POLÍTICA MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO

PREFEITURA DE MANAUS

DECRETO Nº 3.652, DE 15 DE MARÇO DE 2017

Sumário

DECRETO Nº 3.652, DE 15 DE MARÇO DE 2017

INSTITUI a Política Municipal de Segurança da Informação e Comunicação, e dá outras providências.

O PREFEITO DE MANAUS, em exercício, no uso da competência que lhe confere o art. 128, inc. I, da Lei Orgânica do Município de Manaus,

CONSIDERANDO que as normas NBR ISO/IEC 27001:2013 e NBR ISO/IEC 27002:2013, da Associação Brasileira de Normas Técnicas – ABNT estabelecem o sistema de gestão e o código de prática de segurança da informação e recomendam a implantação e revisões periódicas da política de segurança da informação das instituições;

CONSIDERANDO que as informações da Prefeitura de Manaus e aquelas que estejam sob sua responsabilidade, são armazenadas, transportadas ou veiculadas e mantidas por diferentes meios, tais como impresso e eletrônico e, portanto, vulneráveis a incidentes como desastres naturais, acessos ou modificações não autorizados, mau uso, falhas mecânicas e tecnológicas, extravio e furto;

CONSIDERANDO a manifestação nº 115/2016 - ASJUR/SUBCI/SEMEF, com anuência do Subsecretário de Controle Interno;

CONSIDERANDO o Parecer nº 0029/2017 – PA/PGM, aprovado pela Subprocuradora Geral Adjunta do Município; e

CONSIDERANDO o teor do Memo nº 0211/2016-GSS/SUTI/SEMEF, e o que mais conta nos autos do Processo nº 2017/11209/15249/00137,

DECRETA:

Art. 1º Fica instituída a Política de Segurança da Informação e Comunicação da Prefeitura de Manaus - POSIC-PM, 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-PM se aplicará a todos aqueles que estejam envolvidos direta ou indiretamente com a gestão de segurança da informação.

Art. 2º Para fins deste Decreto considera-se:

I - autenticidade: garantia de que uma informação, produto ou documento é do autor a quem se atribui;

II - confidencialidade: garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;

III - disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos recursos correspondentes sempre que necessários;

IV - integridade: salvaguarda de exatidão da informação e dos métodos e recursos de processamento;

V - legalidade: garantia de que ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos tenham validade jurídica;

VI - 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;

VII - gestão de segurança da informação: conjunto de medidas que tem como objetivo, o planejamento, implementação, operação, monitoramento e melhoria da segurança da informação; e

VIII - alta gestão: Prefeito, Vice-Prefeito e Titulares de Pastas.

Art. 3º Para cumprimento do objetivo definido no artigo 1º deste Decreto, a POSIC-PM terá como objetivos básicos:

I - viabilizar o atendimento das finalidades legais da Prefeitura de Manaus, 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; e

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

Art. 4º Para a consecução da POSIC-PM nas Secretarias, Autarquias e Fundações, ficam instituídos os Comitês Gestores de Segurança da Informação – CGSIs, em alinhamento com as recomendações nas normas NBR ISO/IEC 27001:2013 e NBR ISO/IEC 27002:2013, nos termos do Anexo I, cuja atribuição é analisar, definir, coordenar, executar e avaliar ações de segurança da informação relativas aos objetivos estabelecidos na POSIC-PM para elaboração, implementação, manutenção e melhoria da gestão da segurança da informação.

§1º O CGSI-PM irá assessorar o Prefeito de Manaus e será composto pelos Presidentes de cada CGSI, sendo presidido por um Presidente e Coordenador Executivo designados por ato do Prefeito de Manaus.

Art. 5º Para disciplinar o funcionamento de cada CGSI são definidas as seguintes ações:

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

II - o CGSI-PM reunir-se-á de forma ordinária quadrimestralmente 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 e, em caráter excepcional, os membros do CGSI-PM podem delegar sua função para um agente público considerado habilitado pelos demais membros do comitê;

III - os demais CGSIs reunir-se-ão de forma ordinária em intervalos planejados não superiores a 180 (cento e oitenta) dias e, em caráter extraordinário, sempre que convocado pelo Presidente ou Coordenador Executivo, com a presença mínima de metade mais um de seus membros, que em caráter excepcional poderá ser substituído por agente público considerado habilitado pelos demais membros do CGSI, para acompanhar a situação dos controles de segurança e deliberar sobre situações que possam afetar a segurança da informação no escopo de suas responsabilidades;

IV - as reuniões dos CGSIs serão registradas em Ata de Reunião, a qual devem 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; e

V - as decisões tomadas pelos CGSIs serão validadas por meio de votação, necessitando de maioria simples, considerado a presença de número igual ou superior a metade do total de componentes do comitê, sendo que o presidente votará apenas em caso de desempate;

VI - quando no exercício das funções do Comitê, e para a consecução de suas finalidades, os componentes dos CGSIs poderão:

a) ter livre acesso às áreas e informações, sejam elas físicas ou lógicas, ressalvados os impedimento legais e limites estabelecidos pela Alta Gestão da Prefeitura de Manaus;
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 atualizados com as recentes práticas, tecnologias e produtos de segurança do mercado, com o objetivo de melhor atender a execução das ações de segurança; e
d) propor contratação de consultoria com especialistas para desenvolvimento de serviços especializados e produtos com a finalidade de promover soluções de segurança, quando couber.

Art. 6º São atribuições dos CGSIs:

I - aos Presidentes dos CGSIs cabe:

a) assessorar, por meio do CGSI-PM, o Prefeito de Manaus nos assuntos relacionados à segurança da informação;
b) acompanhar os resultados do cumprimento da POSIC- PM, das normas e diretrizes emanadas dos CGSIs e propor medidas legais em caso de inobservância das mesmas;
c) reportar os indicadores de desempenho da segurança da informação;
d) assegurar o atendimento aos requisitos legais, regulamentares e estatuários aplicáveis;

e) avaliar e aprovar normas, planos, procedimentos, mecanismos de proteção e instruções reguladoras específicas, relativas aos assuntos preconizados nas POSICs, exceto quando se tratar de assuntos de alta criticidade ou sigilo, que sejam de competência do Prefeito de Manaus;
f) comunicar e coordenar atividades relacionadas à segurança da informação com agentes externos;
g) aprovar ou destituir os membros da área de segurança da informação, segundo o perfil exigido da função; e
h) convocar reuniões extraordinárias.

II - aos Coordenadores Executivos dos CGSIs cabem:

a) definir e coordenar as atividades dos membros dos Comitês na execução das atividades de segurança prescritas na POSICs;
b) responder pelas atribuições do presidente em sua ausência e impedimentos; e
c) convocar reuniões extraordinárias.

III - aos Membros do CGSI cabem:

a) assessorar o Presidente nos assuntos relacionados à segurança da informação;
b) executar as ações e planos de trabalho definidos pelo CGSI relativas a sua área de atuação; e
c) avaliar os impactos das propostas de normas, procedimentos e controles em suas áreas de atuação.

Parágrafo único. São atribuições comuns a todos os componentes dos CGSIs:

I – executar as ações e planos de trabalho definidos pelos CGSIs;
II – acompanhar o cumprimento da POSIC-PM, das normas e diretrizes emanadas dos CGSIs;
III – produzir e propor normas, planos, procedimentos, mecanismos de proteção e instruções reguladoras específicas, relativas aos assuntos preconizados na POSIC-PM; e
IV – promover no âmbito da Prefeitura de Manaus, 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.

Art. 7º Todos os usuários que se utilizarem de Informações e Sistemas de Informação, no âmbito da Prefeitura de Manaus, deverão assinar o Termo de Uso dos Sistemas de Informação - TUSI e o Termo de Responsabilidade e Sigilo da Informação - TRSI, constante do Anexo II.

§1º A partir de prazo a ser definido pelo CGSI-PM, 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-PM.

§2º No caso de servidores ocupantes de cargos em comissão, celetistas e efetivos em exercício, deverão assinar os Termos previstos no *caput* deste artigo com prazo a ser definido pelo CGSI-PM.
§3º Após a assinatura dos Termos, o usuário assume formalmente a responsabilidade pelo bom uso dos ativos de informações, o compromisso de seguir a POSIC-PM 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.

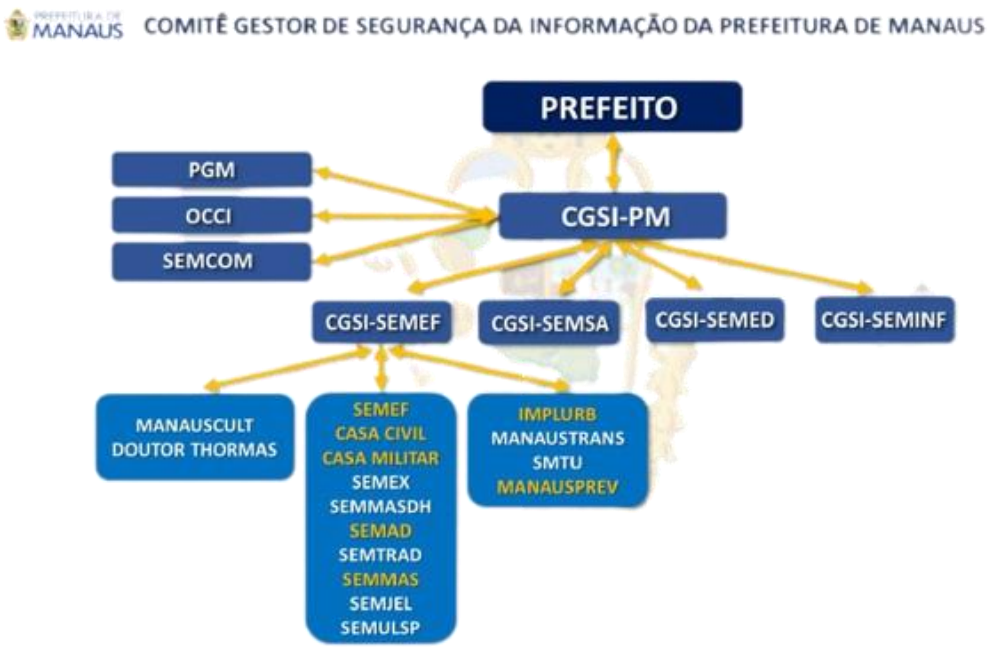
Art. 8º A alta gestão da Prefeitura de Manaus se compromete a apoiar a implantação e gestão da segurança da informação, de acordo com o que prescrevem as normas NBR ISO/IEC 27001:2013 e NBR ISO/IEC 27002:2013, se incluindo extensivamente, a viabilização dos recursos necessários às adequações e implantações de mecanismos de proteção, visando garantir os princípios da Segurança da Informação, respeitadas as condições técnicas, orçamentárias, financeiras e o princípio da oportunidade.

Art. 9º A implementação da POSIC-PM 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. 10. 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 Prefeitura de Manaus.

Manaus, 15 de março de 2017.

ANEXO I


MANAUS
COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO DA PREFEITURA DE MANAUS
PREFEITO
PGM
OCCI
SEMCOM
CGSI-PM
CGSI-SEMEF
CGSI-SEMSA
CGSI-SEMED
CGSI-SEMINF
MANAUSCULT
DOUTOR THORMAS
SEMEF
CASA CIVIL
CASA MILITAR
SEMEX
SEMMASDH
SEMAD
SEMTRAD
SEMMAS
SEMJEL
SEMULSP
IMPLURB
MANAUSTRANS
SMTU
MANAUSPREV

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 da mesma.

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.

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 os mesmos são destinados para fins profissionais;
d) pode haver 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 penal, civil e administrativa, previstas em legislação específica, respeitados os princípios constitucionais do contraditório e da ampla defesa.

Manaus,_____, de _____de _____.

(Assinatura)

POLÍTICA MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO