação do responsável pela segurança da informação;
- Todas as instalações irregulares ou não homologadas serão excluídas no ato de sua constatação sem nenhum aviso prévio e será imediatamente levantada a responsabilidade do usuário;
- A instalação de qualquer tipo de software de jogo é proibida, mesmo os nativos do Windows ou Linux, que serão excluídos quando da instalação inicial do equipamento. Cabe exceção aos jogos educativos exclusivamente instalados para cursos e treinamentos específicos;
- O uso de softwares não legalizados (piratas), quando identificado

por autoridades de proteção de direitos autorais, acarreta o pagamento de multas altíssimas (cerca de 3.000 vezes o valor do software) por software, além de sujeitar o responsável à pena de detenção de até 4 anos.

7. DOS PADRÕES DE CONFIGURAÇÃO DOS RECURSOS DISPONÍVEIS

As configurações definidas a seguir visam obter um ambiente de trabalho padronizado com aspecto agradável, profissional e que traga economia ao IPMM:

- As imagens de fundo da área de trabalho dos computadores (papel de parede) devem possuir a Identificação do "Instituto de Previdência do Município de Mafra".
- Todos os computadores devem possuir um compartilhamento "Público" de arquivos na rede local protegido com senha. Essa medida é necessária para evitar a disseminação de pragas virtuais por compartilhamentos sem senha;
- Todos os computadores devem possuir uma impressora PDF a fim de racionalizar o uso de papel e permitir o envio de documentos não editáveis por meio eletrônico (e-mail, mídias removíveis).

8. DO USO DE EQUIPAMENTOS PARTICULARES OU PARA FINS PARTICULARES

- Não é permitido aos servidores do IPMM o uso de computadores, notebooks ou qualquer dispositivo informático particular para realizar serviços ou atender demandas do Instituto, exceto aos integrantes da equipe de gestão (Diretoria e Supervisores) e mediante autorização da chefia. O IPMM deve fornecer os equipamentos e ferramentas necessárias para que os funcionários cumpram suas funções.
- É vedado ao servidor do IPMM a realização de serviços particulares durante o horário de trabalho, sejam eles realizados com equipamentos particulares ou com quaisquer recursos do Instituto;
- O IPMM se exime de qualquer responsabilidade sobre danos em

equipamentos particulares dentro de suas dependências, bem como perda de informações ou dados particulares, estejam estes em equipamentos do IPMM ou particulares.

9. DA AQUISIÇÃO DE BENS DE TECNOLOGIA DA INFORMAÇÃO

- Todas as solicitações de compra de bens de tecnologia da informação devem ser encaminhadas para o setor de Informática para serem analisadas e aprovadas pela equipe técnica. A aquisição de bens de tecnologia da informação de todos os setores deverá passar antes pela autorização da Diretoria do IPMM.

- Antes de seguirem ao setor de compras. Essa ação visa racionalizar as aquisições e dar suporte ao setor de compras, com informações precisas dos bens a serem adquiridos. O setor de Compras, Contratos e Licitações não está autorizado a efetuar compras de bens de tecnologia da informação sem a validação da Diretoria, seja qual for a origem dos recursos;

- A aquisição de licenças de uso de softwares de todos os setores e para qualquer finalidade deve passar pela autorização do Diretor Presidente. As solicitações para aquisição de licenças de software devem estar acompanhada de uma justificativa plausível que comprove a real necessidade de adquirir o mesmo. Caso haja softwares livres e/ou gratuitos que atendam às mesmas características do software pago que fora requisitado, será dada preferência ao uso do software gratuito. O setor de Compras, Contratos e Licitações não efetivará nenhuma aquisição de software sem a validação do setor de Informática;

- Visando padronizar e unificar os processos licitatórios de aquisição de bens de tecnologia da informação para o IPMM, o setor de Compras, Contratos e Licitações realizará processo de compra de equipamentos na melhor modalidade para a aquisição dos mesmos.

10. BACKUP E RESTAURAÇÃO

Para manter a continuidade do IPMM, é fundamental estabelecer

mecanismos de permitam a guarda dos dados e sua eventual restauração em casos de perda por erro humano, ataques externos, catástrofes naturais. Desta forma, a política de backup das informações eletrônicas no âmbito do IPMM, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados sob a guarda, visando garantir a segurança, integridade e disponibilidade.

Procedimentos de backup

Os backups deverão ser realizados preferencialmente como disposto a seguir:

I. Os backups diários serão executados de segunda a sexta-feira, entre 18h e 6h do dia posterior, em modo incremental;

II. Os backups semanais serão executados nos finais de semana, iniciando aos sábados, em modo incremental. Não haverá execução de backup semanal quando coincidir com o backup mensal ou semestral;

III. Os backups mensais serão executados no primeiro sábado do mês, em modo incremental. Não haverá execução de backup mensal quando coincidir com o backup semestral;

IV. Os backups semestrais serão executados no primeiro sábado dos meses de Janeiro e Julho, em modo completo;

V. Em caso de falha em algum procedimento de backup ou impossibilidade da sua execução, o Administrador de Backup deverá adotar as providências necessárias para promover a salvaguarda das informações através de outro mecanismo, como por exemplo: nova execução do backup em horário de comercial ou cópia dos dados para outro servidor.

Procedimentos de restauração

A recuperação de backups deverá obedecer às seguintes orientações:

I. A solicitação de recuperação de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico, utilizando a ferramenta de controle de atendimentos;

II. O chamado técnico deve conter, ao menos, o nome e setor do usuário, o(s) objeto(s) a ser(em) recuperado(s), localização em que se encontra(m), a data da versão que deseja recuperar, local alternativo para o armazenamento do(s) objeto(s) recuperado(s), se for o caso, e a justificativa para recuperação;

III. Este chamado será encaminhado ao Administrador de Backup, que após a conclusão da tarefa, realizará o fechamento do chamado indicando a restauração do(s) objeto(s);

IV. A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

11. DAS SANÇÕES

O desrespeito às orientações constantes nesta Política autorizará a supervisão do servidor público, no uso de seu poder diretivo e disciplinar, a iniciar procedimentos administrativos com vistas à aplicação das penalidades cabíveis, sejam elas administrativas, civis ou penais.

12. DA VALIDADE

Esta Política de Segurança da Informação entrará em vigor na data de sua publicação.

Mafra, 7 de dezembro de 2020.

CARLOS OTÁVIO SENFF
Diretor Presidente do Instituto de Previdência do
Município de Mafra - IPMM