PORTARIA Nº 551/2022 – GP/MANAUS PREVIDÊNCIA

ALTERA portaria, na forma que especifica.

A DIRETORA-PRESIDENTE DA MANAUS PREVIDÊNCIA, no uso da competência disposta no inciso II do artigo 128 da Lei Orgânica do Município de Manaus, e das atribuições que lhes são conferidas pelo inciso VII do artigo 18 c/c o artigo 19, ambos da Lei nº 2.419, de 29 de março de 2019,

CONSIDERANDO solicitação realizada por meio do Memo Nº 75/2022 – PROJUR, de 18 de outubro de 2022, formalizado sob nº 2022.17848.17913.9.018873,

CONSIDERANDO o que estabelece o Manual do Pró-Gestão RPPS Versão 3.3, com vigência a partir do dia 02 de março de 2022, em seu item 3.1.5, que trata da Política de Segurança da Informação,

CONSIDERANDO o que dispõe o art. 7º, inciso III, da Lei 13.079/2018, que dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD),

CONSIDERANDO o que estabelece a Portaria nº 105/2020-GP/Manaus Previdência, publicada no Diário Oficial do Município – DOM, Edição nº 4793, de 06.03.2020, que trata da designação e composição do **Comitê Gestor de Segurança da Informação – CGSI da Manaus Previdência – MANAUSPREV**, que tem a finalidade de analisar, definir, coordenar, executar e avaliar ações de segurança da informação relativas aos objetivos estabelecidos na Política de Segurança da Informação e Comunicação da Prefeitura de Manaus – POSIC-PM, para elaboração, implementação, manutenção e melhoria da gestão da segurança da informação,

CONSIDERANDO a necessidade de produzir e propor normas, planos, procedimentos, mecanismos de proteção e instruções reguladoras específicas, relativas aos assuntos da POSIC-PM,

CONSIDERANDO o decidido na reunião do Comitê Gestor de Segurança da Informação, realizada em 18 de outubro de 2022.

ALTERAR a PORTARIA Nº 437/2022-GP/MANAUS PREVIDÊNCIA, publicada no DOM de 19 de agosto de 2022, Edição nº 5410, páginas 35-40, que revisou a Política de Segurança da Informação e Comunicação da Manaus Previdência – POSIC-MANAUSPREV, passando vigorar da seguinte forma:

Art. 1º. Fica Instituída a Política de Segurança da Informação e Comunicação da Manaus Previdência – POSIC/Manaus Previdência, tendo por objetivo o estabelecimento das diretrizes estratégicas, a definição de responsabilidades e competências, e a formalização do apoio para a implementação da gestão de segurança da informação:

Parágrafo único. A POSIC/Manaus Previdência se aplicará a todos aqueles que estejam envolvidos direta ou indiretamente com a execução das atividades no âmbito da instituição (Manaus Previdência) e dos recursos que ela dispõe.

Art. 2º. Para fins desta Portaria, considera-se:

I. Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

II. Autenticidade: Garantia de que uma informação, produto ou documento é do autor a quem se atribui;

III. Classificação da Informação: Níveis e critérios adequados de proteção das informações, garantindo a confidencialidade, conforme a importância de determinada informação para a organização (CPADS-MANAUSPREV – Cartilha – Procedimentos para Classificação da Informação em Grau de Sigilo);

IV. Confidencialidade: Garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;

V. Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos recursos correspondentes sempre que necessários;

VI. Integridade: salvaguarda de exatidão da informação e dos métodos e recursos de processamento;

VII. Legalidade: garantia de que ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos tenham validade jurídica;

VIII. Segurança da Informação: conjunto de medidas que tem como objetivo o estabelecimento dos controles necessários à proteção das informações durante sua criação, aquisição, uso, transporte, guarda e descarte, contra destruição, modificação, comercialização ou divulgação indevidas e acessos não autorizados, acidentais ou intencionais, garantindo a continuidade dos serviços e a preservação de seus aspectos básicos de confidencialidade, integridade, disponibilidade, autenticidade e legalidade;

IX. Gestão de segurança da informação: conjunto de medidas que tem como objetivo, o planejamento, implementação, operação, monitoramento e melhoria da segurança da informação;

X. Alta Gestão: Diretor(a)-Presidente e Diretores(as) de Previdência e de Administração e Finanças;

XI. Recursos de Tecnologia da Informação: Microcomputadores de mesa e portáteis (notebook, tablet, smartphone) e seus dispositivos periféricos, como teclados, mouses, caixas de som, microfones, leitoras, gravadoras e demais acessórios conectados ao computador; scanners, impressoras (laser, jato de tinta, matriciais e térmicas), webcams, datashows, telefone com tecnologia Voip, programas de computador adquiridos, sistemas desenvolvidos na Manaus Previdência, equipamentos e serviços da rede que compreende as redes locais da sede e anexos, bem como a rede de comunicação que as interliga, dados armazenados em equipamentos, dispositivos e periféricos e demais equipamentos relacionados à TI que venham a integrar o patrimônio da Manaus Previdência;

XII. Usuário: Toda pessoa que tenha acesso ao ambiente físico e aos recursos que compõem os sistemas de informação, que se encontra sob responsabilidade da Manaus Previdência e a quem está sujeita a POSIC/Manaus Previdência;

XIII. Administrador de sistema computacional: Quaisquer pessoas do quadro funcional, lotadas no Setor de Tecnologia da Informação, que tenham conhecimento autorizado dos códigos de acesso e senhas de administração dos recursos de Tecnologia da Informação, sejam eles de uso geral, sejam de uso restrito a uma unidade, grupo de pessoas ou de uso individual;

XIV. Arquivista: Profissional de nível superior, com formação em Arquivologia, lotado no Setor de Arquivo;

XV. Arquivo: local físico no qual ficam armazenadas a documentação da Manaus Previdência em fase intermediária;

XVI. Acervo: Conjunto de documentos produzidos ou recebidos pela instituição, neste caso em específico pela Manaus Previdência.

XVII. Dado pessoal: informação relacionada a pessoa natural identificada ou identificável

XVIII. Dado pessoal sensível: dado pessoal 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;

XIX. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

XX. Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

XXI. Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

XXIII. Agente de tratamento: o controlador e o operador;

XXIV. Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XV. Incidente de segurança da informação: violação ou ameaça iminente às regras e políticas de segurança da informação

XVI: Violação de dados pessoais: incidente de segurança que afete a confidencialidade, disponibilidade e autenticidade de dados pessoais sob responsabilidade da Manaus Previdência

Art. 3º. Para cumprimento do objetivo definido no artigo 1º desta Portaria, a POSIC/Manaus Previdência terá como objetivos básicos:

I. Viabilizar o atendimento das finalidades legais da Instituição, considerando leis, normas, regulamentações e outros requisitos legais aplicáveis vigentes, através da proteção da confidencialidade, integridade, disponibilidade, autenticidade e legalidade da informação;

II. Minimizar os danos decorrentes do comprometimento da confidencialidade, integridade, disponibilidade, autenticidade e legalidade da informação;

III. Proteger a confidencialidade, integridade, disponibilidade, autenticidade e legalidade da informação, otimizando investimentos por meio de uma abordagem sistemática de gestão de riscos;

IV. Melhorar a segurança da informação sempre que necessário para mantê-la adequada, pertinente e eficaz com relação às diretrizes desta política.

Art. 4º. Das Responsabilidades:

I. Setor de Gestão de Pessoas:

a)Auxiliar a TI quanto às sanções disciplinares ou administrativas;

b) Comunicar à área de Tecnologia da Informação a ausência ou desligamento de funcionários para as devidas providências no controle de acesso aos sistemas de informação;

c) Além disso, a área de recursos humanos deve apoiar a área de tecnologia na coleta de assinaturas do Termo de Responsabilidade de Segurança da Informação, anexando documento assinado à ficha funcional do usuário, bem como nos programas de treinamento e educação para a implementação e manutenção da política de segurança.

II. Usuários:

a) Ler, entender, respeitar e fazer cumprir a política de segurança;

b) Ler, entender e assinar os Termos de Responsabilidade de Segurança da Informação e Termo de Uso dos Sistemas de Informação;

c) Após a assinatura dos termos, o usuário assume formalmente a responsabilidade pelo bom uso dos ativos de informações, o compromisso de seguir a POSIC/Manaus Previdência e de manter o sigilo, em caráter permanente, sobre todos os ativos de informações e processos, mesmo após o seu desligamento ou término de prestação de serviços;

d) Utilizar as informações apenas para os propósitos da Manaus Previdência;

e) Informar imediatamente via canal de comunicação disponível (Mensageiro Interno, Sistemas de Chamados, E-mails, Via Telefone) qualquer incidente ou violação de segurança;

f) Manter nas unidades de armazenamento de rede apenas arquivos que estejam estritamente relacionados às atividades desempenhadas pela autarquia, sendo vedada a gravação de arquivos de músicas, fotos, vídeos e outros, que não atendam a tal finalidade;

g) Todos os arquivos relativos à Instituição deverão ser armazenados no servidor de arquivos da Manaus Previdência;

h) A guarda e a adequada utilização de dispositivos de armazenamento externo (Pen drives, HD Externos, CDs, DVDs, etc);

i) Em viagens, as estações portáteis pertencentes à Manaus Previdência, sob a responsabilidade de usuários, devem ser transportadas como bagagem pessoal devendo o equipamento ser preservado de quaisquer danos;

j) A guarda da senha é de uso pessoal e intransferível, sendo vedado transferir, emprestar ou liberar acessos a terceiros;

k) Exercer o princípio da finalidade para realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

l) Exercer o princípio da adequação na compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

m) Exercer o princípio da necessidade na limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

n) Exercer o princípio da segurança na utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

o) Exercer o princípio da prevenção na adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

p) Exercer o princípio da não discriminação, buscando a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

q) O tratamento de dados pelos usuários dos sistemas informatizados deve estar em conformidade aos princípios e práticas dispostos na Lei Geral de Proteção de Dados, bem como à Política de Privacidade e Termos de Uso da Manaus Previdência;

r) As senhas utilizadas devem cumprir as diretrizes fixadas na Política de Senhas da Manaus Previdência (Anexo I);

s) Ao criar documentos e processos, o usuário deve classificar, adequadamente, o sigilo de cada informação, atentando especialmente para os dados pessoais sensíveis;

t) O usuário não deve reproduzir desnecessariamente dados pessoais em planilhas ou outros documentos criados, optando, caso haja necessidade pela pseudonimização ou anonimização dos dados;

u) Caso o usuário acesse ou utilize serviço de e-mail que não seja o institucional, e nele veicule qualquer informação relacionada ao seu trabalho na Manaus Previdência, deve utilizar de todos os meios de segurança oferecidos pelo sistema, como verificação em duas etapas, dentre outros.

III. Setor de Tecnologia da Informação/Área de Segurança da Informação:

a) Promover ações de conscientização sobre a política de segurança da informação;

b) Definir, implementar e revisar os controles;

c) Identificar os riscos inerentes e residuais da segurança;

d) Implementar os controles de acesso indicados aos documentos digitais conforme a classificação de sigilo;

e) Avaliar os procedimentos de segurança, analisar os seus resultados e discutir as melhorias necessárias em relação a eles;

f) Definir soluções de segurança antes da implementação e durante a manutenção;

g) Elaborar programas de treinamento para capacitação de usuários e proprietários da informação;

h) Desenvolver, implementar e manter planos de continuidade de TI os quais visam garantir as operações em casos de desastre e indisponibilidade dos sistemas de informação;

i) Programar, executar e gerenciar as rotinas de backups;

j) Monitorar o uso da web e do tráfego de mensagens eletrônicas por mensageiros instantâneos homologados pela área de tecnologia;

k) Gestão de ativos da rede;

l) Definir requisitos e especificar instruções para utilização do teletrabalho (*home office*);

m) Prestar assessoramento técnico à Alta Direção e o Encarregado em assuntos referentes à Lei Geral de Proteção de Dados.

IV. Alta Gestão:

a) A alta gestão da Manaus Previdência se compromete apoiar a implantação e gestão da segurança da informação, de acordo com o que prescreve a norma NBR ISO/IEC 27002:2013, se incluindo extensivamente, a viabilização dos recursos necessários às adequações e implantações de mecanismos de proteção, visando garantir os princípios da Segurança da Informação, respeitadas as condições técnicas, orçamentárias, financeiras e o princípio da oportunidade.

b) Atender as determinações da Autoridade Nacional de Proteção de Dados.

c) Nomear encarregado, em cumprimento ao art. 23, II, da Lei 13.709/18;

d) Determinar as medidas necessárias para o cumprimento da Lei Geral de Proteção de Dados.

V. Setor de Arquivo / Protocolo – SARQ:

a) Garantir, através da criação e implantação de procedimentos, a integridade, autenticidade, disponibilidade, não repúdio e a confidencialidade dos documentos/processos físicos, digitais e híbridos, produzidos ou recebidos pela Manaus Previdência, desde a sua entrada até o seu arquivamento e acondicionamento.

VI. Comissão Permanente de Avaliação de Documentos Sigilosos:

a) Opinar sobre a informação produzida no âmbito de sua atuação para fins de classificação em qualquer grau de sigilo;

b) Assessorar a autoridade classificadora ou a autoridade hierarquicamente superior quanto à classificação, desclassificação, reclassificação ou reavaliação de informação classificada em qualquer grau de sigilo;

c) Propor o destino final das informações desclassificadas, indicando os documentos para a guarda permanente;

d) Subsidiar a elaboração do rol anual de informações desclassificadas e documentos classificados em cada grau de sigilo, a ser disponibilizado na internet.

VII. Comitê Gestor de Segurança da Informação:

a) Caberá analisar, definir, coordenar, executar e avaliar ações de segurança da informação relativas aos objetivos estabelecidos na Política de Segurança da Informação e Comunicação da Prefeitura de Manaus – POSIC-PM para elaboração, implementação, manutenção e melhoria da gestão da segurança da informação.

VIII. Encarregado:

a) Garantir o cumprimento da Lei Geral de Proteção de Dados na Manaus Previdência;

b) Informar ao CGSI e Alta Direção qualquer ocorrência referente ao descumprimento de norma da LGPD;

c) Tomar as medidas adequadas, dentro de sua esfera de competência, para cessar qualquer descumprimento à Lei Geral de Proteção de Dados;

d) Informar a Alta Direção sobre atualizações e outras informações pertinentes referentes à LGPD;

e) Intermediar a comunicação entre a Autoridade Nacional de Proteção de Dados, os usuários dos serviços e a Manaus Previdência, na qualidade de controladora de dados.

IX. Procuradoria Jurídica – PROJUR:

a) Prestar assessoramento técnico à Alta Direção e o Encarregado em assuntos referentes à Lei Geral de Proteção de Dados.

b) Suporte jurídico às ações de resposta ao incidente e na gestão de riscos regulatórios

X. ASCOM – Assessoria de Comunicação:

a) Suporte nas atividades de comunicação com titulares, em contexto de incidente de segurança de informação

b) Suporte nas atividades de conscientização da Política de Segurança da Informação

Art. 5º Os recursos (TI e arquivo) pertencentes à Manaus Previdência e que estão disponíveis para os usuários, devem ser utilizados em atividades estritamente relacionadas às funções institucionais desempenhadas pela autarquia.

Art. 6º É vedada a utilização de quaisquer dos recursos de TI da Manaus Previdência com o objetivo de praticar atos contra outros recursos da rede de computadores da Instituição ou redes externas, dentre os quais: equipamentos servidores, estações de trabalho, equipamentos de rede, serviços de segurança e sistemas de informação.

Art. 7º. O uso dos Recursos Computacionais:

I. A estação de trabalho deve manter o padrão estabelecido pelo Setor de Tecnologia da Informação, no tocante ao sistema operacional e aos demais programas de computador instalados;

II. Qualquer programa suspeito que não seja parte das atividades da Manaus Previdência, que não se enquadre nos critérios estabelecidos pela alta direção ou chefia imediata serão desinstalados sem aviso prévio;

III. Qualquer equipamento de uso pessoal só poderá ser utilizado na instituição mediante autorização prévia, com breve justificativa, do Setor de TI;

IV. Somente em casos excepcionais será concedido privilégio de administrador da máquina aos usuários das estações de trabalho, por meio de prévia solicitação por escrito do Chefe do setor de lotação do usuário, ao STIN;

V. Quaisquer movimentações de equipamentos de TI no âmbito da Manaus Previdência devem ser comunicadas por escrito ao Setor de Patrimônio, para atualização de controles e transferências, e ao Setor de TI;

VI. A cada 180 dias o sistema solicitará ao usuário a troca de sua senha de acesso à rede;

VII. O STIN poderá determinar um padrão a ser seguido quanto à definição da senha, incluindo número mínimo de caracteres, utilização de caracteres alfanuméricos e símbolos, à proibição de repetição de senhas anteriores e à quantidade permitida de tentativas, além de outras medidas que visem ao aumento da privacidade da senha.

Art. 8º. O uso dos Recursos de Internet e e-mail:

I. É vedado o acesso às páginas com conteúdo que envolva pornografia, racismo ou preconceitos de quaisquer naturezas, jogos ou outros conteúdos notadamente fora do contexto do trabalho;

II. É vedado obter na Internet arquivos (download) que não estejam relacionados com suas atividades, incluindo vídeos, jogos e programas de qualquer tipo;

III. Os e-mails encaminhados pelo correio eletrônico institucional deverão adotar assinatura conforme sugerido abaixo com as seguintes informações para facilitar a rastreabilidade, caso seja necessário:

1) Nome completo do servidor;
2) Cargo e Setor;
3) Nome da Autarquia, por extenso;
4) Telefones da Manaus Previdência;
5) Endereço do site e correio eletrônico da Manaus Previdência.

IV. Os e-mails não institucionais podem ser utilizados quando:

1) Indisponibilidade do serviço de WebMail da PMM;
2) Aguardar liberação da Caixa Postal do WebMail;
3) O arquivo anexado exceder o tamanho permitido;
4) Esquecimento da senha do WebMail;
5) Estagiários em processo de transição em virtude da rotatividade.

V. A utilização indevida das caixas postais acarretará, na primeira ocorrência, a edição de advertência formal ao titular da caixa de origem. Em caso de reincidência, haverá a suspensão de uso, somente liberado após solicitação do superior imediato do titular da caixa de origem. Em caso de nova utilização indevida, ficará sujeito à aplicação de penalidades administrativas;

VI. É desaconselhável a abertura de mensagens de procedência desconhecida contendo anexos executáveis devido ao risco de contaminação da rede por vírus e outros arquivos prejudiciais, sendo de inteira responsabilidade do usuário as eventuais consequências da inobservância desta recomendação;

VII. Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de Tecnologia da Informação deve ser imediatamente comunicada ao STIN;

VIII. O acesso à Internet deve restringir-se às páginas com conteúdo relacionado às atividades desempenhadas pelo usuário para a autarquia em consultas ou obtenção de informações e dados necessários ao serviço;

IX. Na modalidade de teletrabalho (home office) ficam aplicados todos os dispositivos deste artigo e será implementada conforme orientação do Setor de Tecnologia da Informação.

Art. 9º É vedado a divulgação ou uso de informações contidas nos documentos físicos, digitais e híbridos para qualquer fim que não esteja ligado às atividades da Manaus Previdência.

Art. 10. Os administradores dos sistemas computacionais da Manaus Previdência são responsáveis pelo uso adequado dos recursos sob sua responsabilidade, devendo zelar pela integridade e confidencialidade dos sistemas e dos dados sob seus cuidados, bem como os arquivistas e servidores lotados no SARQ, são responsáveis por manter a integridade, fidedignidade dos documentos físicos e acesso controlado aos documentos que estão sob a responsabilidade do setor SARQ.

Art. 11. O STIN deverá prover os instrumentos tecnológicos necessários ao cumprimento das normas estabelecidas nesta Portaria, bem como zelar pela manutenção, devidamente atualizada, de sistemas operacionais, navegadores e quaisquer programas de detecção e eliminação de códigos e/ou programas indevidos nas estações de trabalho dos usuários.

Art. 12. É atribuição do Setor de Tecnologia da Informação gerir a infraestrutura de hardware e software necessária à prestação dos serviços de acesso à rede interna e à Internet, sendo vedada a instalação de qualquer equipamento neste ambiente, salvo prévia autorização, e do SARQ realizar a gestão documental da autarquia, bem como orientar os setores internos da Manaus Previdência acerca de procedimentos para acesso à documentação, empréstimos, consultas, arquivamentos, acondicionamentos e classificação da informação dos documentos e meios físicos e digitais.

Art. 13. O STIN poderá realizar monitoramento da utilização dos serviços de rede e acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, intervindo sem aviso prévio como:

I. Bloquear temporariamente a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica da Manaus Previdência;

II. Bloquear temporariamente o acesso a impressoras e copiadoras que estejam imprimindo/copiando documentos particulares ou alheios às rotinas inerentes à administração pública;

III. Formalizar um documento relatando as atividades que infrinjam os Incisos I, II do Art. 13, aos respectivos gestores.

Art. 14. A Manaus Previdência poderá designar Comitê Gestor de Segurança da Informação para auxiliar na execução da POSIC/Manaus Previdência e/ou fazer parte de uma Comissão já existente no âmbito do município e adotá-la, uma vez que a instituição Manaus Previdência é parte integrante da estrutura organizacional da Prefeitura Municipal de Manaus.

I. O Comitê Gestor de Segurança da Informação organizado pela Manaus Previdência:

a) Reunir-se-á ordinariamente a cada semestre, com o objetivo de acompanhar o andamento das ações relativas à segurança, e extraordinariamente, por solicitação de qualquer de seus membros para tratar de assuntos pontuais;

b) Poderá se reunir extraordinariamente, mediante convocação da Presidência do Comitê ou da maioria absoluta de seus membros, observado o prazo mínimo de 24 horas entre a convocação e a realização da reunião;

c) Poderá se valer de recursos de teleconferência, videoconferência ou outros meios similares que permitam a comunicação em tempo real, para realizar suas reuniões.

d) Terá suas reuniões instaladas com a participação de, no mínimo, dois terços de seus membros;

e) Terá suas decisões tomadas por maioria simples dos membros presentes à reunião cabendo à Presidência o voto de qualidade, em caso de empate;

f) Realizará suas votações de modo nominal e aberto, e todos os membros titulares do Comitê terão direito a voz e a voto;

g) Terá suas decisões lavradas em atas, que serão redigidas com clareza, tornando-se objeto de aprovação formal;

h) Submeterá suas deliberações ao referendo da Diretoria Executiva, momento em que surtirão efeitos.

Art. 15. A POSIC-Manaus Previdência deverá ser revisada e atualizada periodicamente, no máximo a cada 3 (Três) anos, caso não ocorra atualização da POSIC-PM ou caso não ocorram outros eventos ou fatos relevantes que exijam uma revisão imediata.

Art. 16. O usuário que fizer uso de forma indevida ou não autorizada das informações e dos recursos de Tecnologia da Informação, bem como agir em desacordo com os termos desta Portaria, fica sujeito à aplicação das penalidades previstas no Capítulo II, Seção I, Art. 216 da Lei nº 1.118, de 1º de Setembro de 1971, Art. 32 ao 34 da Lei nº 12.527, de 18 de novembro de 2011 e à legislação em vigor.

Art. 17. Os casos omissos e as dúvidas surgidas na aplicação desta Portaria serão dirimidos pelo Comitê Gestor de Segurança da Informação da Manaus Previdência, em parceria com outras entidades quando necessário.

Art. 18. A implementação da POSIC/Manaus Previdência será feita de forma gradual, de acordo com a disponibilidade técnica, recursos humanos, tecnológicos e financeiros, cujas ações serão priorizadas em virtude de seu grau de relevância, criticidade e impacto e em função dos investimentos envolvidos.

Art. 19. A sensibilização e cultura de segurança, bem como da importância das informações processadas, dos seus riscos e suas vulnerabilidades, bem como dos impactos do não cumprimento ou de falhas de segurança, devem ser desenvolvidas e mantidas por meio de palestras, seminários, treinamentos, e outros canais de comunicação disponíveis no âmbito da Manaus Previdência.

Art. 20. Os arquivos e documentos, disponibilizados nos portais (extranet e intranet), podem ser visualizados e enviados por e-mail, uma vez que esses documentos já foram verificados e avaliados pela Comissão Permanente de Avaliação de Documentos Sigilosos, assegurando o nível de proteção adequado.

Art. 21. Controles Operacionais serão tratados em Procedimentos, Instruções de Trabalhos, Ordem de Serviços, Fluxos e Manuais, pois estão suscetíveis a alterações constantes.

Art. 22. Esta Portaria entrará em vigor na data de sua publicação.

ANEXO I

POLÍTICA DE SENHAS DA MANAUS PREVIDÊNCIA

1. Introdução

Senhas são um aspecto de grande importância para a segurança em dispositivos informáticos. Uma senha mal escolhida pode resultar em prejuízo à organização, pois representa uma vulnerabilidade que pode atingir todo o sistema. Dessa forma, todos os servidores, incluindo funcionários de empresas públicas privadas que prestem serviços à Manaus Previdência, são responsáveis pela observância e cumprimento das disposições desta Política.

2. Propósito

O propósito da Política de Senhas da Manaus Previdência é estabelecer um padrão para a criação de senhas fortes, a proteção dessas senhas e, estabelecer, também, a frequência dessas mudanças.

3. Alcance

3.1 O alcance da Política de Senhas inclui todo colaborador que tem ou teve a responsabilidade por uma conta (ou qualquer forma de acesso a sistemas que requeiram senhas), tenha acesso à rede da Manaus Previdência ou a qualquer sistema operado pela Manaus Previdência ou empresas contratadas;

3.2. Como colaboradores devem ser entendidos: Servidores titulares de cargo efetivo ou comissionado, estagiários, funcionários de empresas públicas ou privadas que prestem serviço à Manaus Previdência e membros de Conselhos e Comissões;

3.3 As diretrizes para a criação e mudança de senhas abrangem também sistemas informatizados não operados pela Manaus Previdência, mas utilizados pelos seus colaboradores para transmitir informações relacionadas ao trabalho, como e-mails, aplicativos para edição de texto, conversão de arquivos e outros. Nesses casos, o usuário deverá observar, com preponderância, as diretrizes do próprio sistema, utilizando aquelas fixadas na Política de Senhas como um reforço àquelas já existentes no sistema;

3.4 Determinadas diretrizes da Política de Senhas abrangem também os segurados que acessem os sistemas operados pela Manaus Previdência, como o ''Portal do Segurado''.

4. Da Política de Senhas

4.1 Diretrizes de troca de senhas:

4.1.1 Todas as senhas em nível ''administrador'' devem ser trocadas, pelo menos, a cada 90 dias;

4.1.2 Todas as senhas de usuário (por exemplo: e-mail, web, siged, etc.) devem ser trocadas, pelo menos, a cada 90 dias e não podem ser reutilizadas as 10 últimas senhas;

4.1.3 As senhas não devem ser inseridas em mensagens de e-mail ou outras formas de comunicação.

4.2 Diretrizes para a construção de senhas:

4.2.1 Mínimo de 8 caracteres em todos os sistemas;

4.2.2 Utilizar letras maiúsculas, minúsculas e números;

4.2.3 Não utilizar sequências contendo três numerais consecutivos (ex: 123, 234, 456, 789, etc);

4.2.4 Não utilizar letras do alfabeto ou posicionadas no teclado em sequência (ex: qwe, abc, def, etc);

4.2.5 Não pode consistir em uma palavra ou um nome;

4.2.6 Não pode corresponder ao ID do usuário;

4.2.7 Deve ser trocada no máximo em 90 dias;

4.2.8 Não pode ser idêntica às últimas 10 senhas;

4.2.9 Não pode ser transmitida em texto fora de um ambiente informático seguro;

4.2.10 Não pode ser mostrada ou visualizada enquanto estiver sendo inserida;

4.2.11 Antes de realizar qualquer procedimento de *''reset''* da senha, o usuário deverá se certificar de que está realizando a operação em um ambiente seguro.

4.3 Diretrizes para a exclusão de senhas:

4.3.1 Todas as senhas que não serão mais utilizadas devem ser deletadas ou desabilitadas imediatamente, o que inclui as seguintes situações, sem prejuízo de outras aqui não previstas:

4.3.1.1 Quando o usuário é desligado, cedido, licenciado, etc;

4.3.1.2 Senhas padrão ou fornecidas para primeiro acesso devem ser imediatamente trocadas em todos os equipamentos;

4.3.1.3 Contas referentes a funcionários terceirizados, quando deixarem de prestar serviços à Manaus Previdência.

4.3.2 Quando uma senha não é mais necessária, as seguintes ações devem ser observadas:

4.3.2.1 O usuário deve informar seu superior imediato;

4.3.2.2 O usuário que preste serviço através de terceirização deve informar o seu supervisor;

4.3.2.3 O SGEP e o STIN devem realizar, imediatamente, todos os procedimentos cabíveis para desabilitação do usuário.

4.4 Medidas para a proteção de senhas

4.4.1 Todas as senhas devem ser tratadas como uma informação sensível. Para isso, os colaboradores devem certificar-se de não revelar ou compartilhar a senha fora de ambientes seguros e autorizados. Abaixo, listam-se uma série de comportamentos a serem observados:

4.4.1.1 Não revelar a senha ao telefone;

4.4.1.2 Não revelar a senha em uma mensagem de e-mail;

4.4.1.3 Não revelar a senha aos seus superiores;

4.4.1.4 Não falar sobre a senha perto de outras pessoas;

4.4.1.5 Não compartilhar a senha em formulários ou questionários;

4.4.1.6 Não deve compartilhar senhas com ninguém, incluindo assistentes ou assessores;

4.4.1.7 Não revelar a senha a familiares;

4.4.1.8 Não compartilhar a senha a colegas de trablho, enquanto de férias;

4.4.1.9 Não utilizar ferramentas como ‘’Lembrar senha’’ ou ‘’Permanecer logado’’;

4.4.1.10 Não escrever senhas e armazená-las no local de trabalho;

4.4.1.11 Não utilizar sequências comuns de letras ou números (ex: abc, qwe, 1234, qwerty, etc);

4.4.1.12 Não utilizar, na criação de senhas, informações pessoais disponíveis a terceiros (ex: nome de familiares, animais de estimação, data de nascimento, etc);

4.4.1.13 Não armazenar senhas em um arquivo no computador sem encriptação;

4.4.1.14 Se algum funcionário requisitar a senha do colaborador, ainda que seja um superior, o usuário deverá negar a requisição e referir o postulante a esta Política de Senhas;

4.4.1.15 Havendo suspeita de comprometimento de senha ou conta de usuário, o fato deve ser imediatamente reportado ao Setor de Tecnologia de Informação;

4.4.1.16 A Manaus Previdência poderá utilizar de expedientes para teste das senhas do usuário e, caso a senha não cumpra com o mínimo de segurança, poderá ser determinado que o usuário mude a senha.

5. Sanções Disciplinares

5.1 Qualquer servidor que violar a política de senha estará sujeito à ação disciplinar, nos termos da Lei nº 1.118/71.

6. Cumprimento da Política de Senhas

6.1 A Política é de cumprimento obrigatório aos servidores e colaboradores terceirizados da Manaus Previdência. Qualquer exceção às regras da Política de Senhas deve ser analisada e aprovada pela Presidência.

ANEXO II

PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

1. Todos os equipamentos que têm a funcionalidade de servidores (dispositivos que disponibilizam informações a outros ligados em rede), tanto físicos quanto virtuais, equipamentos de mesa (PCs), dispositivos móveis e de segurança da informação, devem estar protegidos com sistemas de proteção contra softwares maliciosos e serem atualizados periodicamente, conforme recomendação de disponibilização do fabricante.

2. Da Ferramenta de Proteção Contra Códigos Maliciosos

2.1 A ferramenta de proteção contra códigos maliciosos, disponibilizada pela Manaus Previdência adota as seguintes regras de uso:

2.1.1 Atualização em tempo real (on-line) do arquivo de assinaturas de códigos maliciosos e varredura programadas (plano de execução) nas estações de usuários;

2.1.2 As varreduras programadas devem analisar todos os arquivos em cada unidade de armazenamento das estações de usuários;

2.1.3 As varreduras programadas em servidores corporativos, caso seja necessário, podem ser limitadas a pastas ou arquivos específicos, de modo a evitar o comprometimento do desempenho de recursos computacionais críticos;

2.1.4 As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações de trabalho de usuários;

2.1.5 Os sistemas de proteção contra softwares maliciosos devem ser instalados com controles que não permitam alteração de sua configuração ou remoção da ferramenta, por usuários não autorizados;

2.1.6 Sites, serviços e arquivos baixados da internet e detectados como possíveis ameaças serão automaticamente bloqueados em estações de trabalho de usuários;

2.1.7 Caso uma estação de usuário esteja infectada ou com suspeita de infecção de código malicioso, deverá ser imediatamente isolada da rede corporativa da MANAUS PREVIDÊNCIA e de qualquer comunicação com a internet;

2.1.8 Caso um servidor corporativo esteja infectado ou com suspeita de infecção de código malicioso, deverão ser adotadas medidas para garantir o isolamento da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor.

2.1.9 Periodicamente devem ser realizadas analises de vulnerabilidades de softwares, aplicativos e infraestrutura que suportam os processos críticos do ambiente tecnológico da Manaus Previdência;

2.1.10 A resposta às vulnerabilidades críticas detectadas nos sistemas e ambientes da Manaus Previdência deve ser tratada imediatamente pelo STIN, conforme descrito no Plano de Resposta a Incidentes da Manaus Previdência;

3. Prevenção dos usuários contra códigos maliciosos

3.1. Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários da MANAUS PREVIDÊNCIA devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos;

3.2. Os usuários da MANAUS PREVIDÊNCIA devem seguir as seguintes diretrizes para proteção contra códigos maliciosos:

3.2.1 Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;

3.2.2 Reportar imediatamente ao STIN qualquer infecção ou suspeita de infecção por código malicioso;

3.2.3 Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado em um ambiente controlado;

3.2.4 Não inserir ou conectar equipamentos não homologados pelo STIN nas estações de trabalho;

3.2.5 Para minimizar o risco de infecção por softwares maliciosos, os usuários devem usar, exclusivamente, softwares homologados, licenciados e instalados pelo Setor de Tecnologia da Informação.

3.2.6 Caso o usuário perceba que no seu equipamento de trabalho os sistemas de proteção, como antivírus e firewall, não estejam instalados ou funcionando adequadamente, este deve entrar em contato com o STIN para as devidas providências

3.2.7 Não habilitar MACROS para arquivos recebidos de fontes suspeitas, baixados da internet ou recebidos nos serviços de e-mail não oficiais ou comunicadores instantâneos. Caso necessário, poderá ser solicitado o apoio do STIN para validar se o arquivo representa ou não uma ameaça;

3.2.8 Os sistemas de proteção contra softwares maliciosos devem ser instalados com controles que não permitam alteração de sua configuração ou remoção da ferramenta, por usuários não autorizados;

ANEXO III – Dos Incidentes de Segurança da Informação

1. Da Resposta a Incidentes de segurança da Informação

1.1 Tendo o usuário ou colaborador identificado situação que possa implicar em incidente de segurança da informação, deverá

realizar a comunicação do fato ao **STIN**, através de chamado, que enviará a comunicação, após providências preliminares, ao **CRISI**.

1.2 Havendo necessidade, qualquer servidor do **STIN** tomará as providências necessárias no contexto da ocorrência de incidentes de segurança. A decisão tomada deverá ser comunicada ao Chefe do **STIN** e ao **CRISI**.

1.3 O **Plano de Resposta a Incidentes da Manaus Previdência** deverá ser seguido no desdobramento do incidente de segurança, em especial as ações de recuperação e contenção de sistemas; Ações de investigação e resposta; Governança de Dados, na hipótese do incidente ter resultado em violação de dados pessoais.

2. Do Comitê de Resposta a Incidentes de Segurança da Informação

2.1 São responsabilidades específicas do **Comitê de Resposta a Incidentes de Segurança da Informação (CRISI)** coordenar as atividades de tratamento e resposta a incidentes em redes computacionais, cooperar com outras equipes e realizar a interlocução com entes públicos.

2.2 São atribuições do **CRISI**:

a) Mapear o impacto do incidente;

b) Cooperar com órgãos policiais na investigação do incidente, caso detectados indícios de infração penal;

c) Documentar, de forma detalhada, o incidente de segurança;

d) Avaliar se o incidente resultou em violação de dados pessoais, comunicando a autoridade responsável;

e) Realizar a comunicação da violação dos dados, caso necessário, aos titulares de dados;

f) Adoção de medidas revisionais legais e regulatórias adequadas, após o incidente;

2.3 Fazem parte do Comitê de Resposta a Incidentes de Segurança da Informação:

a) - O Conselho Diretor da Manaus Previdência

b) - O Presidente do CGSI

c) - O Encarregado

d) - O Procurador-Chefe

e) - A Assessoria de Comunicação da Manaus Previdência

2.4. O **STIN** é órgãos de assessoramente ao **CRISI**, competindo-lhe:

a) Gerenciar incidentes de segurança em redes computacionais;

b) Investigar e avaliar danos decorrentes de quebras de segurança;

c) Registrar todos os incidentes de segurança em redes de computadores, com a finalidade de assegurar registro histórico das atividades, fornecendo o resultado ao CRISI;

d) Apoiar a recuperação de sistemas;

e) Realizar análise de ataques e intrusões;

f) Cooperar com outras equipes;

CIENTIFIQUE-SE, PUBLIQUE-SE, CUMPRA-SE.

Manaus, 18 de outubro de 2022.

DANIELA CRISTINA DA EIRA CORRÊA BENAYON
Diretora-Presidente da Manaus Previdência

EXTRATO

1. ESPÉCIE E DATA: Primeiro Termo Aditivo ao Contrato de Prestação de Serviços nº 009/2022, celebrado em 13/10/2022;

2. CONTRATANTES: MANAUS PREVIDÊNCIA – MANAUSPREV, pessoa jurídica de direito público, inscrita no CNPJ/MF nº 07.637.990/0001-12, sediada na Av. Constantino Nery, 2480, Bairro Chapada, CEP 69.050-001, nesta cidade e, o **CONSÓRCIO SEGURANÇA ESCOLAR INTEGRADA DO MATO GROSSO DO SUL – SEIMS**, inscrito no CNPJ/MF nº 45.699.002/0001-59, sediada na Av. Ephigênio Salles, nº 126, Bairro Parque Dez de Novembro, CEP 69.055-736, nesta cidade;

3. OBJETO: O presente Termo Aditivo visa adequação do Contrato de Prestação de Serviços nº 009/2022 em decorrência do Primeiro Termo Aditivo à Ata de Registro de Preços nº 003/SED/2022, que realizou a seguinte modificação: alteração da CONTRATADA da Ata de Registro de Preços nº 003/SED/2022. Assim, a CONTRATADA passa a ser o CONSÓRCIO SEGURANÇA ESCOLAR INTEGRADA DO MATO GROSSO DO SUL – SEIMS, tendo sede em Manaus/AM, à Av. Ephigênio Salles, nº 126, Bairro Parque 10 de Novembro, CEP 69.055-736, formado pelas empresas IIN TECNOLOGIAS LTDA., líder do Consórcio, com sede na cidade de Manaus/AM, Av. Ephigênio Salles, nº 126, Bairro Parque 10 de Novembro, CEP: 69.055-736, inscrita no CNPJ sob o nº 03.211.236/0001-65, neste ato representada por seu sócio administrador, Sr. YORAM YAELI, israelense, solteiro, administrador, portador da Cédula de Identidade de Estrangeiro RNE n. V303139-I CGPI/DIREX/DPF e do CPF/MF n. 227.092.708-70, residente e domiciliado na Avenida Cerina Souto – 210, Bairro Ponta Negra, CEP: 69.037-208, na cidade de Manaus/AM; L.S. INFORMÁTICA E TELECOMUNICAÇÕES LTDA., com sede na cidade de Manaus/AM, Av. Ephigênio Salles, nº 126, Sala D, Bairro Parque 10 de Novembro, CEP: 69.055-736, inscrita no CNPJ sob o nº 06.031.060/0001-58 e SASI COMUNICAÇÃO ÁGIL LTDA., com sede na cidade de São Paulo/SP, Rua Alves Guimarães, nº 462, Conjunto 21, Bairro Pinheiros, CEP: 04.410-000, inscrita no CNPJ sob o nº 35.379.670/0001-45, conforme Registro na Junta Comercial, neste ato representada pelo seu representante legal, Sr. ANDRÉ LUIZ SANTOS DE SOUZA, brasileiro, casado, administrador, portador da cédula de identidade nº 1093943-1-SSP/AM e CPF n° 509.873.642-00, domiciliado em Manaus/AM, residente na Av. José Augusto Loureiro, s/n, Condomínio Alphaville Manaus 3, Bairro Ponta Negra, CEP: 69.037-225.;

4. VIGÊNCIA: O presente Termo Aditivo não modificará a vigência do Contrato, permanecendo o termo final já estipulado.

Manaus-AM, 13 de outubro de 2022.

LYVIA BELÉM MARTINS GUIMARÃES
Diretora de Administração e Finanças

DANIELA CRISTINA DA EIRA CORRÊA BENAYON
Diretora-Presidente da Manaus Previdência

FUNDAÇÃO MUNICIPAL DE CULTURA, TURISMO E EVENTOS

PORTARIA N.º 0108/2022

O DIRETOR-PRESIDENTE DA FUNDAÇÃO MUNICIPAL DE CULTURA, TURISMO E EVENTOS-MANAUSCULT no exercício da competência que lhe confere o inciso II, artigo 128 c/c inciso IV do artigo 86 da Lei Orgânica do Município de Manaus, Lei Delegada n.º 25/2013 e Decreto de 01.01.2021;

CONSIDERANDO o Edital de n° 014/2022 – MANAUSCULT, publicado no DOM 5429 do dia 20/09/2022, republicado no Dom 5432 do dia 23/09/2022, Errata publicado no Dom 5433 do dia 26 de setembro de 2022, de Chamamento de autorização de uso de espaço público de **forma onerosa, para operação de venda de bebidas, inclusive alcóolica por uma empresa da iniciativa privada no segmento de eventos**, durante a realização do evento **ANIVERSARIO DE MANAUS - BOI MANAUS 2022,** realizado no Centro de Convenções Professor Gilberto Mestrinho – Sambódromo, no período de 21 a 23 de outubro de 2022.

CONSIDERANDO a necessidade de nomeação dos membros que irão compor a equipe de fiscalização;

RESOLVE

Art. 1.º Designar os seguintes membros:

Nome	Função	Matrícula
Ronilson Lima de Oliveira	Fiscal	115.865-1 I
Anderson de Oliveira Ramires	Fiscal	133.382-8 C
Sanderson Magalhães Dolzane	Fiscal	121.656-2 C