# PSTIC - POLÍTICA DE SEGURANÇA DE TECNOLOGIA, INFORMAÇÃO E COMUNICAÇÃO

## Diretrizes e Normas

| | |
|---|---|
| **ELABORADO/MODIFICADO** | **APROVADO: 11-02-2021** |
| **Nome: Tercio Passos da Fonseca** | |
| **Nome: Ualace Leal Martins** | |
| **Nome: Patryck Soares de Moura Barbosa** | |

## 1. JUSTIFICATIVA

A **POLÍTICA DE SEGURANÇA DE TECNOLOGIA, INFORMAÇÃO E COMUNICAÇÃO**, também referida como PSTIC, é o documento que orienta e estabelece as diretrizes corporativas da Prefeitura Municipal de Piraí 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 instituição. A presente PSTIC 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. Com a intenção de aumentar a segurança da infraestrutura tecnológica direcionada ao uso institucional, foi desenvolvida paralelamente uma Norma de Segurança da Informação, visando a orientação de nossos clientes para a utilização dos ativos de tecnologia da informação disponibilizados.

Tais documentos encontram-se disponíveis na intranet da Prefeitura Municipal de Piraí, na seção **Normas Tecnológicas**.

## 2. OBJETIVO

Estabelecer diretrizes que permitam aos colaboradores, prestadores de serviço e usuários da Prefeitura Municipal de Piraí seguirem padrões de comportamento relacionados à segurança tecnológicas 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 seu atendimento. Preservar as informações da Prefeitura Municipal de Piraí quanto à:

- 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.

Expressar formalmente as normas de utilização, de todos os recursos e sistemas informatizados utilizados nesta Prefeitura, para discernir as atividades que são consideradas como violação ao uso dos serviços e recursos, os quais são considerados proibidos e incentivar boas práticas que envolvem a segurança de dados, tráfego, conexão e armazenamento.

## 3. APLICAÇÂO

Estas normas se aplicam a todos os órgãos e departamentos que compartilham da infraestrutura tecnológica da Prefeitura Municipal de Piraí.

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e usuários 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 Prefeitura Municipal de Piraí poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. É também obrigação de cada colaborador se manter atualizado em relação a esta PSTIC e aos procedimentos e normas relacionadas, buscando orientação do seu Gestor ou Responsável Superior para nível de informação e ciência e também um contato com o Departamento de Gerência de Projetos, Redes e Sistemas na Secretaria Municipal de Ciência e Tecnologia sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

## 4. PRINCÍPIOS DA PSTIC

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pelo Prefeitura Municipal de Piraí 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, serviços e segurança de redes. A Prefeitura Municipal de Piraí, por meio da Secretaria Municipal de Ciência e Tecnologia/ Departamento de Projetos, Redes e Sistemas, poderá registrar todo o uso dos Sistemas, Serviços de Acesso, Armazenamento e Segurança de Redes, visando garantir a disponibilidade e a segurança das informações utilizadas.

## 5. DEFINIÇÕES

Recursos de TI: Equipamentos e dispositivos utilizados pelos colaboradores tais como: Notebooks e Desktops (gabinete, monitor, teclado, mouse, e outros periféricos), tablets, celulares, impressoras, scanners, dispositivos de conexão a borda e ao core de rede, bem como serviços de TI: e-mails, domínio pirai.rj.gov.br, piraidigital.com.br, links de internet, softwares e afins.

Sistema SGP (Sistema de Gestão Pública) são sistemas de informação que integram todos os dados e processos da organização, contemplando os Sistemas não Estruturantes (SIAFIC – Sistemas Orçamentário, Financeiro e Patrimonial) e os Sistemas de Apoio Estruturantes (E-mail Corporativo, NFe, Protocolo, Frotas, PPA Web, Indicadores, Contratos Web, Procom Digital, Iluminação Pública, Cemitério, Materiais e Serviços). A integração pode ser vista sob perspectiva funcional e sistêmica (sistemas de processamento de transações,

de informações gerenciais, de apoio a decisão...). Generalizando, são plataformas de softwares desenvolvidas para integrar os diversos Departamentos da Prefeitura Municipal de Piraí, possibilitando a automação e armazenamento de todas as informações de negócios/gestão.

## 6. REQUISITOS DA PSTIC

Para a uniformidade da informação, a PSTIC deverá ser comunicada a todos os usuários e colaboradores da Prefeitura Municipal de Piraí a fim de que a política seja cumprida dentro e fora da instituição. Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da tecnologia e informação, doravante designado como Comitê de Gestão e Segurança de Tecnologia e Informação (CGSTIC). Tanto a PSTIC quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Gestão de Segurança.

Deverá constar em todo os contrato da Prefeitura Municipal de Piraí 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 instituição.

A responsabilidade em relação à Segurança da Tecnologia, Informação e Comunicação (PSTIC) 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. Esta responsabilidade e sansões serão apresentadas por meio de um ***Formulário de Termo de Compromisso e Ciência (TCC) – Anexo I***, que dará ciência aos procedimentos de Segurança a qual o colaborador ou usuário terá de se adequar. O formulário será disponibilizado pela Secretaria Municipal de Ciência e Tecnologia por meio do Departamento de Projetos, Redes e Sistemas. Este procedimento de anuência deverá ser realizado após admissão do funcionário.

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/ Departamento de Projetos, Redes e Sistemas e ela, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Gestão e Segurança da Tecnologia, Informação e Comunicação (CGSTIC) 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 ativos de informação.

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.

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, tablets, celulares, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pelo Secretaria Municipal de Tecnologia 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. E somente deverão ser implementados em produção sistemas que passaram por toda a fiscalização, auditoria, testes e homologação de implantação para que possa haver a garantia de funcionamento com o mínimo de riscos.

A Prefeitura Municipal de Piraí 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 PSTIC será implementada na Prefeitura Municipal de Piraí por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função exercida, bem como de vínculo empregatício ou prestação de serviço.

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

## 7. RESPONSABILIDADES

Secretaria de Municipal de Ciência e Tecnologia: Órgão responsável por prestar aos colaboradores da Prefeitura Municipal de Piraí serviços de alta qualidade e, ao mesmo tempo, desenvolver um comportamento extremamente ético e profissional em relação aos serviços e recursos de informática, telecomunicações, redes, cybersegurança, tecnologias IoT, transmissões online, sistemas, desenvolvimento e programação, gestão e gerência tecnológica, videomonitoramento, análise, armazenamento e gestão de dados, além de ser a responsável por gerenciar e analisar a aplicação das normatizações, aos serviços de terceiros dentro da Área de Tecnologia que são oferecidas á Prefeitura Municipal de Piraí. Assim, para

assegurar os altos padrões de qualidade na prestação desses serviços, faz-se necessária a definição de uma política de procedimentos de segurança e utilização destes recursos e serviços.

Usuário(a): Cumprir o estabelecido no procedimento.

### 7.1. DAS RESPONSABILIDADES ESPECÍFICAS

#### 7.1.1. DOS COLABORADORES E USUÁRIOS EM GERAL

Entende-se por colaborador toda e qualquer pessoa física, do quadro efetivo, estágio, contratados, CLT ou 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 a Prefeitura Municipal de Piraí e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

#### 7.1.2. DOS COLABORADORES EM REGIME DE EXCESSÃO (TEMPORÁRIOS)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Gestão e Segurança da Tecnologia, Informação e Comunicação (CGSTIC). 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.

#### 7.1.3. DOS GESTORES DE PESSOAS E/OU PROCESSOS

Ter postura exemplar em relação à Segurança de Tecnologia, informação e Comunicação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de admissão, contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSTIC da Prefeitura Municipal de Piraí. Exigir dos colaboradores a assinatura do ***Formulário de Termo de Compromisso e Ciência (TCC) – Anexo I***, 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 Piraí.

Antes de conceder acesso às informações da instituição, exigir a assinatura do ***Acordo de Confidencialidade dos Colaboradores (ACC) – Anexo II***, 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.

Os processos e procedimentos de Sistemas de Gestão da Execução Orçamentária, Administração Financeira e Controle, também devem atender o decreto do Governo Federal de n.º 10.540 de 05 de novembro de 2020 (SIAFIC). Antes de conceder o acesso aos Sistemas de Gestão, exigir o preenchimento e assinatura do ***Formulário de Registro de Controle SIAFIC – Anexo III***.

A Lei nº 12.965, de 23 de abril de 2014 estabeleceu o Marco Civil de Internet no Brasil norteou princípios, garantias, direitos e deveres para o uso da Internet e determinou as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à ações e procedimentos relacionado ás áreas de Segurança de Sistemas, Internet e Dados como por exemplo os Registros e Controle de Acessos aos Sistemas e Internet, que fazem parte de procedimentos já implementadas na estrutura tecnológica corporativa da Prefeitura Municipal de Piraí por meio de Normatizações e Políticas internas.

Como complemento ao Marco Civil da Internet, ao tratar de valores, como o respeito à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico e a inovação; à livre iniciativa, livre concorrência e defesa do consumidor e aos direitos humanos de liberdade e dignidade das pessoas, o Sistema de Gestão de Segurança de Tecnologia, Informação e Comunicação (SGSTIC) se desenvolve também com prerrogativas da Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP), de nº 13.709/2018, sendo a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

A PSTIC abrangerá um conjunto de novos conceitos jurídicos na Lei LGPD referente a "dados pessoais", "dados pessoais sensíveis", estabelecendo as condições nas quais os dados pessoais podem ser tratados, definindo um conjunto de direitos para os titulares dos dados, gerando obrigações específicas para os controladores dos dados e criando uma série de procedimentos e normas para que haja maior cuidado com o tratamento de dados pessoais e compartilhamento com terceiros. A lei se aplica a toda informação relacionada a pessoa natural identificada ou que possa ser identificável e aos dados que tratem de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, sempre que os mesmos estiverem vinculados a uma pessoa natural.

Ações e penalizações relacionadas as violações de segurança são calçadas na lei de n.º 12.737/2012 popularmente conhecida como “Lei Carolina Dieckmann” que alterou o Código Penal Brasileiro e incluiu tratativas voltada para crimes virtuais e delitos informáticos. Com o avanço da tecnologia e a democratização e o acesso facilitado às redes sociais, o sistema judiciário brasileiro viu a necessidade de tipificar crimes cometidos no ambiente virtual pois acrescenta os artigos 154-A e 154-B ao Código Penal

Brasileiro. Além disso, altera a redação dos artigos 266 e 298. A norma trata de uma tendência do Direito: segurança no ambiente virtual com a redação prevendo os crimes que decorrerem do uso indevido de informações e materiais pessoais que dizem respeito à privacidade de uma pessoa na internet, como fotos e vídeos.

A estruturação da PSTIC tem como referência base a ISO/IEC 27001 e a ISO 27002 que são normas internacionais publicadas pela Standardization Organization (ISO) e pela International Electrotechnical Commission (IEC). Elas definem, respectivamente, os requisitos e as melhores práticas, e suas aplicações serão implementadas em consonância com os Componentes de Controle e Normatização do Sistema de Gestão de Segurança de Tecnologia, Informação e Comunicação (SGSTIC) da Prefeitura Municipal de Piraí.

Aos gestores, cabe adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSTIC, bem como aos termos específicos de normatização de cada área.

## 8. APLICAÇÕES E PROCEDIMENTOS RELACIONADOS AS ÁREAS DE TECNOLOGIA

### 8.1. ÁREA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

- ✓ Testar a eficácia dos controles utilizados e informar aos gestores os riscos 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 PSTIC, e Normas de Segurança da Informação complementares.
- ✓ Os administradores e operadores dos sistemas computacionais podem, pela característica 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, auditorias ou testes no ambiente;
- ✓ Segregar as funções administrativas, operacionais e educacionais 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;
- ✓ Garantir segurança especial para sistemas com acesso público, em todos os ambientes, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação;
- ✓ Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis 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 a Prefeitura Municipal de Piraí;
- ✓ Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela Áreas de TIC (Tecnologia Informação e Comunicação), nos ambientes totalmente controlados por ela.
- ✓ 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.
- ✓ Quando ocorrer movimentação interna dos ativos de TIC (Tecnologia Informação e Comunicação), 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 de negócio;
- ✓ 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:
  - ➢ Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário;
  - ➢ Os usuários (logins) de terceiros, autônomos, estagiários e prestadores de serviço serão de responsabilidade do gestor da área contratante.
- ✓ 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;
- ✓ Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Prefeitura municipal de Piraí em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- ✓ Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivos de áreas específicas que envolvam a TIC (Tecnologia Informação e Comunicação), exigindo o seu cumprimento dentro da empresa;
- ✓ Realizar auditorias periódicas de configurações técnicas e análise de riscos;
- ✓ 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 Prefeitura Municipal de Piraí.
- ✓ Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da Prefeitura Municipal de Piraí 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 da Prefeitura Municipal de Piraí;

- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Prefeitura Municipal de Piraí;
- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante).
- 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);

## 8.2. ÁREA DE SEGURANÇA DA TECNOLOGIA, INFORMAÇÃO E COMUNICAÇÃO

- ✓ Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação;
- ✓ Propor e apoiar iniciativas que visem à segurança dos ativos de informação Da Prefeitura Municipal de Piraí;
- ✓ Publicar e promover as versões da PSTIC e as Normas de Segurança de Tecnologia, Informação e Comunicação, aprovadas pelo Comitê Gestor de Segurança da Tecnologia, Informação e Comunicação (CGSTIC);
- ✓ Promover a conscientização dos colaboradores em relação à relevância da segurança da Tecnologia, Informação e Comunicação (TIC) para o negócio da Prefeitura Municipal de Piraí, mediante campanhas, palestras, treinamentos e outros meios de endomarketing;
- ✓ Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;
- ✓ Analisar criticamente incidentes em conjunto com o Comitê Gestor de Segurança da Tecnologia, Informação e Comunicação (CGSTIC);
- ✓ Apresentar as atas e os resumos das reuniões do Comitê Gestor de Segurança da Tecnologia, Informação e Comunicação (CGSTIC), destacando os assuntos que exijam intervenção do próprio Comitê ou de outros Gestores.
- ✓ Manter comunicação efetiva com o Comitê Gestor de Segurança da Tecnologia, Informação e Comunicação (CGSTIC) sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a Prefeitura Municipal de Piraí.
- ✓ Buscar alinhamento com as diretrizes corporativas da Prefeitura Municipal de Piraí;

## 8.3. COMITÊ GESTOR DE SEGURANÇA DA TECNOLOGIA, INFORMAÇÃO E COMUNICAÇÃO (CGSTIC)

- ✓ Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados por Decreto Municipal para participar do grupo pelo período de dois anos;
- ✓ A composição mínima deve incluir um colaborador de cada uma das Secretaria Municipais e Órgãos Auxiliares.

- ✓ Deverá o CGSTIC reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a Prefeitura Municipal de Piraí;
- ✓ O CGSTIC poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico;
- ✓ Cabe ao CGSTIC:
  - ➢ propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
  - ➢ propor alterações nas versões da PSTIC e a inclusão, a eliminação ou a mudança de normas complementares;
  - ➢ avaliar os incidentes de segurança e propor ações corretivas;
  - ➢ definir as medidas cabíveis nos casos de descumprimento da PSTIC e/ou das Normas de Segurança da Tecnologia, Informação e Comunicação (TIC) complementares.

## 8.4. MONITORAMENTO E AUDITORIA DO AMBIENTE

- ✓ Para garantir que as regras mencionadas nesta PSTIC, sejam aderidas e implementadas, a Prefeitura Municipal de Piraí por meio da Secretaria Municipal de Ciência e Tecnologia, órgão responsável por planejar, executar, monitorar e fiscalizar as ações do PSTIC 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 Secretário Responsável (ou superior) ou por determinação do Comitê Gestor de Segurança da Tecnologia, Informação e Comunicação;
  - ➢ 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.

# 9. DEFINIÇÕES DE PADRONIZAÇÃO E NORMAS DE TECNOLOGIAS E SERVIÇOS

## 9.1. IDENTIFICAÇÃO

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 de Piraí, RJ 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 Piraí, RJ, como o número de registro do colaborador, o crachá, 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 Piraí, RJ 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.

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

O Departamento de Recursos Humanos da Prefeitura Municipal de Piraí, RJ é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores. A Secretaria Municipal de Ciência e Tecnologia (SECTI) é a responsável pela emissão e controles de identificações digitais e de acesso aos recursos, internet e sistemas existentes na Prefeitura Municipal de Piraí, RJ.

A Gerência do Departamento de Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI) responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários de acordo com as normas do PSTIC.

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 trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

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.

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.

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 Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI). Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

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.

A periodicidade máxima para troca das senhas é 180 (Cento e Oitenta) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 90 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. **Portanto, assim que algum usuário for exonerado, demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI), 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 troca ou comparecer pessoalmente ao Departamento de Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI), área técnica responsável para cadastrar uma nova.

### 9.2. CORREIO ELETRÔNICO (E-MAIL)

O objetivo desta norma é informar aos colaboradores da Prefeitura Municipal de Piraí quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo. O uso do correio eletrônico dentro da Prefeitura Municipal de Piraí é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição.

O cliente web de e-mail (webmail) caracteriza-se por uma ferramenta de intercâmbio de informações dentro da rede global da Prefeitura Municipal de Piraí, com alto potencial de automatização de tarefas documentais.

O software é acessado via navegador (browser), porém deverá ser configurado pela Secretaria Municipal de Ciência e Tecnologia (SECTI) por meio do Departamento de Projetos, Redes e Sistemas, conforme solicitação de acesso a qual deverá ser feita através do formulário de solicitação de acesso.

A utilização desta ferramenta de distribuição de documentos e mensagens condiciona os seus usuários a manterem as suas caixas postais organizadas, principalmente quanto ao descarte de mensagens que não serão mais úteis.

A utilização desse serviço não deve ser utilizada para fins pessoais sendo somente permitido seu uso para fins institucionais. O uso responsável é de inteira responsabilidade do usuário

O sistema de e-mail é de propriedade da Prefeitura Municipal de Piraí e destina-se unicamente a ajudar aos seus colaboradores na condução dos negócios da instituição Prefeitura.

A Secretaria Municipal de Ciência e Tecnologia (SECTI) com base nas normas de segurança referenciadas anteriormente adota as seguintes normas e procedimentos sobre o uso do e-mail por seus colaboradores:

- ✓ A Secretaria Municipal de Ciência e Tecnologia tem o direito de entrar no sistema de e-mail, revisar, copiar e deletar qualquer mensagem, desde que sejam detectadas irregularidades e/ou uso indevido da ferramenta. Não presuma que as mensagens sejam confidenciais em função do uso de uma senha, uma vez que essas medidas servem para proteção da Prefeitura Municipal de Piraí, e não dos seus colaboradores que utilizam o sistema;
- ✓ Os usuários de e-mail devem, manter suas mensagens em caráter profissional e evitar usar o sistema para bate-papos e mensagens pessoais;
- ✓ O e-mail não deve ser profano, vulgar, difamatório ou embaraçoso em sua natureza e conteúdo;
- ✓ Os colaboradores da Prefeitura Municipal de Piraí devem reconhecer que as informações confidenciais não devem ser enviadas via e-mail para fora da Prefeitura ou até mesmo para colaboradores dentro da própria Prefeitura, a menos que o recebedor da mensagem esteja autorizado a receber tal informação. Todos devem reconhecer que as informações transmitidas via e-mail podem conter segredos institucionais ou informações confidenciais, e que devem ser tomadas as providências cabíveis para proteger a segurança e tais informações;
- ✓ Os Profissionais Especialistas da Secretaria Municipal de Ciência e Tecnologia podem fornecer orientações sobre as precauções de segurança;
- ✓ Não é permitido o envio e ou recebimento de e-mails que contenham arquivos que não sejam apropriados ao escopo profissional do usuário. Isso vale para os arquivos de vídeo, fotos e multimídia em geral, salvo casos que estes sejam relevantes ao trabalho;
- ✓ O sistema estará bloqueando as mensagens e encaminhando a cópia ao Secretário responsável pelo Departamento de origem do problema, ao qual o usuário pertence, quando necessário;
- ✓ Não é permitido trafegar com "correntes" ou informações que sejam de conduta duvidosa, multiplicando o número de usuários destinatários. E-mails deste tipo são considerados boatos (hoax) e SPAM e, esta prática, poderá acarretar o cancelamento do domínio da Prefeitura Municipal de Piraí pelo Órgão Gestor da Internet no Brasil. Este procedimento resulta em sobrecarga no sistema, afetando as caixas postais dos destinatários com mensagens sem cunho profissional, sendo passível de cancelamento da conta do usuário que faz uso desta ação.

- ✓ Não é permitido receber e replicar as mensagens que se aplicam aos itens acima para listas com cópias ou para vários usuários. Não copiar, ou replicar os arquivos anexados para os dispositivos de armazenamento contidos em seu equipamento ou na rede. (HD, diretórios em geral). As mensagens que se enquadram aos itens acima, deverão ser imediatamente descartadas e deletadas da caixa de entrada.
- ✓ Não deve ser enviado grandes quantidades de informações não solicitadas previamente;
- ✓ A Secretaria Municipal de Ciência e Tecnologia (SECTI) manterá, conforme lhe convier, os endereços de e-mails internos, não sendo autorizada a inclusão de eventuais endereços externos de provedores diversos ou outros endereços que não forem autorizados pela Secretaria Municipal de Ciência e Tecnologia (SECTI).
- ✓ "Empréstimo" de senha é mau procedimento, o qual ensejará em advertência. A reincidência ou contumácia poderá ensejar em processo administrativo disciplinar. Eventual dano constatado, material ou moral, a Prefeitura Municipal de Piraí ou a terceiros, é passível de indenização pelo colaborador que empresta senha e responsabilização pelo dono causado.

Portanto, é proibido aos colaboradores relacionados ao uso do Correio Eletrônico da Prefeitura Municipal de Piraí:

- ✓ ao receber um e-mail, abrir o link em anexo de um site que não seja de conhecimento do colaborador ou usuário e caso haja dúvidas desta referência do link anexado, que o mesmo não seja aberto antes que seja analisado pelos especialistas da Secretaria Municipal de Ciência e Tecnologia (SECTI) para análise diagnóstica e preventiva;
- ✓ enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- ✓ 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;
- ✓ enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o Prefeitura Municipal de Piraí ou suas unidades vulneráveis a ações civis ou criminais;
- ✓ divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- ✓ falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- ✓ apagar mensagens pertinentes de correio eletrônico quando qualquer um dos Departamentos e Setores da Prefeitura Municipal de Piraí estiver sujeita a algum tipo de investigação;
- ✓ produzir, transmitir ou divulgar mensagem que:
  - ➢ contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Prefeitura Municipal de Piraí;
  - ➢ 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 do proprietário;
- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- inclua imagens criptografadas ou de qualquer forma mascaradas;
- contenha anexo(s) superior(es) a 50 MB para envio (interno e internet) e 50 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 sempre deverão incluir assinatura com o seguinte formato:
  - Nome do colaborador
  - Gerência ou departamento
  - Nome da empresa
  - Telefone(s)
  - Correio eletrônico

**9.3. ACESSO A INTERNET**

A ação de utilização do recurso de Acesso à Rede Mundial de informações e serviços (internet), é viabilizada por meio de Conexão a um Provedor de Serviços de Internet por meio de Conexão de Link dedicado e controlada por meio de Equipamentos de Segurança e Acesso (Firewall IDS/IPS, Controladores de Banda, Serviços de Autenticação, etc) de responsabilidade do Departamento de Projetos, Redes e Sistemas (DPRS) da Secretaria Municipal de Ciência e Tecnologia (SECTI).

Caracteriza-se por um navegador (browser) instalado na estação do usuário, devidamente configurado para acesso através de um servidor, sendo executado sobre o ambiente de rede.

O Acesso à Internet é dado através da configuração do navegador na estação e no próprio login de acesso do usuário. A solicitação do acesso deve ser procedida através do preenchimento do Formulário de

***Termo de Compromisso e Ciência (TCC) – Anexo I*** e Formulário ***Acordo de Confidencialidade dos Colaboradores (ACC) – Anexo II***, por meio de solicitação de acesso no Departamento de Projetos e Redes (DPRS) da Secretaria de Ciência e Tecnologia (SECTI).

O Acesso à Internet Corporativo poderá ter ou não limite de horas ou de horário, segundo solicitação do Gestor de cada Unidade ou Setor que fazem uso da mesma.

O Acesso à Internet Pública/ Comunitária é ilimitado abrangendo as regras de controle e leis de Acesso à Internet referenciados nesta PSTIC ao Marco Civil da Internet e a LGPD.

São fatores que configuram a necessidade do acompanhamento e atuação da Secretaria Municipal de Ciência e Tecnologia (SECTI):

- ✓ O acesso da internet em uma porta de entrada na rede da Prefeitura Municipal de Piraí, expondo a ataques de vírus e entidades com fins de manipulação ilícita das propriedades intelectuais da Prefeitura Municipal de Piraí;
- ✓ A utilização da internet acarreta relativa perda de performance no tráfego da rede para o grupo do usuário que a utiliza;
- ✓ A internet caracteriza-se pela diversificação de sites nos quais a Prefeitura Municipal de Piraí não restringe o acesso, salvo sites com risco ou que tenham características maliciosas que necessitem de bloqueio como: pornografia, jogos e atividades subversivas, desta forma limitando o usuário ao acesso de informações restritas a atividades profissionais ligadas a Prefeitura Municipal de Piraí;
- ✓ Não é permitido uso de cartões (pessoais) de crédito ou similares para compra pela internet, via sistema da Prefeitura Municipal de Piraí, configurando falta grave, a Secretaria Municipal de Ciência e Tecnologia (SECTI) não se responsabiliza por qualquer dano que o usuário sofra por estar usando cartões pessoais na rede da Prefeitura Municipal de Piraí, seja cartão de crédito ou movimentação de conta bancária (corrente, poupança etc.).

O acesso à internet é configurado no perfil de rede do usuário requisitante sendo este acesso pessoal e intransferível, onde o usuário é responsável por este recurso e pelos atos cometidos por ações de "empréstimos" de acesso. O "empréstimo" de senha é mau procedimento, o que ensejará, por parte da Secretaria de Ciência e Tecnologia a advertência. A reincidência ou contumácia poderá ensejar em processo administrativo disciplinar. Eventual dano constatado, material ou moral, a Prefeitura Municipal de Piraí ou a terceiros, é passível de indenização pelo colaborador que empresta a senha.

Todas as regras atuais da Prefeitura Municipal de Piraí 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.

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

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 Tecnologia, Informação e Comunicação.

A Prefeitura Municipal de Piraí, 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.

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 nas unidades ou locais de trabalho.

Como é do interesse da Prefeitura Municipal de Piraí 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 Piraí 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 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.

A carga de programas da internet (download) é monitorada, sendo que a Secretaria Municipal de Ciência e Tecnologia (SECTI) tem pleno controle do tráfego dos dados baixados pelos usuários. Os colaboradores com acesso à internet poderão fazer o download (baixa de arquivo da internet para ambiente local) somente de programas ligados diretamente às suas atividades na Prefeitura Municipal de Piraí, mas deverão providenciar o que for necessário para regularizar a licença e o registro desses programas com base em orientações específicas das empresas fornecedoras, desde que autorizados e aprovados tecnicamente pela Secretaria Municipal de Ciência e Tecnologia (SECTI). Vale ressaltar que segundo as normas e padronização de acesso e compartilhamento de arquivos e softwares em rede, somente os Técnicos da Secretaria Municipal de Ciência e Tecnologia (SECTI), com devida autorização em seu usuário com perfil específico, poderá fazer a instalação de qualquer Software necessário para o funcionamento dos Serviços gerais ou específicos que demandem a utilização do mesmo.

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. Qualquer software não autorizado baixado será excluído pela área do Departamento de Projetos, Redes e Sistemas (DPRS).

Os colaboradores não poderão em hipótese alguma utilizar os recursos da Prefeitura Municipal de Piraí, para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional, sendo assim, o usuário/colaborador será responsabilizado administrativamente e de forma criminosa ou penal de acordo com as leis vigentes.

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 no Departamento de Projetos, Redes e Sistemas (DPRS) na Secretaria Municipal de Ciência e Tecnologia (SECTI), o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de cursos relacionados ao desenvolvimento de jogos e afins.

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

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

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

O acesso a softwares peer-to-peer (Microtorrent, BitTorrent e afins) não serão permitidos. Não é permitido acesso a sites de proxy. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (Whatsapp, Telegram, Discord, MS-Teams, Hangout e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente ao Departamento de Projetos, Redes e Sistemas (DPRS) na Secretaria Municipal de Ciência e Tecnologia (SECTI).

A Secretaria Municipal de Ciência e Tecnologia (SECTI) por meio do Departamento de Projetos, Redes e Sistemas (DPRS) monitora o uso da internet nas estações que compõe a sua rede através de ferramentas de análise. O monitoramento do uso da internet é facultado a Secretaria Municipal de Ciência e Tecnologia (SECTI) que detém os direitos sobre os meios informáticos e tecnológicos com exclusividade. As irregularidades serão punidas com advertência e a reincidência poderá acarretar em processo administrativo disciplinar, sem prejuízo das indenizações no caso de dano material ou moral a Prefeitura Municipal de Piraí ou a terceiros, que este tenha que indenizar.

### 9.4. ACESSO A REDE CORPORATIVA

Consiste no meio de tráfego, armazenamento e execução de aplicações e sistemas dentro dos negócios da Prefeitura Municipal de Piraí. Este meio é protegido por níveis de segurança e administrado pela Secretaria Municipal de Ciência e Tecnologia.

O ambiente de rede é composto por servidores de dados, meios físicos de tráfego de dados, estações e ferramentas para execução do mesmo. O usuário possui o recurso dos drivers da rede, composto da seguinte forma: E-mail, internet, pastas do servidor de arquivos, Sistema SGP (Sistemas de Gestão Pública), serviços de impressão, Sistema Planejamento Web (PPA), entre outros.

Não pode ser acessado, exposto, armazenado, distribuído, editado ou gravado através do uso de recursos computacionais da rede:

- ✓ Material de natureza pornográfica, racista e contrário à moral, à ética e aos bons costumes;
- ✓ Jogos, arquivos de músicas e vídeos fora do escopo dos trabalhos da Prefeitura Municipal de Piraí.

A Secretaria Municipal de Ciência e Tecnologia (SECTI) não se responsabiliza por arquivos armazenados nas estações de trabalho para efeito de backup ou integridade. Arquivos que necessitam de

backup devem ser armazenados no servidor de arquivos (Michelangelo) ou em mídias como DVD, Pendrive ou HD Externo.

Havendo utilização irracional dos drivers, constada por auditoria pelo Departamento de Projeto, Redes e Sistemas (DPRS) na Secretaria Municipal de Ciência e Tecnologia (SECTI), esta notificará ao usuário, orientando-o com relação à forma correta de utilização. O usuário estará obrigado a seguir estritamente as orientações da Secretaria Municipal de Ciência e Tecnologia (SECTI). Podendo reincidência ser passível de processo administrativo disciplinar e responsabilização legal relacionados aos danos decorrentes das ações relacionadas ao descumprimento das normas.

O acesso à rede é dado pela Secretaria Municipal de Ciência e Tecnologia (SECTI) por meio do Departamento de Projeto, Redes e Sistemas (DPRS) através da inclusão do funcionário que receberá as chaves de acesso (login e senha).

A solicitação do cadastro é realizada pelo Secretário ou Chefia designada do funcionário ou utilizador terceiro que tenha a necessidade de acesso, sendo este último restrito somente aos privilégios de acesso a terceiros. Todos receberão as chaves de acesso com categorização de privilégios de acordo com níveis de segurança específicos.

Fica determinado que a Secretaria Municipal de Administração (SECADM) por meio do Departamento de Setor Pessoal (RH), órgão responsável pelo desligamento do funcionário na Prefeitura Municipal de Piraí, a responsabilidade de comunicar ao Departamento de Projetos, Redes e Sistemas (DPRS), na Secretaria Municipal de Ciência e Tecnologia (SECTI) o desligamento do funcionário do quadro de funcionários efetivos ou contratados. Fica determinado também a responsabilidade do Gestor da Secretaria Municipal que havia solicitado o acesso a um terceiro que informe o fim de contrato de prestação de serviços para que o mesmo seja retirado dos acessos a ele liberado por solicitação anterior. O não atendimento das orientações deste processo poderá incorrer em responsabilidades administrativas e legais dependendo das ações decorrentes da não retirada do acesso do funcionário e/ou terceiro por parte das Secretarias acima mencionadas por falta de informação de solicitação para este procedimento.

O acesso do usuário/colaborador é pessoal e intransferível, onde o usuário é responsável pelos direitos que lhe são conferidos e pelos atos cometidos por ações de "empréstimos" de acesso. O "empréstimo" de senha constitui falta grave, o que ensejará, por parte da Prefeitura Municipal de Piraí, a advertência formal. A reincidência ou contumácia poderá ensejar em processo administrativo disciplinar, passível de exoneração. Eventuais danos constatados, materiais ou morais, a Prefeitura Municipal de Piraí ou a terceiros, é passível de indenização pelo colaborador que empresta sua senha.

O acesso poderá ser cancelado quando ultrapassar o prazo de validade da senha, ocorrer a rescisão/exoneração de contrato de trabalho do usuário com a Prefeitura Municipal de Piraí; for incorrida má fé na utilização dos recursos do ambiente de rede.

Para ter seu acesso liberado o Usuário/Colaborador precisará elaborar uma senha de tamanho variável possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível. Sugere-se a não utilização de códigos comuns, como o próprio nome, data de nascimento, nomes de parentes, números telefônicos, números sequenciais, como por exemplo 123456, etc.

Antes de ausentar-se do seu local de trabalho, recomenda-se o usuário a fechar todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas e se possível efetuar o logout/logoff da rede ou bloqueio do desktop através de senha. Nunca deixar arquivos da rede em execução (abertos) na hora do almoço ou depois do expediente, pois é exatamente nessas horas (livres) que a Secretaria Municipal de Ciência e Tecnologia (SECTI) agenda manutenções nos servidores de rede, podendo acarretar danos nos arquivos que ficarem "abertos".

Ficam terminantemente proibidas as seguintes ações:

- ✓ Tentativa de obter acessos não autorizados, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como "cracking"). Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;
- ✓ Tentativa de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo "negativa de acesso", provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor;
- ✓ O uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários;
- ✓ O uso de softwares de comunicação instantânea, sem a devida autorização de avaliação técnica de segurança por meio do Departamento de Projetos, Redes e Sistemas (DPRS) da Secretaria Municipal de Ciência e Tecnologia (SECTI) salvo com justificativa de uso e autorização;
- ✓ A utilização de softwares de peer-to-peer (P2P);
- ✓ A utilização de serviços de streaming, tais como Rádios online, Usina do Som e afins;
- ✓ A utilização de software de torrents tais como utorrent, Bit Torrent e afins;
- ✓ Acesso a sites que simulam Proxies;

## 9.5. UTILIZAÇÃO DE SOFTWARES

Constitui-se no ato de manipulação de software (ambientes operacionais, ambientes de rede, aplicativos, ferramentas etc) instalados ou não na estação do usuário.

Caracteriza-se pelo meio de transporte do software (magnético, óptico, ou download), manuais e licença.

A solicitação de instalação de software é efetuada através do sistema de chamados da Secretaria Municipal de Ciência e Tecnologia que efetuará a análise e iniciará o processo de liberação do mesmo.

Os procedimentos para Aquisição de Licenças e Softwares deverão obrigatoriamente ser solicitados a Secretaria Municipal de Ciência e Tecnologia (SECTI) e só serão aprovados após análise e averiguação de forma técnica por parte do Departamento de Projetos, Redes e Sistemas que será o responsável pela elaboração de relatórios de viabilidade técnica/ financeira de acordo com os custos benefícios de mercado e necessidades relacionadas a demanda.

A execução de softwares não licenciados ("piratas") ou de alguma forma tendo seu sistema de bloqueio burlado (utilização de "crack"), será caracterizado como deturpação dos direitos autorais do autor do software, ato este passível de ações legais pelo próprio autor e repudiados pelos padrões de conduta ética da Prefeitura Municipal de Piraí, RJ. A configuração deste ato sujeitará o infrator à advertência e passível de processo administrativo disciplinar, independentemente das indenizações por danos materiais a Prefeitura Municipal de Piraí, RJ ou a terceiros.

## 9.6. UTILIZAÇÃO DE COMPUTADORES E RECURSOS DE HARDWARE

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

Estes podem incluir: computadores, mouses, teclados, impressoras, scanners, notebooks, etc, que estejam instalados ou não na estação do usuário.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Secretaria Municipal de Ciência e Tecnologia (SECTI), ou de quem este determinar. As Secretarias ou Departamentos que necessitarem fazer testes deverão solicitá-los previamente à Secretaria Municipal de Ciência e Tecnologia (SECTI), ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

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 ou ativadas (Windows Defender) e atualizadas permanentemente. O tipo de antivírus e a escolha do mesmo deverá passar por análise técnica da Secretaria Municipal de Ciência e Tecnologia (SECTI). O usuário, em caso de

suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável da Secretaria Municipal de Ciência e Tecnologia (SECTI) mediante registro de chamado no service desk (GLPI).

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 Piraí, RJ, (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 sem comunicação prévia ao usuário***. Caso haja a necessidade de formatação do Sistema Operacional, a Secretaria Municipal de Ciência e Tecnologia (SECTI) não se responsabiliza pelo Backup de informações pessoais e só serão feitos backups de informações utilizadas pelos Sistemas e Atividades relacionadas ao trabalho ser desenvolvido pelo colaborador/ usuário. Portanto, tais informações e arquivos, quando encontrados, poderão ser excluídos permanentemente sem nenhuma responsabilidade por parte da Secretaria Municipal de Ciência e Tecnologia (SECTI) visto que o colaborador já terá a ciência deste procedimento após assinar os Anexos I, II e III identificados anteriormente neste PSTIC.

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 Piraí, 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 da Gerência do Departamento de Projetos, Redes e Sistemas.

Caracteriza-se pelo uso de seus meios físicos ou acesso aos equipamentos, sendo observadas as seguintes regras:

- ✓ Todos os computadores de uso individual deverão ter senha de Bios (interessante, porém deve-se ter organização para não acontecer como as senhas de admin) para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pelo Departamento de Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI), e deverá ser executada pelo Departamento de Manutenção de Computadores que terá acesso a elas para manutenção dos equipamentos.
- ✓ Os colaboradores devem informar a Secretaria Municipal de Ciência e Tecnologia (SECTI) por meio do Sistema Help Desk 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 Manutenção de Computadores ou do Departamento de Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI) ou por terceiros devidamente contratados para o serviço.

- ✓ Qualquer acesso à Internet de forma interna ou externa que não seja o aprovado pelo Departamento de Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI) devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas ou vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização do Departamento de Projetos, Redes da Secretaria Municipal de Ciência e Tecnologia (SECTI).
- ✓ É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
- ✓ O colaborador deverá manter a configuração do equipamento disponibilizado pela Prefeitura Municipal de Piraí, RJ, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Tecnologia, Informação e Comunicação (PSTIC) 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 Piraí 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.
- ✓ É proibido o uso de computadores e recursos tecnológicos para tentar obter acesso não autorizado a outro computador, servidor ou rede.
- ✓ É proibido o uso de computadores e recursos tecnológicos para burlar quaisquer sistemas de segurança.
- ✓ É proibido o uso de computadores e recursos tecnológicos para acessar informações confidenciais sem explícita autorização do proprietário.
- ✓ É proibido o uso de computadores e recursos tecnológicos para vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- ✓ É proibido o uso de computadores e recursos tecnológicos para interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- ✓ É proibido o uso de computadores e recursos tecnológicos para 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;
- ✓ É proibido o uso de computadores e recursos tecnológicos para hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- ✓ É proibido o uso de computadores e recursos tecnológicos para utilizar software pirata, atividade considerada ilícita de acordo com a legislação nacional.

- ✓ É proibida a instalação ou remoção de hardwares, inclusive os PenDrivers, que não forem devidamente acompanhadas pela Secretaria Municipal de Ciência e Tecnologia (SECTI), através de abertura de chamado.
- ✓ É proibida abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo, deverá ocorrer pela Secretaria Municipal de Ciência e Tecnologia (SECTI).
- ✓ Não é permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro.
- ✓ Não é permitido o uso de computadores portáteis pessoais (notebook, netbook, Tablet e Smartphone) na rede da Prefeitura Municipal de Piraí, RJ, salvo os autorizados pela Secretaria Municipal de Ciência e Tecnologia (SECTI). Portanto, será necessário obrigatoriamente uma análise prévia e liberação de acesso por parte da Secretaria Municipal de Ciência e Tecnologia (SECTI). O usuário que desejar usar a rede neste caso, deverá estar ciente de que a Secretaria Municipal de Ciência e Tecnologia (SECTI), precisará executar configurações de controle, acesso e segurança e somente após este processo, poderá haver a liberação. Deve-se ter o entendimento de que algumas configurações feitas, poderão restringir o seu uso pessoal em seu computador pessoal, já que o mesmo precisará obrigatoriamente ser incluído nas políticas de segurança e acesso a rede e sistemas da Prefeitura Municipal de Piraí, RJ por meio da Secretaria Municipal de Ciência e Tecnologia (SECTI). Deverá ser assinado um ***Termo de Responsabilidade de Acesso a Rede Corporativa (Anexo III)***, para a devida liberação do Acesso a Rede por meio de Computador e Dispositivos Pessoais.

## 9.7. UTILIZAÇÃO DE IMPRESSORAS

O acesso às impressoras, deverão ser utilizadas somente no âmbito profissional e para atividades inerentes a Prefeitura Municipal de Piraí, sendo de boa conduta seguir os seguintes procedimentos:

- ✓ Ao mandar imprimir, verifique na impressora se o que foi solicitado já estava impresso, se a mesma está ligada e se não está em pausa. Há várias impressões "sem dono" acumulando-se nas máquinas, com elevado custo de papel e tintas das impressoras;
- ✓ Se a impressão deu errada, o papel pode ser reaproveitado na sua próxima tentativa, recoloque-o na bandeja de impressão. Se o papel servir para rascunho, leve para sua mesa. Se o papel servir para mais nada, jogue-o no lixo ou tratando-se de assunto sigiloso, certifique-se de destruí-lo antes;
- ✓ Não é permitido deixar impressões erradas nas impressoras, na mesa das impressoras, na mesa das pessoas próximas a ela, e tampouco, sobre o móvel da impressora;
- ✓ Se a impressora emitir alguma folha em branco, recoloque-a na bandeja;

- ✓ Se você notar que o papel de alguma das impressoras está no final, faça a gentileza de reabastecê-la. Isso evita que você e outras pessoas tenham seus pedidos de impressão prejudicados e evita acúmulo de trabalhos na fila de impressão;
- ✓ Utilize a impressora colorida somente para versão final de trabalhos e não para testes ou rascunhos.

## 9.8. UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS

A Prefeitura Municipal de Piraí 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 parte do Departamento de Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI), como: notebooks, smartphones e pendrives. 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 Piraí, RJ, 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.

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 Piraí, RJ, 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 Piraí, RJ 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 da Secretaria Municipal de Ciência e Tecnologia (SECTI).

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 Secretaria Municipal de Ciência e Tecnologia (SECTI).

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, desde que sejam mantidas as normativas de segurança de acesso a redes seguras.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Prefeitura Municipal de Piraí, RJ, notificar imediatamente seu gestor direto e a Gerência da Secretaria Municipal de Ciência e Tecnologia (SECTI). 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 responsabilidade 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 Municipal de Piraí, RJ e/ou a terceiros.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da Prefeitura Municipal de Piraí, RJ, deverá submeter previamente tais equipamentos ao processo de autorização do Departamento de Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI). Equipamentos portáteis, como smartphones, tablets, 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 com exceção as orientações descritas no item 9.6.

## 9.9. ACESSO E SEGURANÇA NOS DATACENTERS

O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros. Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.

Deverá ser executada mensalmente uma auditoria nos acessos ao Datacenter por meio do relatório do sistema de registro.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração da Gerência do Departamento de Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI), de acordo com o Procedimento de Controle de Contas Administrativas.

A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, 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 Datacenter, como: troca de fitas de backup, discos rígidos mecânicos e SSDs, instalação e suporte a novos dispositivos, novas conexões, novas tecnologias e equipamentos, 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 Datacenter, bem como assinar o **Termo de Responsabilidade de Acesso Físico e Seguro ao Data Center (Anexo IV)**.

O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter 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 de liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter.

Deverão existir duas cópias de chaves da porta do Datacenter. Uma das cópias ficará de posse da Gerência do Departamento de Projetos e Redes da Secretaria Municipal de Ciência e Tecnologia (SECTI), responsável pelo Datacenter, a outra, de posse dos Técnicos e Analistas de Infraestrutura responsáveis pelo Suporte e Infraestrutura.

O Datacenter 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 Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter por meio da Gerência do Departamento de Projetos Redes e Sistemas, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos disponibilizado pelo Departamento de Patrimônio Municipal da Secretaria Municipal de Administração (SECADM).

No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter.

## 9.10. SISTEMAS DE 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 do Departamento de Projetos e Redes da Secretaria Municipal de Ciência e Tecnologia (SECTI) 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 SSDs, HDS Externos, 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 Datacenter.

As Mídias 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 controlado pelos 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.

As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, distante no mínimo 10 quilômetros do Datacenter.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da Prefeitura Municipal de Piraí, RJ, 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 logo no 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 haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo Coordenador de Infraestrutura e analistas do Departamento de Projetos Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI), nos termos do Procedimento de Controle de Backup e Restore.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha 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.

### 9.11. SISTEMAS DE VIDEOMONITORAMENTO

São procedimentos operacionais definidos pela Secretaria Municipal de Ciência e Tecnologia (SECTI) relacionados ao Sistema de Videomonitoramento Municipal para desenvolvimento a Aplicação de Segurança Física dos Munícipes e de Patrimônio Municipal e de Terceiros.

O Monitoramento é feito por TVs e Somente os Usuários da Equipe Técnica da Secretaria Municipal de Ciência e Tecnologia (SECTI) possuem o Acesso ao Sistema para as Devidos Testes Internos e em Campo , Ajustes e Configurações, sobe a Responsabilidade do Responsável pelo Departamento de Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI).

O Processo se inicia única e exclusivamente com o B.O. registrado em Delegacia Policial Civil, devido as responsabilidades Criminais. As questões Internas, serão tratadas de acordo as orientações abaixo.

A Equipe do Departamento de Projetos e Redes da Secretaria Municipal de Ciência e Tecnologia (SECTI) se resume a verificação que corresponde ao dia e horário da Ocorrência e Retirada das Imagens para ser disponibilizada as autoridades, após aprovação da Equipe de Acompanhamento conforme Solicitações de Autoridades por meios Formais.

Desta forma a PSTIC determina as seguintes orientações:

- ✓ **Crime Flagrante:** Deve-se Verificar autorização para que os Policiais Solicitantes possam Acessar as imagens o mais rápido possível, pouco tempo depois do Flagrante. Deverá existir um Boletim de Ocorrência ou documento formal necessário para a liberação das imagens para fins de investigação e identificação de informações de qualquer ocorrência.
- ✓ **Questões de Segurança Interna:** Serão tratadas Internamente com o Conhecimento dos Fatos sendo levados para conhecimento do Secretário Responsável pela Secretaria Municipal solicitante e conhecimento prévio do Prefeito Municipal.
- ✓ **Questões de Alta Prioridade e Seriedade:** Será necessária a Homologação e Aprovação a ser feita pelo Prefeito Municipal e deverão ser tratadas com Confidencialidade, Discrição e Responsabilidade pelo Departamento de Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI).

A instalação e Configuração de Aplicativos em Celulares será feita pelos Técnicos e Analistas do Departamento de Projetos, Redes e Sistemas da Secretaria Municipal de Ciência e Tecnologia (SECTI) para o devido monitoramento conforme a necessidade ou ocorrência ou até mesmo para a demonstração do Sistema em funcionamento no caso de uma apresentação, somente a pessoas devidamente autorizadas.

Alguns acessos, portanto, poderão ser liberados somente para as câmeras que correspondem a Secretaria ou ao Departamento solicitados para determinados monitoramentos específicos. Não será permitido, portanto, acesso a todos as Câmeras.

Existe um ponto de Monitoramento instalado no Batalhão da Polícia Militar em Piraí, RJ, para que possam estar verificando e executando o seu trabalho Municipal de Monitoramento da Segurança da Cidade, podendo desta forma, elaborar estratégias de atuação, com inteligência e conhecimento devido ao acompanhamento de fluxo de ações por monitoramento visual de localidades e pontos específicos do Município. Estes pontos são responsáveis apenas pela visualização e não possuem autorização de ter acesso as Imagens gravadas. Caso alguma ocorrência cheguem a estes locais, o procedimento se dará de acordo com a orientação padrão.

Novos Pontos de Monitoramento poderão ser direcionados e instalados com a devida aprovação da Secretaria Municipal de Ciência e Tecnologia (SECTI) com a devida ciência e aprovação do Prefeito Municipal.

### 9.12. SISTEMA DE GESTÃO PÚBLICA

O sistema de Gestão Pública (SGP) monitora suas operações e sua navegação de informações/módulos protegidas com login/senha controlando sua utilização e o tipo de informação que terá acesso, onde os menus são customizados de forma que cada usuário visualize e tenha acesso somente às operações que lhe são designadas.

Lembrando que o login do usuário é atrelado ao seu número de CPF como manda a lei geral de proteção de dados (LGPD).

### 9.13. SISTEMAS DE MONITORAMENTO

Para garantir as regras a aplicação, a implementação e a manutenção das normas mencionadas nesta Política de Segurança de Tecnologia, Informação e Comunicação (PSTIC) a Prefeitura Municipal de Piraí, RJ, por meio da Secretaria Municipal de Ciência e Tecnologia (SECTI) se reserva no direito de:

- ✓ Implantar softwares e sistemas que possam monitorar e gravar todos os usos de internet através da rede e das estações de trabalho da empresa;
- ✓ Inspecionar qualquer arquivo armazenado na rede e das estações de trabalho da Prefeitura;
- ✓ Inspecionar qualquer arquivo armazenado na rede esteja no local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política;
- ✓ Foi instalada uma série de softwares e hardwares para proteger a rede interna e garantir a integridade dos dados e programas, incluindo um firewall, que é a primeira, mas não a única barreira entre a rede interna e a internet;

## 10. MEDIDAS PUNITIVAS

O não cumprimento pelo funcionário, usuário ou colaborador das normas ora estabelecidas nesta Política de Segurança de Tecnologia, Informação e Comunicação (PSTIC), sejam isoladas ou acumulativas, poderá, ensejar de acordo com a infração cometida, as seguintes punições:

- ✓ **Comunicação de Descumprimento**: Será encaminhado ao funcionário, um COMUNICADO informando o descumprimento da norma, com indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto a Procuradoria na respectiva pasta funcional do infrator.
- ✓ **Registro**: Será feito o registro por meio de Análise de Ocorrência e desenvolvimento de um Acervo de Ocorrências pessoais.
- ✓ **Advertência**: Nas hipóteses previstas na lei 964, de 11 de agosto de 2009 (Dispõe sobre o Regime Jurídico dos Servidores do Município de Piraí, RJ, e dá outras providências) da aplicada, por escrito, nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade.
- ✓ **Processo Administrativo Disciplinar:** Após verificações e audiências constatada a responsabilidade, as ações poderão ser passíveis de exoneração e processo judicial civil ou criminal.

## 11. DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Prefeitura Municipal de Piraí, RJ. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição e precisará ser analisado seriamente por esta Política de Segurança de Tecnologia, Informação e Comunicação (PSTIC) e aplicada as normas aqui definidas.