TERESÓPOLIS
acima de tudo!

Ciência e Tecnologia

PLANO OPERACIONAL POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Anexo ao Decreto nº 6018/2023

Versão 3.0

Janeiro / 2025

TERÊGOV DIGITAL

Prefeitura Municipal de Teresópolis

Secretaria Municipal de Ciência e Tecnologia

GESTÃO

José Leonardo Vasconcellos de Andrade
Prefeito

André Muniz Pinto
Secretário Municipal de Ciência e Tecnologia

Larissa Pinheiro Rezende do Nascimento
Subsecretária Municipal de Ciência e Tecnologia

Cleiton Evandro Corrêa Pimentel
Diretor de Governança e Dados

Edmo de Macedo Gonçalves
Assessor Administrativo

André Washington Garcia Suarez
Gestor de Infraestrutura / Rede
Encarregado de Proteção de Dados (DPO)

Carlos Augusto Vargas
Gestão de Sistemas

Bernardo Rodrigues de Oliveira
Analista Técnico

Gabriel da Costa Garcia
Analista Técnico

Giorgia Pietroluongo Holig
Estagiário / Segurança da Informação

INTRODUÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes institucionais do município de Teresópolis para a proteção dos ativos de informação e a prevenção de riscos para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da Administração Pública Municipal.

A presente PSI está baseada nas recomendações propostas pelas normas **ABNT/NBR ISO/IEC 27001 e 27002:2005**, que compõem a **Família ISO/IEC 27000**, sendo reconhecida mundialmente como códigos de práticas para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país, onde enfatizamos a legislação que trata do acesso à informação e proteção de dados pessoais.

1.1 OBJETIVOS da PSI

Estabelecer diretrizes que permitam aos colaboradores do município de Teresópolis seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seus atendimentos.

A proteção e preservação das informações do município de Teresópolis deverá observar os seguintes princípios:

- **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.
- **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

• **Autenticidade**: garante a verdadeira autoria da informação, ou seja, garante integridade da informação.

1.2 APLICAÇÕES DA PSI

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 das referidas empresas poderão ser monitorados e gravados, com prévias informações, conforme previstas nas leis brasileiras.

É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação dos seus gestores, DPO, Segurança da Informação – SI e/ou da Diretoria de TI sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

1.3 PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da de atividade profissional contratadas pelo município de Teresópolis 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.

O município de Teresópolis, por meio dos seus Gestores, de Segurança da Informação, DPO e/ou da Diretoria de TI, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

1.4 REQUISITOS DA PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da Prefeitura Municipal de Teresópolis a fim de que a política seja cumprida no âmbito do setor público, conforme prevê Legislação Correlata e Contrato firmado entre as partes. 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 das Gestores de Segurança e TI.

Deverá constar em todos os contratos do município de Teresópolis o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela Administração Pública.

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. Eles devem assinar um termo de responsabilidade. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Secretaria Municipal de Ciência e Tecnologia, através de seus representantes legais, como tais os Gestores de Segurança da Informação e/ou de TI para análise.

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 ativosde informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser acompanhados pelos seguintes agentes: Gestor de Segurança da Informação e TI – Secretaria Municipal de Ciencia e Tecnolgia, a fim de que possam 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.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades - LOGs, 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 pelo município de Teresópolis ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação. O município de Teresópolis 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.

Esta PSI será implementada no município de Teresópolis por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função da Municipalidade, 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 da instituição e sujeitará os usuários às medidas administrativas e legais cabíveis.

1. DAS RESPONSABILIDADES ESPECÍFICAS

3.1 - Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada por regime da CLT, Cargos Comissionados, bem como os prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao município de Teresópolis e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas serão responsabilizados e podendo sofrer punições, de acordo com o Decreto Municipal nº 6018/2023.

3.1 - Dos Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelos Gestores Técnicos de SI e TI. 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 contratual.

3.2 - Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

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 do município de Teresópolis.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, segundo a Lei de Acesso à Informação (LAI), lei nº 12.527 de 18 de Novembro de 2011, mesmo quando desligado, sobre todos os ativos de informações do município de Teresópolis.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade 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.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

4 DA AREA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - TIC

Testar a eficácia dos controles utilizados e informar aos gestores técnicos de SI e TI os riscos incidentais, residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar 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.

Os administradores e operadores dos sistemas computacionais podem e tem o dever de agir, pelas características de seus privilégios como usuários, 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 - (BACKUPs), auditorias ou testes no ambiente.

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 auditorias das suas próprias ações.

Garantir segurança especial para sistemas com acesso público - (Portais e Sites Institucionais), fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação e notificações de incidentes a ANPD, seguindo as Diretrizes da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD, regulamentado pelo Decreto Municipal 5932, de 09 de março de 2023.

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

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o município deTeresópolis.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela SI/TIC, nos ambientes totalmente controlados por elas.

Os gestores da Segurança da informação e de TIC devem ser previamente informados sobre o fim do prazo de retenção, estipulados por Decreto Municipal, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

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

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

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável - (Gerentes de Sistemas), como pessoa física, sendo que:

- os usuários (logins), com acessos individuais de responsabilidade, não podendo ser emprestados, em hipótese alguma, com isso ferindo o – Princípio da Confidencialidade e Privacidade Hierárquica dos Dados no Sistema Geral de Segurança da Informação – SGSI, podendo ser responsabilizado e com isso, sofrer Penalização, de acordo com o Decreto 6018/2018;
- os usuários (logins) de terceiros serão de responsabilidade dos usuários dos mesmos, respondendo sofrer Sanções Disciplinares, solidariamente os Usuários, Gerentes de Unidades e Gestores das áreas em questão, de acordo com o Decreto 6018/2023;

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, via Software antivírus e/ou similares e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado, passando por averiguação rígida, pelo Departamento competente de TIC - (Departamento de Infraestrutura e Redes).

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 responsabilizaçãono caso de uso de terceiros.

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 no âmbito da administração pública de Teresópolis, em suas dependências Funcionais.

Realizar auditorias periódicas de configurações técnicas e análise de riscos, das empresas terceirizadas, juntamente com representante legal do Departamento de TI da municipalidade, afim de garantir a Integridade dos Dados e Confiabilidade, que são pilares da Segurança da Informação.

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

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, sendo imediatamente comunicado ao Departamento de Governança de Dados deste município, para as devidas providencias e comunicação as autoridades competentes .

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

Monitorar o ambiente de TIC, 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);

4 Da Área de Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação, conforme preconiza a Lei N. 13709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS - LGPD.

Propor e apoiar iniciativas que visem à segurança dos ativos de informação do município de Teresópolis.

Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Chefe do Executivo, juntamente com o Secretário responsável pela cadeira da Secretaria Municipal de Ciência e Tecnologia e demais Secretários envolvidos no processo, e evidamente observado pelo Comitê Gestor de Proteção de Dados e pelo Comitê de Governo Digital.

Promover a conscientização dos colaboradores, funcionários, em relação à relevância da segurança da informação, mediante campanhas, palestras, treinamentos e outros meios de endomarketing com a confecção de Cartilhas Educativas, Ebooks, Sites, em obediência ao Principio da Publicidade Constitucional, (CF/1988).

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços, seguindo como Diretrizes normativas as ISOs da familia N. 27.000 e congeneres, bem como as demais normas aplicáveis.

4.1 Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta PSI, o município deTeresópolis poderá:

- 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;
- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior);
- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;
- Restrição de uso de Redes sociais - (Facebook, Instagram e Similares), nos horários de expediente, bem como uso de APPs de bate-papos - (Whatsapp, Telegram e Similares), a fim de garantir a

celeridade dos serviços ao cidadão, sendo passível de Responsabilização e Penalizações em decorrência de Lei Vigente para tal situação – vide Decreto Municipal 6018/2023.

4.2 CORREIO ELETRÔNICO

O objetivo desta norma é informar aos colaboradores da Prefeitura Municipal de Teresópolis quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico das estruturas administrativas do município de Teresópolis é para fins institucionais e relacionados às atividades dos servidores dentro da instituição. Não será permitida a utilização desse serviço para fins pessoais.

A Instrução Normativa para a utilização de e-mails instuitucionais é parte integrante desta política de segurança da informação de Teresópolis.

Nenhuma estrutura administrativa ou de seus representantes poderão usar e-mails fora do domínio contido na Instrução Normativa.

Deve-se ter especial atenção em todos os e-mails, na observância de riscos potenciais em que:

- contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- vise obter acesso não autorizado a outro computador, servidor ou rede;
- vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- vise burlar qualquer sistema de segurança; vise vigiar secretamente ou assediar outro usuário;
- vise acessar informações confidenciais sem explícita autorização doproprietário;
- vise acessar indevidamente informações que possam causar prejuízos aqualquer pessoa;

- inclua imagens criptografadas ou de qualquer forma anonimizadas, (LGPD, 2018);
- contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)
- tenha conteúdo considerado impróprio, obsceno ou ilegal;
- seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas; tenha fins políticos locais ou do país (propaganda política);
- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico institucionais, sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador (Servidor Efetivo, Cargo Comissionado);
- Gestor, Gerência ou Departamento;
- Nome da empresa;
- Telefone(s);
- Correio eletrônico institucional.

4.3 INTERNET

Todas as regras atuais da Prefeitura Municipal de Teresópolis 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 aporta para riscos significativos para os ativos de informação, pertencentes a Municipalidade.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a Prefeitura Municipalde Teresópolis, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos as mesmas.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de responsabilidade da instituição (Prefeitura Municipal de Teresópolis), que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio e/ou aplicações armazenados na rede/internet, estejam eles em disco local, nas estações de IClaud(Nuvem) ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação - PSI.

A Prefeitura Municipal de Teresópolis, ao monitorar a rede interna, Nuvem ou qualquer outra forma de armazenamento de dados, 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 dequalquer 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.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, não poderá ser utilizada para fins pessoais, somente em casos de prévia autorização por parte dos Gestores das devidas Secretarias, acusando prévia justificativa, que será analisada pela Secretaria Municipal de Ciência e Tecnologia, desde que não prejudique o andamento dos trabalhos na instituição.

Como é do interesse da Prefeitura Municipal de Teresópolis 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.

Somente os colaboradores que estão devidamente autorizados a falar em nome da Prefeitura Municipal de Teresópolis para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, Podcast, seja por documento físico, entre outros.

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.

É proibido o uso, em horário de expediente, e 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.

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na Prefeitura Municipal de Teresópolis e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Diretoria de TIC, bem como seguirem às normas e orientações do Comitê de Governo Digital.

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, sem nenhuma exceção.**
Qualquer software não autorizado baixado será excluído pelo Departamento deTIC.
Os colaboradores não poderão em hipótese alguma utilizar os recursos da Prefeitura Municipal de Teresópolis para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com alegislação nacional.

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.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso, cabendo responsabilização do usuário e respondendo Processo Administrativo junto a Procuradoria Geral, vide Decreto 6018/2023, bem como outras medidas cabíveis.
Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado a Prefeitura Municipal de Teresópolis ou de dados de

sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo Departamento de TIC da Secretaria Municipal de Ciência e Tecnologia, podendo sofrer as sanções derivadas do Decreto Municipal vigente 6018/2023 e demais normativas pelo Comitê de Governo Digital.
Os colaboradores não poderão utilizar os recursos da Prefeitura Municipal de Teresópolis para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, de qualquer tipo, perturbação ou programas de controle de outros computadores, caso ocorra algum destes delitos, ocasinar-se-á, Processo Administrativo Perante a Procuradoria desta Municipalidade e sendo reincidente passivo de Demissão e/ou Exoneração, vide Decreto 6018/2023.

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 da Secretaria Municipal de Ciência e Tecnologia via Departamento de TIC. Não é permitido acesso a sites de proxy, cabendo punição Disciplinar.

4.4 **IDENTIFICAÇÃO**

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar poroutra perante a Prefeitura Municipal de Teresópolis e/ou terceiros.
O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 - falsa identidade).

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

Todos os dispositivos de identificação utilizados na Prefeitura Municipal de Teresópolis, 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.

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

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

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a Prefeitura Municipal de Teresópolis e a legislação (civil e criminal) será solidária entre o Secretario Gestor, a Chefia imediata e os usuários que deles se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado o mesmo deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas, caso aconteça, a chefia imediata responderá solidariamente com usuário, dono da credencial, vide Decreto 6018/2023.

O Departamento de Recursos Humanos da Prefeitura Municipal de Teresópolis é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

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

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

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá troca imediatamente a sua senha conforme as orientações apresentadas, conforme especificado no Código de Condutas dos Funcionários Públicos Municipais – Compliance, Decreto 6018/2023.

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

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, comopróprio 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.

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 TIC, Setor de Sistemas. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Os usuários devem alterar, com frequência minima de 02 (dois) meses, a própria senha, e devem ser orientados e se possivel, lembrados via sistemas, a fazê-lo.Em caso de suspeitas de que terceiros venham a obter acesso indevido ao seu login/senha, seja reformulada nova senha imediatemente.
Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato a Secretaria Municipal de Ciência e Tecnologia via Departamento de Tecnologia da Informação e Comunicação, 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.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a sua chefia imediata, a troca da mesma, à área técnica responsável, que é o Departamento de TIC, cujo ser uma de suas prerrogativas cadastrar uma nova.

4.5 **COMPUTADORES E RECURSOS TECNOLÓGICOS**

Os equipamentos disponíveis aos colaboradores são de propriedade da Prefeitura Municipal de Teresópolis, 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.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do Departamento de TIC, 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.

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 de TIC, responsável mediante registro de chamado no servicedesk.

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.

Arquivos pessoais e/ou não pertinentes ao negócio da Prefeitura Municipal de Teresópolis (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 deverão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

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.

Os colaboradores da Prefeitura Municipal de Teresópolis e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede desta Municipalidade sem a prévia solicitação e a autorização da Secretaria Municipal de Ciência e Tecnologia via Departamento de TIC.

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

- Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pelo Departamento de TI da Prefeitura Municipal de Teresópolis, que terá acesso a elas para manutenção

dos equipamentos, sob a Gestão da Secretaria Municipal de Ciência e Tecnologia;

- Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;
- 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 do Departamento de TIC, credenciado pela Secretaria de Ciência e Tecnologia ou por terceiros devidamente contratados;
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidadede uso para planos de contingência mediante a autorização dos gestores das áreas e da área de TIC.
- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesade trabalho e próximo aos equipamentos.
- O colaborador deverá manter a configuração do equipamento disponibilizado pela Prefeitura, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação - PSI e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.
- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.
- Todos os recursos tecnológicos adquiridos pela Prefeitura Municipal de Teresópolis devem ter imediatamente suas senhas padrões (default) alteradas.

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

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Prefeitura Municipal de Teresópolis.

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede, sem autorização prévia – TESTE DE PENETRAÇÃO OU PENTESTs;
- Burlar quaisquer sistemas de segurança – USO DE TECNICAS HACKERs BLACKHATs;
- Acessar informações confidenciais sem explícita autorização do proprietário– USO DE TECNICAS HACKERs BLACKHATs;
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual ou moral, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

4.6 DISPOSITIVOS MÓVEIS

A Prefeitura Municipal de Teresópolis deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis. 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, devendo passar pelo Departamento de SI/TIC, para assegurar a integridade dos mesmos.

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.

A Prefeitura Municipal de Teresópolis, na qualidade de proprietário ou contratante dos

equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.
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 Municipal de Teresópolis, mesmo depois de terminado o vínculo contratual mantido com a instituição.

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.
O suporte técnico aos dispositivos móveis de propriedade da Prefeitura Municipal de Teresópolis e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.
Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

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 do Departamento de TIC.

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 do Departamento de TIC da Prefeitura Municipal de Teresópolis.
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.

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

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivomóvel fornecido pela Prefeitura Municipal de Teresópolis, notificar imediatamente seu gestor direto e o Departamento de TIC. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

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 oúnico responsável por quaisquer danos, diretos ou indiretos, presentes oufuturos, que venha causar a Prefeitura Municipal de Teresópolis e/ou a terceiros.

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

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.

4.7 **DATACENTER**

O acesso ao Data center somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros.

Todo acesso ao Data center, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.

Deverá ser executada semanalmente uma auditoria nos acessos ao Data center por meio do relatório do sistema de registro.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do coordenador de infra-estrutura, de acordo com o Procedimento de Controle de Contas Administrativas.

A lista de funções com direito de acesso ao Data center deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Data center, e salva no diretório de rede.

Nas localidades em que não existam colaboradores da área de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do Data center, como: troca de fitas de backup, suporte em eventuais problemas, e assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao Data center, bem como

assinar o Termo de Responsabilidade.
O acesso ao Data center, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Data center for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração deliberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Data center.
O Data center deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.
Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.
A entrada ou retirada de quaisquer equipamentos do Data center somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Data center, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.
No caso de desligamento de empregados ou colaboradores que possuamacesso ao Data center, imediatamente deverá ser providenciada a sua exclusãodo sistema de autenticação forte e da lista de colaboradores autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Data center.

4.7 **BACKUP**

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.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes 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.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Data center.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controladopelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.
É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.
Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.
É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da Prefeitura Municipal de Teresópolis, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logono primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e Restore.

Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.
Para formalizar o controle de execução de backups e restores, deverá haverum formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infra-estrutura, nos termos do Procedimento de Controle de Backup e Restore.
Os colaboradores responsáveis descritos nos devidos procedimentos e naplanilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

5 DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Prefeitura Municipal de Teresópolis. Qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição e pela legislação vigente.