PORTARIA Nº 969/2021-GP/IPAM, DE 29 DE NOVEMBRO DE 2021.

Súmula: Dispõe sobre a Política de Segurança da Informação – PSI, no âmbito do Instituto de Previdência e Assistência do Município – IPAM, e dá outras providências.

A PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA E ASSISTÊNCIA DO MUNICÍPIO – IPAM, no uso de suas competências legais e estatutárias, e:

CONSIDERANDO que Política de Segurança da Informação – PSI, consiste em um conjunto de normas, procedimentos, ações técnicas e boas práticas, cujo objetivo é minimizar riscos e diminuir a vulnerabilidade dos sistemas de dados, funcionando como um código de conduta interno;

CONSIDERANDO que a instituição de uma Política de Segurança da Informação - PSI é de vital importância e relevância, uma vez que informações configuram um dos ativos mais valiosos e diligentes, dada as especificidades e essencialidades de alguns dados para o desempenho das atividades de um órgão;

CONSIDERANDO que uma boa Política de Segurança da Informação - PSI é uma ferramenta importante aplicada na administração pública e privada para minimizar os impactos de incidentes de Segurança da Informação e elevar o nível de maturidade da área das informações.

RESOLVE:

Art. 1º. Instituir no âmbito do Instituto de Previdência e Assistência do Município – IPAM a Política de Segurança da Informação - PSI.

Parágrafo Único - A Política de Segurança da Informação – PSI, tem o objetivo de garantir a disponibilidade, integridade, confidencialidade e privacidade dos dados necessários para a realização das atividades do Instituto de Previdência e Assistência do Município de São Luís.

Art. 2º. A Política de Segurança da Informação - PSI será aplicada a todos os servidores públicos, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento de dados do IPAM ou que tenham acesso às informações de domínio do Instituto de Previdência e Assistência do Município de São Luís.

Art. 3º. Todos os servidores, ainda que transitórios e/ou temporários que utilizarem os recursos computadorizados do IPAM são responsáveis pela proteção, segurança e integridade das informações e dos equipamentos de informática do Instituto.

Art. 4º. O descumprimento da Política de Segurança da Informação – PSI do

IPAM e/ou qualquer ato que exponha o IPAM a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados e/ou de informações ou ainda da perda de equipamentos, que envolva a violação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos governamentais, o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou outro dispositivo governamental, serão punidos com os rigores da legislação aplicável à espécie.

Art. 5º. É dever de todos os servidores do IPAM, quanto a Política de Segurança da Informação – PSI, considerar a informação como um bem da entidade, um dos recursos críticos para a realização das atividades e de grande valor devendo ser tratada, sempre, com profissionalismo.

Art. 6º. É de responsabilidade dos Superintendentes, Coordenadores e Chefes de Setores, nas suas respectivas áreas de atuação, estabelecer critérios relativos aos níveis de confidencialidade da informação (relatórios e/ou mídias) considerando o seu caráter:

a) Público;

b) Interno;

c) Confidencial.

I – Por Informação Pública entende-se toda informação que pode ser acessada por servidores do Instituto, usuários, fornecedores, prestadores de serviços e público em geral;

II - Informação Interna é toda informação que só pode ser acessada por servidores do Instituto. São informações que possuem um grau de confidencialidade que pode comprometer a imagem do IPAM;

III - Informação Confidencial é toda informação que pode ser acessada por servidores e parceiros do Instituto, porém, sua divulgação não autorizada pode causar impacto de ordem financeira, de imagem ou operacional aos serviços do Instituto;

IV - Informação Restrita é toda informação que pode ser acessada somente por servidores do Instituto explicitamente indicado pelo nome ou por área a que pertence e sua divulgação não autorizada pode causar sérios danos ao Instituto e/ou comprometer a estratégia da organização.

V – Dados Pessoais – informação relacionada à pessoa natural identificada ou identificável. (LGPD – art. 5, item I). São dados pessoais: nome, RG, CPF, gênero, data e local de nascimento, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer, endereço de IP (Protocolo da Internet) e cookies, entre outros. (DADOS PESSOAIS, Serviço Federal de Processamento de Dados)

VI – Dados Pessoais Sensíveis – dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (LGPD – art. 5, item II)

Art. 7º. É vedado a todos os setores do IPAM acumular ou manter, ainda que não intencionalmente, Dados Pessoais de Servidores e Segurados, salvo aqueles relevantes na condução de suas respectivas atividades.

§1º Todos os Dados Pessoais de Servidores e Segurados são considerados dados confidenciais.

§2º Dados Pessoais de Servidores e Segurados, sob a responsabilidade do IPAM, não serão usados para fins diferentes daqueles para os quais foram coletados.

§3º Dados Pessoais de Servidores e Segurados não serão transferidos para terceiros, exceto quando exigido pelo exercício da atividade da Instituição, e desde que tais terceiros mantenham a confidencialidade dos referidos dados.

Art. 8º. É terminantemente proibido o uso de programas ilegais (PIRATAS), de fontes duvidosas ou não relacionados à atividades do Instituto de Previdência e Assistência do Município – IPAM.

§1º Responderão nos rigores da lei aqueles servidores, ainda que temporários e/ou transitórios, que instalarem qualquer tipo de "software" considerado ilegal (programa ilegal) nos seus respectivos equipamentos de trabalho ou de qualquer outro do IPAM.

§2º Periodicamente, o Setor de Informática fará verificações nos dados nos computadores dos servidores, visando garantir a correta aplicação do disposto neste Artigo.

§3º O uso de novos aplicativos ou sistemas deve ser submetido à avaliação do Setor de Informática.

Art. 9. Quando da necessidade de cadastramento de um novo servidor para utilização da "rede", sistemas ou equipamentos de informática do IPAM, o setor de origem do novo servidor deverá comunicar ao Setor de Informática, por meio do Formulário de Abertura de Usuário, informando o nome completo, setor, contatos e seus acessos a uma ou mais pastas compartilhadas.

§1º Caberá ao Setor de Informática fazer o cadastramento solicitado e informar ao novo servidor qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada a cada 180 (cento e oitenta) dias.

§2º Por medida de segurança, o Setor de Informática recomendará que as senhas tenham sempre um mínimo de 08 (oito) caracteres alfanuméricos.

Art. 10. A situação cadastral dos usuários dos recursos computacionais do IPAM, alteração, ampliação, restrição ou bloqueio de acesso, deve ser encaminhada ao Setor de Informática pelo responsável do setor de origem do servidor ou pelo Coordenador de Administração Interna, por meio de memorando interno ou e-mail.

Parágrafo Único - O setor de informática fica obrigado a informar os critérios técnicos de uso dos recursos computacionais do IPAM.

Art. 12. Cópias de segurança do sistema integrado e servidores de rede são de

responsabilidade do Setor de Informática e deverão ser feitas diariamente.

Parágrafo Único - Quaisquer mudanças quanto à periodicidade do serviço de cópias de segurança do sistema integrado e servidores de rede devem ser analisadas entre o Setor de Informática e o setor solicitante.

Art.13. É obrigatório o armazenamento nas pastas setoriais compartilhadas, de arquivos ou documentos, de suas respectivas estações de trabalho, considerados de fundamental importância para a continuidade das atividades do IPAM.

Art.14. A política de acesso à Internet deve ser de conhecimento de todos os servidores e sua aplicação definida pelo o Setor de Informática.

Parágrafo único - A flexibilização da Política de Acesso à Internet é restrita ao Setor de Informática e, após análise, poderá ser feita quando solicitada pelo responsável de cada setor.

Art.15. Aos Superintendentes, Coordenadores e Chefes de setores cabe orientar seus subordinados quanto à Política da Mesa e Tela Limpas, que reúne diversas práticas de segurança visando proteger dados e informações, em formato digital ou impresso, do acesso, divulgação ou uso não autorizados, bem como perda, fraude ou outro tipo de dano.

§1º São orientações a serem seguidas pelo usuário durante o expediente, quando se ausentar de sua mesa ou ao fim:

a) Não deixe documentos em papéis e mídias removíveis, como pendrives e HDs externos, sobre sua mesa desnecessariamente;

b) Atente-se para não deixar à vista anotações, recados e lembretes importantes, incluindo aqueles colados em seu monitor ou divisórias, como post-it;

c) Nunca anote senhas em papéis, memorize-as ou armazene em um local seguro, como gerenciadores de senhas virtuais;

d) Ao sair de uma sala de reunião, verifique se todos os papéis foram retirados;

e) Não fazer refeições e lanches sobre a mesa;

f) Da mesma forma que sua mesa, procure manter a área de trabalho do seu computador limpa e organizada, com os arquivos guardados em pastas, devidamente identificados;

g) Adote uma cultura de diminuição do uso de papel, não imprima documentos de forma desnecessária, apenas para leitura. Prefira ler na tela do computador, tablet ou celular sempre que possível;

h) Ao final do expediente, sempre limpe e organize sua área de trabalho, desligue o computador, principalmente aqueles que estão em rede, e verifique se não há nenhuma mídia removível conectada nele.

§2º Quanto às informações sensíveis e confidenciais, dever-se-á observar os seguintes cuidados:

a) Documentos com informações estratégicas, internas ou dos segurados, devem ser devidamente guardados em gavetas ou armários quando não estiverem em uso e ao final do dia;

b) Mantenha agendas, cadernos e pertences pessoais em gavetas fechadas;

c) Documentos impressos que contenham informações sensíveis devem ser destruídos completamente, de preferência em fragmentadoras, antes de serem descartados;

d) Evite que papéis sobre a mesa sejam visíveis de janelas ou corredores.

Art.16. Os critérios para uso dos ativos computacionais do IPAM foram estabelecidos com base na Política de Uso Aceitável de Ativo.

§1º O IPAM disponibiliza para seus usuários equipamentos para o uso exclusivamente em suas atividades profissionais.

§2º Todo usuário deve observar as seguintes disposições quanto ao uso de equipamentos de propriedade do IPAM:

a) Os equipamentos disponibilizados com o objetivo específico de permitir aos usuários desenvolverem suas atividades profissionais são de propriedade do IPAM, sendo expressamente proibida a utilização para fins particulares;

b) A alteração e/ou a manutenção de qualquer equipamento de propriedade do IPAM, inclusive periféricos, é uma atribuição específica do Setor de Informática, que, a seu critério, poderá delegar formalmente outro responsável. Demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção ou modificação nos equipamentos;

c) Os equipamentos do IPAM devem ser utilizados com cuidado visando garantir sua preservação e seu funcionamento adequado;

d) Computadores de mesa (desktops) ou móveis (notebooks) devem ser desligados no final do expediente ou sempre que um usuário estiver ausente por um período prolongado, excetuando-se quando existir uma justificativa plausível em virtude de atividades de trabalho;

e) A desconexão (log off) da rede deverá ser efetuada nos casos em que o usuário não for mais utilizar o equipamento ou venha a ausentar-se por um período prolongado;

f) O bloqueio de tela protegido por senha deverá ser ativado sempre que o usuário se afastar do computador que esteja utilizando;

g) Ao final do contrato de trabalho, os equipamentos disponibilizados para a execução de atividades profissionais devem ser devolvidos em estado de conservação adequado quando no desligamento ou término da relação do usuário com o IPAM;

h) Qualquer dano aos equipamentos do IPAM será devidamente analisado pelo Setor de Informática havendo a constatação de que tal dano decorreu de ação direta ou omissão do usuário, caberá ao IPAM exercer seu direito de reparação ao prejuízo, através da tomada das medidas cabíveis;

i) Armazenar os arquivos com informações corporativas nos servidores de arquivos disponibilizados na rede interna de comunicação de dados. Deve-se evitar o armazenamento nas estações de trabalho.

Art.17 A retirada de processo físico e documento dos setores do IPAM deverá ser protocolada, informando a descrição do documento (número do processo, número de páginas, assunto ou autor) data da retirada, nome do solicitante e setor.

Parágrafo único – A entrega de documentos previdenciários ou de outra natureza, sob a responsabilidade do IPAM, somente é permitida ao titular requerente, ou a outrem, desde que possua procuração pública, lavrada em Cartório de Notas.

Art.18. Os casos omissos nesta Portaria devem serão dirimidos pelo Setor de Informática e submetidos à Presidência do IPAM.

Art.19. O não cumprimento do disposto nesta Política de Segurança da Informação – PSI, implica em falta grave e poderá ser punido, considerando sua gravidade, com advertência formal, instauração de Processo Administrativo Disciplinar - PAD, sem prejuízo das cominações legais cabíveis.

Art.20. Fica revogada a Portaria Nº 466/2021 – GP/IPAM, de 19 de Maio de 2021 e disposições outras em contrário e anteriores.

Art.21. Dê-se Ciência, Publique-se e Cumpra-se.

NÁDIA MARIA FRANÇA QUINZEIRO
Presidente do Instituto de Previdência e Assistência do Município