DECRETO Nº 12.417, DE 24 DE NOVEMBRO DE 2021.

Institui a Política de Tecnologia e Segurança da Informação e Comunicação do Poder Executivo do Município de Lajeado.

O PREFEITO MUNICIPAL DE LAJEADO, Estado do Rio Grande do Sul, no uso de suas atribuições legais, em conformidade ao que dispõe o Art. 54, VIII da Lei Orgânica do Município;

CONSIDERANDO a necessidade de instituir a Política de Tecnologia e Segurança da Informação e Comunicação (PTSIC) no âmbito do Poder Executivo do Município de Lajeado;

CONSIDERANDO a necessidade de disciplinar a utilização dos recursos computacionais e estabelecer a finalidade do uso aceitável e seguro dos mesmos;

CONSIDERANDO as disposições da Lei Federal nº 13.709/2018, que instituiu a Lei Geral de Proteção de Dados Pessoais - LGPD, DECRETA:

CAPÍTULO I
DAS REGRAS GERAIS

Art. 1º Institui no âmbito do Poder Executivo Municipal de Lajeado a Política de Tecnologia e Segurança da Informação e Comunicação (PTSIC), conforme disposto neste Decreto.

Art. 2º A Política de Tecnologia e Segurança da Informação e Comunicação (PTSIC) passa a integrar o Sistema de Gestão Corporativo do Poder Executivo Municipal, com base nas normas técnicas reconhecidas internacionalmente e amplamente aceitas no Brasil.

Art. 3º As siglas e definições constantes nesta Política estão especificadas no Anexo II.

CAPÍTULO II
DOS OBJETIVOS

Art. 4º A Política de Tecnologia e Segurança da Informação e Comunicação (PTSIC), tem como objetivos implementar, estabelecer, operar, monitorar, analisar criticamente, manter e melhorar as boas práticas no que diz respeito à segurança da informação e a gestão dos recursos de Tecnologia da Informação e Comunicação (TIC).

Art. 5º A PTSIC, também tem como objetivo alcançar níveis adequados de proteção às informações do Poder Executivo ou sob sua responsabilidade, bem como, a maximização dos resultados no uso dos recursos de tecnologia.

CAPÍTULO III
DOS PRINCÍPIOS ORIENTADORES DA PTSCI

Art. 6º A PTSIC possui princípios orientadores a serem considerados nas diretrizes, normas administrativas e procedimentos de TIC com impacto em ações de planejamento, implantação de serviços, programas e projetos relacionados à disponibilização e uso da infraestrutura tecnológica, considerando o canal de relacionamento com o cidadão e a sua integração aos processos existentes e que possam vir a existir no âmbito do Poder Executivo Municipal:

I - Uso Estratégico de TIC: prover serviços apoiados por plataformas digitais que suportem a estratégia de governo e o apoio à tomada de decisão, mediante organização de recursos, processos e técnicas, visando a obtenção, processamento, armazenamento, o uso e disseminação de informações;

II - Governança de TIC: manter um modelo de governança que vise assegurar o alinhamento das decisões e ações do DTI à estratégia de governo, priorizando o planejamento, a avaliação e o monitoramento centralizado dos serviços e projetos de TIC;

III - Foco no Cidadão: considerar os processos administrativos e o atendimento ao cidadão, visando a oferta de novos serviços e a melhoria dos atuais, com foco em princípios como mobilidade, simplicidade, usabilidade e acessibilidade, fortalecendo assim o canal de relacionamento entre governo e sociedade;

IV - Integração e digitalização dos Processos e Serviços: assegurar a integração e digitalização de processos e serviços, zelando pela padronização de tecnologias, serviços e soluções, objetivando sempre a racionalização e otimização dos recursos públicos;

V - Evolução dos serviços e soluções: monitorar as tendências tecnológicas com foco em pessoas, retenção de talentos e qualificação continuada, com vistas a mitigar os gaps tecnológicos e o tempo com tramitações desnecessárias;

VI - Da segurança e adequado tratamento da Informação: o tratamento das informações ocorre em diferentes meios de suporte, armazenamento e comunicação, estando os mesmos expostos à vulnerabilidades, bem como, a fatores externos e internos que podem comprometer a sua segurança, daí a necessidade do adequado tratamento das informações.

CAPÍTULO IV
DO COMITÊ GESTOR DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (CGTSIC)

Art. 7º Fica instituído o Comitê Gestor de Tecnologia e Segurança da Informação e Comunicação (CGTSIC), na forma de colegiado multidisciplinar consultivo, propositivo e

deliberativo.

Art. 8º O CGTSIC será composto por representantes das Secretarias Municipais, que serão nomeados por ato do Prefeito Municipal.

Parágrafo único. O Presidente do CGTSIC será escolhido dentre os seus membros.

Art. 9º São atribuições do CGTSIC:

I - estabelecer as regras sobre o seu funcionamento;

II - apresentar propostas à Secretaria de Administração e ao Gabinete do Prefeito referentes ao escopo, aplicação, priorização e integração de novos projetos de Tecnologia e Segurança da Informação e Comunicação (TSIC);

III - deliberar sobre respostas a incidentes e planos de contingência e sua continuidade, entre outros.

CAPÍTULO V
DA APLICABILIDADE DA PTSIC

Art. 10. As diretrizes, normas administrativas e procedimentos que integram a presente PTSIC aplicam-se a todo e qualquer agente público, seja do Poder Executivo Municipal de Lajeado, dos demais órgãos e poderes da Federação, além de prestadores de serviços e cidadãos em geral, que possuíram, possuem ou possam vir a ter qualquer tipo de vínculo, acesso e ou uso a qualquer recurso computacional, informações e ativos tecnológicos providos pelo Poder Executivo do Município de Lajeado e ou que esteja sob sua responsabilidade.

§ 1º A Política de Tecnologia e Segurança da Informação e Comunicação deve garantir o alinhamento das ações de Tecnologia e Segurança da Informação e Comunicação (TSIC) ao plano estratégico institucional, racionalizar o uso destes recursos e serviços com foco em inovação, incentivar o uso de serviços públicos, visando maior eficiência e eficácia no atendimento ao cidadão e orientar a Governança de TSIC para a administração pública municipal.

§ 2º Os agentes públicos, prestadores de serviço, munícipes, membros da sociedade civil e demais autoridades mencionadas no caput deste artigo serão identificados nesta política como usuários das informações e dos recursos de TIC do Poder Executivo do Município de Lajeado.

Art. 11. O conteúdo da Política de Tecnologia e Segurança da Informação e Comunicação deve ser de domínio de todos os usuários da informação e recursos de TIC.

§ 1º A utilização de sistemas, computadores e redes ou o acesso físico às dependências do Poder Executivo Municipal poderão ser monitorados e gravados com o objetivo de gerar

evidências.

§ 2º Os agentes públicos deverão ser orientados sobre como acessar o conteúdo da presente política por meio de mídias digitais.

§ 3º A assinatura e entrega do Termo de Uso e Compromisso de observância à presente política constante no Anexo I, é pré-requisito obrigatório para obter acesso aos recursos de TIC.

§ 4º É obrigação de cada usuário da informação e dos recursos de TIC manter-se atualizado em relação a esta política bem como às diretrizes e normas relacionadas, buscando orientação junto ao seu gestor ou ao Departamento de Tecnologia da Informação, sempre que não estiver absolutamente seguro quanto a qualquer aspecto ou evento que envolva a sua aplicação.

CAPÍTULO VI
DAS DIRETRIZES

Art. 12. Para nortear o cumprimento dos objetivos e princípios orientadores são definidas as seguintes diretrizes:

I - Referências e Padrões: deverão ser estabelecidos e mantidos padrões de hardware, software e plataforma tecnológica a serem utilizados para o atendimento aos serviços de TSIC pelo Poder Executivo Municipal;

II - Prestação de serviços: a aquisição, execução, desenvolvimento, manutenção, monitoramento e gestão dos serviços e recursos deverão ser centralizados e executados por equipe interna, ou terceirizada, quando considerada técnica e economicamente como a opção mais adequada e efetiva;

III - Processo de Aquisição e Gestão de Contratos: a aquisição de bens e serviços de TIC em qualquer Secretaria da Prefeitura deverá ser realizada de forma corporativa e orientada por padrões e arquiteturas tecnológicas pré-definidas, objetivando agilidade nas ações locais e na integração com processos e serviços;

IV - Avaliação e Encaminhamento de Projetos: a apreciação e encaminhamento de novas demandas e projetos institucionais de âmbito estratégico, tático e operacional que envolvam qualquer aquisição ou prestação de serviço em TIC deverá seguir um processo previamente definido pelo Governo Municipal, com a participação obrigatória do DTI.

V - Segurança da Informação: todos os processos e ou serviços que sejam apoiados, mantidos ou suportados por TICs deverão estar alinhados com as Diretrizes de Segurança da Informação, garantindo:

a) orientação quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

b) resguardo das informações do Poder Executivo Municipal, em conformidade com a legislação vigente, garantindo os requisitos básicos;

c) prevenção contra possíveis causas de incidentes através da adoção de medidas preventivas, objetivando evitar prejuízos ao Poder Executivo e responsabilidade legal dos seus agentes públicos, prestadores de serviços e munícipes;

d) minimização dos riscos de perdas financeiras e ou de qualquer outro impacto negativo nas atividades do Poder Executivo Municipal como resultado de falhas de segurança;

e) desenvolvimento de um comportamento ético e profissional, para que todos os usuários da informação possam utilizar da melhor forma as ferramentas e serviços de TIC e as informações por elas geradas e tratadas.

VI - Desenvolvimento de Competências em Segurança e Tecnologia da Informação e Comunicação (STIC): promover e fortalecer o foco em pessoas, visando a promoção do desenvolvimento de habilidades e competências, operacionais, técnicas e gerenciais por meio da capacitação contínua;

VII - Computação em Nuvem: priorizar modelos que permitam o acesso a um conjunto compartilhado de recursos de computação, assim como software (SaaS - Software como Serviço) e infraestrutura (IaaS - Infraestrutura como Serviço), visto que podem ser provisionados e liberados rapidamente;

VIII - Redes Sociais: as plataformas, redes e todos os tipos de mídias sociais deverão visar a colaboração on-line possibilitando às pessoas compartilhar conhecimentos e ideias independentemente do cargo, experiência ou função, priorizando mensagens e conversas sobre o trabalho de modo responsável, transparente e prudente, sem descuidar das premissas de segurança da informação e privacidade;

IX - Marco Civil da Internet: deverão existir procedimentos que promovam a neutralidade da rede, liberdade de expressão e privacidade sem prejuízo das obrigações do Poder Executivo Municipal em relação à Lei Federal nº 12.965/2014;

X - Acesso à Informação: manter a publicidade e a transparência das informações sob a guarda do Município, visto que são consideradas públicas, conforme a Lei Federal nº 12.527/2011;

XI - Proteção de Dados Pessoais: deverá ser estabelecido e mantido um programa de governança de dados visando a privacidade e a segurança das informações, com cuidado adequado no tratamento de dados, conforme disciplina a Lei Federal nº 13.709/2018;

XII - Respeito ao Direito Autoral e à Propriedade Intelectual: devem ser observadas as regras atinentes à proteção dos direitos intelectuais, conforme preconizado nas Leis Federais nº 9.609/1998, 9.610/1998, 9.279/1996 e 3.129/1982.

XIII - Observância das regras atinentes à Segurança da Informação, em especial:

a) confidencialidade: o acesso à informação deve ser limitado unicamente ao proprietário

da informação e a quem possuir autorização de acesso.

b) integridade: não é permitida a manipulação das informações, portanto, são proibidas alterações, supressões e adições de conteúdo nas informações, salvo se expressamente autorizadas pelo proprietário.

c) disponibilidade: sistemas e informações devem estar disponíveis para o uso legítimo dos usuários autorizados, sempre que necessário ou demandado;

d) autenticidade: é através da autenticidade que se garante que a informação é proveniente da fonte anunciada, ou seja, não sofreu nenhuma alteração durante o processo, é garantir que os usuários são quem dizem ser, pois identifica e registra o usuário que está enviando ou modificando alguma informação.

e) legalidade/conformidade: deve-se buscar e garantir a conformidade com as leis, regulamentos e padrões aplicáveis.

f) irretratabilidade/não repúdio: visa garantir que as ações de uma pessoa e ou entidade sejam devidamente rastreadas e atribuídas unicamente à sua autoria, isso confere suporte ao isolamento de falhas, à detecção e prevenção de incidentes, à irretratabilidade e ao não repúdio, elementos estritamente importantes para eventual processo judicial, em que será necessário verificar os registros de atividades, rastrear e identificar violações de segurança.

CAPÍTULO VII
GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO

Seção I
Do Acesso Aos Ativos de Tic ou Ambientes Físicos Controlados

Art. 13. O acesso aos ativos de TIC e/ou a ambientes físicos controlados envolvendo recursos computacionais somente será concedido a usuários autorizados, devidamente cadastrados em base de autenticação informatizada, centralizada e com o status de ativo, conforme discriminado em normas específicas.

§ 1º Somente senhas criptografadas podem ser armazenadas nas bases de autenticação.

§ 2º Os acessos são viabilizados mediante a concessão de credenciais de acesso.

§ 3º As referidas credenciais de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais.

§ 4º Toda credencial de acesso é pessoal do usuário e intransferível, sendo o usuário integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que realizado por outro indivíduo e/ou organização de posse de suas credenciais de acesso.

§ 5º As credenciais identificam os usuários nos sistemas e serviços, de forma que qualquer ação executada por intermédio das referidas credenciais terá a autoria e responsabilidade atribuída ao seu titular.

§ 6º Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro às informações e aos recursos de TIC, em especial as credenciais de acesso.

§ 7º A criação das credenciais de acesso é realizada de acordo com o vínculo dos usuários.

§ 8º Os procedimentos de conduta e boas práticas serão explicitados em norma específica.

Seção II
Do Perfil de Acesso

Art. 14. A autorização e nível permitido de acesso é feita com base em papéis e perfis que definem o nível de permissão dos usuários nos mais variados serviços e recursos disponibilizados pelo Poder Executivo, de acordo com as necessidades de cada usuário.

§ 1º A seu critério exclusivo, o Poder Executivo poderá ativar uma cota (de acordo com o perfil de acesso de cada usuário) para a utilização de serviços e ou armazenamento de arquivos em sua infraestrutura computacional local ou serviços de armazenamento remoto (nuvem).

§ 2º Usuários que têm acesso autorizado a permissões avançadas em sistemas e recursos deverão possuir uma credencial específica para este propósito.

§ 3º A credencial específica deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades do dia a dia.

Art. 15. A concessão de credenciais de acesso (login e senha) a usuários e sua posterior vinculação a papéis e perfis é condicionada ao aceite pelo usuário do Termo de Uso e Compromisso de Utilização dos Recursos de TIC, o qual deverá ser assinado juntamente com os documentos de admissão, solicitados pela equipe do Departamento de Recursos Humanos.

§ 1º No caso de outros usuários (a exemplo de profissionais terceirizados, estagiários, membros de outros órgãos públicos e sociedade civil em geral), o referido Termo deverá ser assinado quando da criação do acesso, nas mesmas condições apresentadas no caput deste artigo.

§ 2º Os alunos da rede pública municipal e usuários da comunidade, também deverão firmar assinatura (mesmo que na forma de aceite e ou assinatura eletrônica) no termo de uso e compromisso.

§ 3º Todos os atuais usuários das informações e dos recursos de TIC (à época da

publicação desta política) deverão assinar o Termo de Uso e Compromisso, a ser disponibilizado no Departamento de Recursos Humanos.

Seção III
Dos Certificados Digitais

Art. 16. O Certificado digital é um documento eletrônico que contém dados sobre a pessoa física ou jurídica que o utiliza, servindo como identidade virtual, conferindo validade jurídica e aspectos de segurança digital em transações eletrônicas de documentos, mensagens e dados.

§ 1º Caberá a Secretaria de Administração, Procuradoria e DTI, mediante norma específica, estabelecer os tipos de certificado digital mais apropriados para cada necessidade, bem como para quais atividades e funções o seu uso será necessário.

§ 2º Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo.

§ 3º O usuário deverá informar ao DTI sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital.

§ 4º O usuário que for exonerado ou demitido do Poder Executivo terá o certificado digital expedido pela Prefeitura imediatamente revogado.

Seção IV
Do Acesso Remoto

Art. 17. O acesso remoto às informações e recursos computacionais do Poder Executivo é restrito aos usuários que necessitem deste acesso para a execução das atividades profissionais, conforme norma específica.

Art. 18. Todos os procedimentos realizados remotamente bem como a informação que é acessada, transmitida, recebida ou produzida através deste tipo de acesso está sujeita a monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade.

Art. 19. O acesso remoto realizado pelo DTI às máquinas de trabalho dos agentes públicos municipais poderá ser realizado unicamente para fins de atendimento e prestação de suporte técnico, mediante anuência prévia do usuário.

CAPÍTULO VIII
DA SEGURANÇA FÍSICA

Art. 20. O DTI deverá implementar e zelar pela manutenção da segurança física para os ambientes que contenham as instalações relacionadas ao processamento e guarda das

informações bem como da infraestrutura básica, seja a relacionada a rede de dados, energia elétrica, infraestrutura de telecomunicações, entre outros.

§ 1º Deverá ser elaborada norma específica que trata do acesso físico e requisitos de segurança com finalidade de implementar e divulgar os procedimentos de controle para bloquear, desestimular, impedir, detectar, defender e atrasar acessos indevidos a qualquer ambiente onde se encontrem ativos de TIC e informações sensíveis para o município.

§ 2º Caberá ao DTI a definição, implantação e manutenção de sistemas redundantes e de alta disponibilidade para o suprimento de energia, acesso à internet e resfriamento dos ambientes sensíveis ou de acesso restrito, assim como a disponibilização de sistemas de monitoramento e controle de acesso aos mesmos.

CAPÍTULO IX
DO REGISTRO, GUARDA E ACESSO AOS LOGS

Art. 21. Todo e qualquer acesso e utilização de recursos de TIC poderá gerar registros e histórico de uso (logs) os quais devem ser armazenados pelo DTI em mídia específica, observando o seguinte conjunto de regras:

I - manter cópias de segurança dos arquivos de logs no sistema de backup;

II - o acesso aos arquivos de log que contém dados pessoais e/ou dados sensíveis somente poderá ser solicitado pelo titular dos dados, e pela autoridade administrativa, policial ou judicial;

III - o DTI poderá acessar os arquivos de log tão somente para fins de monitoramento, segurança e controle.

CAPÍTULO X
DO USO DA INFRAESTRUTURA DE REDE LOCAL

Art. 22. O acesso à rede local será efetuado mediante identificação única pelo nome de usuário e senha de acesso.

Art. 23. Toda a infraestrutura de rede local somente poderá ser provida e disponibilizada pelo Poder Executivo Municipal.

Parágrafo único. É vedada a instalação ou adição de qualquer dispositivo privado ou particular que interfira na topologia, cobertura ou funcionamento da infraestrutura de rede do Poder Executivo Municipal sem a prévia anuência do DTI.

Art. 24. Com relação ao uso da rede local e da intranet, compete ao DTI, através de norma específica, estabelecer parâmetros de gerenciamento, segurança, acesso, segurança, registros de log e demais procedimentos necessários, observando:

I - implantar e aplicar o gerenciamento de configuração com objetivo de documentar mudanças de configuração em qualquer sistema, assim como evitar a alteração ou instalação não autorizada de softwares de qualquer natureza;

II - empregar mecanismos de segurança e contingência visando garantir a disponibilidade e a recuperação nos equipamentos servidores de rede;

III - monitorar a disponibilidade e os níveis de utilização de todos os dispositivos de comunicação (DCEs), de processamento (Servidores) e de armazenamento (Storage) de modo proativo e preventivo;

IV - manter os registros (logs) de todas as atividades realizadas que visam o acesso a todos os dispositivos de comunicação (DCEs), de processamento (Servidores) e de armazenamento (Storage), tanto para o tráfego com origem interna quanto para o tráfego com origem externa;

V - padronizar a aquisição e a utilização de equipamentos gerenciáveis que permitam total compatibilidade, garantindo o atendimento às demandas de operação, gestão e segurança do Poder Executivo Municipal;

VI - garantir que as novas instalações da infraestrutura de rede sigam as normas relacionadas ao cabeamento estruturado, bem como a adequação da infraestrutura já instalada.

Art. 25. A infraestrutura Wi-Fi, condicionada à viabilidade técnica, deverá estar disponível em todos os ambientes que demandam mobilidade e acesso a partir de dispositivos móveis.

§ 1º O acesso ocorrerá mediante autenticação segura e obrigatória para todo e qualquer dispositivo que acesse a infraestrutura Wi-Fi.

§ 2º Os acessos à Rede WI-FI serão segmentados conforme o perfil de acesso do usuário.

CAPÍTULO XI
DO ACESSO A INTERNET, DO E-MAIL, DO USO DE COMUNICADORES INSTANTÂNEOS E DO COMPORTAMENTO CORPORATIVO EM MÍDIAS E REDES SOCIAIS

Seção I
Do Acesso à Internet

Art. 26. O acesso e utilização da internet estão condicionados à observância das normas e diretrizes estabelecidas no Capítulo XI e na Lei nº 12.965/2014, denominada Marco Civil da Internet.

§ 1º O Poder Executivo Municipal fornecerá acesso à internet para os usuários

devidamente autenticados na base, conforme o perfil de acesso, ou usuários da comunidade, conforme norma específica.

§ 2º A autenticação do usuário é pré-requisito para a obtenção da autorização para acesso à internet.

§ 3º O acesso à internet será fornecido a usuários ativos e a visitantes devidamente autorizados por meio dos recursos da rede local.

§ 4º Toda informação que é acessada, transmitida, recebida ou produzida através do acesso à internet fornecido pelo Poder Executivo Municipal está sujeita ao monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade.

§ 5º O uso de equipamentos de telefonia móvel e afins, em situação de comodato, que estejam sob responsabilidade do Poder Executivo Municipal, também devem seguir os termos da presente política.

§ 6º Acessos realizados por intermédio de equipamentos privados a serviços de internet móvel ou infraestrutura de terceiros, estão fora do escopo desta política.

Art. 27. Com relação ao uso da internet, compete ao DTI:

I - Empenhar os melhores esforços, considerando o atual estado da técnica, para implementar mecanismos de controle que objetivem não permitir o download, o upload, a inclusão, a disponibilização, a visualização, a edição, a instalação, o armazenamento e/ou a cópia de qualquer conteúdo que possa representar risco à segurança, bem como que tenha relação expressa ou subjetiva, direta ou indireta, com racismo, misoginia, pornografia, intolerância religiosa entre outros que não estejam de acordo com os princípios éticos, morais e legais;

II - Dispor de meios para apresentar relatórios e paineis eletrônicos com as estatísticas de acesso, consumo de banda, vazão e disponibilidade, fornecendo desta forma subsídios para a tomada de decisão por parte dos gestores municipais e condições de investigar qualquer anomalia ou acesso indevido.

Art. 28. Deverá ser editada norma específica para regulamentar as categorias de conteúdo que deverão ser filtradas, bem como, os procedimentos necessários para a requisição de exceções às regras de acesso, que deverão estar devidamente justificadas.

Seção II
Do Acesso e Uso do E-mail

Art. 29. O Poder Executivo Municipal fornece o serviço de e-mail institucional para o uso de seus usuários autorizados, sendo considerado como ferramenta de trabalho disponibilizado para uso exclusivo nas funções laborais.

Parágrafo único. A titularidade do endereço eletrônico é do Poder Executivo Municipal, que reserva o direito de monitorar e acessar todas as mensagens transitadas ou armazenadas, sempre que for necessário, já que não se trata de conteúdo protegido por privacidade.

Art. 30. Não será permitido o uso de serviços de e-mail que não sejam aqueles oficialmente fornecidos pelo Poder Executivo Municipal.

Art. 31. Os e-mails institucionais são de propriedade do Poder Executivo Municipal.

Art. 32. Os e-mails corporativos estão sujeitos a:

I - monitoramento e verificação automatizada, mesmo sem prévio aviso, para averiguar a presença de conteúdos impróprios, ilegais ou que comprometam a segurança da rede, dos dispositivos ou dados, que possam ferir direitos autorais, e atestar o respeito às regras contidas nesta norma, bem como, para produzir evidências relativas à eventual violação das mesmas e/ou à legislação em vigor;

II - limitação impositiva do tamanho dos anexos ou quantidade de destinatários com o propósito de preservar o uso e a disponibilidade dos recursos computacionais.

Art. 33. Cada usuário, a critério da Secretaria à qual está vinculado e de acordo com a necessidade das atividades que desempenha, poderá ter acesso a caixas de correio eletrônico corporativo:

I - para uso e acesso individual;

II - para uso por Secretarias, Departamentos e ou Serviços para os quais tenha sido designado como responsável.

§ 1º Não será permitida a utilização de duas ou mais caixas de correio eletrônico individuais por usuário.

§ 2º Norma específica estabelecerá os critérios que deverão ser observados quando da criação de um endereço de e-mail, bem como, as determinações e recomendações quanto ao uso do mesmo por parte dos usuários autorizados.

Art. 34. Recomenda-se a criação de listas de e-mail sempre que houver necessidade de transmissões recorrentes ou para grupos de usuários.

Seção III
Do Uso de Comunicadores Instantâneos

Art. 35. O serviço de mensagens instantâneas é provido por ferramenta que permite

interações para troca de mensagens rápidas, visando o compartilhamento de ideias e a colaboração on-line, independentemente do cargo, experiência ou função.

§ 1º Mensagens de interesse do Poder Executivo Municipal não devem ser compartilhadas com outros grupos que não aqueles diretamente relacionados ao interesse legítimo em questão.

§ 2º Ao utilizar a ferramenta, o servidor deverá ser cordial, transparente e prudente e não descuidar das premissas de segurança da informação.

§ 3º Utilizar preferencialmente ferramentas de caráter corporativo, evitando as plataformas de redes sociais de caráter pessoal.

§ 4º O usuário é o responsável exclusivo pelo uso inadequado dos serviços de comunicação instantânea.

Art. 36. Aplica-se às mensagens transitadas nos comunicadores instantâneos as mesmas políticas de monitoramento, segurança e acesso elencadas na seção que trata sobre o acesso e uso do e-mail.

Seção IV
Do Uso de Serviços de Videoconferência

Art. 37. O serviço de videoconferência, sempre que utilizado, deve considerar:

I - acessar o serviço prioritariamente mediante o uso de contas institucionais do Poder Executivo Municipal;

II - não permitir gravações, exceto quando de interesse do Poder Executivo Municipal;

III - evitar a exposição de pessoas que não estejam relacionadas ao interesse da reunião virtual;

IV - evitar expor indevidamente dados, informações e ou imagens do ambiente que possam ser capturados pelas câmeras dos aplicativos de videoconferência;

V - evitar a utilização de ferramentas e serviços que não possuam relação com o desempenho de suas atividades profissionais no âmbito do Poder Executivo Municipal.

Parágrafo único. A infraestrutura de TIC do Poder Executivo Municipal deve disponibilizar ferramentas de viés corporativo para fins de mensagens instantâneas e videoconferência.

Seção V
Do Comportamento Corporativo em Mídias e Redes Sociais

Art. 38. A publicação de conteúdo referente ao Poder Executivo Municipal em mídias e redes sociais é prerrogativa da Coordenadoria de Comunicação e Gestão Estratégica e dos servidores que possuem tal atribuição, restando vedado aos demais servidores publicar qualquer tipo de informação em nome do órgão público.

Art. 39. Caso o agente público não possua a atribuição citada no artigo anterior, mas estiver utilizando suas mídias e redes sociais particulares, deverá observar as seguintes regras em relação ao Poder Executivo:

I - Não é permitido o uso da logomarca, bem como de qualquer parte da identidade visual do Poder Executivo Municipal sem autorização prévia e expressa da autoridade competente;

II - Não é permitida a criação, participação ou interação comquaisquer perfis, comunidades, grupos, tópicos de discussão e afins que empreguem o nome, marca ou outros sinais distintivos do Poder Executivo Municipal, excetuando-se os canais oficiais do órgão público;

III - Não é permitida a publicação de qualquer tipo de conteúdo, comentários, entre outros, relacionados ao Poder Executivo Municipal, ao seu ambiente corporativo, servidores, terceiros contratados e prestadores de serviços, sem a expressa autorização, excetuando-se o material divulgado em canais oficiais do ente público.

CAPÍTULO XII
DO USO DE ATIVOS, EQUIPAMENTOS, SOFTWARES, RECURSOS E SERVIÇOS

Seção I
Do Uso Dos Recursos e Sistemas Computacionais

Art. 40. Os equipamentos, recursos e serviços fornecidos aos servidores pelo Poder Executivo Municipal, devem ser utilizados no uso profissional e de acordo com o papel e perfil de cada usuário/servidor.

Art. 41. Os servidores/usuários devem observar as seguintes disposições quanto ao uso de equipamentos, recursos e serviços de propriedade, sob responsabilidade e/ou disponibilizados pelo Poder Executivo Municipal:

I - Os equipamentos do Poder Executivo Municipal devem ser utilizados com cuidado visando garantir sua preservação e o funcionamento adequado;

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

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

IV - O bloqueio de tela protegido por senha deverá ser ativado sempre que o servidor/usuário se afastar do computador que esteja utilizando;

V - Por ocasião do desligamento do servidor/usuário do Poder Executivo Municipal, os equipamentos disponibilizados para a execução de atividades profissionais devem ser devolvidos em estado de conservação adequado;

VI - Eventuais danos aos equipamentos do Poder Executivo serão analisados pelo DTI e, havendo a constatação de que o mesmo decorreu de ação intencional ou em razão da omissão do servidor/usuário, caberá ao ente público postular a reparação do dano;

VII - O usuário deverá priorizar a digitalização dos documentos ou preferencialmente utilizá-los em formato digital e, quando estritamente necessária a impressão, observar as normas e boas práticas de sustentabilidade e segurança da informação.

Art. 42. O acesso a serviços e mensagens eletrônicas de qualquer natureza, que não seja realizado pelos meios e contas oficiais do Poder Executivo Municipal é de total responsabilidade do servidor/usuário que responde individualmente por qualquer dano decorrente.

Parágrafo único. Também é de responsabilidade do servidor/usuário a observância quanto à compatibilidade dos horários de trabalho e os referidos acessos.

Seção II
Dos Meios de Armazenamento

Art. 43. O Poder Executivo Municipal, determinará, a seu critério exclusivo, os meios e os locais onde seus servidores/usuários deverão realizar o tratamento e armazenamento das informações.

§ 1º Os recursos, capacidades e demais funcionalidades são estabelecidas de acordo com o papel e perfil de cada servidor/usuário devendo ser utilizados unicamente para a finalidade definida.

§ 2º Para dispositivos móveis ou com capacidade de armazenamento removível, o servidor/usuário deverá observar que:

I - é o responsável direto pela segurança física e lógica dos dispositivos sob sua guarda, sendo que os mesmos não devem ficar fora de seu alcance em locais públicos e/ou onde haja acesso não controlado de pessoas;

II - durante seus deslocamentos o servidor/usuário deverá dar preferência para compartimentos de armazenamento resistentes;

III - a instalação de ferramentas de proteção para dispositivos móveis é realizada pelo DTI e é obrigatória para todos os equipamentos corporativos;

IV - em caso de perda ou furto de um dispositivo de armazenamento removível, o usuário deve comunicar imediatamente a Secretaria de Administração para que possam ser tomadas as medidas cabíveis.

§ 3º O Poder Executivo poderá disponibilizar espaço para armazenamento remoto de arquivos na nuvem, através de sua solução corporativa, não sendo permitido o uso de qualquer outra solução de armazenamento na nuvem, que não seja a oficialmente adotada pelo órgão público e homologada pela equipe do DTI.

§ 4º Todos os arquivos relacionados ao exercício das suas funções deverão ser armazenados de forma centralizada no ambiente indicado pelo DTI.

§ 5º Nenhuma informação poderá permanecer armazenada em dispositivos de uso pessoal de propriedade do Poder Executivo ou particular (BYOD), nos termos do art. 45 e seguintes.

Art. 44. É expressamente proibido o armazenamento de informações de caráter pessoal, de informações e conteúdos que infrinjam direitos autorais, de caráter discriminatório, ilegais ou que não sejam de interesse do Poder Executivo Municipal em sua estrutura computacional local ou serviços de armazenamento remoto (nuvem).

Seção III
Do Uso de Equipamento Pessoal (byod)

Art. 45. A seu critério exclusivo, o Poder Executivo Municipal poderá permitir o uso de dispositivos de computação pessoal de caráter privado para execução de atividades profissionais ou manuseio de informações sob responsabilidade da municipalidade.

§ 1º A permissão para o uso deve ser autorizada pelo Secretário Municipal responsável pelo servidor/usuário e validada pelo DTI.

§ 2º O servidor/usuário deverá estar formalmente autorizado e concordar integralmente com os termos desta norma, antes de fazer uso de dispositivos pessoais no ambiente corporativo.

§ 3º O uso não autorizado de qualquer dispositivo de computação pessoal no ambiente corporativo será considerado uma violação desta PTSIC e tratado como um incidente de segurança da informação, estando o responsável sujeito às sanções e punições cabíveis.

§ 4º O Poder Executivo não será responsável por fornecer suporte, atualização, manutenção, reposição de peças, licenciamento de softwares, reembolso ou cobrir qualquer tipo de custo referente ao uso de dispositivos privados, os quais permanecerão sob irrestrita responsabilidade de seus proprietários.

§ 5º O dispositivo de computação privado utilizado pelo servidor/usuário deverá possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes do Poder Executivo Municipal, além de estar com todas as atualizações e licenciamentos de softwares em conformidade, sendo proibido conter, gerar ou distribuir qualquer tipo de conteúdo ilícito.

§ 6º O DTI tem autonomia para efetuar o bloqueio imediato do dispositivo caso constatar atividade suspeita ou ilegal.

§ 7º O uso de dispositivos de computação privado para atividades de trabalho não modifica a propriedade sobre as informações criadas, enviadas, recebidas, modificadas ou excluídas, permanecendo qualquer direito de propriedade intelectual do Poder Executivo Municipal.

Art. 46. O DTI poderá determinar a realização de inspeção prévia no equipamento de forma a garantir a adequação do mesmo aos requisitos e controles de segurança adotados.

Art. 47. É vedada a instalação e vinculação de qualquer hardware, software e serviço, de propriedade particular ou de terceiros, na infraestrutura do Poder Executivo sem a conformidade com os termos previstos nesta seção e sem o acompanhamento do DTI.

Seção IV
Do Cumprimento Aos Termos de Uso e Licenciamento de Software e Propriedade Intelectual

Art. 48. A utilização de qualquer software ou serviço de TIC sempre deve ser realizada em conformidade com os Termos de uso e Licenciamento de Software, de acordo com as diretrizes do fabricante ou prestador do serviço, devendo estar em conformidade com a Lei de Direitos Autorais e Lei de Software.

Art. 49. Para toda e qualquer licença de uso de software de propriedade do Poder Executivo ou por ela licenciado e para todo hardware ou sistema computacional de sua propriedade ou responsabilidade, fica estabelecido que seus servidores/usuários:

I - Devem estar cientes que os softwares são protegidos por direitos autorais e por licenças de uso e cessão que devem ser observados, mesmo naqueles rotulados como Domínio Público;

II - Não deverão realizar cópia de software para qualquer propósito com exceção daqueles cuja cópia é permitida no acordo de licença;

III - Não deverão disponibilizar o software para outras pessoas e ou empresas usarem ou

copiarem, se assim estiver previsto no termo de licenciamento;

IV - Não deverão instalar, ou induzir outros usuários a instalarem cópias ilegais de software sem as devidas licenças, em qualquer recurso de TIC de propriedade ou sob responsabilidade do Poder Executivo Municipal.

Art. 50. Toda licença de uso de software adquirida pelo Poder Executivo Municipal, deve ser guardada pelo DTI, que fará a gestão e o uso quando da instalação, reinstalação ou reparação da mesma nos dispositivos dos usuários.

Art. 51. Os softwares livres também devem ter sua licença/termo de uso analisados antes de seu download e/ou instalação, pois existem vários tipos de licenças e termos de uso, cada uma com suas peculiaridades.

Art. 52. Os servidores/usuários dos recursos de TIC devem respeitar a propriedade intelectual e o direito autoral, sendo considerada violação desta Política o download, armazenamento, utilização e compartilhamento de arquivos de áudio, vídeo, dados, softwares e até mesmo serviços, sem a devida autorização do proprietário ou em desconformidade com a licença ou os termos e condições de uso.

§ 1º As determinações deste artigo aplicam-se a todos os servidores/usuários que fizerem uso de recursos de TIC de propriedade ou sob responsabilidade do Poder Executivo Municipal, independente da utilização ocorrer nas suas dependências ou em qualquer lugar externo.

§ 2º Mediante regulamentação em norma específica, caberá ao DTI a verificação periódica quanto ao cumprimento dos servidores/usuários em relação aos deveres explicitados neste artigo, sem necessidade de consulta ou autorização prévia.

Seção V
Do Atendimento e Suporte ao Usuário

Art. 53. O Departamento de Tecnologia da Informação (DTI) manterá o serviço de atendimento de chamados técnicos objetivando o esclarecimento de dúvidas, manutenção, configuração e aplicação de melhorias para os recursos de Tecnologia e Segurança da Informação e Comunicação.

§ 1º Os chamados técnicos serão atendidos seguindo os critérios de ordem de chegada, observadas as indicações de criticidade e urgência declaradas pelo servidor/usuário demandante.

§ 2º O DTI poderá reclassificar o chamado quanto à criticidade e urgência mediante análise de impacto para o Poder Executivo Municipal.

§ 3º Os chamados técnicos deverão ser solicitados pelo servidor/usuário através do

sistema de registro de chamados, disponibilizado pelo DTI.

§ 4º Na impossibilidade do servidor/usuário fazer a abertura do chamado via sistema, o mesmo deverá ser realizado por contato telefônico e registrado no sistema pelo atendente do DTI.

§ 5º Os encaminhamentos referentes a cada chamado técnico deverão ser documentados no sistema de registro de chamados pelo servidor do DTI.

§ 6º Os chamados técnicos são exclusivos para ativos de Tecnologia e Segurança da Informação e Comunicação licenciados e/ou de propriedade e responsabilidade do Poder Executivo Municipal.

Art. 54. O DTI é responsável pelo conserto, configuração e substituição de qualquer componente de hardware ou software, estando o mesmo coberto ou não pela garantia do fabricante, contudo, quando houver custo de reposição, este deverá ser realizado pela Secretária em que está tombado o bem.

Art. 55. As ações de manutenção preventiva, sempre quando possível, serão realizadas mediante prévio agendamento e ampla divulgação, sendo que neste casos, o registro de chamado técnico é de responsabilidade do DTI.

CAPÍTULO XIII
DA AQUISIÇÃO DOS ATIVOS DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (TSIC)

Art. 56. A aquisição de todos os tipos de ativos de TSIC deverá ser previamente homologada pelo DTI com o objetivo de garantir a integração dos serviços, a racionalização e a padronização das tecnologias, bem como a funcionalidade e desempenho esperados.

§ 1º Para equipamentos, caberá ao DTI determinar os melhores perfis de hardware baseado nas necessidades de recursos computacionais, priorizando a relação custo-benefício e finalidade de uso.

§ 2º Para softwares que integram o conjunto de soluções disponíveis para a realização das atividades profissionais, será priorizado, sempre que possível, a instalação de software livre ou a sua disponibilização a partir de soluções em nuvem (cloud computing).

§ 3º A aquisição de soluções ou serviços pagos somente poderá ocorrer após a evidenciação prévia de sua real necessidade.

§ 4º Sempre que possível, deverão ser priorizadas soluções que sejam aderentes aos modelos e arquiteturas SaaS (Software as a Service - Software como Serviço) e ou IaaS (Infrastructure as a Service - Infraestrutura como Serviço).

§ 5º Os sistemas de gestão devem ser avaliados por uma comissão que envolva, pelo

menos, um representante do DTI e um representante da Secretaria demandante.

§ 6º Os sistemas de gestão também devem permitir e suportar a interligação de recursos e serviços, entre módulos desse e de outros sistemas e estarem plenamente adequados à LGPD.

§ 7º O Poder Executivo Municipal apenas aceitará a doação de equipamentos de TSIC, após avaliação e emissão de laudo favorável pelo DTI.

CAPÍTULO XIV
DA CLASSIFICAÇÃO, ROTULAGEM E MANUSEIO DAS INFORMAÇÕES

Art. 57. Para efeitos de classificação da informação, o Poder Executivo Municipal utiliza as seguintes categorias:

§ 1º Informação Pública: Informação oficialmente liberada pelo Poder Executivo Municipal para consulta do público em geral, já que sua divulgação não possui vedação ou causará problemas para o ente público, seus colaboradores, fornecedores entre outros, desde que, mantida a sua integridade.

§ 2º Informação de Uso Interno: Informação liberada exclusivamente para servidores/usuários e departamentos específicos do Poder Executivo Municipal, não podendo ser compartilhada com o público em geral e, caso haja necessidade, tais informações somente poderão ser compartilhadas mediante autorização expressa, conforme determina a LAI.

§ 3º Informação Confidencial: Informação de caráter sigiloso, podendo ser comunicada exclusivamente a sevidores/usuários especificamente autorizados e que necessitem conhecê-las para o desempenho de suas tarefas profissionais.

Art. 58. A classificação da informação deverá ser realizada pelos gestores da informação, ou colaboradores designados por estes.

§ 1º A responsabilidade pela acertividade do nível selecionado é de responsabilidade do gestor da informação.

§ 2º Os gestores da informação são os agentes públicos designados pelo Secretário Municipal ou chefe do Poder Executivo Municipal.

§ 3º Compete aos gestores da informação:

I - Definir a classificação das informações sob sua responsabilidade com base nas categorias de classificação constantes desta norma, mantendo um registro atualizado dos itens classificados;

II - Controlar as informações geradas em seu Departamento e ou área de atuação;

III - Revisar periodicamente a classificação das informações sob sua guarda.

Art. 59. Constará em norma específica a regulamentação necessária para a rotulagem (identificação), manuseio e descarte das informações, bem como, dos processos e cuidados necessários na digitalização de documentos, temporalidade e ciclo de vida, entre outros.

CAPÍTULO XV
DA PROTEÇÃO, MONITORAMENTO E BACKUP DAS INFORMAÇÕES E SERVIÇOS

Seção I
Da Proteção Contra os Códigos Maliciosos

Art. 60. O Poder Executivo Municipal disponibiliza ferramentas para proteção dos seus ativos de informação e recursos computacionais, incluindo computadores e servidores corporativos, contra ameaças e códigos maliciosos.

§ 1º Apenas as ferramentas disponibilizadas pelo ente público poderão ser utilizadas.

§ 2º As soluções utilizadas incluem Antivírus, Firewall, IDS, IPS, SIEM, podendo outras virem a ser adotadas.

Art. 61. Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os servidores/usuários do Poder Executivo Municipal deverão adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos.

Parágrafo único. Caberá à Secretaria de Administração e ao DTI promover campanhas que promovam a sensibilização e a conscientização dos servidores/usuários a respeito dos cuidados e boas práticas de segurança.

Seção II
Do Monitoramento

Art. 62. Qualquer serviço ou recurso computacional disponibilizado pelo Poder Executivo Municipal, bem como, qualquer outro recurso computacional com acesso aos mesmos, poderá ser monitorado a qualquer momento.

§ 1º Os ativos/serviços de informação, recursos computacionais do Poder Executivo Municipal, bem como, toda informação trafegada ou armazenada nos mesmos, incluindo conta de e-mail corporativa e a navegação em sites e serviços da Internet, estão sujeitos à monitoração, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa monitorada, visando resguardar a segurança dos serviços e recursos computacionais, bem como da segurança jurídica do ente público.

§ 2º Não há expectativa de privacidade na utilização da Infraestrutura tecnológica da

Prefeitura.

§ 3º As informações dos ativos/serviços de informação ou recursos computacionais do Poder Executivo Municipal podem ser interceptadas, gravadas, e lidas nas situações estabelecidas nesta Política.

§ 4º As informações dos ativos/serviços de informação podem incluir dados sensíveis criptografados para cumprir as exigências de confidencialidade e de privacidade, sendo que tais registros somente poderão ser requisitados:

I - por ordem judicial;

II - por autorização formal da Secretaria de Administração em conjunto com a Procuradoria-Geral;

III - para fins de obter dados de monitoramento ou estabelecimento de mecanismo de segurança pelo DTI;

IV - todo o material acessado ou coletado deverá preservar os requisitos de inviolabilidade e não repúdio.

Art. 63. O Poder Executivo Municipal realiza o monitoramento do seu ambiente físico interno e externo com o uso de circuito interno de televisão e câmeras de filmagem instaladas em suas dependências.

§ 1º As câmeras de filmagem estão dispostas de forma a resguardar a dignidade humana, sendo vedada a sua instalação em banheiros, lavabos e na área reservada ao atendimento médico de servidores públicos.

§ 2º A filmagem descrita nesta norma tem por objetivo assegurar a segurança física do ambiente do Poder Executivo Municipal e a sua segurança patrimonial, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa filmada.

§ 3º As imagens captadas dentro das dependências do Poder Executivo Municipal serão arquivadas conforme procedimento adotado pelo ente público e mantidas em caráter estritamente confidencial, somente podendo ser divulgadas em caso de infração às regras e legislação vigente.

§ 4º As imagens referidas neste artigo somente poderão ser requisitadas por:

I - por ordem judicial;

II - por autorização formal da Secretaria de Administração em conjunto com a Procuradoria-Geral.

§ 5º O Poder Executivo não permite o uso de qualquer dispositivo de gravação

audiovisual em seus prédios e instalações, excetuando-se os casos em que o servidor/usuário estiver formalmente autorizado.

Art. 64. A Prefeitura empregará esforços para exibir mensagens de aviso legal para garantir que usuários e demais pessoas e entidades que objetivem acesso a ativos/serviços de informação ou recursos computacionais da organização estejam cientes das regras de segurança adotadas, bem como do monitoramento realizado nos termos desta norma.

Seção III
Do Backup

Art. 65. O Poder Executivo Municipal deve manter rotinas de backup, que objetivam resguardar suas informações, registros e sistemas.

Parágrafo único. O procedimento de backupserá detalhado e formalizado em norma específica.

Seção IV
Da Resposta a Incidentes de Segurança da Informação

Art. 66. As ocorrências de segurança em TIC que possam vir a ter impacto negativo devem ter considerados ao menos os requisitos de disponibilidade, confiabilidade e recuperação, pois são essenciais à continuidade das operações do Poder Executivo Municipal.

§ 1º Todo o incidente deverá ser tratado de maneira a minimizar qualquer tipo de impacto a partir de respostas rápidas com foco no restabelecimento da normalidade operacional e manutenção das operações, mesmo que parcialmente, inclusive no caso de incidente de grandes proporções.

§ 2º O plano de respostas a incidentes deve ser orientado pelas normas técnicas ABNT NBR 15999-1:2007 e ABNT NBR 15999-2:2008, e operado por membros do Comitê Gestor de Tecnologia e Segurança da Informação e Comunicação.

§ 3º Constarão em norma específica todos os procedimentos que deverão ser adotados, a exemplo de:

I - priorização dos serviços e recursos afetados;

II - comunicação ao DTI e áreas envolvidas/afetadas;

III - análise do impacto causado e das medidas mais adequadas para contenção e restabelecimento da normalidade;

IV - plano de contingência contra interrupção da capacidade de prover os os principais

serviços do Poder Executivo;

V - disponibilização de roteiro que possibilita a restauração de serviços essenciais, dentro do tempo estabelecido e do nível acordado, denominando-se Plano de Continuidade Operacional;

VI - primazia pela capacidade de gerenciar uma interrupção dos serviços, preservando a reputação do Poder Executivo Municipal;

VII - restauração da capacidade do Poder Executivo Municipal no fornecimento dos seus principais serviços, dentro de um período de tempo previsível e aceitável, denominado-se Plano de Recuperação de Desastres;

VIII - atuação efetiva na minimização de possíveis ações judiciais;

IX - coordenação da comunicação com as partes impactadas.

CAPÍTULO XVI
DAS RESPONSABILIDADES

Seção I
Dos Usuários

Art. 67. Os servidores/usuários das informações e dos recursos de TIC, possuem as responsabilidades a seguir descritas:

I - ler, compreender, cumprir e estar atualizado quanto a esta Política de Tecnologia e Segurança da Informação e Comunicação (PTSIC), bem como sobre as demais normas e procedimentos de segurança vigentes;

II - encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre esta Política, normas e procedimentos para o DTI;

III - comunicar ao CGTSIC qualquer evento que viole esta Política ou possa comprometer a segurança das informações e/ou dos recursos computacionais do Poder Executivo Municipal;

IV - não divulgar, compartilhar e transmitir informações a pessoas e ou terceiros que não tenham nível de autorização suficiente;

V - assinar o Termo de Uso e Compromisso com os Recursos de Tecnologia da Informação e Comunicação do Poder Executivo Municipal, formalizando a ciência e o aceite integral das disposições desta Política, bem como, das demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

VI - responder pela inobservância desta Política, normas e procedimentos, conforme definido no item sanções e punições;

VII - utilizar as informações, recursos computacionais e ferramentas tecnológicas exclusivamente para o desempenho de suas atividades profissionais;

VIII - responder pelo conteúdo das informações que disponibilizar na rede e por aquelas mantidas em qualquer meio de armazenamento sob sua responsabilidade;

IX - desligar os equipamentos (computadores, monitores, impressoras, scanners, etc) ao fim do expediente;

X - zelar pela integridade física dos equipamentos de tecnologia da informação e comunicação colocados à sua disposição, evitando submetê-los a condições de risco, mantendo-os afastados de líquidos, alimentos ou qualquer material ou utensílio que possa danificá-los, devendo comunicar imediatamente ao DTI qualquer anormalidade ou defeito;

XI - controlar o acesso físico e lógico aos recursos computacionais sob sua responsabilidade;

XII - usar programas de proteção contra vírus e atualizá-los periodicamente conforme instruções disponibilizadas pelo DTI;

XIII - zelar pela segurança das contas e senhas que lhes foram exclusivamente atribuídas e que não devem ser compartilhadas com outras pessoas;

XIV - proteger os equipamentos, informações e sistemas colocados à sua disposição contra acesso, tentativa de acesso, destruição ou divulgação não autorizadas;

XV - comunicar ao DTI qualquer evidência de violação das normas em vigor, não podendo acobertar ou ajudar a acobertar violações de terceiros.

Seção II
Dos Agentes Políticos

Art. 68. Os Secretários Municipais possuem as seguintes responsabilidades quanto aos termos da presente política:

I - autorizar ou não, de modo formal, que servidores/usuários sob sua responsabilidade possam acessar os recursos computacionais;

II - instruir os servidores públicos, prestadores de serviços e demais membros sobre os termos desta política e sua forma de acesso;

III - orientar e supervisionar seus subordinados, promovendo a adequada utilização dos

recursos de TIC, cumprindo assim os dispositivos desta política;

IV - comunicar imediatamente ao DTI situações em que constatar uso inadequado ou indevido dos recursos de TIC e das informações de propriedade ou sob responsabilidade do Poder Executivo Municipal.

Seção III
Da Procuradoria Geral do Município

Art. 69. Para atendimento da presente política, compete à Procuradoria-Geral do Município supervisionar e coordenar as atividades de natureza jurídica, prestando assessoramento e apoiando com a elaboração de atos normativos.

Seção IV
Da Secretaria Municipal de Administração

Art. 70. Compete à Secretaria Municipal de Administração:

I - assegurar que a implementação desta política e de seus controles sejam realizados em todo o Poder Executivo Municipal;

II - prover os recursos necessários para que o DTI cumpra com suas obrigações no âmbito desta política.

Art. 71. O Departamento de Recursos Humanos deverá:

I - informar prontamente ao DTI todos as exonerações, demissões, afastamentos, retornos ao trabalho, nomeações e quaisquer modificações no quadro funcional;

II - apoiar a gestão de identidades enviando ao DTI relatórios periódicos sobre servidores/usuários com alteração de função solicitada ao Departamento;

III - apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação fornecendo informações sobre os servidores/usuários;

IV - dar ciência e divulgar aos servidores do quadro e àqueles que serão nomeados/contratados, os termos da presente política;

Art. 72. São responsabilidades do DTI:

I - propor adequações às normas de Segurança da Informação e sobre a presente política;

II - planejar e coordenar a execução dos programas, planos, projetos e ações relativas a

esta política;

III - promover a divulgação da política, normas e melhores práticas para todo o Poder Executivo Municipal;

IV - promover a cultura da Segurança da Informação por meio de ações de sensibilização e conscientização;

V - definir, promover e administrar, direta ou indiretamente, estudos sobre novas tecnologias, modelos e métodos de gerenciamento que promovam a melhor utilização dos recursos e serviços de TIC;

VI - garantir os níveis de alinhamento das atividades de Segurança e TIC a todas as políticas, normas e procedimentos estabelecidos;

VII - apoiar técnica e administrativamente as reuniões e demais atividades do CGTSIC, incluindo o gerenciamento da execução de suas resoluções;

VIII - supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;

IX - identificar controles físicos, administrativos e tecnológicos para mitigação do risco;

X - propor, e quando aprovado pelo CGTSIC, implantar e gerenciar o programa de continuidade de negócios dos serviços e sistemas de informação do Poder Executivo Municipal;

XI - constituir e coordenar um Grupo de Tratamento e Resposta a Incidentes, formado por membros do DTI, que deverá:

a) coordenar as atividades de tratamento e resposta a incidentes de Segurança da Informação;
b) promover o tratamento e a recuperação de serviços de TIC;
c) acompanhar e apurar os incidentes de segurança e encaminhar os fatos apurados para o CGTSIC com vistas a aplicação das penalidades previstas;
d) recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, informando aos respectivos gestores sobre as ações corretivas ou de contingência em cada caso.

XII - coordenar a instalação, configuração e movimentação de equipamentos de TIC e softwares de qualquer natureza.

Art. 73. São responsabilidades do CGTSIC:

I - regulamentar as diretrizes, normas e procedimentos desta política;

II - acompanhar e orientar a implantação das políticas e normas de Segurança da Informação nas Secretarias e Departamentos do Poder Executivo Municipal;

III - promover postura estratégica de governo e alinhamento de decisões de soluções e investimentos, priorizando o planejamento para médio e longo prazo, de acordo com os princípios orientadores desta política;

IV - receber, analisar e consolidar os resultados relativos à auditorias de nível de conformidade das Secretarias e Departamentos quanto a esta política e suas normas;

V - gerenciar os riscos de segurança da informação associados aos processos e serviços do Poder Executivo Municipal;

VI - deliberar sobre a implementação das ações de Segurança da Informação;

VII - elaborar e propor normas em conformidade com esta política e suas normas complementares;

VIII - receber denúncias, suspeitas e apontamentos de incidentes que envolvam a Segurança da Informação e o descumprimento desta política e suas normas;

IX - determinar e acompanhar a apuração e resposta a incidentes;

X - informar à Secretaria de Administração os responsáveis identificados em incidentes que afrontem este regramento, para fins de verificação sobre a instauração de sindicância ou processo administrativo disciplinar;

XI - aprovar e acompanhar a implantação e o gerenciamento do Plano de Continuidade Operacional dos serviços e sistemas de informação do Poder Executivo Municipal.

CAPÍTULO XVII
DAS PROIBIÇÕES E PENALIDADES

Seção I
Das Proibições

Art. 74. São proibidas, estando sujeitas à penalidades, as seguintes atividades:

I - distribuir voluntariamente mensagens não solicitadas, como cartas, circulares comerciais ou outros que possam ser caracterizados como spam, que venham prejudicar o trabalho, causar excessivo tráfego na rede ou sobrecarregar os sistemas computacionais;

II - acessar, enviar, reenviar ou propagar qualquer mensagem com conteúdo pornográfico, preconceituoso, discriminatório ou pedofílico e demais mensagens contrárias ao bom-senso e ética, independente da vontade do destinatário em receber tais mensagens;

III - instalar, armazenar, utilizar ou divulgar qualquer tipo de software, conteúdo ou mensagem eletrônica que esteja fora do escopo das atividades profissionais do usuário e que possa ferir os princípios de conduta moral e ética;

IV - acessar sites que apresentem conteúdo ilegal e incompatível ao ambiente de trabalho e ao exercício das atividades profissionais, salvo por questões de trabalho devidamente justificadas e autorizadas, bem como aqueles que incitem qualquer tipo de preconceito ou discriminação, ou ainda aqueles que possibilitem a realização de atividades ilegais ou que prejudiquem a imagem do órgão público perante a sociedade;

V - fazer-se passar por outra pessoa ou camuflar a identidade quando em utilização dos recursos computacionais;

VI - utilizar comunicadores instantâneos de forma abusiva e por motivos particulares de forma que venham a impactar na produtividade e desempenho das atividades ou prejudicar o desempenho das conexões de rede e/ou internet;

VII - utilizar-se dos recursos computacionais para constranger, molestar, assediar ou ameaçar qualquer pessoa;

VIII - violar, tentar violar ou permitir a violação dos sistemas de segurança dos recursos computacionais;

IX - alterar as configurações dos equipamentos e sistemas, salvo autorização expressa do DTI, mediante solicitação;

X - instalar qualquer tipo de equipamento, software ou recursos que não sejam de propriedade do Poder Executivo Municipal no ambiente de trabalho sem o acompanhamento e a autorização expressa do DTI;

XI - utilizar os recursos computacionais para fazer o download ou distribuição de software ou dados não legalizados de qualquer natureza.

Seção II
Das Penalidades

Art. 75. As infrações ao disposto nesta política sujeitarão o infrator às normas disciplinares estabelecidas no Regime Jurídico dos Servidores Públicos Municipais, mediante a instauração do procedimento cabível, sem prejuízo das demais sanções nas esferas civil e criminal.

§ 1º O processo disciplinar instaurado será instruído pela Comissão sindicante, que deverá solicitar a análise do Comitê Gestor de Tecnologia e Segurança da Informação e Comunicação (CGTSIC), quanto a gravidade da infração, efeito alcançado e recorrência.

§ 2º O CGTSIC, considerando a gravidade da infração, poderá recomendar a aplicação de sanção disciplinar à Comissão Sindicante.

§ 3º No caso de terceiros contratados ou prestadores de serviço, o CGTSIC deverá analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato, recomendando à Procuradoria do Município as ações apropriadas.

§ 4º Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano ao Poder Executivo Municipal, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo às demais sanções e penalidades previstas nesta política.

CAPÍTULO XVIII
DOS CASOS OMISSOS

Art. 76. Os casos omissos e as dúvidas deverão ser submetidas para avaliação do Comitê Gestor de Tecnologia e Segurança da Informação e Comunicação (CGTSIC) para análise, deliberação e posterior encaminhamento.

Art. 77. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos não se esgotam em razão da contínua evolução tecnológica e do constante surgimento de novas ameaças.

§ 1º A política ora instituída deve ser observada por todos os servidores/usuários das informações e dos recursos de TIC.

§ 2º Além das medidas estabelecidas nesta política, o DTI deverá ser diligente na busca de outras medidas de segurança e de boa prática, com o objetivo de garantir o uso racional e adequado dos recursos de TIC bem como, proteção às informações do Poder Executivo Municipal.

CAPÍTULO XIX
DAS DISPOSIÇÕES FINAIS

Art. 78. Os recursos computacionais deverão ser utilizados, única e exclusivamente, em serviços e atividades que visem atender aos objetivos e interesses do Poder Executivo Municipal e para uso exclusivo dos servidores/usuários autorizados nos termos desta política, sendo expressamente vedado o uso para fins particulares.

Art. 79. Pessoas sem vínculo efetivo com o Poder Executivo Municipal poderão utilizar os recursos computacionais desde que no interesse do serviço e em atividades prestadas por intermédio de instrumentos jurídicos firmados junto ao ente público, estando acompanhadas e fiscalizadas por servidor indicado pela chefia da Secretaria.

Art. 80. Este Decreto entra em vigor na data de sua publicação.

LAJEADO, 24 DE NOVEMBRO DE 2021.

MARCELO CAUMO
PREFEITO

Elisângela Hoss de Souza,
Secretária de Administração.

ANEXO I

TERMO DE USO E COMPROMISSO COM OS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

CONSIDERANDO que o Poder Executivo Municipal de Lajeado-RS disponibiliza a seus servidores/usuários ativos de informação e recursos computacionais exclusivamente para que os mesmos possam desempenhar suas atividades profissionais;

CONSIDERANDO que o Poder Executivo Municipal de Lajeado-RS é a detentora dos ativos de informação e recursos computacionais, não existindo qualquer tipo de expectativa de privacidade no uso dos recursos acima mencionados;

CONSIDERANDO a necessidade de minimizar os riscos que o Poder Executivo Municipal pode sofrer em decorrência da má utilização de seus ativos de informação e recursos computacionais;

DECLARO:

1. Tenho conhecimento e acesso a Política de Tecnologia e Segurança da Informação e Comunicação, instituída pelo Decreto nº 12.417/2021, bem como, das demais normas e procedimentos necessários ao meu trabalho, que se encontram disponíveis no portal do servidor (portal.lajeado.rs.gov.br), os quais li na íntegra, tomando conhecimento e ciência de suas disposições;

2. Compreendo completamente os termos, diretrizes, conceitos e condições de uso da Política de Tecnologia e Segurança da Informação e Comunicação, bem como, as demais normas e procedimentos necessários ao meu trabalho, me comprometendo a cumprir integralmente as disposições constantes em tais documentos;

3. Estou ciente e de acordo que, tanto os ativos de informação, quanto a infraestrutura tecnológica do Poder Executivo somente poderão ser utilizados para fins exclusivamente profissionais e relacionados às atividades da organização;

4. Estou ciente de que é realizado o monitoramento de todos os acessos, usos e comunicações ocorridos através da infraestrutura tecnológica do Poder Executivo Municipal;

5. Estou ciente de que violações da Política de Tecnologia e Segurança da Informação e Comunicação (PTSIC), bem como, das demais normas e procedimentos são passíveis de sanções e punições, podendo incorrer em responsabilização legal nas esferas administrativa, cível e penal, nos termos da legislação em vigor;

6. Comprometo-me a não revelar fato ou informações de qualquer natureza a que tenha conhecimento por força das minhas atribuições, mesmo após o encerramento do vínculo com o Poder Executivo Municipal de Lajeado;

7. Comprometo-me a não divulgar ou compartilhar qualquer senha de acesso, seja a(s) minha(s) ou de terceiros (a qual por ventura venha a ter conhecimento);

8. Tenho ciência que as senhas de acesso são pessoais e intransferíveis;

9. Comprometo-me a não obter acesso ilícito a informações, serviços ou recursos de TIC,

~~através de qualquer meio, sob responsabilidade de outros usuários, dentro ou fora do domínio do Poder Executivo Municipal;~~
~~10. Comprometo-me a não forjar ou fazer-me passar por outra pessoa ou usuário perante os recursos de TIC;/~~
~~Lajeado, _____ de _____ de 20___~~
~~_____~~
~~Assinatura do Declarante~~
~~SE AGENTE PÚBLICO~~
~~Nome Completo:_____~~
~~Cargo/Função:_____~~
~~CPF:_____~~
~~#~~
~~SE TERCEIRIZADO OU MEMBRO DE OUTRO ÓRGÃO PÚBLICO~~
~~Nome Completo:_____~~
~~Cargo/Função:_____~~
~~CPF:_____~~
~~Empresa Representada: _____~~
~~Contrato: _____~~

ANEXO I

TERMO DE USO E COMPROMISSO COM OS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Eu _____, matrícula nº _____, portador(a) do CPF nº _____, DECLARO que:

1 - Tenho conhecimento e acesso à Política de Tecnologia e Segurança da Informação e Comunicação (PTSIC), instituída pelo Decreto nº 12.417/2021, bem como das demais normas e procedimentos atinentes às atividades profissionais, que se encontram disponíveis no portal do servidor (portal.lajeado.rs.gov.br), os quais li na íntegra, tomando conhecimento e ciência de suas disposições;

2 - Compreendo e aceito os termos, diretrizes, conceitos e condições presentes na PTSIC, me comprometendo a cumprir integralmente as disposições constantes em tais documentos, observando possíveis atualizações;

3 - Estou ciente de que violações da Política de Tecnologia e Segurança da Informação e Comunicação (PTSIC), bem como as demais normas e procedimentos são passíveis de sanções e punições, podendo incorrer em responsabilização legal na esfera administrativa, cível e penal, nos termos da legislação em vigor;

4 - Estou ciente e de acordo que, tanto os ativos de informação quanto a infraestrutura tecnológica do Poder Executivo somente poderão ser utilizados para fins relacionados às atividades da Prefeitura, a qual é garantida a prerrogativa de monitorar e auditar todos os acessos, usos e comunicações ocorridos através da infraestrutura tecnológica;

5 - Comprometo-me a manter sigilo, integridade e segurança de todos os dados e/ou fatos de qualquer natureza a que tiver acesso ou conhecimento por força das minhas atribuições, mesmo após o encerramento do vínculo com a Prefeitura Municipal de Lajeado,

respeitando especialmente a Lei de Acesso à Informação - LAI (Lei nº 12.527/2011) e a Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018);

6 - Tenho ciência que as senhas de acesso são pessoais e intransferíveis e comprometo-me a não divulgar ou compartilhar qualquer senha de acesso, sejam minhas ou de terceiros (que por ventura venham a ter conhecimento);

7 - Estou ciente que os dados de interesse do Poder Executivo Municipal não devem ser armazenados em dispositivos locais (Pcs, notebooks, etc.), mas sim, exclusivamente em unidades de armazenamento específicas, indicadas pelo departamento de TI;

8 - Compreendo que os dados pessoais repassados ao setor de Recursos Humanos serão usados para criação de credenciais objetivando o uso de assinaturas eletrônicas vinculadas a mim de forma unívoca e as admito como válidas conforme exigido no inciso II do artigo 4º da Lei nº 14.063/2020.

Lajeado, ___ de _____ de 20____.

_____

Assinatura do Declarante. (Redação dada pelo Decreto nº 13307/2023

ANEXO II

GLOSSÁRIO

I - APLICATIVOS DE MENSAGENS: programa de computador com a finalidade de trocas de mensagens entre dispositivos de comunicação de modo online e/ou sob demanda;

II - ATIVO DE TIC: sinônimo para TIC;

III - TIC - Tecnologia da Informação e Comunicação. O conjunto de soluções e atividades relacionadas a diferentes elementos como hardware, software, redes e banco de dados, com a finalidade de processar, analisar, produzir, armazenar e transmitir informações, considerando o gerenciamento e a segurança inerentes.

IV - PTSIC - Política de Tecnologia e Segurança da Informação e Comunicação;

V - TI - Tecnologia da Informação;

VI - TSIC - Tecnologia e Segurança da Informação e Comunicação;

VII - DTI - Departamento de Tecnologia da Informação;

VIII - CGTSIC - Comitê Gestor de Tecnologia e Segurança da Informação e Comunicação;

IX - LGPD - Lei Geral de Proteção de dados pessoais;

X - BYOD (Bring Your Own Device): é um conceito de TI que considera a utilização dos

aparelhos pessoais dos próprios usuários para desempenharem as atividades, normalmente conectados à infraestrutura de rede da organização;

XI - COMPUTAÇÃO EM NUVEM: disponibilização de serviços de computação e informática, incluindo processamento, armazenamento, bancos de dados, rede, sistemas de informação gerencial, correio eletrônico, etc. pela Internet ("a nuvem");

XII - CORREIO ELETRÔNICO: serviço baseado em programas de computador com a finalidade de troca de conteúdos e mensagens em formato eletrônico entre usuários e entre sistemas;

XIII - CREDENCIAL DO USUÁRIO: combinação de identificação de usuário (user id) e senha (password) ou a combinação destes com sistemas biométricos, tokens e certificados digitais a serem utilizados nos processos de autenticação e autorização, visando o acesso à infraestrutura e serviços de TIC;

XIV - DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO - DTI: unidade executiva responsável pelo planejamento, coordenação, organização, controle, supervisão e manutenção dos recursos relacionados às TICs;

XV - DOWNLOAD: cópia de arquivo da Internet utilizando os recursos de conexão em determinado equipamento;

XVI - HARDWARE: conjunto de componentes físicos, normalmente compostos por uma carcaça, que organiza a unidade central de processamento, memória, os componentes eletrônicos, circuitos integrados e placas, que se comunicam através de barramentos e interfaces;

XVII - INCIDENTES DE SEGURANÇA: qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que representem uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo;

XVIII - INFRAESTRUTURA COMO SERVIÇO (IaaS - Infrastructure as a Service): é um modelo de Computação em Nuvem que disponibiliza recursos computacionais acessados via internet ou rede privada como processamento, armazenamento, banco de dados e servidores;

XIX - INTERNET: rede mundial de computadores que objetiva conectar pessoas, serviços e organizações de várias partes do mundo, permitindo acesso a diversos conteúdos e de diversas formas;

XX - INTRANET: rede local de computadores a partir da qual são utilizados os mesmos serviços e protocolos de comunicação empregados para o funcionamento da Internet.

XXI - NAVEGADOR WEB (BROWSER): programa de computador que permite o acesso à Internet a partir de uma interface gráfica;

XXII - PAPEL DO USUÁRIO: uma função específica a ser executada por algum usuário;

XXIII - PERFIL DO USUÁRIO: conjunto de permissões de acesso aos recursos computacionais. O gerenciamento do perfil objetiva liberar e limitar os acessos de cada usuário;

XXIV - RECURSOS DE TIC: de acordo com a RFC 2828, (Internet Security Glossary), trata-se dos dados contidos em um sistema de informação, dos serviços disponibilizados por um sistema, capacidade do sistema (poder de processamento ou largura de banda de comunicação, item de equipamento do sistema (um componente do sistema, hardware, firmware, software ou documentação) e instalação que abriga operações e equipamentos de sistema. São exemplos:

a) computadores e periféricos (ETD - Equipamento Terminador de Dados);
b) equipamentos de rede (ECD - Equipamento de Comunicação de Dados);
c) sistemas (sistemas operacionais, bancos de dados, servidores de arquivos, de impressão, de correio eletrônico, sites e home pages (WEB) e gestão corporativa)
d) documentos eletrônicos (textos, planilhas, representações gráficas e textuais produzidas por sistemas de informações gerenciais, etc.);
e) ambientes de acesso restrito (data center);

XXV - REDE LOCAL (Local Area Network - LAN): infraestrutura de rede e comunicação de dados responsável por interligar os ETDs e ECDs das unidades da prefeitura, assim como o Centro Administrativo Municipal, Secretarias, Postos de Saúde e Escolas e estas entre si e à Internet;

XXVI - REDES SOCIAIS: sistema informatizado normalmente disponibilizado na Internet que visa a conexão de pessoas e organizações a partir de valores ou interesses;

XXVII - SOFTWARE COMO SERVIÇO (SaaS - Software as a Service): é a disponibilização de softwares e soluções de tecnologia por meio da internet ou nuvem privada que passa a ser visto como um serviço. Não são mais instalados ou gerenciados em computadores pessoais;

XXVIII - SISTEMA INFORMATIZADO: organização de computadores, periféricos e softwares para a realização de um propósito específico. Dispositivos eletrônicos capazes de processar dados e informações de acordo com um software ou conjunto de softwares;

XXIX - SITE (Sítios WEB): local virtual onde se encontram informações relativas a um determinado assunto;

XXX - SOFTWARE: algoritmo, rotina ou conjunto de instruções que organizam e controlam o funcionamento de um computador e/ou a realização de uma atividade computacional. O termo software livre é atribuído ao software que a concede liberdade de acesso, execução, modificação e distribuição do código fonte aos seus usuários;

XXXI - SSID (Service Set Identifier): Conhecido como Identificador do Conjunto de Serviços e objetiva facilitar a identificação das redes Wi-Fi disponíveis em uma área de cobertura específica a partir das quais os usuários podem obter sua conexão.

XXXII - UNIDADES DE ARMAZENAMENTO: infraestrutura de armazenamento disponibilizada em equipamentos específicos para a guarda temporária ou permanente de dados e informações relevantes ao Poder Executivo Municipal;

XXXIII - USUÁRIO: qualquer servidor, estagiário, funcionário de empresa contratada ou auditor de outros órgãos da administração pública em caráter temporário devidamente identificado por um nome (login) e uma senha de uso exclusivo para acesso aos recursos computacionais;

XXXIV - VLAN (Virtual LAN): Organizam a utilização de uma Rede Local (LAN) a partir de múltiplos segmentos lógicos objetivando agrupar tráfegos afins.

XXXV - WEBMAIL: página da Internet que, através de usuário e senha, permite o acesso à caixa postal de correio eletrônico.

XXXVI - WI-Fi (Wireless Fidelity - Rede Local Sem Fio): É a marca registrada da Wi-Fi Alliance que certifica produtos pertencentes a classe de dispositivos de rede local sem fios (WLAN) embasados no padrão IEEE 802 e que não fazem uso de cabos.