ESTADO DO AMAZONAS
CÂMARA MUNICIPAL DE MANACAPURU
SECRETARIA ADMINISTRATIVA
Avenida Eduardo Ribeiro, nº 1161 – Centro – Manacapuru – Amazonas – CEP: 69.400-901 - Fone/Fax: (092) 3361-3000
www.ale.am.gov.br/manacapuru/ - legislativomanaca_1948@hotmail.com - camaramanacapuru@outlook.com

DECRETO LEGISLATIVO Nº 174, DE 18 DE DEZEMBRO DE 2017.

Dispõe sobre a Política de Segurança da Informação e Comunicação – PSIC, no âmbito da Câmara Municipal de Manacapuru.

CONSIDERANDO a necessidade de melhorias na qualificação dos serviços para provimento de respostas objetivas e maior eficiência na incorporação das novas demandas da Câmara Municipal de Manacapuru;

O Presidente da Câmara Municipal de Manacapuru, Estado do Amazonas, no uso de suas atribuições legais,

DECRETA:

CAPÍTULO I - DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO – PSIC

Art. 1º A Política de Segurança da Informação e Comunicação – PSIC, a ser implantada no âmbito da Câmara Municipal de Manacapuru, passa a ser regida por este decreto, 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.

§1°. A PSIC se aplicará a todos aqueles que estejam envolvidos direta ou indiretamente com a gestão de segurança da informação.

§2°. A Política de Segurança da Informação e Comunicação – PSIC, orienta e estabelece as diretrizes corporativas da Câmara Municipal de Manacapuru para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários, e deverá ser cumprida e aplicada em todas as áreas da instituição.

§3°. A presente PSIC está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes no País.

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;

VIII - **alta gestão**: Presidente da Câmara e Chefes das Diretorias;

IX – **maturidade**: o grau de aderência a um determinado conjunto de requisitos que tenham como referência as melhores práticas dos processos de tecnologia da informação e comunicação utilizadas por

diferentes esferas de governo e entidades privadas, e que será definido por meio de avaliação realizada pelo Órgão Central.

X – ***backup***: é uma cópia de segurança. O termo em inglês é muito utilizado por empresas e pessoas que guardam documentos, imagens, vídeos e outros arquivos no computador ou na nuvem, hospedados em redes online como *Dropbox e Google Drive*. Para tanto a Câmara Municipal de Manacapuru disponibilizar espaços em seu servidor para armazenamento de tais informações. Bem como tratara da segurança e proteção dos mesmos, utilizando boas práticas de segurança da informação como armazenamento de mídias de backups em locais seguros externos.

Seção I – Dos Objetivos da Política de Segurança da Informação e Comunicação – PSIC

Art. 3º Para cumprimento do objetivo definido no art. 1º deste Decreto, a PSIC terá como objetivos básicos:

I - viabilizar o atendimento das finalidades legais da Câmara Municipal de Manacapuru, considerando leis, normas, regulamentações e outros requisitos legais aplicáveis vigentes, através da proteção da confidencialidade, integridade, disponibilidade, autenticidade e legalidade da informação;

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

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

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

V - promover o aumento de maturidade em tecnologia da informação e comunicação no âmbito da Câmara Municipal de Manacapuru;

VI - permitir o planejamento, a organização, a integração e o monitoramento das ações, bem como o estabelecimento de padrões técnicos a serem implantados pelos órgãos da Câmara Municipal de Manacapuru;

VII - fomentar ações de modernização relativas ao uso geral e estratégico de tecnologia da informação e comunicação;

VIII - implantar modelos que gerenciem e integrem as bases de dados municipais e sistemas de informação e comunicação dos órgãos da Câmara Municipal de Manacapuru;

IX - promover o uso de novas tecnologias visando fomentar processos de inovação, em especial aqueles que propiciem melhoria, ampliação e democratização do acesso da população aos serviços oferecidos pela Câmara Municipal de Manacapuru;

X - promover a utilização de bens e serviços de tecnologia da informação e comunicação de forma racional, sob os aspectos orçamentário-financeiros, tecnológicos e socioambientais;

XI - Estabelecer diretrizes que permitam aos usuários (funcionários, vereadores e visitantes, quando couber) e clientes da Câmara Municipal de Manacapuru seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades da instituição e de proteção legal da mesma e do indivíduo;

XII - Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento;

XIII - Preservar as informações da Câmara Municipal de Manacapuru quanto à:

a) **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

b) **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

c) **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Seção II – Das Diretrizes da Política de Segurança da Informação e Comunicação – PSIC

Art. 4º A Política Municipal de Governança de Tecnologia da Informação e Comunicação observará as seguintes diretrizes:

I - **planejamento de tecnologia da informação e comunicação**: os órgãos que compõem a Câmara Municipal de Manacapuru deverão elaborar seu plano diretor setorial de tecnologia da informação e comunicação que reflita as necessidades tecnológicas a serem materializadas no período, definindo ações prioritárias para o alcance dos objetivos da PSIC, bem como métricas e indicadores de acompanhamento;

II - **inovação**: os órgãos que compõem a Câmara Municipal de Manacapuru deverão explorar o potencial da inovação tecnológica para criar novas oportunidades de gestão e de prestação de serviços, identificando necessidades e materializando iniciativas com foco na melhoria da qualidade dos serviços e processos;

III - **transparência e participação social**: o planejamento de tecnologia da informação e comunicação, bem como a consecução das ações resultantes devem ser permeáveis à participação da sociedade civil, por meio dos mecanismos de transparência e de recebimento de contribuições já existentes na legislação.

Art. 5º As diretrizes aqui estabelecidas deverão ser seguidas por todos os usuários, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

§1º. A PSIC dá ciência a cada usuário de que os ambientes, sistemas, computadores e redes do órgão poderão ser monitorados e gravados, conforme previsto nas leis brasileiras.

§2º. É também obrigação de cada usuário manter-se atualizado em relação a PSIC e aos procedimentos e normas relacionadas, buscando orientação do gestor ou da Gerência de Tecnologia da Informação (GTI) sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Art. 6º Toda informação produzida ou recebida pelos usuários como resultado da atividade profissional contratada pertence à referida instituição, sendo as exceções explícitas e formalizadas em contrato entre as partes.

§1º. Os equipamentos de informática e comunicação, sistemas e informações que são utilizados pelos usuários para a realização das atividades profissionais são de propriedade da instituição referida, sendo que o uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

§2º. A Câmara Municipal de Manacapuru, por meio da Gerência de Tecnologia da Informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

Subseção Única – Das Segurança em Recursos Humanos

Art. 7º As responsabilidades pela segurança da informação devem ser definidas nas descrições de cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos da Câmara Municipal.

I - Todos os usuários devem ser conscientizados e treinados nos procedimentos de segurança da informação;

II - O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa;

III - Quando do afastamento, mudança de responsabilidades e de lotação ou atribuições dentro da organização faz se necessária a revisão imediata dos direitos de acesso e uso dos ativos;

IV - Quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuído;

V - Todo ativo produzido pelo usuário, desligado, deverá ser mantido pela Gerência de Tecnologia da Informação garantindo o reconhecimento e o esclarecimento da propriedade do acervo para Instituição.

VI - Os servidores devem ser capacitados quanto aos métodos de segurança para prevenir ataques cibernéticos e também devem ser orientados para não abrirem e-mails duvidosos, que possam conter vírus.

Parágrafo Único. Para aperfeiçoar a Gerência de Tecnologia da Informação adotar estratégias simples, mas eficientes como treinamento da Equipe, e atualização constante de tecnologias disponíveis para aumentar a segurança da informação na Câmara Municipal.

CAPÍTULO II - GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO (GTI)

Art. 8º A Gerência de Tecnologia da Informação (GTI), compreende as atividades de planejamento, governança, coordenação, organização, operação, controle e supervisão dos recursos de tecnologia da informação e comunicação e telecomunicação dos órgãos e entidades da Câmara Municipal de Manacapuru.

§1º. A Gerência de Tecnologia da Informação, no âmbito da Câmara Municipal, e tem as seguintes atribuições:

I - fomentar o aumento de maturidade em tecnologia da informação e comunicação;

II - fixar as normas e padrões de tecnologia da informação e comunicação para a Câmara Municipal, provendo a devida publicidade;

III - propor ao gestor ou agente superior da Câmara Municipal o Plano Estratégico de Tecnologia da Informação e Comunicação, no âmbito da Diretoria Administrativa;

IV - aprovar o Plano de Tecnologia da Informação e Comunicação e acompanhar a execução de seus projetos e ações, além de outras de eventual interesse da Câmara Municipal, que o integrarão;

V - propor ao diretor administrativo da Câmara Municipal as orientações técnicas gerais referentes a aquisição de bens e contratação de serviços em tecnologia da informação e comunicação;

VI - elaborar planos de formação, desenvolvimento e capacitação técnica dos recursos humanos envolvidos.

§2º. A Gerência de Tecnologia da Informação é a unidade da Câmara Municipal de Manacapuru provida do conjunto das atribuições referentes à tecnologia da informação e comunicação, à qual cabe coordenar a execução PSIC.

CAPÍTULO III - DA AQUISIÇÃO DE BENS E DA CONTRATAÇÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 9º. A Câmara Municipal de Manacapuru poderá adquirir bens e contratar serviços de Tecnologia da Informação e Comunicação em conformidade com o respectivo Plano de Tecnologia da Informação e Comunicação, bem como com as Orientações Técnicas publicadas pela Gerência de Tecnologia da Informação.

Art. 10. A Câmara Municipal de Manacapuru poderá contratar com a PRODAM ou com terceiros, de acordo com a legislação vigente, a aquisição de bens e serviços de tecnologia da informação e comunicação.

Art. 11. Fica delegada a Gerência de Tecnologia da Informação, com o apoio da PRODAM, ou de acordo com as necessidades, a realização de procedimento licitatório para fins de Registro de Preços para as aquisições de bens e contratações de serviços de Tecnologia da Informação e Comunicação.

CAPÍTULO IV – DOS REQUISITOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO – PSIC

Art. 12. Para a uniformidade da informação, a PSIC deverá ser comunicada a todos os usuários da instituição a fim de que a política seja cumprida dentro e fora da mesma.

§1º Tanto a PSIC quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão da GTI.

§2º A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos usuários, sendo orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos, e assinarão termo de responsabilidade.

§3º Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à GTI.

§4º Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

§5º Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Art. 13. Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, *notebook*, nos acessos à *Internet*, no correio eletrônico, nos sistemas comerciais e financeiros.

§1º. A Câmara Municipal de Manacapuru exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus usuários, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

§2º Todo usuário deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel, devendo, também, manter estes *backup's* separados de seu dispositivo móvel, ou seja, não carregá-los juntos.

§3º O objetivo da ação é o usuário se resguardar de uma ocasional perda de arquivos originais, seja por ações despropositadas do usuário como perder um CD/DVD e ter um problema com o HD, ou ainda mau funcionamento dos sistemas, ter uma cópia de segurança permite restaurar os dados perdidos.

§4º Poderão ser utilizadas algumas formas ou equipamentos para promoção da cópia de segurança:

I - ***Backup* no computador**: Uma mídia física, gravando os dados em CD, DVD e *Blu-ray,* devidamente etiquetados, utilizando um dos diversos programas de gravação que permite ao usuário salvar seus arquivos com segurança, e poderão ser guardados em lugares seguros, como um cofre na sede Câmara Municipal, ou em agencia devidamente contratada; observará, sempre que possível os programas para fazer *backup* no PC com Windows;

II – ***Pendrive***: dispositivo mais versátil usado para guardar uma cópia de segurança dos arquivos, que permite o fácil manuseio dos arquivos, podendo levá-los consigo para qualquer ambiente; observar-se-á se o backup reunir número grande de dados, maior capacidade de armazenamento ou mais de um dispositivo.

III – **HD externo**: possui um grande espaço de armazenamento, pode ser guardado em um cofre e também se conecta facilmente ao computador.

IV – **Arquivos na nuvem**: existem diversos serviços online que permitem o armazenamento de arquivos na nuvem, como o *Google Drive, Dropbox*, *oneDrive* e *ADrive* – observando-se os planos de cada um, para manter uma cópia de segurança dos dados, permitindo acessar os dados online, sem precisar de mídia física. O recurso de nuvem, é possível fazer a cópia de segurança tanto de documentos, fotos e vídeos salvos no computador, quanto nos smartphones ou *tablets*.

V – **Servidor de arquivo**: este serviço e disponibilizado uma quantidade de espaço no servidor para armazenamento de arquivos.

VI – **Tecnologia da informação**: a Câmara municipal de Manacapuru, dará todo o aparato tecnológico para a implementação de serviços de tecnologia da informação como: servidores, rede cabeada, *racks, routers,*

links de internet, softwares licenciados e outros que se façam necessários para melhorar os serviços de tecnologia da informação disponibilizados pela câmara municipal de Manacapuru.

Art. 14. A PSIC será implementada na Câmara Municipal de Manacapuru por meio de procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

CAPÍTULO V – DAS RESPONSABILIDADES ESPECÍFICAS

Art. 15. Entende-se por usuário toda e qualquer pessoa física, servidor, vereador, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Parágrafo Único. Será de inteira responsabilidade de cada servidor, todo prejuízo ou dano que vier a sofrer ou causar a Câmara Municipal de Manacapuru e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Seção I - Dos Usuários em Regime de Exceção

Art. 16. Os usuários em regime de exceção (temporários – visitantes) devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pela Gerencia da Tecnologia da Informação.

Parágrafo Único. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o usuário que o recebeu não estiver cumprindo as condições definidas no aceite.

Seção II - Dos Gestores de Pessoas e/ou Processos

Art. 17. Os gestores de pessoas e/ou processos terão postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os usuários sob a sua gestão.

§1° Atribui-se aos usuários, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSIC.

§2° Exigir dos usuários a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações.

§3° Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos usuários casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

§4° Adaptar-se-ão as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSIC.

Seção III - Dos Custodiantes da Informação

Art. 18. Cabe a Área de Tecnologia da Informação:

I - Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

II - Configurar os equipamentos, ferramentas e sistemas concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSIC.

III - Segregar as funções administrativas, operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

IV - Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

V - Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes, sendo que para as trilhas geradas e/ou mantidas em meio eletrônico, deve-se implantar controles de integridade para torná-las juridicamente válidas como evidências.

VI – Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes.

VII – Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

VIII – Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

a) o usuário (*login*) individual de servidores ou vereadores serão de responsabilidade do próprio funcionário.

b) o usuário (*login*) de terceiro serão de responsabilidade do gestor da área contratante.

IX - Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

X - Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

XI - Definir as regras formais para instalação de *software* e *hardware* em ambiente de produção corporativo, exigindo o seu cumprimento dentro da empresa.

XII - Realizar auditorias periódicas de configurações técnicas e análise de riscos.

XIII - Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

XIV - Monitorar o ambiente de TI, gerando indicadores e históricos de:

a) uso da capacidade instalada da rede e dos equipamentos;

b) tempo de resposta no acesso à Internet e aos sistemas críticos;

c) períodos de indisponibilidade no acesso à Internet e aos sistemas críticos;

d) incidentes de segurança (vírus, *trojans*, furtos, acessos indevidos, e assim por diante);

e) atividade de todos os usuários durante os acessos às redes externas, inclusive *Internet* (por exemplo: site visitado, *e-mail* recebido/enviado, *upload/download* de arquivos, entre outros).

XV - Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida.

§1º Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários; isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

§2º Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Seção IV - Da Área de Segurança da Informação

Art. 19. Cabe a Área de Segurança da Informação:

I - Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

II - Propor e apoiar iniciativas que visem à segurança dos ativos de informação.

III - Publicar e promover as versões da PSIC e as Normas de Segurança da Informação.

IV - Promover a conscientização dos usuários em relação à relevância da segurança da informação para instituição, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

V - Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

VI - Buscar alinhamento com as diretrizes corporativas da instituição.

Seção V - Do Monitoramento e da Auditoria do Ambiente

Art. 20. Para garantir as regras da PSIC, a Câmara Municipal de Manacapuru poderá:

I - implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a *Internet*, dispositivos móveis ou *wireless* e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

II - tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação da Gerencia de Tecnologia da Informação;

III - realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

IV - instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

V - gerar de relatórios dos sites acessados por usuário e se necessário a publicação desse relatório.

Subseção I - Serviços de Mensagens

Art. 21. O objetivo desta norma é informar aos usuários quais são as atividades permitidas e proibidas quanto ao uso dos Serviços de Mensagens eletrônica corporativo ou não.

Art. 22. O uso dos serviços de mensagens eletrônica é para fins corporativos e relacionados às atividades do usuário dentro da instituição.

§1º. A utilização desse serviço para fins pessoais será permitida desde que feita com bom senso e não cause impacto no tráfego da rede.

§2º Acrescentamos que é proibido aos usuários o uso do correio eletrônico:

I - enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

II - enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o a Câmara Municipal de Manacapuru vulneráveis a ações civis ou criminais;

III - divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

IV - falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

V - apagar mensagens pertinentes de correio eletrônico quando a instituição estiver sujeita a algum tipo de investigação;

VI - produzir, transmitir ou divulgar mensagem que:

a) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da instituição;

b) contenha ameaças eletrônicas, como: *spam, mail bombing*, vírus de computador;

c) contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

d) vise obter acesso não autorizado a outro computador, servidor ou rede;

e) vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

f) vise burlar qualquer sistema de segurança;

g) vise vigiar secretamente ou assediar outro usuário;

h) vise acessar informações confidenciais sem explícita autorização do proprietário;

i) vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

j) inclua imagens criptografadas ou de qualquer forma mascaradas;

k) tenha conteúdo considerado impróprio, obsceno ou ilegal;

l) seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

m) contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

n) tenha fins políticos locais ou do país (propaganda política);

o) inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

§3º. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

a) nome do servidor;

b) gerência ou departamento;

c) nome da empresa;

d) telefone(s);

e) correio eletrônico.

§4º. Os comunicadores instantâneos, também chamados de mensageiros instantâneos, são aplicativos que permitem o envio e recebimento de mensagens em tempo real, quando usado com responsabilidade pode se tornar uma poderosa ferramenta de apoio nos serviços, atividades e auxilio a dúvidas e comunicados na empresa.

I - A Câmara Municipal de Manacapuru disponibilizará serviço de mensagens, instalados nos computadores da mesma, bem como grupos de aplicativo de mensagens instantânea para celulares, para os usuários que utilizam celulares e tenham instalados os aplicativos em seu dispositivo.

II - Cada usuário deverá seguir regras para se manter a objetividade do grupo:

a) vinculação admissional com o Poder Legislativo ou ser vereador, e ainda membro da equipe de Tecnologia da Informação;

b) as comunicações deverão ser realizadas única e exclusivamente a serviço visando a comunicação pertinentes a Câmara Municipal de Manacapuru;

c) não divulgar do número de contato a terceiros, sob nenhuma hipótese;

d) inclusão no grupo de usuários, após assinar o termo de responsabilidade;

e) é vedado ao usuário repassar ao grupo de usuários mensagens, vídeos, fotos ou assemelhados que não sejam vinculados ao objetivo do grupo, de modo que essa ferramenta tem o fim específico de auxiliar na comunicação da Câmara Municipal de Manacapuru;

f) a divulgação de imagens, fotos, vídeos, correntes, material erótico, político religioso e outros de não interesse da Câmara Municipal de Manacapuru poderá acarretar em exclusão do grupo e outras medidas administrativas disciplinares;

g) todas as mensagens trocadas através dos serviços de mensagens interna está sujeita a auditoria, caso seja constatada alguma negligência com a Política de Segurança da Informação o usurário estará sujeito a medidas administrativas;

h) havendo o usuário mais o número do telefone cadastrado no grupo, por qualquer razão, deverá comunicar imediatamente o administrador, que procederá na sua exclusão;

i) qualquer infração as normas existentes neste Decreto, será automaticamente excluído do grupo;

j) a alimentação e atualização das comunicações nos grupos de aplicativo de mensagens instantânea para celulares será feita diretamente pelos usuários, que têm responsabilidade exclusiva sobre as publicações;

k) a manutenção e o suporte do aplicativo de mensagens instantânea para celulares do grupo de contato são realizados pela empresa que fornece o aplicativo, de forma gratuita;

l) é facultado ao usuário, participar ou não dos grupos de aplicativo de mensagens instantânea para celulares, devendo cientificar por escrito ao departamento de tecnologia da informação.

III - O departamento de tecnologia da informação não poderá garantir que o aplicativo de mensagens instantânea para celulares funcione sempre sem interrupções, atrasos ou falhas, haja vista uma série de fatores que pode afetar a qualidade de sua comunicação e o uso do aplicativo;

IV - A Câmara Municipal de Manacapuru não se responsabiliza por eventuais cortes, interrupções ou atrasos causados por falha ou inadequação de qualquer um desses itens ou quaisquer outros itens sobre os quais não temos controle.

Subseção II – Da Internet

Art. 23. Todas as regras atuais da Câmara Municipal de Manacapuru visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da Internet; embora a conexão direta e permanente da rede corporativa da instituição com a *Internet* ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Art. 24. Qualquer informação que é acessada, transmitida, recebida ou produzida na *Internet* está sujeita a divulgação e auditoria; portanto, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Art. 25. Os equipamentos, tecnologia e serviços fornecidos para o acesso à Internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/*Internet*, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua PSIC.

Art. 26. A Câmara Municipal de Manacapuru, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas, e toda tentativa de alteração dos parâmetros de segurança, por qualquer servidor, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor.

§1º. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

§2º. Como é do interesse da instituição que seus usuários estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

§3°. Apenas os usuários autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

Art. 27. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na *Internet*.

Art. 28. Os usuários com acesso à *Internet* poderão fazer o *download* (baixa) somente de programas ligados diretamente às suas atividades e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela GTI.

§1°. Os usuários não poderão em hipótese alguma utilizar os recursos da Câmara Municipal de Manacapuru para fazer o *download* ou distribuição de *software* ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

§2°. O *download* e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias; para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial.

Art. 29. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de cursos relacionados ao desenvolvimento de jogos.

Art. 30. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso, e caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.

Art. 31. Usuários com acesso à *Internet* não poderão efetuar *upload* (subida) de qualquer *software* licenciado ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo *software* ou pelos dados.

§1°. Os usuários não poderão utilizar os recursos da Câmara Municipal de Manacapuru para deliberadamente propagar qualquer tipo de vírus, *worm*, cavalo de troia, *spam*, assédio, perturbação ou programas de controle de outros computadores.

§2°. O acesso a *software peer-to-peer (Torrents e afins)* não serão permitidos, porem os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos.

§3°. Não é permitido acesso a sites de *proxy*.

Subseção III – Das Contas de Usuário

Art. 32. As contas de usuário do sistema operacional serão divididas em duas partes os Administradores e Usuários padrão.

I - Administradores: terão acesso a todos os recursos do sistema operacional.

II - Usuários padrão: terão acessos limitados aos recursos do sistema operacional.

§1°. Os usuários do corpo administrativo terão contas de usuário administrador, porém podendo ser alterado pelo GTI conforme a necessidade.

§2º. Todos os gabinetes de Vereadores serão usuários padrões, para evitar que sejam alteradas as configurações por parte dos funcionários; e conforme a necessidade poderá ser bloqueada acesso a outras ferramentas.

CAPÍTULO VI – DOS COMPUTADORES E RECURSOS TECNOLÓGICOS

Art. 33. Os equipamentos disponíveis aos usuários são de propriedade da Câmara Municipal de Manacapuru, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

§1º. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação.

§2º. É de responsabilidade do usuário do equipamento zelar pelo mesmo, mantendo a boa aparência, não sendo permitido personalizar o equipamento colocando adesivos, fotos, riscar, raspar e retirar etiqueta de patrimônio.

§3º. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Art. 34. Os sistemas e computadores devem ter versões do *software* antivírus instaladas, ativadas e atualizadas permanentemente.

Parágrafo único. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado.

Art. 35. Arquivos pessoais e/ou não pertinentes a instituição (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores, sendo identificada a existência desses arquivos, eles poderão ser excluídos definitivamente.

Art. 36. No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

I - Todos os computadores de uso individual deverão ter controle para restringir o acesso de usuários não autorizados; tais credenciais serão definidas pela Gerência de TI, que terá acesso a elas para manutenção dos equipamentos.

II - Os usuários devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

III - É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Gerência de TI ou por terceiros devidamente contratados para o serviço.

IV - É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

V - O usuário deverá manter a configuração do equipamento disponibilizado, seguindo os devidos controles de segurança exigidos pela PSIC e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

VI - Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos usuários, datas e horários de acesso.

Parágrafo Único. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos.

I - Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

II - Burlar quaisquer sistemas de segurança.

III - Acessar informações confidenciais sem explícita autorização do proprietário.

IV - Vigiar secretamente outrem por dispositivos eletrônicos ou *software*, como, por exemplo, analisadores de pacotes (*sniffers*).

V - Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

VI - Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

VII - Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no País, a moral, os bons costumes e a ordem pública.

CAPÍTULO VII – DOS DISPOSITIVOS MÓVEIS

Art. 37. Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência de TI, como: *notebook*, *smartphone* e *pendrive*.

Parágrafo Único. Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os usuários que utilizem tais equipamentos.

Art. 38. A Câmara Municipal de Manacapuru, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

§1°. O servidor, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na instituição, mesmo depois de terminado o vínculo contratual mantido com a instituição.

§2°. O suporte técnico aos dispositivos móveis de propriedade da Câmara Municipal de Manacapuru e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

§3°. Todo usuário deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Art. 39. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da Gerência de TI.

§1°. O usuário deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Gerência de TI.

§2°. A reprodução não autorizada do *software* instalado nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

Art. 40. É responsabilidade do servidor, no caso de furto ou roubo de um dispositivo móvel fornecido pela Câmara Municipal, notificar imediatamente seu gestor direto e a Gerência de TI, bem como deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

§1°. O usuário deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a instituição.

§2º. O usuário que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da Câmara Municipal deverá submeter previamente tais equipamentos ao processo de autorização da Gerência de TI.

§3º. O GTI não se responsabiliza por prestar manutenção ou instalar *software* em computadores que não sejam os da instituição.

§4º. O GTI tem o direito de, periodicamente, auditar os *notebook's* utilizados na instituição, visando proteger suas informações bem como garantir que aplicativos ilegais não estejam sendo executados na instituição.

§5º. É de reponsabilidade do proprietário a instalação do Sistema Operacional que será utilizado, bem como dos aplicativos a serem utilizados no *notebook*.

§6º. É de responsabilidade do proprietário manter sempre o aplicativo de antivírus atualizado em seu *notebook*, e caso não tenha nenhum aplicativo de antivírus instalado em seu *notebook*, o uso do mesmo fica proibido na instituição.

§7º. Não podem ser executados nos *notebook's* aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede, bem como a captura de informações confidenciais, como por exemplo: senhas de usuários.

Art. 41. Fica proibida a apropriação de arquivos que não sejam de uso pessoal do proprietário do *notebook*.

§1º. Todos os arquivos que pertençam ao órgão não podem ser carregados nos *notebook's* ou dispositivos de armazenamento móvel (ex.: *pendrive*), sem autorização da área responsável pelos dados.

§2º. Equipamentos portáteis, como *smart phones, palmtops, pen drives* e *players* de qualquer espécie, quando não fornecidos ao usuário pela instituição, não serão validados para uso e conexão em sua rede corporativa.

CAPÍTULO VIII – DAS PENALIDADES

Art. 42. O não cumprimento dos requisitos previstos nesta PSIC e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

§1º. A segurança deve ser entendida como parte fundamental da cultura interna da Câmara Municipal de Manacapuru, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

§2º. O não cumprimento das determinações da PSIC sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos da Câmara Municipal;

§3º. O descumprimento das disposições constantes nessa PSIC sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil;

§4º. O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na legislação pertinente.

CAPÍTULO IX – DOS TERMOS

Art. 43. Para garantir as regras mencionadas acima a instituição se reserva no direito de:

I - Implantar *software* e sistemas que podem monitorar e gravar todos os usos de *Internet* através da rede e das estações de trabalho da instituição;

II - Inspecionar qualquer arquivo armazenado na rede, seja no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política.

Art. 44. Todos os usuários que se utilizarem de Informações e Sistemas de Informação, no âmbito da Câmara Municipal de Manacapuru, deverão assinar o Termo de Uso dos Sistemas de Informação - TUSI e o Termo de Responsabilidade e Sigilo da Informação - TRSI, constante do Anexo I.

§1° 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 PSIC.

§2° No caso de servidores ocupantes de cargos em comissão, celetistas e efetivos em exercício, deverão assinar os Termos previstos no *caput* deste artigo.

§3° Após a assinatura dos Termos, o usuário assume formalmente a responsabilidade pelo bom uso dos ativos de informações, o compromisso de seguir a PSIC 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.

CAPÍTULO X - DAS DISPOSIÇÕES FINAIS

Art. 45. A implementação da PSIC 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. 46. 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 Câmara Municipal de Manacapuru.

Art. 47. Os casos omissos serão submetidos a Gerência de Tecnologia da Informação, para deliberação.

Art. 48. Este decreto entrará em vigor na data de sua publicação.

Sala das Sessões da Câmara Municipal de Manacapuru, 18 de dezembro de 2017.

Ver. FRANCISCO COELHO DA SILVA
Presidente da Câmara

Verª. LINDYNES LEITE PERES
Secretária Geral da Mesa

CÂMARA MUNICIPAL DE MANACAPURU
Publicado nos termos do
art. 88 da Lei Orgânica de Manacapuru
dia. ___/___/___
Funcionário (a)

ANEXO I - TERMO DE RESPONSABILIDADE E SIGILO DA INFORMAÇÃO

Termo de Responsabilidade e Sigilo da Informação (FRENTE)

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

Nos termos da Política de Segurança da Informação e Comunicação da Câmara Municipal de Manacapuru (PSIC), 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 Câmara Municipal de Manacapuru, 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 nº 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.

Manacapuru-AM, _____, de _____ de _____.

_____
(Assinatura do Usuário)
Servidor (Contratado)

Termo de Responsabilidade e Sigilo da Informação (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 à 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.

ANEXO II - TERMO DE USO DOS SISTEMAS DE INFORMAÇÃO

Termo de Uso dos Sistemas de Informação

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

CONSIDERANDO que a Câmara Municipal de Manacapuru:

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 Câmara Municipal de Manacapuru, apresentada na entrevista de admissão e disponibilizada de inteiro teor na *Intranet*;

b) da realização do monitoramento dos recursos tecnológicos disponibilizados, indispensável para a manutenção do nível de segurança adequado da organização;

c) que a Câmara Municipal de Manacapuru pode realizar auditoria interna sobre os recursos de *hardware* e software disponibilizados para as atividades profissionais.

d) que o descumprimento da PSIC está sujeito às sanções previstas na norma especifica, 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.

e) das regras de uso dos serviços de mensagens internas e externas.

f) da Política de Segurança da Informação e Comunicação da Câmara Municipal de Manacapuru, apresentada na entrevista de admissão e disponibilizada de inteiro teor na Intranet;

g) da realização do monitoramento dos recursos tecnológicos disponibilizados, indispensável para a manutenção do nível de segurança adequado da organização;

h) que a Câmara Municipal de Manacapuru pode realizar auditoria interna sobre os recursos de hardware e software disponibilizados para as atividades profissionais.

i) que o descumprimento da PSIC está sujeito às sanções previstas na norma especifica, 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.

j) das regras de uso dos serviços de mensagens internas e externas.

Por fim, autorizo o uso de minha imagem, vídeo, som da minha voz e nome, além de todo e qualquer material entre fotos e documentos por mim apresentados e ou confeccionado pela equipe de comunicação da câmara municipal de Manacapuru, para que estas sejam destinadas à divulgação ao público em geral através da mídias sociais, portais, sites de noticias, materiais gráficos e/ou para formação de acervo histórico.

Manacapuru-AM, _____, de _____ de _____.

_____

(Assinatura)

ÍNDICE