



# **SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO**



## **PSI - Política de Segurança da Informação Diretrizes e Normas**



## Sumário

Sumário .....	2
1. OBJETIVO .....	3
2. CONCEITOS E DEFINIÇÕES .....	3
3. ÂMBITO DA POLÍTICA .....	8
4. DIRETRIZES GERAIS.....	9
5. CLASSIFICAÇÃO DA INFORMAÇÃO .....	9
6. COMPETÊNCIAS E RESPONSABILIDADES.....	10
7. NORMAS COMPLEMENTARES .....	11
8. PENALIDADES .....	12
9. CONSIDERAÇÕES FINAIS .....	12
NC 01 – Política de Controle de Acesso.....	13
NC 02 – Política de Acesso à Internet .....	17
NC 03 – Política de Uso de Equipamentos de Informática .....	19
NC 04 – Política de Uso de E-mail Corporativo .....	23
NC 05 – Política de Publicações no Portal do Município.....	25
NC 06 – Política para uso de Serviço de Nuvem - Cloud.....	26
NC 07 – Política do Sistema de Videomonitoramento (CFTV) .....	27
NC 08 – Administração do Sistema de Controle de Acesso de Pessoas .....	29
NC 09 – Política de Administração de Servidores/Datacenter.....	30



## 1. OBJETIVO

O objetivo deste documento é estabelecer diretrizes que permitam aos colaboradores da Prefeitura Municipal de Paranaguá seguirem padrões de comportamento relacionados à segurança da informação, adequados às necessidades de negócio e da proteção legal da instituição, em consonância com a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, e o Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, preservando as informações no tocante a:

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

Dessa forma, busca-se desenvolver um comportamento ético e profissional para que todos possam utilizar da melhor forma as ferramentas de TI e as informações por elas geradas, e, ao mesmo tempo, busca-se reduzir ameaças através da adoção de medidas preventivas para evitar possíveis incidentes que tragam prejuízos à instituição.

## 2. CONCEITOS E DEFINIÇÕES

Para os fins dessa Política, considera-se:

- **Acesso Não Autorizado** – acesso indevido ou não previsto, obtido por quaisquer meios, procedimentos e a qualquer título, à revelia da política ou do controle de acesso vigentes, ou ainda decorrente de falhas ou imperfeições nos mecanismos de controle de acesso. Contrasta com acesso autorizado.
- **Acesso Lógico** – acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;
- **Acesso Remoto** – ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;
- **Ameaça** – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- **Análise/avaliação de riscos** – processo completo de análise e avaliação de



riscos;

- **Ativo** – qualquer bem, tangível ou intangível, que tenha valor para a organização;
- **Ativo da Informação** – os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
- **Auditoria** – verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;
- **Autenticação** – é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;
- **Autenticidade** – propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
- **Banco de Dados (ou Base de Dados)** – é um sistema de armazenamento de dados, isto é, um conjunto de registros que tem como objetivo organizar e guardar as informações;
- **Bloqueio de acesso** – processo que tem por finalidade suspender temporariamente o acesso;
- **Classificação da informação** – atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;
- **Colaborador** – servidores público municipais, cargos comissionados, contratados por tempo determinado, estagiários e prestadores de serviços que exercem atividades no âmbito da Prefeitura Municipal de Paranaguá.
- **Confidencialidade** – propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada/credenciada;
- **Contingência** – descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à instituição;
- **Controle de Acesso** – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
- **Cópia de Segurança (Backup)** – copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;



- **Correio Eletrônico** – é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;
- **Credenciais ou contas de acesso** – permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e biometria ou lógica como identificação por usuário (username) e senha (password);
- **Criptografia** – é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta");
- **Dado** – representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;
- **Disponibilidade** – propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
- **Download** – (baixar) copiar arquivos de um servidor (site) na internet para um computador;
- **Gestão de Continuidade de Negócios** – processo de gestão global que identifica potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia a dia;
- **Gestão de Risco** – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
- **Gestão de Segurança da Informação e Comunicações** – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
- **Hardware** – É a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressoras, teclado, mouse e outros;
- **Incidente de Segurança** – é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das



redes de computadores;

- **Informação** – dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- **Informação sigilosa** – informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;
- **Integridade** – propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- **Internet** – rede mundial de computadores;
- **Intranet** – rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito a mesma;
- **Log** – é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu histórico de comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;
- **Logon** – procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;
- **Norma** – documento interno que regulamenta formal e administrativamente, de maneira geral ou específica, aspectos ou diretrizes expressas na PSI, no todo ou em parte da instituição. As normas mapeiam a PSI na organização técnico-administrativa da instituição, estabelecendo regras para a sua implementação.
- **Peer-to-peer (P2P)** – (ponto a ponto) permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;
- **Perfil de acesso** – conjunto de atributos de cada usuário em um determinado sistema, inerentes as atribuições do cargo, e é definido previamente para credencial de acesso;
- **Política de Segurança da Informação (PSI)** – documento aprovado pela Secretaria Municipal de Administração, que é a autoridade responsável pelo Departamento de Tecnologia da Informação, com o objetivo de fornecer



diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação na instituição;

- **Protocolo** – convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;
- **Proxy** – é um serviço intermediário entre as estações de trabalho de uma rede e a Internet. O servidor de rede proxy serve para compartilhar a conexão com a Internet e melhorar o desempenho do acesso, além de gerir o acesso as páginas e sites;
- **Recursos Computacionais** – recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;
- **Rede Corporativa** – conjunto de todas as redes locais sob a gestão do Departamento de Tecnologia da Informação;
- **Rede Pública** – rede de acesso a todos;
- **Responsabilidade** – obrigações e deveres decorrentes da legislação vigente, ofício, cargo, função ou por força de contrato, na proteção dos ativos de informação de qualquer natureza;
- **Senha ou Credencial de Acesso** – credencial que concede, de maneira prevista, o direito de acesso, físico ou lógico, a determinado ativo de informação de qualquer natureza, ou local que o abrigue. Uma senha ou credencial fraca é toda aquela que não obedece aos critérios e requisitos mínimos de qualidade vigentes;
- **Servidor de Rede** – recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas de informação;
- **Software** – são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;
- **Site** – conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;
- **Streaming** – transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet;
- **Termo de Responsabilidade** – termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir



responsabilidades decorrentes de tal acesso;

- **Tratamento de Incidentes de Segurança em Redes Computacionais** – serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;
- **Usuário** – servidores público municipais, cargos comissionados e estagiários da Prefeitura Municipal de Paranaguá que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Prefeitura Municipal de Paranaguá, solicitada via ofício e formalizada por meio da assinatura do Termo de Responsabilidade;
- **VLAN (Virtual Local Area Network ou Virtual LAN)** – (Rede Local Virtual) é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local;
- **VPN (Virtual Private Network)** – (Rede Privada Virtual) é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN, pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada;
- **Vulnerabilidade** – conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;
- **Wireless (rede sem fio)** – rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

### 3. ÂMBITO DA POLÍTICA

- 3.1. As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores que exercem atividades no âmbito da administração pública direta na Prefeitura Municipal de Paranaguá, qualquer pessoa e/ou empresa que venha a ter acesso a dados ou informações e em qualquer meio ou suporte.
- 3.2. Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da instituição poderão ser monitorados e gravados conforme previsto nas leis brasileiras.



# PREFEITURA MUNICIPAL DE PARANAGUÁ

Secretaria Municipal de Administração  
Departamento de Tecnologia da Informação



3.3. É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou do Departamento de Tecnologia da Informação, sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

## 4. DIRETRIZES GERAIS

- 4.1. Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos a fim de preservar o princípio de continuidade na Instituição;
- 4.2. Toda informação gerada pelos colaboradores, utilizando integralmente ou parcialmente recursos da Prefeitura Municipal de Paranaguá, são de propriedade da instituição;
- 4.3. Ameaças e riscos devem ser reavaliados periodicamente para garantir que a Instituição esteja efetivamente protegida;
- 4.4. O acesso às informações, produzidas ou recebidas pelas Secretarias Municipais, devem ser limitadas às atribuições necessárias ao desempenho das respectivas atividades dos seus usuários/colaboradores;
- 4.5. Os processos de aquisição ou contratação de bens e serviços de tecnologia da informação, a qualquer título, devem refletir esta PSI e seus documentos acessórios, sem prejuízo da observância da legislação em vigor;
- 4.6. Os equipamentos de informática e comunicação, sistemas e informações deverão ser utilizados exclusivamente para a realização das atividades profissionais.
- 4.7. Esta política de Segurança da Informação pode ser revisada periodicamente e eventualmente revista sempre que eventos ou fatos relevantes ocorram;
- 4.8. Os colaboradores devem evitar a circulação das informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras e mídias em locais de fácil acesso. Prezar pelo conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.
- 4.9. A revisão da Política de Segurança da Informação (PSI) é de responsabilidade da CTTI - Comissão Técnica de Tecnologia da Informação, e qualquer alteração na PSI só pode ser realizada mediante aprovação pela maioria absoluta dos membros dessa comissão.

## 5. CLASSIFICAÇÃO DA INFORMAÇÃO

- 5.1. É de responsabilidade do Secretário de cada pasta estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) geradas por sua



área de acordo com a tabela abaixo:

- **Pública** – É toda informação que pode ser acessada por usuários da instituição, clientes, fornecedores, prestadores de serviços e público em geral.
- **Interna** – É toda informação que só pode ser acessada por funcionários da instituição. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da instituição.
- **Confidencial** – É toda informação que pode ser acessada por usuários da instituição e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.
- **Restrita** – É toda informação que pode ser acessada somente por usuários da instituição explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

## 6. COMPETÊNCIAS E RESPONSABILIDADES

### 6.1. Secretária Municipal de Administração – SEMAD:

- Assegurar que a implementação dos controles de segurança da informação tenha uma coordenação e permeie toda a instituição.
- Apoiar a Política e manter compromisso com sua continuidade e resultados.

### 6.2. Departamento de Tecnologia da Informação – DTI:

- Promover cultura de segurança da informação e comunicações;
- Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- Propor recursos necessários às ações de segurança da informação e comunicações;
- Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
- Propor Normas Complementares e Procedimentos de Segurança da Informação e das Comunicações;
- Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança da informação;
- Apurar os incidentes de segurança críticos e encaminhar os fatos apurados para aplicação das penalidades previstas;



# PREFEITURA MUNICIPAL DE PARANAGUÁ

Secretaria Municipal de Administração  
Departamento de Tecnologia da Informação



- Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;
- Identificar controles físicos, administrativos e tecnológicos para mitigação do risco;
- Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, informando aos respectivos gestores sobre as ações corretivas ou de contingência em cada caso;

## 6.3. Cabe aos Colaboradores da PREFEITURA MUNICIPAL DE PARANAGUÁ:

- Cumprir com todas as diretrizes e normas estabelecidas por esta Política;
- Estar sempre atualizado e ciente das políticas, normas e procedimentos vigentes;
- Não divulgar, compartilhar ou transmitir informações a pessoas que não tenham nível de autorização suficiente;
- Não conduzir, transportar, enviar, transmitir, compartilhar ou deixar que dados e informações alcancem ambiente ou destinatário fora das dependências ou controle da instituição, sem autorização formal da Secretaria Municipal de Administração.

## 6.4. Cabe ao Departamento de Administração de Pessoal da SEMAD:

- Informar ao Departamento de Tecnologia da Informação todos os desligamentos, afastamentos, retornos e modificações no quadro funcional.

## 6.5. Cabe à Procuradoria Geral do Município – PROGEM:

- Prestar assessoramento de natureza jurídica, supervisionar e coordenar as atividades de natureza jurídica, inclusive aquelas relacionadas com a elaboração de atos normativos.

## 7. NORMAS COMPLEMENTARES

7.1. O detalhamento da Política de Segurança da Informação está segmentado nas seguintes Normas Complementares:

- 7.1.1. NC 01 - Política de Controle de Acesso;
- 7.1.2. NC 02 - Política de Acesso à Internet;
- 7.1.3. NC 03 - Política de uso de Equipamentos de Informática;
- 7.1.4. NC 04 - Política de uso de E-mail Corporativo.



# PREFEITURA MUNICIPAL DE PARANAGUÁ

Secretaria Municipal de Administração  
Departamento de Tecnologia da Informação



- 7.1.5. NC 05 - Política de Publicações no Portal do Município
- 7.1.6. NC 06 - Política para uso de Serviço de Nuvem - Cloud
- 7.1.7. NC 07 - Política do Sistema de Videomonitoramento (CFTV)
- 7.1.8. NC 08 - Administração do Sistema de Controle de Acesso de Pessoas
- 7.1.9. NC 09 - Política de Administração de Servidores/Datacenter

## 8. PENALIDADES

- 8.1. O descumprimento das disposições constantes nessa Política e nas Normas Complementares sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, dependendo da gravidade do caso, este poderá acarretar também em processo civil e penal;

## 9. CONSIDERAÇÕES FINAIS

- 9.1. Os casos omissos e dúvidas deverão ser submetidos à CTTI - Comissão Técnica de Tecnologia da Informação.



## ANEXO I

### NORMAS COMPLEMENTARES

#### NC 01 – Política de Controle de Acesso

##### 1. OBJETIVO

Estabelecer critérios para a disponibilização e administração do acesso aos serviços de Tecnologia da Informação, bem como estabelecer critérios relativos às senhas das respectivas contas dos usuários.

##### 2. DIRETRIZES GERAIS

- 2.1. A conta de acesso é o instrumento para identificação do usuário na rede da Prefeitura Municipal de Paranaguá e caracteriza-se por ser de uso individual e intransferível, sua divulgação é vedada sob qualquer hipótese;
- 2.2. Todo cadastramento de conta de acesso à rede da Prefeitura Municipal de Paranaguá deve ser formalizado mediante solicitação via ofício, assinado pelo Secretário da pasta do requerente e endereçada aos Administradores de Rede lotados no Departamento de Tecnologia da Informação.
- 2.3. Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário aos quais as informações estão vinculadas;
- 2.4. Todas as senhas, de usuários comuns, para autenticação na rede da Prefeitura Municipal de Paranaguá devem seguir os seguintes critérios mínimos:
  - I. Toda senha deve ser constituída de, no mínimo, 8 caracteres, sendo obrigatório o uso de caracteres alfanuméricos (letras e números);
  - II. A senha não poderá ser a mesma palavra passe das 2 últimas cadastradas/atualizadas;
  - III. Será obrigatória a troca de senha ao efetuar o primeiro login;
- 2.5. A base de dados de senhas deve ser armazenada com criptografia;
- 2.6. O acesso aos serviços de tecnologia de informação da Prefeitura Municipal de Paranaguá deve ser disponibilizado aos usuários que oficialmente executem atividade vinculada à atuação institucional de suas respectivas Secretarias;
- 2.7. O processo de aprovação do acesso deve ser iniciado pelo superior do colaborador, com a autorização do Secretário da pasta, os privilégios garantidos continuarão em efeito até que o usuário mude suas atividades ou deixe o Órgão Público. Se um desses dois eventos ocorrer, a chefia deve notificar imediatamente a unidade



responsável.

- 2.8. Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos nos sistemas de Tecnologia da Informação deve ser imediatamente comunicada ao Departamento de Tecnologia da Informação;
- 2.9. As contas com alto privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades e necessidades atribuídas. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos Técnicos e Administradores de Rede do Departamento de Tecnologia da Informação.
- 2.10. A administração dos servidores e máquinas virtuais desta municipalidade é de responsabilidade exclusiva dos Administradores de Rede, sendo expressamente vedado o acesso aos servidores e máquinas virtuais por outros servidores e cargos comissionados que não sejam os Administradores de Rede.
- 2.11. Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.

### 3. ACESSO REMOTO

- 3.1. O acesso remoto aos serviços corporativos somente deve ser disponibilizado aos colaboradores que, oficialmente, executem atividades vinculadas à atuação institucional na Prefeitura Municipal de Paranaguá, desde que solicitado formalmente pelo Secretário da pasta, justificando seu acesso.
- 3.2. A liberação de acesso remoto só será efetivada após avaliação e aprovação pelos Administradores de Rede do Departamento de Tecnologia da Informação, para que se evitem ameaças à integridade e sigilo das informações contidas na rede da Prefeitura Municipal de Paranaguá;
- 3.3. As Conexões remotas à rede da Prefeitura Municipal de Paranaguá devem ocorrer da seguinte maneira:
  - I. Utilização de autenticação;
  - II. As senhas e as informações que trafegam entre a estação remota e a rede da Prefeitura Municipal de Paranaguá devem estar criptografadas;
  - III. É vedada a utilização do acesso remoto para fins não relacionados às atividades da instituição.
- 3.4. O acesso remoto aos recursos da prefeitura é estritamente controlado e limitado à equipe responsável pela administração de redes e suporte de sistemas. Apenas os membros



autorizados desta equipe têm permissão para se conectar aos sistemas remotamente. Isso garante que apenas indivíduos de confiança e com o devido conhecimento tenham acesso aos dados e sistemas críticos da organização. Qualquer tentativa não autorizada de acesso remoto será prontamente detectada e tratada de acordo com os procedimentos de segurança estabelecidos.

- 3.5. Além do acesso remoto restrito à equipe designada, a utilização de máquinas virtuais (VMs) e Docker nas instalações da prefeitura também está sujeita a políticas de segurança da informação. A criação, configuração e uso de máquinas virtuais e Docker deve estar em conformidade com as diretrizes estabelecidas pelo Departamento de TI. Apenas os Administradores de Redes são autorizados a criar e gerenciar VMs e Docker, garantindo a integridade e a segurança dos sistemas virtuais. Em casos excepcionais que demandem a criação ou gestão de uma VM ou Docker por indivíduos fora da equipe designada, solicitações justificadas e aprovadas pela maioria absoluta dos administradores de redes podem ser consideradas, desde que as medidas de segurança apropriadas sejam implementadas e documentadas.

## 4. ACESSO A BASE DE DADOS

- 4.1. O acesso a base de dados será permitido somente ao Administrador de Banco de Dados, por meio de senha de uso pessoal e intransferível, vedada sua divulgação;
- 4.2. É vedado ao administrador de banco de dados, responsável pela base de dados, o acesso com o objetivo de:
  - I. Compartilhar sem autorização da chefia imediata, no todo ou em parte, as informações contidas na base de dados;
- 4.3. É de responsabilidade do administrador de banco de dados que possui acesso as bases de dados:
  - I. Manter em sigilo sua senha de acesso as bases de dados;
  - II. Fechar o aplicativo de acesso a base de dados (SGBD – Sistema gerenciador de Base de Dados) toda vez que se ausentar, evitando o acesso indevido;
- 4.4. Do acesso a base de dados à terceiros:
  - I. Deverá ser firmado Termo de Responsabilidade, pela Prefeitura Municipal de Paranaguá e a entidade interessada, sobre as informações que deverão ser compartilhadas.
  - II. A documentação apresentada, conforme disposto no item 4.4.1, deve ser



analisada pelo jurídico, devendo o mesmo dar parecer favorável sobre a legalidade da liberação das informações solicitadas.

- III. A responsabilidade da guarda dos dados da Prefeitura Municipal de Paranaguá, obtidos através de integrações entre sistemas deverá ser da entidade solicitante.

#### 4.5. Armazenamento e Backup:

- I. Os backups devem ser conservados em local protegido, sob acesso exclusivo do Administrador de Banco de Dados, mantendo a confidencialidade de todas as informações armazenadas.
- II. A distribuição de cópias do backup a indivíduos não autorizados é proibida. Portanto, é dever do Administrador de Banco de Dados não divulgar a senha de acesso aos backups para pessoas não autorizadas por documento oficial ou guardar os arquivos em locais de acesso público.
- III. Para a gravação de backups históricos, deve-se utilizar mídias removíveis ou storage offline, protegendo os dados com criptografia ou senha. Estas mídias ou storage devem ser mantidos em locais seguros e adequados às necessidades climáticas específicas do meio de armazenamento.

## 5. CONTROLE DE ACESSO FÍSICO

- 5.1. Os controles de acesso físico visam restringir o acesso aos equipamentos de Tecnologia da Informação;
- 5.2. O acesso ao Datacenter somente poderá ser feito por pessoas autorizadas pelos Administradores de Rede, que são os responsáveis pelo Datacenter;
- 5.3. O acesso de visitantes ou terceiros ao Datacenter somente poderá ser realizado mediante agendamento prévio, com acompanhamento de um colaborador da área de Tecnologia de Informação;
- 5.4. 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;
- 5.5. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto famífero ou inflamável;



## NC 02 – Política de Acesso à Internet

### 1. OBJETIVO

Estabelecer critérios para administração e utilização de acesso aos serviços de Internet e Intranet, no âmbito da Prefeitura Municipal de Paranaguá, em consonância com a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018 e o Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014.

### 2. DIRETRIZES GERAIS

- 2.1. O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pela instituição;
- 2.2. Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;
- 2.3. 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 de trabalho ou em áreas privadas da rede, visando assegurar o cumprimento desta Política de Segurança da Informação;
- 2.4. Toda alteração de nível de acesso somente será realizada mediante solicitação formal, pela chefia imediata do usuário, contendo a devida justificativa, com a autorização do Secretário responsável pela pasta que será avaliada pelos Administradores de Rede do Departamento de Tecnologia da Informação, podendo esta solicitação ser negada em caso de risco ou vulnerabilidade a segurança e a integridade da rede da Prefeitura Municipal de Paranaguá;
- 2.5. É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como:
  - a. Pornografia, pedofilia, preconceitos, vandalismo, entre outros;
  - b. Acessar ou obter na Internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede da Prefeitura Municipal de Paranaguá;
  - c. Uso recreativo da internet em horário de expediente;
  - d. Uso de proxy anônimo, VPN e tuneladores;
  - e. Acesso a rádio e TV em tempo real (serviços de streaming), exceto os canais corporativos em horário de expediente;
  - f. Acesso a jogos;
  - g. Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;



- h. Envio a destino externo de qualquer software licenciado à Prefeitura Municipal de Paranaguá ou dados de sua propriedade ou de seus usuários, salvo expressa e fundada autorização do responsável pela sua guarda;
  - i. Contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas do Departamento de Tecnologia da Informação;
  - j. Utilização de softwares de compartilhamento de conteúdo na modalidade peer-to-peer (P2P);
- 2.6. Caso os Administradores de Rede julguem necessário, haverá bloqueios de acesso a arquivos e sites não autorizados que comprometam o uso de banda da rede, o desempenho e produtividade das atividades do colaborador, bem como, que exponham a rede a riscos de segurança;
- 2.7. É proibido utilizar os recursos da Prefeitura Municipal de Paranaguá para fazer o download ou distribuição de software ou dados não legalizados;
- 2.8. Haverá auditoria dos sites acessados por usuário para verificação da adequação à política vigente;
- 2.9. Comprovada a utilização irregular, o usuário envolvido poderá ter o seu acesso à Internet bloqueado, sendo comunicado o fato à chefia imediata, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa.



## **NC 03 – Política de Uso de Equipamentos de Informática**

### **1. OBJETIVO**

Estabelecer critérios para a utilização dos equipamentos de informática na Prefeitura Municipal de Paranaguá.

### **2. DIRETRIZES GERAIS**

- 2.1. Os recursos computacionais somente devem ser utilizados para a execução de atividades de interesse da Prefeitura Municipal de Paranaguá;
- 2.2. Cada estação de trabalho possui controle de IP (Protocolo Internet), os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário. Por isso, sempre que ausentar do ambiente de trabalho tenha certeza que efetuou o logoff ou bloqueou a estação de trabalho;
- 2.3. Não é permitido gravar localmente nas estações de trabalho e na Rede da Prefeitura Municipal de Paranaguá: arquivos de música, MP3, filmes, fotos pessoais, software com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria;
- 2.4. Todos os dados e arquivos relativos às atividades da Prefeitura Municipal de Paranaguá devem ser mantidos no servidor de arquivos ou utilizar o serviço de Nuvem Municipal, onde existe sistema de backup diário e confiável;
- 2.5. Os arquivos gravados em diretórios temporários (pastas públicas) podem ser acessados por todos os usuários que utilizarem a rede local, portanto não garante sua integridade, podendo ser alterados ou excluídos sem prévio aviso, por qualquer usuário;
- 2.6. Não será feito cópia de segurança (backup) dos arquivos criados no computador local (estação de trabalho) dos colaboradores. O próprio usuário deve fazer cópia de segurança dos arquivos locais e verificar o que pode ser eliminado, evitando acúmulo de dados desnecessários em sua estação de trabalho;
- 2.7. É proibida a abertura física dos computadores para qualquer tipo de finalidade, caso seja necessário reparo, o mesmo deverá ser solicitado via abertura de chamado ao Suporte Técnico do Departamento de Tecnologia da Informação, através dos canais oficiais;
- 2.8. Quanto à utilização de equipamentos de informática particulares (celulares, notebooks, tablets e/ou qualquer dispositivos móveis que venham acessar a rede sem fio ou rede estruturada), o colaborador deverá comunicar a chefia imediata, que



# PREFEITURA MUNICIPAL DE PARANAGUÁ

Secretaria Municipal de Administração  
Departamento de Tecnologia da Informação



deverá solicitar formalmente sua liberação, justificando o acesso e encaminhando ao Departamento de Tecnologia da Informação. O pedido será analisado pelos Administradores de Rede, e os equipamentos deverão obrigatoriamente ser gerenciados pela equipe Técnica do Departamento de Tecnologia. Fica vedada a utilização em caso de risco detectado pelos Administradores de Rede. A utilização de equipamentos particulares não é recomendada, devendo somente os casos extremamente excepcionais serem analisados;

- 2.9. Em caso de eventos no ambiente da Prefeitura Municipal de Paranaguá, que necessitem utilizar os recursos de TI, tais como: seminários, licitações, etc., deverá ser solicitado com antecedência mínima de 15 dias úteis ao Departamento de Tecnologia da Informação.
- 2.10. Em caso de dano, inutilização ou extravio do equipamento, o colaborador deverá comunicar imediatamente ao Departamento de Tecnologia da Informação, que deverá adotar as providências cabíveis;
- 2.11. Em caso de furto ou roubo, o colaborador deverá providenciar Boletim de Ocorrência junto à Polícia Civil e entregá-lo na Secretaria Municipal de Administração, com cópia ao Departamento de Tecnologia da Informação, que deverão adotar as providências necessárias;
- 2.12. É proibido colar adesivos com ímãs nos equipamentos;
- 2.13. É dever do colaborador zelar pela integridade do equipamento estritamente como instrumento de trabalho, juntamente com os acessórios que foram utilizados;
- 2.14. Não é permitido alterar as configurações de rede e da BIOS das máquinas, bem como efetuar qualquer modificação que possa causar algum problema futuro;
- 2.15. Não é permitido retirar ou transportar qualquer equipamento de informática da Prefeitura Municipal de Paranaguá sem autorização prévia do Departamento de Tecnologia da Informação. Mesmo dentro da mesma repartição, toda e qualquer movimentação deve ser solicitada à equipe de Suporte Técnico através da abertura de chamado. Em caso de mudança de repartição, deve ser oficiado com o autorizo do Secretário da Pasta e informado ao Departamento de Patrimônio da Secretaria Municipal de Administração e Recursos Humanos;
- 2.16. Fica proibida a utilização, sem o devido consentimento, da utilização de equipamentos de informática por pessoas sem vínculo com a Prefeitura Municipal de Paranaguá;
- 2.17. É vedado retirar e/ou danificar placas identificadoras de patrimônio, travas e lacres de segurança dos equipamentos de informática;



- 2.18. Não é permitido conectar e/ou configurar equipamento à rede, sem a prévia liberação dos Administradores de Rede do Departamento de Tecnologia da Informação;
- 2.19. O antivírus deve estar atualizado e com a autoproteção ativa na estação de trabalho;
- 2.20. O usuário deve obrigatoriamente executar o antivírus nos dispositivos removíveis antes de sua abertura quando inseridos na estação de trabalho.
- 2.21. É vedada a utilização dos equipamentos de informática da Prefeitura Municipal em redes particulares. Todos os equipamentos devem ser utilizados exclusivamente dentro da rede municipal, salvo exceções que deverão ser oficialmente solicitadas e justificadas, com eventual liberação condicionada à análise e aprovação dos Administradores de Redes. Além disso, a utilização e instalação de links de internet particulares dentro dos próprios municipais não são permitidas. Essa medida visa garantir a segurança e a integridade das operações municipais, assegurando que todos os dados e informações sejam trafegados apenas através das redes oficiais e seguras da prefeitura.

### **3. POLÍTICA DE BACKUP E RESTAURAÇÃO DE ARQUIVOS**

- 3.1. Todos os backups são automatizados por sistemas de agendamento, eles são feitos preferencialmente em horários em que não há nenhum ou pouco acesso de usuários ou processos aos sistemas de informática e arquivos.
- 3.2. A restauração de arquivos armazenados no servidor de arquivos só será possível em dados que foram gerados backup no dia anterior;
- 3.3. Os arquivos são retidos por 30 dias úteis na rotina diária e por 60 meses na rotina mensal. A rotina mensal do backup é efetuada uma vez por mês até atingir os 60 meses. É fundamental destacar que somente os dados brutos armazenados no servidor de arquivos estão abrangidos por essa rotina. A retenção de backup de máquinas virtuais é administrada pelo próprio sistema hospedeiro, com rotinas de backup realizadas de uma até três vezes por semana e um histórico de 7 restaurações;
- 3.4. É de responsabilidade de cada usuário o armazenamento dos arquivos inerentes ao seu departamento no servidor de arquivos para garantir o backup dos mesmos;
- 3.5. É dever do usuário, a manutenção no diretório que tem acesso, mantendo organizado, evitando acúmulo de arquivos e duplicadas;



- 3.6. Não será feito backup do compartilhamento “Público” e “Temporário” dentro do servidor de arquivos;
- 3.7. Haverá limpeza periódica dos arquivos de rede armazenados na pasta “Lixeira” e “Pública”, para que não haja acúmulo desnecessário de arquivos e de recursos computacionais;
- 3.8. Os Administradores de Rede, 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;
- 3.9. Todos os acessos dentro do servidor de arquivos são auditados;

#### **4. POLÍTICA DE USO DE IMPRESSORAS**

- 4.1. Todas as impressões deverão ser executadas nos seus respectivos setores/departamentos;
- 4.2. Não é permitido imprimir documentos que não estejam dentro das atividades de trabalho;
- 4.3. Os toners de impressão e cartuchos de tinta deverão ser retirados no Departamento de Tecnologia da Informação, dentro do horário de funcionamento, que é de segunda a sexta-feira, das 08:00 às 11:00 e das 13:00 às 18:00. A entrega do novo insumo será feita mediante a apresentação do toner e/ou cartucho vazio. A retirada e substituição são de responsabilidade do usuário, não sendo necessário abrir um chamado técnico para essa demanda. Para os usuários da Secretaria de Saúde, especificamente da UPA, é mantido um estoque regulador dentro da unidade, cuja manutenção é responsabilidade do responsável pela unidade.
- 4.4. Não é permitido deixar “impressões erradas” na mesa ou em cima das impressoras.
- 4.5. Não é permitido deixar material ou objeto em cima do equipamento, bem como colar adesivos.
- 4.6. Os documentos deverão, preferencialmente, ser impressos frente e verso, para economia de papel.



## NC 04 – Política de Uso de E-mail Corporativo

### 1. OBJETIVO

Estabelecer critérios para disponibilização e utilização do serviço de correio eletrônico corporativo da Prefeitura Municipal de Paranaguá aos usuários (<https://mail.paranagua.pr.gov.br>). O e-mail institucional utiliza recursos do Sistema Zimbra, homologado previamente pelo Departamento de Tecnologia da Informação.

### 2. DIRETRIZES GERAIS

- 2.1. O serviço de correio eletrônico tem como finalidade o envio e o recebimento de mensagens e documentos relacionados com as funções institucionais na Prefeitura Municipal de Paranaguá;
- 2.2. São usuários do serviço de correio eletrônico corporativo aqueles que executam atividade vinculada à atuação institucional da Prefeitura Municipal de Paranaguá, sendo vedada a criação de contas institucionais para estagiários da instituição e terceiros;
- 2.3. A concessão de contas de correio eletrônico depende de solicitação formal via ofício da chefia imediata do usuário, endereçada ao Departamento de Tecnologia da Informação;
- 2.4. É vedado aos administradores o acesso ao conteúdo das mensagens tramitadas por meio do serviço de correio eletrônico corporativo, salvo nas hipóteses previstas em lei;
- 2.5. O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível, vedada sua divulgação;
- 2.6. É vedado ao usuário o uso do serviço de correio eletrônico corporativo com o objetivo de:
  - I. Praticar crimes e infrações de qualquer natureza;
  - II. Executar ações nocivas contra outros recursos computacionais da Prefeitura Municipal de Paranaguá ou de redes externas;
  - III. Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;
  - IV. Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo “corrente”, vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede da



Prefeitura Municipal de Paranaguá;

- V. Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pela Prefeitura Municipal de Paranaguá;
- VI. Divulgar, no todo ou em parte, os endereços eletrônicos institucionais constantes do catálogo de endereços do serviço;
- VII. Executar outras atividades lesivas, tendentes a comprometer a intimidade dos usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional.

2.7 É de responsabilidade do usuário do correio eletrônico:

- I. Manter em sigilo sua senha de acesso ao correio eletrônico;
- II. Fechar o sistema de correio (navegador/brownsner) toda vez que se ausentar, evitando o acesso indevido;
- III. Comunicar imediatamente ao Departamento de Tecnologia da Informação quando do recebimento de mensagens com vírus ou que venham a trazer algum tipo de dano aos sistemas de informática;
- IV. Efetuar a manutenção de sua caixa postal, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo.

2.8 É de responsabilidade do Departamento de Tecnologia da Informação:

- I. Criar e manter o cadastro dos usuários e das caixas postais;
- II. Cancelar os acessos ao serviço de correio eletrônico dos usuários que se desvinculem da instituição;
- III. Propor a divulgação de orientação sobre o uso correto do correio eletrônico;
- IV. Fiscalizar a utilização do serviço de correio eletrônico, observados os critérios estabelecidos nesta norma;
- V. Desenvolver demais ações que garantam a operacionalização desta norma.



## NC 05 – Política de Publicações no Portal do Município

### 1. OBJETIVO

- 1.1. Garantir confiabilidade, clareza e descentralização das publicações no portal do município (<http://www.paranagua.pr.gov.br>).
- 1.2. Proporcionar um espaço unificado, interativo e integrado para o acervo de informações da Prefeitura Municipal de Paranaguá.

### 2. DIRETRIZES GERAIS

- 2.1. O Portal da Prefeitura Municipal de Paranaguá é o sitio da internet que aglomera e distribui o conteúdo e notícias dos diversos órgãos municipais. Os sítios, sob o domínio paranagua.pr.gov.br, contemplarão os conteúdos dos órgãos municipais, promovendo o acesso aberto aos mesmos, nos termos da legislação nacional, das normativas internas da Prefeitura Municipal de Paranaguá e do interesse público.
- 2.2. São atribuições do Departamento de Tecnologia da Informação (DTI):
  - I. Orientar os órgãos municipais em vista do cumprimento das normas e dos padrões de disponibilização de conteúdo;
  - II. Realizar publicações, somente através de ofício com o autorizo do secretário da pasta do requerente;
  - III. Gerenciar a definição, padronização e atualização da identidade visual do Portal da Prefeitura Municipal de Paranaguá;
  - IV. Gerenciar a validação das solicitações de criação de sítio(s) e encaminhá-las ao setor responsável pela sua criação, nos casos deferidos;
  - V. Gerenciar a permissão de acesso ao sistema do responsável pela publicação e manutenção dos conteúdos.
- 2.3. São atribuições da Secretaria Municipal de Comunicação Social
  - I. Atualizar e manter todo o conteúdo jornalístico do Portal da Prefeitura Municipal de Paranaguá;
  - II. Gerenciar as notícias produzidas pelos órgãos municipais quanto à legibilidade, clareza, simplicidade, objetividade e atualidade das informações;
  - III. Apoiar o treinamento de servidores designados pelos órgãos municipais para atuar na publicação e manutenção de notícias.
  - IV. Todas as solicitações de publicação no Portal da Prefeitura Municipal de Paranaguá deverão ser encaminhadas via ofício de requerimento ou protocolados



## NC 06 – Política para uso de Serviço de Nuvem - Cloud

### 1. OBJETIVO

Estabelecer critérios para disponibilização e utilização do serviço de nuvem (Cloud) na Prefeitura Municipal de Paranaguá (<https://drive.paranagua.pr.gov.br> e <https://cloud.paranagua.pr.gov.br>). O armazenamento na nuvem utiliza o recurso do Sistema NextCloud, homologado previamente pelo Departamento de Tecnologia da Informação.

### 2. DIRETRIZES GERAIS

- 2.1 Não é permitida a utilização de quaisquer outros sistemas ou serviços de nuvem através da rede da Prefeitura, exceto o sistema homologado pelo Departamento de Tecnologia da Informação.
- 2.2 Documentos superiores à 20MB (Megabytes) que necessitem ser transmitidos para fora da rede (intranet), deverá obrigatoriamente utilizar o sistema Drive/Cloud institucional;
- 2.3 O serviço de Drive/Cloud serve para hospedar e compartilhar somente arquivos compatíveis com as atribuições do serviço público prestado pelos seus colaboradores, não sendo permitidos o envio de arquivos de cunho pessoal, ilegal, pornografia, etc.
- 2.4 A responsabilidade pelo vazamento de informações e arquivos armazenados e compartilhados na nuvem é inteiramente do usuário;



## NC 07 – Política do Sistema de Videomonitoramento (CFTV)

### 1. OBJETIVO

Esta normativa visa estabelecer diretrizes claras e procedimentos para a administração segura e eficaz do Sistema de Videomonitoramento (CFTV), administrado pelo Departamento de Tecnologia da Informação da Prefeitura Municipal de Paranaguá, assegurando a vigilância e a segurança patrimonial através do monitoramento eficiente e do armazenamento seguro das imagens captadas.

### 2. DIRETRIZES GERAIS

#### 2.1 Responsabilidade Exclusiva:

A gestão técnica e administração dos sistemas de Videomonitoramento (CFTV) serão de exclusividade dos técnicos especializados em TI do Departamento de Tecnologia da Informação do município. Contudo, a operação contínua do sistema, incluindo o monitoramento dos alertas e alarmes emitidos pelos sistemas, será responsabilidade da Secretaria Municipal de Segurança, incumbência naturalmente atribuída aos guardas civis municipais.

#### 2.2 Controle de Acesso e Segurança das Imagens:

O acesso às imagens gravadas pelo Sistema de Videomonitoramento (CFTV) e a sua administração deve ser restrito a indivíduos autorizados. Deve-se implementar medidas rigorosas de segurança digital para proteger contra acessos não autorizados, perda, dano ou vazamento das imagens.

#### 2.3 Monitoramento e Manutenção:

O sistema deve ser monitorado continuamente para garantir seu funcionamento adequado. A manutenção preventiva e corretiva deve ser realizada regularmente, assegurando a qualidade e a disponibilidade das imagens para fins de segurança.

#### 2.4 Proteção da Privacidade:

Deve-se garantir a proteção da privacidade conforme as leis aplicáveis, limitando o monitoramento a áreas públicas e de interesse para a segurança patrimonial, excluindo áreas privadas sem consentimento explícito.

#### 2.5 Armazenamento das imagens

As imagens capturadas serão armazenadas de forma segura nos servidores instalados no data center do Departamento de Tecnologia da informação.

#### 2.6 Período de retenção e descarte de imagens:



As imagens têm um período de retenção de 30 dias corridos. Em caso de ocorrência constatada, é necessário contatar o Departamento de Tecnologia da Informação para que as imagens sejam reservadas. Sua liberação só será possível mediante formalização da solicitação através de processo administrativo autorizado pelo Secretário da pasta.

## 2.7 Solicitação de Imagens:

Para instruir processos administrativos e/ou inquéritos policiais, as imagens devem ser solicitadas especificando a data/hora da ocorrência, com a devida autorização dos Secretários Municipais envolvidos, justificando o pedido por meio de ofício protocolado ao Departamento de Tecnologia da Informação.

## 2.8 Acesso ao sistema e imagens para terceiros:

Será possível estabelecer parcerias, desde que haja um convênio formalmente firmado entre a Prefeitura de Paranaguá e a entidade interessada, devendo o mesmo ser apreciado pelo Departamento Jurídico quanto à legalidade, respeitando:

- I. Proposta de Convênio: A entidade interessada deve apresentar uma proposta detalhada, especificando os objetivos da parceria, as necessidades de acesso ao sistema e imagens, e os benefícios esperados para ambas as partes.
- II. Análise Jurídica: O convênio proposto será submetido ao Departamento Jurídico da Prefeitura de Paranaguá para uma análise minuciosa. Esta etapa é crucial para garantir que todas as disposições do convênio estejam em conformidade com a legislação vigente, assegurando a legalidade e a segurança jurídica do acordo.
- III. Aprovação e Assinatura: Após a aprovação do Departamento Jurídico, o convênio será encaminhado para assinatura das partes envolvidas. Esta formalização é necessária para oficializar a parceria e definir as responsabilidades e obrigações de cada parte.



## NC 08 – Administração do Sistema de Controle de Acesso de Pessoas

### 1. OBJETIVO

Estabelecer diretrizes e procedimentos para a administração do Sistema de Controle de Acesso em instalações da Prefeitura Municipal, garantindo a segurança das instalações através do gerenciamento efetivo de entradas e saídas.

### 2. DIRETRIZES GERAIS

#### 2.1 Responsabilidade Exclusiva:

A administração do Sistema de Controle de Acesso será realizada exclusivamente por profissionais designados pela Secretaria de Administração, que possuam conhecimento técnico específico nesta área ou que recebam capacitação e treinamento para operar os sistemas

#### 2.2 Cadastro e Autenticação:

Todos os usuários dos sistemas devem ser cadastrados previamente, com a coleta de informações necessárias para sua identificação e autenticação.

#### 2.3 Auditoria e Monitoramento:

O sistema deve registrar todas as tentativas de acesso, permitindo a auditoria de entradas e saídas em tempo real e a investigação de incidentes de segurança.

#### 2.4 Atualização e Manutenção:

O Sistema de Controle de Acesso deve ser mantido atualizado em relação às tecnologias de segurança e receber manutenção regular para garantir sua eficácia e confiabilidade.

#### 2.5 Treinamento e Conscientização:

Os usuários do sistema devem receber treinamento sobre as práticas e procedimentos de segurança, e o uso adequado do sistema de controle de acesso, promovendo uma cultura de segurança na instituição.

Estas normativas visam fortalecer a segurança das instalações e a integridade dos sistemas de vigilância e controle de acesso, através de uma administração focada, competente e em conformidade com as legislações aplicáveis



## **NC 09 – Política de Administração de Servidores/Datacenter**

### **1. OBJETIVO**

Esta política estabelece diretrizes estritas e procedimentos para a administração dos servidores da Prefeitura Municipal, visando assegurar uma gestão exclusiva, segura e eficiente dos recursos críticos de TI por parte dos Administradores de Rede concursados. O objetivo é proteger a infraestrutura crítica e garantir a integridade e a disponibilidade dos sistemas de informação vitais para o funcionamento da Prefeitura.

### **2. DIRETRIZES GERAIS**

#### **2.1 Exclusividade de Administração:**

A responsabilidade pela administração dos servidores e da infraestrutura do datacenter é estritamente reservada aos Administradores de Rede, que são funcionários públicos concursados e qualificados para esta função. Esta exclusividade tem como finalidade primordial a proteção contra vulnerabilidades de segurança, garantindo a estabilidade operacional e a integridade dos dados.

#### **2.2 Restrição de Acesso:**

Acesso administrativo aos servidores e recursos do datacenter será negado a indivíduos que não sejam Administradores de Rede, abrangendo cargos comissionados e agentes políticos, entre outros. Esta medida é crucial para a manutenção da segurança, prevenindo acessos não autorizados e mitigando potenciais ameaças internas.

#### **2.3 Capacitação e Responsabilidade:**

É mandatório que todos os Administradores de Rede participem de treinamentos contínuos focados em segurança da informação, gestão de sistemas e nas mais recentes atualizações tecnológicas, assegurando que estejam plenamente capacitados para administrar a infraestrutura de TI com eficiência e responsabilidade.

#### **2.4 Processo de Acesso:**

O procedimento de acesso aos servidores e ao datacenter por parte dos Administradores de Rede deve ser rigorosamente controlado através de métodos de autenticação forte, reforçando a segurança e o controle de acesso.

#### **2.5 Gerenciamento de Incidentes:**

Na ocorrência de qualquer incidente de segurança que impacte os servidores ou a rede, é imperativo que o Secretário da Pasta seja imediatamente informado. Os



# PREFEITURA MUNICIPAL DE PARANAGUÁ

Secretaria Municipal de Administração  
Departamento de Tecnologia da Informação



Administradores de Rede devem tomar todas as ações necessárias para a rápida resolução do problema, seguindo protocolos de resposta a incidentes preestabelecidos.

## 2.6 Revisão e Atualização da Política:

Para garantir sua efetividade e relevância, esta política deverá ser revisada exclusivamente pelos administradores de rede anualmente ou sempre que houver alterações significativas na infraestrutura de TI ou no cenário de ameaças cibernéticas. Isso assegura que as estratégias de segurança estejam atualizadas e alinhadas com as melhores práticas do setor. A revisão desta normativa é uma prerrogativa reservada aos administradores de rede, enfatizando a importância de seu papel na manutenção da segurança da informação.

Esta política reafirma o compromisso da Prefeitura com a segurança da informação e a gestão eficiente de seus recursos de TI, garantindo que a administração dos servidores e do datacenter seja conduzida de maneira exclusiva, competente e responsável.

Paranaguá, 15 de julho de 2024.

Comissão Técnica de Tecnologia da Informação

---

Alan Glaison dos Santos Mozer  
Membro CTTI

---

Alexander Fabiano Schley  
Membro CTTI

---

Andreia Soares  
Membro CTTI

---

Helison Zola dos Santos  
Membro CTTI

---

Luiz Andre Megiolaro dos Santos  
Membro CTTI

---

Michele dos Santos  
Membro CTTI

---

Ronei Ruiz Soares  
Membro CCTI



# PREFEITURA MUNICIPAL DE PARANAGUÁ

Secretaria Municipal de Administração  
Departamento de Tecnologia da Informação



---

Jaci Ricardo Leal Passos  
Presidente CTTI

---

Renan da Silva França  
Secretário CTTI

---

Tabajara Machado de Souza Junior  
Superintendente de Tecnologia da Informação

---

Marcela Paula Henrique da Silva  
Secretária Municipal de Administração