DECRETO Nº 2036/2023, DE 19 DE JANEIRO DE 2023.

INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO- PSI NO ÂMBITO DA PREFEITURA DO MUNICÍPIO DE JUQUIÁ E DÁ OUTRAS PROVIDÊNCIAS.

GILBERTO TADASHI MATSUSUE, Prefeito do Município de Juquiá, Estado de São Paulo, no uso das atribuições que lhe são conferidas por Lei e;

CONSIDERANDO a necessidade de normatizar o uso apropriado dos recursos da tecnologia da informação no âmbito da Prefeitura do Município de Juquiá, promovendo a proteção dos usuários, dos equipamentos, dos softwares, dos dados dos contribuintes e da própria Administração Pública;

CONSIDERANDO a necessidade de garantir a segurança das informações geradas, adquiridas, processadas, armazenadas e transmitidas no âmbito da Administração Municipal, de forma a atender aos princípios da confidencialidade, integridade, disponibilidade, autenticidade e legalidade;

CONSIDERANDO que os servidores públicos devem zelar pelas informações que lhes são confiadas no exercício de suas funções;

CONSIDERANDO que as ações de segurança da informação reduzem custos e riscos e aumentam os benefícios prestados aos cidadãos, ao permitir a oferta de processos, produtos e serviços suportados por sistemas de informações mais seguros;

Considerando que a Política de Segurança da Informação- PSI, é o documento que orienta e estabelece as diretrizes corporativas da Prefeitura Municipal de Juquiá para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da administração.

Considerando que a PSI 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 em nosso país.

DECRETA:

CAPÍTULO I
DOS OBJETIVOS

Art. 1º. Fica instituída a Política de Segurança da Informação- PSI, no âmbito da Prefeitura do Município de Juquiá, estabelecendo diretrizes que permitam aos colaboradores desta Prefeitura seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da instituição e do indivíduo, norteando a definição de normas e procedimentos específicos de segurança da informação,

bem como a implementação de controles e processos para seu atendimento, preservando assim, as informações da Prefeitura Municipal de Juquiá 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.

CAPÍTULO II
DAS APLICAÇÕES E DOS PRINCÍPIOS DA PSI

Art. 2º. As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte. Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da instituição poderão ser monitorados e gravados, com prévia informação, conforme previsto nas legislações brasileiras.

Parágrafo único: É obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou dos Técnicos em Informática sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Art. 3º. Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela Prefeitura pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

Parágrafo único: A Administração, por meio dos Técnicos em Informática, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

CAPÍTULO III
DOS REQUISITOS DA PSI

Art. 4º. Para a uniformidade da informação, a PSI deverá ser comunicada a todos os seus colaboradores, a fim de que a política seja totalmente cumprida.

Art. 5º. Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão dos Técnicos em Informática.

Art. 6º. Deverá constar em todos os contratos da Prefeitura, o anexo de Termo de Responsabilidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela administração.

Art. 7º. A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos, devendo assinar o respectivo termo de responsabilidade. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente aos Técnicos em Informática, para análise.

Art. 8º. 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.

Art. 9º. 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. 10º. 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, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas gerenciais desenvolvidos pela Prefeitura Municipal de Juquiá ou por terceiros.

Art. 11. Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação. A Prefeitura Municipal de Juquiá exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, 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.

Art. 12. Esta PSI será implementado na Prefeitura por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou prestação de serviço. O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas desta instituição e sujeitará o usuário às medidas administrativas legais.

CAPÍTULO IV
DAS RESPONSABILIDADES ESPECÍFICAS DOS COLABORADORES

Art. 13. Entende-se por colaborador toda e qualquer pessoa física ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Art. 14. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a Prefeitura Municipal de Juquiá e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Art. 15. Os Colaboradores em Regime Temporários, devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelos Técnicos em Informática. 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 colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

Art. 16. Os Gestores de Pessoas e/ou Processos, deverão ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Art. 17. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da Prefeitura Municipal de Juquiá.

Art. 18. Exigir dos colaboradores a assinatura do Termo de Responsabilidade, 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 da Prefeitura Municipal de Juquiá.

Art. 19. Antes de conceder acesso às informações da instituição, exigir-se-á a assinatura do Termo de Responsabilidade dos colaboradores 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, deverão adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

CAPÍTULO V
DOS CUSTODIANTES DA INFORMAÇÃO E DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

Art. 20. Deverá ser testada a eficácia dos controles utilizados e informar aos gestores, os riscos residuais e acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes, configurando os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, e em sua versão educacional, pelas Normas de Segurança da Informação complementares.

Art. 21. Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários:

I) Acessar os arquivos e dados de outros usuários. No entanto, 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.

II) Segregar as funções administrativas e 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.

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

IV) Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Prefeitura Municipal de Juquiá.

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

VI) O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

VII) 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.

VIII) Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

IX) 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) os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

b) os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

c) 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.

d) 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.

e) Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

f) Realizar auditorias quando solicitadas de configurações técnicas e análise de riscos.

g) Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

h) 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. Tal desligamento deverá ser informado pela Divisão de Recursos Humanos.

i) Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

j) Monitorar o ambiente de TI, gerando indicadores e históricos de: uso da capacidade instalada da rede e dos equipamentos; tempo de resposta no acesso à internet e aos sistemas críticos; períodos de indisponibilidade no acesso à internet e aos sistemas críticos; incidentes de segurança (vírus, trojans, furtos, acessos indevidos); atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

CAPÍTULO VI
DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

Art. 22. A área de segurança da informação, deverá:

a) Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação, apoiando as iniciativas que visem à segurança dos ativos de informação da Prefeitura Municipal de Juquiá.

b) Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelos Técnicos em Informática.

c) Promover a conscientização dos colaboradores em relação à relevância da segurança da informação, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

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

CAPÍTULO VII
DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Art. 23. Para garantir as regras mencionadas nesta PSI, a Prefeitura Municipal de Juquiá poderá:

a) 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;

b) tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior);

c) realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

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

CAPÍTULO VIII
DO CORREIO ELETRÔNICO

Art. 24. O objetivo desta norma é informar aos colaboradores da Prefeitura Municipal, quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo, sendo seu uso, estritamente para fins corporativos e relacionados às atividades do colaborador usuário dentro desta instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudicando a Prefeitura Municipal e também não causando impacto no tráfego da rede.

CAPÍTULO IX
DAS PROIBIÇÕES

Art. 25. É PROIBIDO aos colaboradores o uso do correio eletrônico da Prefeitura Municipal de Juquiá:

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

b) enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

c) enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Prefeitura Municipal de Juquiá ou suas unidades vulneráveis a ações civis ou criminais;

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

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

f) apagar mensagens pertinentes de correio eletrônico quando a Prefeitura Municipal de Juquiá estiver sujeita a algum tipo de investigação.

g) produzir, transmitir ou divulgar mensagem que contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Prefeitura Municipal de Juquiá; contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;

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

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

j) que interrompam um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

k) burlar qualquer sistema de segurança, vigiando secretamente ou assediando outro usuário;

l) o acesso a informações confidenciais sem explícita autorização do proprietário, bem como o acesso indevido que possam causar prejuízos a qualquer pessoa, incluindo imagens criptografadas ou de qualquer forma mascaradas;

m) anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet), que tenha conteúdo considerado impróprio, obsceno ou ilegal, seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

n) conteúdo que contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas; tenha fins políticos locais ou do país (propaganda política); ou inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

Art.26. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- Gerência ou departamento;
- Nome da instituição;
- Telefone(s);
- Correio eletrônico.

CAPÍTULO X
DAS REGRAS PARA USO DA INTERNET

Art. 27. Todas as regras atuais da Prefeitura Municipal de Juquiá 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. 28. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a Prefeitura Municipal de Juquiá, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Art. 29. 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 Política de Segurança da Informação.

Art. 30. A Prefeitura Municipal de Juquiá, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. 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.

Art. 31. A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos na instituição.

Art. 32. Como é do interesse da Prefeitura Municipal de Juquiá que seus colaboradores 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.

Art. 33. Somente os colaboradores que estão devidamente autorizados a falar em nome da Prefeitura Municipal de Juquiá para os meios de comunicação poderão manifestar-se, seja por email, entrevista on-line, podcast, seja por documento físico, entre outros.

Art. 34. Apenas os colaboradores 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. 35. 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. 36. Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na Prefeitura Municipal de Juquiá e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pelos Técnicos em informática.

Art. 37. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

Art. 38. Qualquer software não autorizado baixado será excluído pelos Técnicos em Informática. Os colaboradores não poderão em hipótese alguma utilizar os recursos da Prefeitura Municipal de Juquiá para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Art. 39. 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. 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 a alguma atividade específica.

Art. 40. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Art. 41. Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado a Prefeitura Municipal de Juquiá ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Art. 42. Os colaboradores não poderão utilizar os recursos da Prefeitura Municipal para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

Art. 43. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos após análise do Departamento de TI. Não é permitido acesso a sites de proxy.

CAPÍTULO XI
DOS DISPOSITIVOS DE IDENTIFICAÇÃO E SENHAS

Art. 44. Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Prefeitura Municipal e/ou terceiros.

Art. 45. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 - falsa identidade).

Art. 46. Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Art. 47. Todos os dispositivos de identificação utilizados na Prefeitura, como o número de registro do colaborador, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

Art. 48. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Art. 49. Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Art. 50. Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a Prefeitura Municipal de Juquiá e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

Art. 51. É proibido o compartilhamento de login para funções de administração de sistemas.

Art. 52. A Diretoria de Recursos Humanos, é a responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

Art. 53. O Departamento de TI responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

Art. 54. Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas.

Art. 55. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Art. 56. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

Art. 57. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.

Art. 58. Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o Departamento de TI. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Art. 59. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Art. 60. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, a Diretoria de Recursos Humanos, deverá imediatamente comunicar tal fato aos Técnicos da Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Art. 61. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou solicitar pessoalmente à área técnica responsável para cadastrar uma nova.

CAPÍTULO XII
COMPUTADORES E RECURSOS TECNOLÓGICOS

Art. 62. Os equipamentos disponíveis aos colaboradores são de propriedade da Prefeitura, 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.

Art. 63. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um Técnico em Informática, ou de quem este determinar. 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. 64. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no servicedesk.

Art. 65. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Art. 66. Arquivos pessoais e/ou não pertinentes ao negócio da Prefeitura (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Art. 67. Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Art. 68. Os colaboradores da Prefeitura e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização dos Técnicos da TI.

Art. 69. No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

Art. 70. Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

Art. 71. 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 Prefeitura ou por terceiros devidamente contratados para o serviço.

Art. 72. É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

Art. 73. O colaborador deverá manter a configuração do equipamento disponibilizado pela Prefeitura, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

Art. 74. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Prefeitura Municipal de Juquiá:

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

b) Burlar quaisquer sistemas de segurança;

c) Acessar informações confidenciais sem explícita autorização do proprietário;

d) Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);

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

f) 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;

g) Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;

h) Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

CAPÍTULO XIII
DOS DISPOSITIVOS MÓVEIS

Art. 75. A Prefeitura Municipal de Juquiá deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis.

Art. 76. 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 Sistemas, como: notebooks, smartphones e pendrives.

Art. 77. Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

Art. 78. A Prefeitura, 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.

Art. 79. O colaborador, 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 Prefeitura, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Art. 80. Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não carregá-los juntos.

Art. 81. O suporte técnico aos dispositivos móveis de propriedade da Prefeitura Municipal de Juquiá e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Art. 82. Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Art. 83. 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 de TI.

Art. 84. O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da tecnologia da informação da Prefeitura.

Art. 85. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

Art. 86. É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

Art. 87. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Prefeitura de Juquiá, notificar imediatamente seu gestor direto e os técnicos de TI. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

Art. 88. O colaborador 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 Prefeitura de Juquiá e/ou a terceiros.

Art. 89. O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da Prefeitura de Juquiá deverá submeter previamente tais equipamentos ao processo de autorização do Departamento de TI.

Art. 90. Equipamentos portáteis, como smartphones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

CAPÍTULO XIV
BACKUP

Art. 91. Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" - períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Art. 92. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas freqüentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

CAPÍTULO XV
DAS DISPOSIÇÕES FINAIS

Art. 93. Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Prefeitura, ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

Art. 94. Este Decreto entra em vigor na data de sua publicação.

PREFEITURA MUNICIPAL DE JUQUIÁ, 19 DE JANEIRO DE 2023.

GILBERTO TADASHI MATSUSUE
Prefeito Municipal

VINÍCIUS KABATA
Secretário Municipal de Governo e Administração

PAULA RIGUETE DA VEIGA
OAB/SP 348.657
Secretária Municipal de Assuntos Jurídicos

TERMO DE RESPONSABILIDADE

Eu, _____, matrícula n.º _____, CPF n.º _____, RG n.º _____,lotado(a) no(a) _____ocupante do cargo de _____, doravante denominado simplesmente SERVIDOR, em razão do seu vínculo com a Prefeitura Municipal de Juquiá, com sede na Rua Mohamad Said Hedjazi, nº 42- Bairro Floresta, nesta cidade de Juquiá/SP, CEP. 11.800-000, inscrito no CNPJ sob o nº 46.585.964/0001-40, doravante denominado PREFEITURA, firma o presente TERMO DE RESPONSABILIDADE, mediante as estipulações consignadas neste instrumento:

1. O SERVIDOR declara expressamente, por neste ato:

1.1. Conhecer os termos do Decreto nº 2036/2023, de 19 de janeiro de 2023, (Política de Segurança da Informação) e demais normas e procedimentos em segurança da informação da Prefeitura;

1.2. Estar ciente de minhas obrigações quanto à salvaguarda das informações por mim acessadas em virtude de minhas atribuições funcionais na Prefeitura;

1.3. Estar em concordância em cumprir os regulamentos apresentados, ciente de que o seu não cumprimento poderá acarretar a aplicação de sanções administrativas, civis e penais, na forma da Lei;

1.4. Estar ciente de que não devo criar expectativa de privacidade em relação a minhas atividades no ambiente computacional corporativo e que meus acessos poderão ser registrados, auditados ou investigados pela Prefeitura em caso de incidentes de segurança da informação.

2. Este Termo tem natureza irrevogável e irretratável, vigorando a partir da data de sua assinatura. E por estar de acordo com o inteiro teor deste Termo, o assina nesta data, para que produza seus jurídicos e legais efeitos.

_____, ___/___/_____.

_____