PORTARIA Nº 186/2025-GS/SEMEF

O **SECRETÁRIO MUNICIPAL DE FINANÇAS, PLANEJAMENTO E TECNOLOGIA DA INFORMAÇÃO – SEMEF**, no exercício da competência que lhe confere o inciso II do artigo 128 da **Lei Orgânica do Município de Manaus**, e

CONSIDERANDO as Diretrizes da Política de Segurança da Informação e Comunicação da Prefeitura de Manaus - POSIC-PM, estabelecidas pelo DECRETO N 3.652, de 15 de março de 2017; e

CONSIDERANDO as finalidades da SEMEF, especialmente a previsão do artigo 1º, XI da LEI Nº 2.828, de 20 de dezembro de 2021;

CONSIDERANDO a necessidade de atualização das nomenclaturas/siglas dos setores relacionados à Subsecretaria de Tecnologia da Informação – SUBTI/SEMEF;

CONSIDERANDO os termos do Memorando n° 056/2025 – SUBTI/SEMEF, constante do E-doc. n° 2025.11209.11214.9.093710;

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação e Comunicação da Secretaria Municipal de Finanças, Planejamento e Tecnologia da Informação - POSIC-SEMEF, o que envolve:

I- o desdobramento dos objetivos definidos na POSIC-PM considerando o contexto da SEMEF;
II- a definição de responsabilidades e competências específicas da SEMEF para a segurança da informação;
III- a implementação da gestão de segurança da informação;
IV- o comprometimento com a melhoria contínua dos processos e o;
V- o atendimento aos requisitos legais, regulamentares e contratuais.

Parágrafo único. A POSIC-SEMEF se aplicará a todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública no âmbito da SEMEF.

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

I - Conceitos e definições:

Aceitação de Risco - decisão de aceitar um risco [ISO/IEC Guia 73:2009].
Ambiente de Desenvolvimento - utilizado para o desenvolvimento de novas soluções de software ou ainda em projetos de manutenção evolutiva e corretiva de soluções existentes;
Ambiente de Homologação - utilizado para validar as implementações das novas funcionalidades antes de ser disponibilizada em produção;
Ambiente de Produção - disponibilizado para atender a demanda de execução dos sistemas de informações utilizados nas atividades diárias dos usuários.
Ambiente de Teste - utilizado para executar e validar alterações e incrementos na codificação em atendimento a uma nova funcionalidade ou na alteração de uma funcionalidade existente;
Ameaça - Causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização.
Análise de risco - Uso sistemático de informações para identificar fontes e estimar o risco.
Análise/avaliação de riscos - Processo completo de análise de risco e avaliação de riscos.
Anonimização - utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Áreas sensíveis – Data Center, Infraestrutura, Segurança da Informação e Sistemas.
Ataque - tentativa de destruir, expor, alterar, desabilitar, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um ativo.
Atendimento TI – Ferramenta ITSM (IT Service Management) CitSmart utilizada para realizar solicitação de serviços para uma determinada área específica, buscando prover qualidade alinhada às necessidades do negócio.
Autenticidade - propriedade que uma entidade é o que afirma ser.
Autoridade Nacional de Proteção de Dados Pessoais (ANPD) - órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD - Lei Geral de Proteção de Dados Pessoais (LEI Nº 13.709, DE 14 DE AGOSTO DE 2018) em todo o território nacional brasileiro;
Avaliação de risco - processo de comparar o risco estimado com critérios de riscos predefinidos para determinar a importância do risco;
Bloqueio - suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
BYOD *(Bring Your Own Device)* - utilizar o próprio dispositivo computacional, visando uma maior produtividade e redução de custos;
CFTV – Circuito Fechado de Televisão;
Comunicação de risco: troca ou compartilhamento de informações sobre riscos entre o tomador de decisões e outras partes interessadas;
Confiabilidade: propriedades de comportamento desejado, consistente e de resultados;
Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
Consentimento - manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
Continuidade do negócio: processo e/ou procedimento para garantir a contínua operação do negócio;
Controlador - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
Controle de acesso - meios para assegurar que o acesso a ativos é autorizado e restrito com base nos requisitos de segurança e de negócios;
Controle: meios de gerenciamento de risco, incluindo políticas, procedimentos, guias, práticas ou estruturas organizacionais, que podem ser administrativas, técnicas, de gestão ou de natureza legal;
Convidado – conta utilizada para acesso temporário ao sistema;
Critérios de risco: termos de referência pelos quais são avaliadas a importância do risco;
Dado Anonimizado - dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
Dado Pessoal - informação relacionada a pessoa natural identificada ou identificável;
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;
DEPAD – Departamento de Administração;
DSITI – Departamento de Segurança e Infraestrutura de TI;
DESIS - Departamento de Sistemas de Informações;
Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;
DPO (Data Protection Officer) - Encarregado de Dados - é o principal responsável por manter a conformidade das organizações com a LGPD;
Eficácia - extensão na qual as atividades planejadas são realizadas e os resultados planejados alcançados;
Eficiência - relação entre o resultado alcançado e os recursos usados;
Eliminação - exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
Estimativa dos riscos - atividade para atribuir valores a probabilidade e consequências de um risco;
Evento de segurança da informação - uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma

situação previamente desconhecida, que possa ser relevante para a segurança da informação;
Evento - ocorrência de um determinado conjunto de circunstâncias;
Gestão de riscos - atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos;
Impacto - mudança adversa ao nível dos objetivos de negócios alcançado;
Incidente de segurança da informação - um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação, afetando as propriedades de confidencialidade, integridade e disponibilidade;
Indisponibilidade – ação resultante da paralisação de determinado serviço essencial para a atividade pública prestada ao contribuinte;
Integridade - propriedade de salvaguarda da exatidão e completude dos ativos;
Intranet – rede de computadores de característica interna;
LGPD - Lei Geral de Proteção de Dados Pessoais;
Login – ação ou efeito de se conectar às atividades em um determinado momento;
Logoff – ação ou efeito de desconectar das atividades em um determinado momento;
Não-repúdio - capacidade de provar a ocorrência de um evento alegado ou de ação e de suas entidades de origem, a fim de resolver disputas sobre a ocorrência ou não ocorrência de evento ou ação e envolvimento de entidades no evento;
Negação de Serviço – ação resultante da paralisação de parte ou todo do arcabouço tecnológico que mantém os serviços da prefeitura disponibilizados (*on-line*) aos contribuintes da PM – Prefeitura de Manaus;
Nota: adicionalmente, outras propriedades, tais como a autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.
Operador – pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
Política - intenção e direção como formalmente expressado pela alta direção;
PM – Prefeitura de Manaus;
Risco de Segurança da Informação - potencial que uma ameaça irá explorar uma vulnerabilidade de um ativo ou grupo de ativos e, assim, causar danos à organização;
Risco residual - risco remanescente após o tratamento de riscos;
Risco – combinação da probabilidade de um evento e suas consequências [ISO/IEC Guia 73:2009]. Efeito da incerteza nos objetivos;
Segurança da Informação - a preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da SEMEF;
SEMEF – Secretaria Municipal de Finanças, Planejamento e Tecnologia da Informação;
SEMEFMAIL - serviço de e-mail corporativo que permite ao usuário enviar e receber mensagens usando um navegador de *internet*;
Sistema de Gestão da Segurança da Informação (SGSI) – a parte do sistema de gestão global, baseada na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação;
SPAM - termo usado para se referir às mensagens eletrônicas que são enviadas para um determinado usuário sem o seu consentimento;
SUBTI – Subsecretaria de Tecnologia da Informação;
TI – Tecnologia da Informação;
Titular – pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
Tratamento de dados pessoais - 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;
Tratamento do risco – processo de seleção e implementação de medidas para modificar um risco;
USB (*Universal Serial Bus)* - barramento serial universal;
Usuário da informação – servidor público da SEMEF ou terceiros

alocados na prestação de serviços à SEMEF, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar, manipular qualquer ativo de informação da SEMEF para o desempenho de suas atividades profissionais;
Violação de dados pessoais – situação em que dados pessoais são processados violando um ou mais requisitos relevantes de proteção da privacidade;
Vulnerabilidade – fraqueza de um ativo ou controle que pode ser explorada por uma ameaça;
Webmail - serviço de *e-mail* (*gmail, hotmail, yahoo etc.*) gratuito que permite ao usuário enviar e receber mensagens usando um navegador de *internet*.

II - Recursos de Tecnologia da Informação:

1. **Ativo**: aquilo que tem valor tangível ou intangível para a SEMEF, tais como: dado, conjunto de dados, informação, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado, independentemente do meio em que estão armazenados ou da forma pela qual sejam veiculadas, softwares, serviços, imagem institucional, processos internos e recursos humanos (servidores, colaboradores, terceirizados e visitantes).
2. **Ativo de TI:** informações eletrônicas, serviço de correio eletrônico, dados corporativos, documentos administrativos, programas de computadores adquiridos de terceiros ou desenvolvidos, recebidos em doação e mantidos pela equipe do DESIS e os arquivos que estejam armazenados no Data Center, na SEMEF.

Equipamentos de informática de qualquer espécie podendo ser constituídos de:

a. servidores, microcomputadores de mesa e portáteis (notebook, tablets, smartphones) e seus dispositivos periféricos, como teclados, mouses, caixas de som, microfones, leitoras, gravadoras e demais acessórios conectados ao computador;
b. scanners, impressoras (laser, jato de tinta, matriciais e térmicas), webcams, data shows, telefone com tecnologia Voip e demais equipamentos relacionados à TI que venham a integrar o patrimônio da SEMEF;

Equipamentos de redes e de comunicações de qualquer espécie que:

a. compreende as redes locais da sede e anexos, bem como a rede de comunicação que as interliga;
b. dados armazenados em equipamentos, dispositivos e periféricos;

Arquivos de configuração que sejam armazenados, executados ou transmitidos por meio da infraestrutura computacional da SEMEF.

3. **Controle de acesso:** são restrições de acesso a um ativo da SEMEF;
4. **Usuário:** toda e qualquer pessoa que tenha acesso aos ativos de informação e aos recursos que compõem os sistemas de informação da SEMEF que se encontra sob responsabilidade da SEMEF e a quem está sujeita a POSIC.
5. **Administrador de sistema computacional:** quaisquer pessoas do quadro funcional, lotadas no DESIS e DSITI, 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.
6. ***Schema*:** um schema na terminologia Oracle é um conjunto de vários objetos de bancos de dados que estão associados a um usuário específico do banco de dados (também chamado de *owner* ou proprietário).
7. ***Owner***: um *owner* é um usuário do banco de dados que tem poder total de ação sobre os objetos de banco de dados do *schema* a que está associado sem precisar de algum direito ou privilégio especial para isso. Ele pode executar comandos DML e DDL naturalmente.
8. ***Script* de Banco de Dados:** considera-se script de banco de dados qualquer conjunto de instruções SQL (padrão mundial de linguagem estruturada de consulta para bancos de dados relacionais) ou PL/SQL (PL/SQL é específico do banco de dados Oracle) que permitam criar ou alterar objetos de banco de dados tais como tabelas, chaves, *constraints*, índices, procedimentos, funções etc.

9. **Dicionário de Dados:** é a parte de um banco de dados que possui os dados do próprio banco de dados, ou seja, dados sobre a sua estrutura, composição, funcionamento, objetos de banco de dados contido nele, usuários, segurança em geral etc.
10. **DBA**: o termo DBA é uma sigla de origem inglesa para *Database Administrator* (Administrador de Banco de Dados), ou seja, é o responsável por gerenciar e administrar o banco de dados.

Art. 3º Para efeitos das diretrizes desta Portaria, a POSIC-SEMEF terá como objetivos básicos:

I – Estabelecer diretrizes para a segurança no manuseio, no tratamento e no controle da proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos no provimento dos serviços de tecnologia da informação que viabilizem o atendimento das finalidades legais das secretarias, autarquias e fundações que compõem a PM;

II – Assegurar a confidencialidade, integridade, disponibilidade, autenticidade e legalidade dos dados e informações das secretarias, autarquias e fundações que mantêm seus ativos de informação nos Data Centers da PM, sob responsabilidade da SEMEF/SUBTI;

III – Disponibilizar o acesso à informação com proteção proporcional ao nível de classificação da informação e/ou do ambiente a ser protegido;

IV – Assegurar que o acesso à informação tanto no âmbito do exercício profissional quanto no acesso pelos cidadãos, estejam de acordo com os termos previstos na legislação vigente;

V – Alertar e conscientizar as organizações parceiras, prestadoras de serviços sobre a importância das informações processadas e sobre os seus riscos e vulnerabilidades;

VI – Estabelecer responsabilidades do usuário sobre a informação da qual é detentor, seja em mídia de armazenamento digital ou impressa, sobre seus acessos e uso dos sistemas de informação e serviços de redes de computadores da SEMEF, extensivas aos prestadores de serviços, observados os termos contratuais;

VII – Manter a segurança na divulgação e troca de informações por meios convencionais e eletrônicos, internamente à organização e com entidades externas, estabelecendo medidas preventivas, orientações e treinamento, incluindo-se os aspectos relativos às ameaças da engenharia social;

VIII – Sistematizar e estabelecer medidas que permitam a identificação, notificação e tratativa em tempo hábil de violações de segurança e que protejam os processos críticos e minimizem os impactos em casos de falhas ou desastres significativos, assegurando a sua retomada em tempo hábil;

IX – Melhorar continuamente os controles de segurança da informação de forma a mantê-los adequados aos objetivos de assegurar a contínua confidencialidade, integridade, disponibilidade, autenticidade e legalidade da informação.

Art. 4º A consecução da POSIC-SEMEF é atribuição do Comitê Gestor de Segurança da Informação da SEMEF - CGSI-SEMEF, cuja designação será publicada em ato próprio pelo Titular da Pasta, tendo a seguinte estrutura de componentes:

a) 1 (um) Presidente;
b) 1 (um) Coordenador Executivo; e
c) No mínimo 3 (três) e no máximo 10 (dez) Membros.

Art. 5º Para disciplinar o funcionamento do CGSI-SEMEF são definidas as seguintes diretrizes:

I - O CGSI-SEMEF deverá revisar e atualizar periodicamente a POSIC, no máximo a cada 2 (dois) anos, caso não ocorra atualização da POSIC-PM, ou caso não ocorram outros eventos ou fatos relevantes que exijam uma revisão imediata;

II - O CGSI-SEMEF reunir-se-á de forma ordinária trimestralmente e, em caráter extraordinário, sempre que convocado pelo Presidente ou Coordenador Executivo, com a presença mínima de metade mais um de seus membros, para acompanhar a situação dos controles de segurança e/ou deliberar sobre situações que possam afetar a segurança da informação. Em caráter excepcional, membros do CGSI-SEMEF podem delegar sua função para uma pessoa considerada habilitada pelos demais membros do comitê;

III - As reuniões do CGSI-SEMEF devem ser registradas em Ata de Reunião, na qual deve constar o registro dos integrantes presentes, a pauta dos assuntos tratados, as ações e providências deliberadas, os responsáveis e o prazo de execução das atividades;

IV - As decisões tomadas pelo CGSI-SEMEF serão validadas por meio de votação, necessitando de maioria simples, considerado a presença de número igual ou superior à metade do total de componentes do comitê, sendo que o presidente votará apenas em caso de desempate;

V - Quando no exercício das funções do comitê, e para a consecução de suas finalidades, os componentes do CGSI-SEMEF poderão:

a) ter livre acesso às áreas e informações, sejam elas físicas ou lógicas, ressalvados os impedimentos legais e limites estabelecidos pela alta gestão da SEMEF;
b) participar de associações ou comitês regionais ou nacionais de segurança da informação com o objetivo de obter ou compartilhar conhecimentos;
c) participar de cursos de capacitação, de eventos ou seminários pertinentes, a fim de manter os integrantes do CGSI-SEMEF atualizados com as recentes práticas, tecnologias e produtos de segurança do mercado, com o objetivo de melhor atender a execução das ações de segurança;
d) convidar especialistas ou propor contratação de consultoria para desenvolvimento de serviços especializados e produtos com a finalidade de promover soluções de segurança, quando couber.

Art. 6º São atribuições do Presidente do CGSI-SEMEF:

I- Acompanhar os resultados do cumprimento da POSIC-SEMEF, das normas e diretrizes emanadas dos CGSIs, o alinhamento deles com a POSIC-PM e propor medidas legais em caso de inobservância das regras;
II- Reportar os indicadores de desempenho da segurança da informação;
III- Assegurar o atendimento aos requisitos legais, regulamentares e estatuários aplicáveis;
IV- Avaliar e aprovar normas, planos, procedimentos, mecanismos de proteção e instruções reguladoras específicas, relativas aos assuntos preconizados na POSIC-SEMEF, exceto quando se tratar de assuntos de alta criticidade ou sigilo, que sejam de competência do Secretário da SEMEF;
V- Comunicar e coordenar atividades relacionadas à segurança da informação com agentes externos;
VI- Aprovar ou destituir os colaboradores da área de segurança da informação, segundo o perfil exigido da função;
VII- Convocar reuniões extraordinárias.
VIII- Garantir que os incidentes de segurança, desvios e problemas registrados no período sejam analisados criticamente e recomendar as correções analisadas, além da avaliar a eficácia das ações tomadas;

IX- Garantir que os riscos de Segurança da Informação sejam analisados, avaliados e tratados de acordo com o risco definido pelo CGSI-SEMEF;
X- Analisar recomendações para a implementação de controles quanto a seu custo e benefício.

Art. 7º São atribuições do Coordenador Executivo do CGSI-SEMEF:

I- Definir e coordenar as atividades dos membros do Comitê na execução das atividades de segurança prescritas na POSIC-SEMEF;
II- Responder pelas atribuições do presidente em suas ausências e impedimentos;
III- Convocar reuniões extraordinárias.

Art. 8º São atribuições dos demais membros do CGSI-SEMEF:

I- Assessorar o Secretário da SEMEF nos assuntos relacionados à segurança da informação;
II- Executar as ações e planos de trabalho definidos pelo comitê;
III- Acompanhar o cumprimento da POSIC-SEMEF, das normas e diretrizes emanadas do comitê;
IV- Produzir e propor normas, planos, procedimentos, mecanismos de proteção e instruções reguladoras específicas, relativas aos assuntos preconizados na POSIC-SEMEF;
V- Promover, no âmbito da SEMEF, a conscientização e a mentalidade de segurança da informação, bem como a importância das informações processadas, dos seus riscos e vulnerabilidades e impactos do não cumprimento de controle e de falhas de segurança;
VI- Executar as ações e planos de trabalho definidos pelos CGSIs relativas à sua área de atuação;
VII- Avaliar os impactos das propostas de normas, procedimentos e controles em suas áreas de atuação;
VIII- Revisar os principais documentos do Sistema de Gestão da Segurança da Informação (políticas, normas etc.), mantendo o foco para que reflitam a cultura da SEMEF e após a aprovação, publicá-los e promover a divulgação dos documentos entre os servidores da SEMEF;
IX- Propor e apoiar iniciativas que visem à segurança dos ativos de informação;
X- Manter comunicação efetiva dentro da SEMEF, com o objetivo de manter os servidores adequadamente informados sobre assuntos relacionados à Segurança da Informação e que afetem ou tenham potencial para afetar a SEMEF;
XI- Receber as denúncias sobre violações da Política e das Normas devendo promover a tratativa das informações, identificação do plano de ação, mitigação de risco, acionamento do CGSI e aplicação da sanção cabível (Penalidades).

Art. 9º As atividades realizadas pelos membros do CGSI-SEMEF não serão remuneradas.

Art. 10. Todos os usuários que se utilizem de informações e de Sistemas de Informações, no âmbito da SEMEF, devem assinar o Termo de Uso dos Sistemas de Informações e Termo de Responsabilidade e Sigilo da Informação, constantes do **Anexo II.**

§1º A assinatura dos Termos previstos no *caput* deste artigo se dará durante o processo de admissão, nomeação ou posse, momento em que será apresentada a POSIC-SEMEF. Havendo um número expressivo de pessoas, o CGSI-SEMEF poderá realizar esta atividade, bem como a palestra de divulgação e sensibilização da POSIC-SEMEF, de forma centralizada, em local e data oportuna.

§2º No caso de servidores temporários, comissionados, celetistas, efetivos e em plena atividade, deverão assinar os Termos previstos no *caput* deste artigo em prazo a ser definido pelo CGSI-SEMEF.

§3º No caso de prestadores de serviços, a assinatura dos Termos previstos no *caput* deste artigo se dará durante atividade de divulgação e sensibilização da POSIC-SEMEF, antes de lhes ser concedido acesso às informações e sistemas de informação.

§4º Após a assinatura dos Termos, o usuário assume formalmente a responsabilidade pelo bom uso dos ativos de informações, o compromisso de seguir a POSIC-SEMEF e de manter o sigilo sobre todos os ativos de informações e processos, mesmo após o seu desligamento ou término de prestação de serviços.

Art. 11. Os gestores da SEMEF se comprometem a apoiar a implantação e gestão da segurança da informação, de acordo com o que prescrevem as normas ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27002:2022.

Art. 12. A sensibilização e cultura de segurança, bem como a divulgação da importância das informações processadas, seus riscos e vulnerabilidades, e ainda os impactos do não cumprimento ou falhas de segurança devem ser desenvolvidas e mantidas por meio de palestras, seminários, treinamentos, e outros canais de comunicação disponíveis no âmbito da SEMEF.

Art. 13. Os recursos de TI pertencentes à SEMEF que estão disponíveis para os usuários devem ser utilizados em atividades estritamente relacionadas com a prática e o desempenho funcional.

Art. 14. É vedado aos usuários o fornecimento de informações a terceiros sobre especificações técnicas, administrativas, financeiras ou qualquer outra que implique riscos, violação e outras consequências que comprometam a segurança dos ativos de TI e dos Sistemas de Informação da SEMEF.

Art. 15. É vedada a utilização de quaisquer recursos de TI da SEMEF com o objetivo de praticar atos danosos contra os próprios recursos ou terceiros, dentre os quais: equipamentos servidores, estações de trabalho, equipamentos de rede, serviços de segurança e sistemas de informação.

Art. 16. Qualquer anormalidade percebida pelo usuário quanto aos privilégios de seu acesso aos recursos de Tecnologia da Informação deve ser imediatamente comunicada ao DSITI.

Art. 17. Todos os usuários receberão uma conta na caixa de correio eletrônico institucional (*e-mail*) destinada às comunicações internas e externas através da internet.

Art. 18. O DSITI 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. E:

§1º No caso de incidente de segurança, deverá bloquear temporariamente, sem aviso prévio, o dispositivo computacional que esteja realizando atividade que coloque em risco a segurança da rede de dados, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica da SEMEF.

§2º Deverá bloquear temporariamente, sem aviso prévio, acesso a impressoras e copiadoras que estejam imprimindo/copiando documentos particulares ou alheios às rotinas inerentes à administração pública.

Art. 19. O usuário que fizer uso de forma indevida ou não autorizada dos recursos de Tecnologia da Informação, bem como violar ou agir em desacordo com os termos ou qualquer dispositivo 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 e a sanções administrativas, civil e penais da legislação em vigor, com um adicional de ressarcimento material e ou financeiro à SEMEF, quando assim se fizer necessário.

Art. 20. São diretrizes para a Privacidade de Dados Pessoais:

I- Garantir ao titular a finalidade e a adequação ao tratamento de seus dados pessoais, mesmo que por obrigações legais, a legislação vigente permita a coleta e o processamento de dados pessoais sem o consentimento inequívoco do titular;
II- Limitar a coleta de dados pessoais estritamente ao que é necessário, minimizando, onde possível, a coleta dos referidos dados pessoais.
III- Limitar o uso, retenção, divulgação e transferência de dados pessoais ao necessário para cumprir com objetivos específicos, explícitos e legítimos;
IV- Reter os dados pessoais apenas pelo tempo necessário para o cumprimento das obrigações legais;
V- Não realizar mais nenhum tratamento dos dados pessoais, quando não mais existir a finalidade para a qual foi submetida sua coleta;
VI- Ao expirar o tempo necessário, os dados pessoais deverão ser destruídos, salvo quando por força de obrigações contratuais e/ou de legislação, necessitem ser armazenados por um tempo determinado, contexto em que deverão sofrer processo de anonimização ou pseudoanonimização.
VII- Garantir a precisão e a qualidade dos dados pessoais tratados, excetuando-se casos em que exista uma base legal para manter os dados desatualizados.
VIII- Garantir a rastreabilidade e prestação de contas durante todo o tratamento de dados pessoais, principalmente, quando os dados pessoais forem compartilhados com terceiros.
IX- Tratar integralmente as violações de dados pessoais, garantindo que sejam adequadamente registradas, classificadas, investigadas, corrigidas e documentadas.
X- Garantir que, na ocorrência de uma violação de dados pessoais, todas as partes interessadas sejam notificadas, conforme requisitos e prazos previstos na legislação.
XI- Documentar e comunicar, conforme apropriado, todas as políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados.
XII- Garantir a existência de um sub encarregado de dados, responsável por documentar, implementar e comunicar políticas, procedimentos e práticas relacionadas à proteção de dados na SEMEF, e quando invocado, atuar diretamente com o encarregado de dados (DPO) da Prefeitura de Manaus;
XIII- Adotar controles de segurança da informação, tanto técnicos quanto administrativos, suficientes para garantir níveis de proteção adequados para os Dados Pessoais.
XIV- Disponibilizar políticas, normas e procedimentos para proteção de dados pessoais a todas as subsecretarias subordinadas à SEMEF.
XV- Garantir a educação e conscientização de servidores, terceirizados, parceiros contratados sobre as práticas de proteção de dados pessoais adotadas pela SEMEF.
XVI- Melhorar continuamente a Gestão de Proteção de Dados Pessoais através da definição e revisão sistemática de objetivos de privacidade e proteção de dados pessoais em todos os níveis da SEMEF.
XVII- Garantir a não discriminação no tratamento de dados pessoais, impossibilitando que estes sejam usados para fins discriminatórios, ilícitos ou abusivos.
XVIII- Garantir a conformidade integral com legislações e regulamentações vigentes que tratam sobre proteção e privacidade de dados pessoais.
XIX- Notificar aos titulares de dados quando ocorrerem alterações significativas no tratamento dos seus dados pessoais.
XX- Fornecer aos titulares dos dados pessoais informações claras e facilmente acessíveis sobre as políticas, procedimentos e práticas com relação ao tratamento de dados pessoais realizado, incluindo quais dados são efetivamente tratados, a finalidade desse tratamento e informações sobre como entrar em contato para obter mais detalhes acerca do assunto;
XXI- Garantir que os titulares de dados tenham a possibilidade de acessar e revisar seus dados pessoais e que não exista nenhuma restrição legal a esse acesso ou à revisão dos dados pessoais.

XXII- Este acesso deverá ocorrer através de um mecanismo que realize a autenticação do titular dos dados em um nível garantido de segurança.

Art. 21. É atribuição da área de Infraestrutura de TI e Suporte Técnico (DSITI) instalar e configurar o hardware, acesso à rede intranet, internet, bem como instalar e configurar o software necessário à prestação dos serviços.

Art. 22. O uso aceitável de ativos de informação, classificação da informação, controle de acesso, correio eletrônico, ações que violam a política de segurança da informação, acesso à internet, combate a softwares maliciosos etc. serão realizados conforme diretrizes específicas, constantes do **Anexo I**.

Art. 23. Os casos omissos e as dúvidas surgidas na aplicação desta Portaria serão dirimidos pelo CGSI-SEMEF.

Art. 24. Esta Portaria entra em vigor na data de sua publicação, revogadas as disposições em contrário, em especial a Portaria nº 144/2022-GS/SEMEF, de 13 de setembro de 2022, publicada no DOM, edição nº 5424.

Manaus, 23 de julho de 2025.

CLÉCIO DA CUNHA FREIRE
Secretário Municipal de Finanças, Planejamento
e Tecnologia da Informação – SEMEF

ANEXO I

DIRETRIZES ESPECÍFICAS

1. CLASSIFICAÇÃO DA INFORMAÇÃO

Para efeitos de classificação da informação, a SEMEF se molda no artigo 33 do Decreto Municipal nº 4.157/2018, que regula o acesso a informações no âmbito do Poder Executivo Municipal e na norma de segurança ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27002:2022 estabelecendo as seguintes categorias:

PÚBLICA: informação liberada para o público geral. A divulgação desse tipo de informação não causa problemas à SEMEF, podendo ser compartilhada livremente com o público geral, desde que seja mantida sua integridade.
RESERVADA: quando tramita no âmbito da SEMEF e cujo conteúdo, se divulgado, possa comprometer a SEMEF e/ou outrem;
SECRETA: quando pode ser acessada apenas por um grupo restrito de pessoas, de forma que sua divulgação não autorizada pode implicar em perdas financeiras ou prejudicar a reputação/imagem da SEMEF;
ULTRASSECRETA: quando dirigida a um grupo extremamente limitado de pessoas, nominalmente identificadas. A divulgação de seu conteúdo pode permitir acesso a informações estratégicas podendo causar sérios prejuízos à SEMEF.

Para diretrizes e informações complementares sobre classificação, manuseio e rotulagem dos ativos de informação da SEMEF, consultar a NORMA – CLASSIFICAÇÃO DA INFORMAÇÃO no endereço eletrônico:

https://leismunicipais.com.br/a1/am/m/manaus/decreto/2018/415/4157/decreto-n-4157-2018-regulamenta-o-acesso-as-informacoes-no-ambito-do-poder-executivo-do-municipio-de-manaus-e-da-outras-providencias

2. INCIDENTES DE SEGURANÇA DA INFORMAÇÂO

2.1. Caso haja qualquer ocorrência de indisponibilidade aos serviços de sistemas de informações, deve-se proceder de imediato à correção do incidente que ocasionou a sua indisponibilidade, retornando imediatamente o serviço ao seu estado anterior. E em seguida, realizar o registro na ferramenta ***ITSM – CitSmart no endereço: https://atendimentoti.manaus.am.gov.br/citsmart/login/login.load***
2.2. Caso seja identificado a potencialidade de que vulnerabilidades exploradas e/ou expostas apontem para um mínimo de indício de vazamento de dados, deverá informar imediatamente a equipe de Segurança da Informação do DSITI, o DESIS e ao Subsecretário de Tecnologia da Informação, e:

1) Caso o vazamento de dados se estenda para dados pessoais, o Sub encarregado de Dados Pessoais da SEMEF deverá ser acionado, para, após análise, juntamente com a equipe, reportar o incidente à Agência Nacional de Proteção de Dados Pessoais (ANPD) e ao titular de dados pessoais, conforme preconiza a Lei 13.709/2018, Lei Geral de Proteção de Dados (LGPD);

3. RESPOSTAS A INCIDENTES DE SEGURANÇA DA INFORMAÇÂO

3.1. Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos, dos serviços e dos recursos de informação e computacionais da SEMEF serão caracterizadas como um incidente de segurança da informação.
3.2. Todos os incidentes e as suspeitas de segurança da informação devem ser imediatamente reportados através da ferramenta ITSM – CitSmart no endereço: https://atendimentoti.manaus.am.gov.br/citsmart/login/login.load, e comunicados ao DSITI;
3.3. O DSITI deverá determinar a criticidade do incidente, informar os membros do CGSI-SEMEF, o Time de Resposta a Incidentes de Segurança da Informação e, quando pertinente, comunicar outras partes interessadas como, por exemplo, Secretário da SEMEF, Subsecretário de TI e o DESIS;
3.4. Na ocorrência de um incidente de segurança da informação, ativos e serviços de informação ou recursos computacionais com suspeita de ter sua segurança comprometida, devem ser isolados do ambiente de produção, de forma a mitigar a contenção do incidente;
3.5. Incidentes de segurança da informação podem resultar em perda, dano ou acesso não-autorizado às informações. Quando da sua ocorrência, devem ser priorizados com base na criticidade dos ativos e serviços de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista;
3.6. A extensão dos danos do incidente de segurança da informação deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente. Medidas devem ser estabelecidas para minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos ativos e serviços de informação ou recursos computacionais afetados;
3.7. Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, as vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de ações adicionais para evitar a recorrência do incidente.

4. USO ACEITÁVEL DE ATIVOS DE INFORMAÇÃO

4.1. Os equipamentos disponibilizados pela SEMEF são exclusivamente para o atendimento de suas atividades profissionais, sendo expressamente proibida a utilização para fins particulares;
4.2. A alteração e ou a manutenção de qualquer dispositivo computacional e afins de propriedade da SEMEF é uma atribuição específica do DSITI, salvo os equipamentos classificados como proprietários que possuem manutenção técnica especializada.
4.3. Computadores de mesa (desktops) ou portáteis (notebooks, smartphones, tablets e etc.) devem ser desligados no final do expediente, excetuando-se quando existir uma justificativa plausível para mantê-lo ligado em virtude de atividades de trabalho;
4.4. A desconexão (*logoff*) 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 de tempo prolongado;
4.5. No momento em que o usuário se ausentar da sua estação de trabalho, o mesmo deverá bloqueá-la para fins de impedir o acesso não autorizado;
4.6. Os usuários são responsáveis pelos recursos computacionais disponibilizados pela SEMEF para a realização de suas atividades, devendo preservar sua integridade e a continuidade de uso. Caso seja constatado dano decorrente de ação direta ou omissão do usuário, caberá à SEMEF exercer seu direito de reparação ao prejuízo, solicitando ressarcimento material ou financeiro do recurso computacional danificado;
4.7. A critério exclusivo, será avaliada a permissão de utilização de equipamento particular (*BYOD*) para o desempenho de atividades profissionais, na rede administrativa da SEMEF, seja em segmentos cabeados ou sem fio. Tais equipamentos devem passar por inspeção pelo DSITI, de forma a garantir adequação aos requisitos e controles de segurança adotados pela SEMEF;
4.8. Ao final do contrato de trabalho, os equipamentos disponibilizados para a execução de atividades profissionais devem ser devolvidos em

estado de conservação adequado, quando do desligamento ou término da relação do usuário com a SEMEF;
4.9. A estação de trabalho deve manter o padrão estabelecido pelo DSITI, no tocante ao sistema operacional e aos demais programas de computador instalados.
4.10. A instalação de software nas estações de trabalho deverá ser realizada por técnico do DSITI, podendo ainda utilizar ferramentas de acesso remoto ou pela rede *intranet*;
4.11. Quanto à necessidade de instalação de *softwares* de categorias de domínio público (não protegido por *copyright*) e/ou cópias de demonstração que não sofram ação de direitos autorais, deverá ser previamente solicitada pela chefia imediata do demandante ao DSITI;
4.12. O DSITI, por meio de seu corpo técnico de suporte, efetuará remoção de *softwares* instalados em estações de trabalho, bem como os que não se enquadram nos critérios estabelecidos neste anexo;
4.13. Somente em casos especiais será concedido privilégio de administrador da máquina aos usuários das estações de trabalho, por meio de prévia solicitação por escrito pela chefia imediata. É vedado aos usuários com privilégio de administrador da máquina o compartilhamento de recursos ou ativação de serviços de rede nas estações de trabalho, sem autorização do DSITI;
4.14. É vedada a instalação de qualquer *software* ou de quaisquer componentes ou placas de *hardware* que alterem a configuração original do equipamento e que não tenham sido adquiridos pela SEMEF ou realizados por técnico do DSITI;
4.15. É vedada a conexão de dispositivos móveis à rede sem fio da SEMEF, exceto quando houver prévia autorização do DSITI;
4.16. É vedado armazenar na estação de trabalho arquivos que não possuem relação com as atividades profissionais do usuário. Arquivos pessoais devem ser armazenados em dispositivos computacionais com acesso a porta de comunicação (USB) do dispositivo, tais como HD (*Hard Disk*) externo, *pendrive*, s*martphone* e ou similares;
4.17. Arquivos de caráter institucional devem ser salvos em unidade de rede compartilhada para esse fim ou em dispositivos de armazenamento (*Hard Disk* – HD, *Pendrive* ou similares) externo de propriedade da instituição.
4.18. Compete ao DSITI agendar o processamento de software antivírus nas estações de trabalho, definindo sua periodicidade, podendo, antecipadamente, realizar varredura nos equipamentos sempre que julgar necessária;
4.19. Quando do envio de equipamentos para leilão e ou doação, deverá ser realizado procedimento operacional para sanitização de dados no disco rígido do dispositivo computacional, bem como se houver necessidade, aplicar técnicas *Anti-forense* para evitar recuperação de dados formatados e ou excluídos anteriormente, durante seu uso na secretaria.
4.20. Previamente, ao enviar equipamentos para manutenção externamente à SEMEF, deverá ser realizado procedimento operacional para preservar informações relevantes no dispositivo computacional, adicionando controle e tratativa para o tratamento de dados pessoais referente à Lei 13.709/2018 – LGPD.

Dispositivos portáteis e móveis

4.21. Os dispositivos computacionais portáteis e ou móveis quando adquiridos devem possuir desejável tecnologia de proteção por criptografia de disco e ou memória;
4.22. O usuário é o responsável direto pela segurança física e lógica dos dispositivos portáteis e ou móveis sob sua guarda. Havendo necessidade de se deslocar em ambiente externo com os dispositivos supracitados, deverá ter conduta discreta e dar preferência para compartimentos de armazenamento resistentes e não chamativos;
4.23. Em caso de perda ou furto do dispositivo portátil e ou móvel sob sua guarda, o usuário deverá registrar BO na delegacia competente, em seguida, comunicar imediatamente à chefia imediata e ao DSITI;

Identificação digital

4.24. A SEMEF poderá, a seu critério exclusivo, mas não obrigatório, disponibilizar certificados digitais para usuários que executem atividades profissionais específicas, devendo ser observadas as seguintes diretrizes:
a) Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte;
b) O usuário deverá informar a equipe de segurança da informação sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital;
c) Em caso de perda ou furto do certificado digital sob sua guarda, o usuário deverá registrar BO na delegacia competente, em seguida, comunicar imediatamente à chefia imediata e ao DSITI;

Equipamentos de impressão e reprografia

4.25. O uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse da SEMEF ou que estejam relacionados com o desempenho das atividades profissionais do usuário.
4.26. O usuário deve observar as seguintes disposições específicas quanto ao uso de equipamentos de impressão e reprografia:
a) retirar imediatamente da impressora ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia que contenham informações da SEMEF, classificadas como de uso interno, confidencial ou restrita;
b) a impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada;
c) não será admissível, em nenhuma hipótese, o reaproveitamento de páginas já impressas contendo informações classificadas como de uso interno, confidencial ou restrita, devendo, portanto, ser descartadas/destruídas utilizando processo de picote.

5. SEGURANÇA FÍSICA

5.1. As instalações de processamento de dados da SEMEF serão mantidas em áreas seguras, cujo perímetro físico possui controle contra o acesso não autorizado.
5.2. O usuário deve observar as seguintes disposições específicas quanto à segurança física:
a) Crachás de identificação são pessoais e intransferíveis. Sob nenhuma circunstância será permitido o seu compartilhamento;
b) Enquanto permanência em áreas sensíveis, os usuários devem portar crachás de identificação que exibam claramente seu nome e fotografia.
c) É resguardado à SEMEF o direito de monitorar seus ambientes físicos, através de sistema de CFTV (ou ainda outros sistemas que venham a substituí-los), nas áreas comuns. As imagens obtidas serão armazenadas por um período de tempo de 20 dias;
d) O ambiente físico em que se encontram os ativos de informação da SEMEF é de acesso, preferencialmente, aos integrantes do DESIS e DSITI.
e) Devem ser adotados controles de barreira física (dispositivos de biometria, catracas eletrônicas, entre outros etc.) que restrinjam a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança e habilitando o acesso apenas de pessoal autorizado.
f) Os documentos classificados como internos ou confidenciais não deverão ser deixados expostos, assim, ao se ausentar, cabe ao usuário o dever de mantê-los guardados ou descartá-los de acordo com os procedimentos determinados pela Política de Segurança da Informação desta secretaria;
g) Não é permitido consumir qualquer tipo de alimento, bebida ou fumar em áreas apontadas como sensíveis.

6. CONTROLE DE ACESSO

6.1. A senha de acesso é de uso pessoal e intransferível e sua divulgação é vedada, sob qualquer hipótese.
6.2. O DSITI 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.
6.3. Ao ser credenciado para uso dos recursos de Tecnologia da Informação, o perfil atribuído ao usuário corresponderá a seus direitos e privilégios para acesso a serviços e informações. Essa credencial ocorrerá mediante a autenticação do usuário via login e senha de acesso. Esse perfil será definido pela chefia imediata.
6.4. Sempre que se fizer necessário, deverá ser revisado o nível de permissões de acesso dos usuários, para fins de identificar possíveis privilégios indevidos que possam comprometer a segurança dos dados e dos recursos computacionais da SEMEF.
6.5. O acesso a redes externas à SEMEF ou à Internet dar-se-á, exclusivamente, por meios autorizados e configurados pelo DSITI, sendo vedado o uso de qualquer forma de conexão alternativa, salvo autorização expressa do Diretor do DSITI ou Subsecretário da SUBTI.
6.6. Poderá ser disponibilizado permissões de acesso distintas ao perfil do usuário, desde que devidamente autorizadas pela chefia imediata, mediante documento próprio de solicitação de alteração de perfil.
6.7. Os acessos caracterizados específicos e privilegiados, tais como: acesso a sistemas internos e/ou portais, ferramentas técnicas, unidade de rede, e outros que se fizerem necessários, irão variar de acordo com o cargo e perfil de trabalho a ser executado, e serão solicitados pela chefia imediata, formalizado via documento encaminhado à área específica de controle para a liberação dos acessos.
6.8. No caso de ausência do local de trabalho, mesmo que temporariamente, o usuário deverá bloquear o acesso à sua estação de trabalho (efetuar logoff), devendo informar novamente sua senha para efetuar o desbloqueio.
6.9. Os usuários deverão estar cientes de que serão responsabilizados por suas ações ou por atos de infração cometidos durante a sua permanência na SEMEF.
6.10. Os gestores de cada área são responsáveis por comunicar o afastamento definitivo de usuários ao DEPAD.
6.11. Os privilégios concedidos a usuários temporários, a título de convidado, deverão ser revogados, assim que não se fizerem mais necessários.
6.12. As solicitações de concessão de privilégios adicionais aos usuários, devem estar relacionadas ao perfil e às atividades a serem exercidas pelo servidor na SEMEF e serão avaliadas pela chefia imediata ou pelo DSITI.
6.13. Os privilégios concedidos e classificados com o grau elevado deverão sofrer revisão sempre que se fizer necessário.
6.14. Qualquer questão ou dúvida sobre controle de acesso deverá ser direcionada para o DSITI.

7. DEPARTAMENTO ADMINISTRATIVO (DEPAD) / Divisão de Gestão de Pessoas

7.1. Após finalização dos trâmites para contratação de um novo servidor público, deverá ser solicitada ao DSITI a disponibilização de acesso aos serviços básicos, tais como: conta de correio eletrônico, acesso a aplicativos para produtividade, acesso à internet etc.
7.2. Colher a assinatura do Termo de Responsabilidade e Sigilo da Informação, Termo de Uso dos Sistemas de Informação dos usuários de recursos de tecnologia da informação, arquivando-o nos respectivos prontuários;
7.3. Deverão ser informadas ao DSITI as alterações relacionadas com os usuários tais como: aposentadorias efetivadas, suspensão, fruição de férias, licença-maternidade, licença-prêmio ou qualquer outra alteração que necessite a revogação dos acessos e bloqueio aos recursos computacionais temporária e/ou definitivamente.

7.4. Na ocorrência de desligamento de um servidor do quadro funcional da SEMEF, o DEPAD deverá informar o desligamento de forma imediata ao DSITI para a revogação de todos os privilégios concedidos, bem como atribuir status de inativo na sua conta de *login*.
7.5. Caso o usuário mude de setor (lotação), os acessos e privilégios concedidos serão revogados, e novos acessos e privilégios serão concedidos de acordo com a nova funcionalidade exercida, e, sempre, após solicitação por escrito ou por meio eletrônico da chefia imediata ou do DEPAD.

8. BANCO DE DADOS

8.1. Os processos de desenvolvimento, manutenção, bem como a aquisição de sistemas de informação que envolvam a tarefa de manipulação de banco de dados deverão adequar-se aos ambientes de trabalho abaixo:
a) **Ambiente de Desenvolvimento:** utilizado para o desenvolvimento de novas soluções de software ou ainda em projetos de manutenção evolutivas e corretivas de soluções existentes;
b) **Ambiente de Teste:** utilizado para executar e validar alterações e incrementos na codificação em atendimento a uma nova funcionalidade ou na alteração de uma funcionalidade existente;
c) **Ambiente de Homologação:** utilizado para validar as implementações das novas funcionalidades antes de ser disponibilizada em produção;
d) **Ambiente de Produção:** disponibilizado para atender a demanda de execução dos sistemas de informações utilizados nas atividades diárias dos usuários.

9. AÇÕES QUE VIOLAM A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

9.1. Revelar ou permitir o acesso a códigos de identificação que atribua autenticação e autorização nos sistemas de informação administrados pela SEMEF;
9.2. Ceder as credenciais de acesso de uso pessoal (conta, senhas, chaves privadas etc.) que permita a terceiros fazer uso de recursos de nível gerencial ou que facilite obter este tipo de perfil;
9.3. Divulgar informações sobre usuários e/ou serviços específicos, a partir de qualquer recurso de Tecnologia da Informação administrado pela SEMEF, salvo, as de natureza pública ou mediante prévia autorização pelo departamento gestor da informação com validação do DSITI/SUBTI;
9.4. Interferir sem prévia autorização em um ou mais serviços, podendo causar indisponibilidade do(s) mesmo(s), comprometendo, assim, a continuidade do negócio;
9.5. Elaborar ou cooperar com ataques de negação de serviços oriundos de meios internos ou externos, salvo, as diretrizes aplicadas pelo DSITI/SUBTI, quando da utilização de ferramentas que simulem acesso à rede e aplicações no ato de investigar, examinar ou testar vulnerabilidades através da metodologia de Testes de Intrusão (*PenTest*);
9.6. Adulterar registro de logs de eventos dos sistemas de informação, sistemas operacionais e softwares aplicativos administrados pela SEMEF, afim de encobrir rastros de acessos e ações indevidas;
9.7. Monitorar ou interceptar o tráfego de rede no âmbito dos sistemas de informação administrados pela SEMEF, sem a prévia autorização do DSITI/SUBTI;
9.8. Utilizar jogos *on-line* sem prévia autorização pelo DSITI/SUBTI;
9.9. Usar recurso tecnológico da SEMEF para fins pessoais no âmbito de atividades comerciais de qualquer natureza;
9.10. Manter arquivos de caráter pessoal em dispositivos computacionais ou em unidade de rede compartilhada pela SEMEF;
9.11. Instalar e utilizar softwares que estejam em desacordo com aqueles definidos pelo DSITI/SUBTI;
9.12. Modificar o cabeçalho de qualquer protocolo de comunicação de dados, para fins de executar atividades maliciosas no âmbito dos sistemas de informação administrados pela SEMEF;
9.13. Executar atividades que simulem ou realizem o povoamento de dados em tabelas de nível mínimo ao crítico nos sistemas de informação em execução no âmbito da SEMEF, sem um plano de execução ou

contingência aprovado pelo DSITI e pelo Comitê de Segurança da Informação;
9.14. Utilizar dispositivo computacional (computador desktop, notebook, *smartphones*, *tablets* etc.) fornecido pela SEMEF para uso exclusivo na execução das atividades profissionais, para realização de atividades de cunho pessoal que possuam características de ganhos financeiros extra.

10. CORREIO ELETRÔNICO

10.1. Usuário e Gestores deverão estar cientes das responsabilidades e consequências (está sujeito a sanções e penalidades) quanto à conta de correio eletrônico que lhe foi disponibilizada;

Geral

10.2. A SEMEF fornece o serviço de *e-mail* para seus usuários, exclusivamente para o desempenho de suas atividades profissionais e o seu conteúdo não possui perspectiva de sigilo;
10.3. O acesso ao conteúdo de *e-mail* por técnicos da SEMEF ocorrerá somente quando em situações que imponham risco à imagem, ao negócio e prejuízo à SEMEF;
10.4. Os usuários do serviço de *e-mail* devem adotar a assinatura padrão, formatada de acordo com o que for definido pela SEMEF:
a) Ao final do *e-mail*, após a assinatura, deverá ser exibido o seguinte aviso de confidencialidade: "*As informações contidas nesta mensagem e quaisquer outras informações adicionais em arquivo(s) anexado(s), são confidenciais e seu sigilo protegido por lei, e somente o(s) destinatário(s) esta(ao) autorizado(s) a fazer uso das mesmas. Caso não seja o destinatário pretendido e tenha recebido esta mensagem por engano, por favor, notifique o remetente e em seguida destrua este e-mail, observando que deverá abster-se: de divulgar, distribuir, examinar, armazenar, encaminhar, imprimir, copiar ou utilizar a informação contida em seu conteúdo, caso contrário, estará sujeito às sanções e penalidades da legislação em vigor. Os dados pessoais constantes nesta mensagem serão tratados de acordo com a finalidade para a qual foram coletados, utilizando-se de meios que garantam a proteção dos mesmos, em consonância com o Art. 6 da Lei Geral de Proteção de Dados Pessoais - LGPD - Lei 13.709/2018*";

10.5. Utilizar *e-mail* pessoal (de domínio próprio ou *webmail*) para as atividades profissionais exercidas na SEMEF, salvo quando estritamente necessário e com a anuência da chefia imediata;

Monitoramento

10.6. O serviço de *e-mail* da SEMEF é continuamente monitorado com o objetivo de proteger a organização, atestar o respeito às regras contidas nessa norma, bem como produzir evidências relativas à eventual violação das regras e/ou à legislação vigente;
10.7. Durante o monitoramento, a SEMEF se resguarda o direito de, sem qualquer notificação ou aviso: monitorar, interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais todas as mensagens enviadas ou recebidas pelos usuários através de seu serviço de *e-mail*;

Vedado

10.8. Utilizar o serviço de *e-mail* em caráter pessoal ou para fins que não sejam de interesse da SEMEF;
10.9. Utilizar de termos ou palavras de baixo calão na redação de mensagens;
10.10. Enviar informação classificada como **RESERVADA, SECRETA, ULTRASSECRETA** para endereços eletrônicos que não fazem parte do domínio corporativo da SEMEF, excetuando-se quando expressamente necessária e autorizada;
10.11. Inscrever o endereço de *e-mail* disponibilizado em listas de distribuição e grupos de discussão que não estejam relacionadas com as atividades exercidas ou do interesse da SEMEF;
10.12. Fazer uso de qualquer técnica de falsificação ou simulação de falsa

identidade e manipulação de cabeçalhos de *e-mail*. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas conforme decisão do Comitê de Segurança da Informação;
10.13. Tentar a interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que expressamente autorizado;
10.14. Utilizar o serviço de *e-mail* para o envio de mensagens indesejadas (*spam*) ou qualquer tipo de técnica que possa levar à sobrecarga do serviço de *e-mail*;
10.15. Usar o serviço de *e-mail* para o envio de mensagens cujo conteúdo incite uso de drogas ilícitas, terrorismo, práticas subversivas, violência, aborto, conteúdo pornográfico, práticas racistas e ainda disseminar ou transmitir mensagens de caráter injurioso, calunioso, assim como quaisquer outros atos que não estejam disponíveis nesta seção e que possam trazer outras violações infringindo a legislação vigente.

11. ACESSO À INTERNET

11.1. A SEMEF fornece acesso à Internet aos seus usuários conforme as necessidades inerentes ao desempenho de suas atividades profissionais;
11.2. O acesso à internet pode ser fornecido tanto através da rede corporativa da SEMEF, quanto através da disponibilização de serviços de internet móvel, prestados por terceiros, contratados pela SEMEF;
11.3. Toda informação acessada, transmitida, recebida ou produzida através do acesso à internet fornecido pela SEMEF está sujeita a monitoramento para verificação de atendimento à Política de Segurança da Informação e Comunicação;
11.4. Durante o monitoramento do acesso à internet, a SEMEF se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais incluindo investigações criminais, toda informação trafegada seja originada de sua rede interna e destinada à rede externa ou o processo contrário;
11.5. Durante o acesso à Internet fornecido pela SEMEF não será permitido o *download*, o *upload*, a inclusão, a disponibilização, a visualização, a edição, a instalação, o armazenamento e/ou a cópia de qualquer conteúdo relacionado expressa ou subjetivamente, direta ou indiretamente, com:
a) Qualquer espécie de exploração sexual;
b) Qualquer forma de conteúdo adulto, erotismo, pornografia;
c) Qualquer tipo de Pornografia infantil;
d) Qualquer forma de ameaça, chantagem, assédio moral ou sexual;
e) Qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;
f) Preconceito baseado em cor, sexo, opção sexual, raça, origem, condição social, crença, religião, deficiências e necessidades especiais;
g) Incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam essas lícitas ou não;
h) A prática e/ou a incitação de crimes ou contravenções penais;
i) A prática de propaganda política nacional ou internacional;
j) A prática de quaisquer atividades comerciais desleais;
k) O desrespeito à imagem ou aos direitos de propriedade intelectual da SEMEF;
l) A disseminação de códigos maliciosos e ameaças virtuais;
m) Tentativa de expor a infraestrutura computacional da SEMEF a ameaças virtuais;
n) Divulgação não autorizada de qualquer informação da SEMEF classificada como **RESERVADA, SECRETA, ULTRASSECRETA**;
o) Uso de sites ou serviços que busquem contornar controles de acesso à internet.
p) Comportamento corporativo em mídias e redes sociais;
11.6. A publicação de conteúdo referente à SEMEF em mídias e redes sociais é feita por setores e usuários que possuem essa responsabilidade específica, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da instituição;
11.7. Quando no uso de suas mídias e redes sociais os usuários devem observar as seguintes restrições:
a) Não é permitido o uso da logomarca, bem como de qualquer parte da identidade visual da SEMEF, sem autorização prévia e expressa, salvo,

as redes sociais (*Whatsapp*) utilizadas para comunicação interna;
b) Não é permitida a criação, participação ou interação de/com quaisquer perfis, comunidades, grupos, tópicos de discussão e afins que empreguem o nome, marca ou outros sinais distintivos da SEMEF/PM, excetuando-se os canais oficiais da instituição e as redes sociais (*Whatsapp*) utilizadas para comunicação interna;
c) Não é permitida a publicação de conteúdo ou comentários diretamente relacionados à SEMEF, seus servidores, terceiros contratados e prestadores de serviço;
d) Não é permitida a publicação de qualquer tipo de imagem, foto, vídeo, áudio relacionado ao ambiente corporativo da SEMEF sem a expressa autorização da instituição, excetuando-se material divulgado em canais oficiais;

12. COMBATE A SOFTWARES MALICIOSOS

Ferramenta de proteção contra códigos maliciosos

12.1. A SEMEF disponibiliza ferramentas para proteção dos seus ativos, serviços de informação e recursos computacionais, incluindo estações de usuários, dispositivos móveis e servidores corporativos contra ameaças de códigos maliciosos tais como:
a) vírus, cavalos de tróia, *worms*, *screenloggers* (captura de tela) e *keyloggers* (captura de dados digitados), softwares de propaganda e similares;
12.2. A ferramenta de proteção contra códigos maliciosos, disponibilizada pela SEMEF adota as seguintes regras de uso:
a) Atualização em tempo real (on-line) do arquivo de assinaturas de códigos maliciosos e varredura programada (plano de execução) nas estações de usuários;
b) As varreduras programadas devem analisar todos os arquivos em cada unidade de armazenamento das estações de usuários;
c) 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;
d) As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações de trabalho de usuários;
12.3. Sites, serviços e arquivos baixados da internet e detectados como possíveis ameaças serão automaticamente bloqueados em estações de trabalho de usuários;
12.4. Caso uma estação de usuário esteja infectada ou com suspeita de infecção de código malicioso, deverá ser imediatamente isolada da rede corporativa da SEMEF e de qualquer comunicação com a internet;
12.5. Caso um servidor corporativo esteja infectado ou com suspeita de infecção de código malicioso, deverão ser adotadas medidas para garantir o isolamento do equipamento da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor;

Prevenção dos usuários contra códigos maliciosos

12.6. Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários da SEMEF devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos;
12.7. Os usuários da SEMEF devem seguir as seguintes regras para proteção contra códigos maliciosos, conforme abaixo:
a) Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;
b) Reportar imediatamente ao DSITI qualquer infecção ou suspeita de infecção por código malicioso;
c) Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado em um ambiente controlado;
d) Habilitar varredura automática da ferramenta de proteção contra códigos maliciosos fornecida pela SEMEF, antes de utilizar arquivos armazenados em mídias removíveis, baixados da internet ou recebidos nos serviços de *e-mail* ou comunicadores instantâneos;

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 DSITI para validar se o arquivo representa ou não uma ameaça.

ANEXO II

TERMO DE RESPONSABILIDADE E SIGILO DA INFORMAÇÃO

Eu,_____, RG nº_____, CPF nº_____, pertencente a(o), _____, cargo:_____, sob a matrícula funcional nº _____,

Nos termos do Decreto Municipal Nº 3224, de 23 de novembro de 2015, e da Política de Segurança da Informação e Comunicação da Prefeitura de Manaus (POSIC-PM), declaro que tenho pleno conhecimento de minhas responsabilidades no que concerne ao sigilo que deve ser mantido em relação aos ativos e informações sigilosas das quais tenha tido acesso ou possa vir a acessar ou ter conhecimento, em decorrência das atividades funcionais desempenhadas no exercício do cargo, função ou prestação de serviço no âmbito da SEMEF, ou fora do citado órgão.

Comprometo-me a guardar o sigilo necessário a que sou obrigado, estando ciente das penalidades nos termos da legislação vigente, especialmente dos art. 153 e art. 325 do Código Penal (Decreto-lei n. º 2.848, de 07 de dezembro de 1940) e demais legislações constantes do verso, bem como de quaisquer sanções administrativas que poderão advir.

A vigência da obrigação de sigilo, assumida pela minha pessoa por meio deste termo, terá validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa ou entidade, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste termo.

Neste Termo, as seguintes expressões serão assim definidas:

Informação Sigilosa significará toda informação, apresentada sob forma escrita, verbal ou por quaisquer outros meios, que possui restrição de acesso público em razão de sua criticidade para a segurança da sociedade e do município.

Informação Sigilosa inclui, mas não se limita à informação relativa às operações, processos, planos ou intenções, informações sobre produção, instalações, equipamentos, sistemas, dados, habilidades especializadas, projetos, métodos e metodologia, fluxogramas, especializações, componentes, fórmulas, produtos e questões relativas ao desempenho das atividades laborais.

Manaus, ___, de_____de_____.

(Assinatura do Usuário)

Servidor (Contratado)

VERSO COMPROMISSO LEGAL

CÓDIGO PENAL BRASILEIRO

DIVULGAÇÃO DE SEGREDO – Art. 153 § 1º. A divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em Lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção de 1(um) a 4(quatro) anos e multa.

INVASÃO DE DISPOSITIVO INFORMÁTICO – Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa (Lei 12.737/2012).

INSERÇÃO DE DADOS FALSOS EM SISTEMA DE INFORMAÇÕES – Art. 313-A Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou banco de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão de 2(dois) a 12(doze) anos e multa.

MODIFICAÇÃO OU ALTERAÇÃO NÃO AUTORIZADA DE SISTEMA DE INFORMAÇÕES – Art. 313-B. Modificar ou alterar, o funcionário, sistema de informação ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção de 3(três) meses a 2(dois) anos e multa. Parágrafo único: As penas são aumentadas de um terço até a metade se a modificação ou alteração resulta em dano para a Administração Pública ou para o administrado.

FALSIDADE IDEOLÓGICA – Art. 299 – Omitir, em documento público ou particular, declaração que dele deva constituir, ou nele inserir, fazer inserir declaração falsa ou diversa da que deva ser escrita, com fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. Pena – Reclusão de 01 (um) a 05 (cinco) anos e multa se o documento é público, e reclusão de 01 (um) a 03 (três) anos e multa se o documento é particular. Parágrafo único – Se o agente é funcionário público e comete o crime prevalecendo-se do cargo ou se a falsificação ou alteração é de assentamento de registro civil, aumenta-se a pena da sexta parte.

VIOLAÇÃO DE SIGILO FUNCIONAL – Art. 325 – Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena: detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.

Art. 325 § 1º-Nas mesmas penas deste artigo incorre quem: I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistema de informações ou banco de dados da Administração Pública, II – se utiliza, indevidamente, do acesso restrito.

§ 2º - Se da ação ou omissão resulta dano à Administração Pública ou a outrem: Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.

FUNCIONÁRIO PÚBLICO – Art. 327 – Considera-se funcionário público para os efeitos penais, quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública. Art. 327 § 1º – Equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal e quem trabalha para empresa prestadora de serviço contratada ou conveniada para execução de atividade típica da Administração Pública. Art. 327 § 2º – A pena será aumentada da terça parte quando os autores dos crimes previstos neste capítulo forem ocupantes de cargos em comissão ou de função de direção ou assessoramento de órgão da administração direta, sociedade de economia mista, empresa pública ou fundação instituída pelo poder público.

Av. Brasil, 2971, Compensa, CEP 69036-110. Telefone (92) 3672-1574

TERMO DE USO DOS SISTEMAS DE INFORMAÇÃO

Eu,_____, RG nº_____,

CPF nº_____, pertencente a(o), _____, cargo:_____, sob a matrícula funcional nº _____, CONSIDERANDO que a SEMEF:

a) disponibiliza a infraestrutura tecnológica, como ferramenta de trabalho, para o pleno desenvolvimento das atividades profissionais;
b) detém a exclusiva propriedade da infraestrutura tecnológica disponibilizada;
c) torna explícito que não há expectativa de privacidade sobre os ativos, informações e recursos institucionais, tendo em vista que são destinados para fins profissionais;
d) pode ter prejuízos pela má utilização dos recursos disponibilizados.

DECLARO, estar ciente e ter pleno conhecimento:

a) da Política de Segurança da Informação e Comunicação da POSIC - SEMEF apresentada na entrevista de admissão e disponibilizada de inteiro teor na Intranet;
b) da realização de monitoramento dos recursos tecnológicos disponibilizados, indispensável para a manutenção do nível de segurança adequado da organização;
c) de que a SEMEF pode realizar auditoria interna sobre os recursos de *hardware* e *software* disponibilizados para as atividades profissionais e;

d) que o descumprimento da POSIC-SEMEF está sujeito às sanções previstas na LEI Nº 1.118 – DE 01 DE SETEMBRO DE 1971, Estatuto dos Servidores Públicos do Município de Manaus, cláusulas contratuais e demais legislações vigentes, sem prejuízo das ações penais, civis e administrativas, previstas em legislação específica, respeitados os princípios constitucionais do contraditório e da ampla defesa.

Manaus,_____, de _____de _____.

(Assinatura)