PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento de Normas e Diretrizes Administrativas

"Todo servidor (concursado/comissionado) que fará uso dos recursos computacionais da Prefeitura Municipal de Paranaguá, tem o dever e a responsabilidade de zelar pela segurança e a integridade das informações e dos equipamentos de informática "

Esta PSI tem como base e referência:

- Norma ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação
- Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI): Regulamenta o acesso a informações públicas e estabelece critérios de transparência e proteção de dados.
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD): Determina regras para o tratamento de dados pessoais e sensíveis no setor público e privado.
- Decreto nº 10.222/2020 (Estratégia Nacional de Segurança Cibernética – E-Ciber): Define diretrizes para segurança digital nos órgãos públicos.
- Constituição Federal (Art. 37): Determina os princípios da administração pública (legalidade, impessoalidade, moralidade, publicidade e eficiência).
- Norma ISO/IEC 27001 e 27002: Estabelece padrões internacionais de segurança da informação.
- Marco Civil da Internet (Lei nº 12.965/2014): Define princípios, garantias e direitos no uso da internet no Brasil.

HISTÓRICO DE VERSÕES:

Versão 1.0 - 2025
Criação: Aline Abalem Stahlschimidt / Rafael Carneiro Sacoman / Weslley José Silveira
Aprovação: Comitê de Revisão e Governança da Segurança da Informação (Decreto n°570)

SUMÁRIO

Esta PSI tem como base e referência: 1

HISTÓRICO DE VERSÕES: 1

ARTIGO PRIMEIRO - OBJETIVOS 3

ARTIGO SEGUNDO- REQUISITOS DA PSI 3

ARTIGO TERCEIRO - DAS RESPONSABILIDADES ESPECÍFICAS 4

3.1 Dos Servidores (concursados/comissionados) em Geral 4

3.2 Dos Detentores da Informação 4

3.3 Da Área de Segurança da Informação 5

3.4 Do Comitê de Segurança da Informação 5

ARTIGO QUARTO - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE 6

ARTIGO QUINTO - DA MATRIZ DE ACESSO 7

ARTIGO SEXTO - SEGURANÇA DA INFORMAÇÃO 7

ARTIGO SÉTIMO – E-MAIL 7

ARTIGO OITAVO - INTERNET 8

ARTIGO NONO - IDENTIFICAÇÃO 9

ARTIGO DÉCIMO - COMPUTADORES E RECURSOS TECNOLÓGICOS 11

ARTIGO DÉCIMO PRIMEIRO - DISPOSITIVOS MÓVEIS 12

ARTIGO DÉCIMO SEGUNDO - DATACENTER 13

ARTIGO DÉCIMO TERCEIRO - TRILHAS DE AUDITORIA 13

ARTIGO DÉCIMO QUARTO - BACKUP 13

ARTIGO DÉCIMO QUINTO – NORMAS COMPLEMENTARES 14

ARTIGO DÉCIMO SEXTO - DAS DISPOSIÇÕES FINAIS 14

NC 01 – Política de Controle de Acesso 15

NC 02 – Política de Publicações no Portal do Município 18

NC 03 – Política para uso de Serviço de Nuvem – Cloud (DriveLocal) 19

NC 04 – Política do sistema de Circuito Fechado de Televisão (CFTV) 20

NC 05 – Administração do Sistema de Controle de Acesso de Pessoas 21

NC 06 – Política de Administração de Servidores/Datacenter 22

PSI – POLÍTICA DE SEGURANÇAS DA INFORMAÇÃO – 2025
Prefeitura Municipal de Paranaguá

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes da Prefeitura Municipal de Paranaguá 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 Prefeitura Municipal de Paranaguá. A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27001, 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.

ARTIGO PRIMEIRO - OBJETIVOS

O presente documento tem como objetivo:

1.1 Estabelecer diretrizes que permitam aos servidores (concursados/comissionados) seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades do Município e de proteção legal da Prefeitura Municipal de Paranaguá. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Garante a proteção das informações quanto à:

a) Integridade: garantia de que a informação seja mantida em seu estado original não sendo adulterada falsificada ou furtada, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
b) Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
c) Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário, mesmo com as interrupções involuntárias de sistemas, ou seja, não intencionais.

1.2 Aplicar a PSI a todos os servidores (concursados/comissionados) da Prefeitura Municipal de Paranaguá e a qualquer pessoa detentora de informações, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade intelectual, industrial **(Lei nº 9279)** e de direitos autorais, **(Lei nº 9610).**

ARTIGO SEGUNDO- REQUISITOS DA PSI

2.1 Para a uniformidade da informação, a PSI deverá ser comunicada a todos os servidores (concursados/comissionados) da Prefeitura Municipal de Paranaguá a fim de que a política seja cumprida.

2.2 Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Segurança da Informação (CSI).

2.3 A PSI deverá ser revista e atualizada periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança da Informação (CSI).

2.4 A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos servidores (concursados/comissionados). Todos os servidores (concursados/comissionados) devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar uma cópia desta PSI e, a cada mudança, além da nova ciência, deverão assinar novamente.

2.5 Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Superintendência, conforme a cadeia hierárquica, e se este julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

2.6 Deverão ser criados e instituídos controles apropriados, como registros de atividade (logs), em todos os pontos e sistemas em que a Prefeitura Municipal de Paranaguá julgar necessário para reduzir os riscos dos seus ativos de informação

como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico e nos sistemas.

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

2.8 A Prefeitura Municipal de Paranaguá exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus servidores (concursados/comissionados), 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.

2.9 Esta PSI é obrigatória para todos os servidores (concursados/comissionados), independentemente do nível hierárquico ou função na Prefeitura Municipal de Paranaguá, bem como de vínculo empregatício ou prestação de serviço.

2.10 O não cumprimento dos requisitos previstos nesta PSI acarretará violação às regras internas e sujeitará o usuário às medidas administrativas e legais cabíveis.

2.11 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.

ARTIGO TERCEIRO - DAS RESPONSABILIDADES ESPECÍFICAS

3.1 Dos Servidores (concursados/comissionados) em Geral

3.1.1 Entende-se por servidor (concursado/comissionado) toda e qualquer pessoa física, contratada, estatutário ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da Prefeitura Municipal de Paranagua.

3.1.2 Será de inteira responsabilidade de cada servidor (concursado/comissionado), todo prejuízo ou dano que vier a sofrer ou causar à Prefeitura Municipal de Paranaguá e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

3.2 Dos Detentores da Informação

3.2.1 Da Área de Tecnologia da Informação

3.2.1.a. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

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

3.2.1.c. Configurar os equipamentos, ferramentas e sistemas concedidos aos servidores (concursados/ comissionados) com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

3.2.1.d. Os administradores de rede, suporte quanto Diretor de Infraestrutura podem, pelas características de seus privilégios, 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 testes entre outros

3.2.1.e. Segregar as funções operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

3.2.1.f. 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.

3.2.1.g. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes.

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

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

3.2.1.j. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida.

3.2.1.k. 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:

3.2.1.l. Os usuários (logins) individuais de servidores (concursados/comissionados) serão de responsabilidade do próprio servidor (concursado/comissionado).

3.2.1.m. Os usuários (logins) de terceiros serão de responsabilidade do secretário da área contratante.

3.2.1.n. Proteger continuamente todos os ativos de informação da Prefeitura Municipal de Paranaguá 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.

3.2.1.o. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Prefeitura Municipal de Paranaguá em processos de mudança.

3.2.1.p. Definir as regras formais para instalação de software e hardware em ambiente de produção, exigindo o seu cumprimento dentro da Prefeitura Municipal de Paranaguá.

3.2.1.q. Realizar auditorias periódicas de configurações técnicas e análise de riscos.

3.2.1.r. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais, caso tenha autorização para tal.

3.2.1.s. Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Prefeitura Municipal de Paranaguá, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Prefeitura Municipal de Paranaguá.

3.2.1.t. Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da Prefeitura Municipal de Paranaguá operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

3.2.1.u. Monitorar o ambiente de TI, gerando indicadores e históricos de:

3.2.1.v. Tempo de resposta no acesso à internet e aos sistemas críticos;

3.2.1.w. Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);

3.3 Da Área de Segurança da Informação

3.3.1 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 Paranaguá.

3.3.2 Promover a conscientização dos servidores (concursados/comissionados) em relação à relevância da segurança da informação para o negócio.

3.3.3 Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

3.3.4 Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a Prefeitura Municipal de Paranaguá.

3.4 Do Comitê de Segurança da Informação

3.4.1 Deve ser formalmente constituído por servidores (concursados/comissionados) com nível tecnico compativel com a função.

3.4.2 Deverá o CSI 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 Paranaguá.

3.4.3 O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

3.4.4 Cabe ao CSI:

3.4.4.a Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;

3.4.4.b Propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;

3.4.4.c Avaliar os incidentes de segurança e propor ações corretivas;

3.4.4.d Definir as medidas cabíveis nos casos de descumprimento da PSI;

3.4.4.e Assessorar na implementação das ações de segurança da informação;

3.4.4.f Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

3.4.4.g Propor Normas e Procedimentos internos relativos à segurança da informação em conformidade com as legislações existentes sobre o tema.

3.4.4.h Sugerir ações visando ao alinhamento do plano de desenvolvimento de tecnologia da informação com o planejamento estratégico da Prefeitura Municipal de Paranaguá como um todo;

3.4.4.i Apresentar sugestões e críticas com a finalidade de alinhar as áreas de negócio e todas as áreas envolvidas na disponibilização da infraestrutura tecnológica dos órgãos, no âmbito da Segurança da Informação;

3.4.4.j Uniformizar as políticas de Segurança da Informação;

3.4.4.k Elaborar a Política de Segurança da Informação e sua respectiva atualização;

3.4.4.l Elaborar o Plano de Continuidade de Negócios, o Plano de Administração de Crises, Plano de Contingência, o Plano de Recuperação de Desastres e o Plano de Continuidade Operacional dentro do Programa de Gestão da Continuidade de Negócios além da sua respectiva atualização;

3.4.4.m Analisar as necessidades em relação a Segurança da Informação;

3.4.4.n Apreciar e emitir parecer sobre os relatórios das atividades desenvolvidas;

ARTIGO QUARTO - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

4.1 Para garantir as regras mencionadas nesta **PSI**, a Prefeitura Municipal de Paranaguá poderá:

4.1.1 Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, 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;

4.1.2 Tornar públicas as informações obtidas pelos sistemas de monitoramento, no caso de exigência judicial, solicitação de um nivel hierarquico superior ou por determinação do Comitê de Segurança da Informação;

4.1.3 Realizar, a qualquer tempo, inspeção física e/ou virtual nas máquinas de sua propriedade;

4.1.4 Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

ARTIGO QUINTO - DA MATRIZ DE ACESSO

5.1 Para que se cumpra de maneira efetiva, são efetuados mapeamento de logs e registros de acesso, que são conferidos periodicamente pelo Comitê de Segurança da Informação, a fim de que se tenha Gestão de Identidades, Controle de Acessos, Revisões de Acessos, Controles de Vazamentos de informações e Prevenções de Fraudes.

Os níveis de acessos ao sistema são distribuídos da seguinte forma

5.1.1 NIVEL 1 - **Nível Básico:** é quem recebem as demandas de atendimento da Prefeitura Municipal de Paranaguá. É o primeiro contato do suporte, que pode ser realizado por chat, e-mail ou telefone. Se a demanda for de pouca complexidade, ele está apto a resolver. É responsável pelo atendimento e registro de todas as solicitações, direcionando os chamados para os níveis superiores. Os servidores (concursados/comissionados) que se enquadram neste nível, tem acesso limitado ao sistema, por este motivo, estão capacitados a resolver problemas de baixa complexidade, como configurações simples, com pequenas alterações, que podem ser feitas por ele ou orientadas aos servidores.

5.1.2 NIVEL 2 - **Nível Intermediário:** destinado a questões mais técnicas e aprofundadas, como falhas mais complexas do software. Este nível é exercido por cargo de Supervisão, e é responsável por todos os chamados encaminhados pelo nível 3. Cabe a ele analisar os atendimentos com critérios técnicos e, estando fora dos seus níveis de acesso, repassar a demanda ao nível 1.

5.1.3 NIVEL 3 - **Nível Máster:** analisa problemas mais complexos do software, sendo exercido pelos cargos de Gerência. Atende a todos os problemas não solucionados pelos níveis anteriores. Possuem conhecimento amplo do software e tem acesso total ao sistema como um todo.

ARTIGO SEXTO - SEGURANÇA DA INFORMAÇÃO

6.1 O Servidor (concursado/comissionado) assume o compromisso de não utilizar, revelar ou divulgar a terceiros e pessoas não autorizadas, 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, mesmo depois de terminado o vínculo contratual mantido com a Prefeitura Municipal de Paranaguá.

ARTIGO SÉTIMO – E-MAIL

O objetivo desta norma é informar aos servidores (concursados/comissionados) quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo:

7.1 O uso do correio eletrônico é para fins corporativos e relacionados às atividades do servidor (concursados/comissionados) dentro da Prefeitura Municipal de Paranaguá. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso e não prejudique ou cause impacto no tráfego da rede.

7.2 É proibido aos servidores (concursados / comissionados), o uso do correio eletrônico para:

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

7.2.2 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;

7.2.3 Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Prefeitura Municipal de Paranaguá vulneráveis a ações civis ou criminais;

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

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

7.2.6 Apagar mensagens pertinentes de correio eletrônico quando qualquer servidor (concursados/comissionados) estiver submetido ou sujeito a algum tipo de investigação.

7.2.7 Produzir, transmitir ou divulgar mensagem que:

7.2.7.a Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Prefeitura Municipal de Paranaguá;

7.2.7.b Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador, entre outros;

7.2.7.c Contenha arquivos com código executável ou qualquer outra extensão que represente um risco à segurança;

7.2.7.d Vise obter acesso não autorizado a outro computador, servidor ou rede;

7.2.7.e Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

7.2.7.f Vise burlar qualquer sistema de segurança;

7.2.7.g Vise vigiar secretamente ou assediar outro usuário;

7.2.7.h Vise acessar informações confidenciais sem explícita autorização do proprietário;

7.2.7.i Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

7.2.7.j Inclua imagens criptografadas ou de qualquer forma mascaradas;

7.2.7.k Tenha conteúdo considerado impróprio, obsceno ou ilegal;

7.2.7.l Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

7.2.7.m Contenha perseguição preconceituosa baseada em genero, etinia, raça, incapacidade física e/ou mental entre outras situações protegidas;

7.2.7.n Tenha fins políticos locais ou do país (propaganda política);

7.2.7.o Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

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

- Brasão da Prefeitura de Municipal de Paranaguá;
- Nome do servidor (concursados/comissionados);
- Departamento;
- Secretária;
- Telefone(s) *(quando houver);*
- Correio eletrônico;
- Endereço;
- Link oficial da Prefeitura Municipal de Paranaguá;
- Termo de Confidencialidade – *Usar modelo abaixo:*
  "Esta mensagem e qualquer arquivo anexo são confidenciais e destinados apenas ao uso do(s) destinatário(s) mencionado(s). Se você não for o destinatário pretendido, por favor, notifique o remetente imediatamente e apague esta mensagem de seu sistema. Qualquer uso, divulgação, cópia ou distribuição não autorizada desta mensagem é estritamente proibida."

ARTIGO OITAVO - INTERNET

8.1 Todas as regras atuais visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. **Embora a conexão direta e permanente da rede corporativa com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.**

8.2 Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria.

Portanto, a Prefeitura Municipal de Paranaguá, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

8.3 Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da Prefeitura Municipal de Paranaguá, 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 privativas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

8.4 A Prefeitura Municipal de Paranaguá, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas.

8.5 Toda tentativa de alteração dos parâmetros de segurança, por qualquer servidor (concursados/comissionados), sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao servidor (concursados/comissionados) 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 Prefeitura Municipal de Paranaguá cooperará ativamente com as autoridades competentes.

8.6 A internet disponibilizada pelo Departamento de Tecnologia da Informação (DTI) aos seus servidores (concursados/ comissionados), independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos, podendo ser bloqueado caso ocorra abuso.

8.7 Como é do interesse da Prefeitura Municipal de Paranaguá que seus servidores (concursados/comissionados) 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.

8.8 Apenas os servidores (concursados/comissionados) autorizados pela Prefeitura Municipal de Paranaguá poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

8.9 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, ou qualquer outra tecnologia correlata que venha surgir na internet, podendo sofrer sanções administrativas.

8.10 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 Gestão do Departamento Tecnologia da Informação.

8.11 Os servidores (concursados/comissionados) não poderão em hipótese alguma utilizar os recursos para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

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

8.13 Servidores (concursados/comissionados) com acesso à internet não poderão efetuar upload de qualquer software licenciado ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

8.14 Os servidores (concursados/comissionados) não poderão utilizar os recursos da Prefeitura Municipal de Paranaguá para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, software para fins de assédio, perturbação ou programas de controle de outros computadores.

8.15 O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente.

8.16 Não é permitido acesso a sites de proxy e VPN;

8.17 Não é permitido usar navegadores (Tor, I2P, Freenet, ...) para DeepWeb ou correlacionados.

ARTIGO NONO - IDENTIFICAÇÃO

9.1 Os dispositivos de identificação e senhas protegem a identidade do servidor (concursado/comissionado), evitando e prevenindo que uma pessoa se faça passar por outra perante a Prefeitura Municipal de Paranaguá e/ou terceiros. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no **Código Penal Brasileiro (Art. 307 do Decreto-lei nº 2.848).** Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os servidores (concursado/comissionado).

9.2 Todos os dispositivos de identificação utilizados, como o número de matrícula do servidor (concursados / comissionados), o crachá, as identificações de acesso aos sistemas, os certificados e as assinaturas digitais, têm de estar associadas a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

9.3 O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a Prefeitura Municipal de Paranaguá e a legislação (cível e criminal).

9.4 Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no **Código Penal Brasileiro (art. 307 – falsa identidade).**

9.5 Se existir login de uso compartilhado por mais de um servidor (concursados / comissionados), a responsabilidade perante a Prefeitura Municipal de Paranaguá e a legislação **(cível e criminal)** será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação (oficializado) do gestor de uso compartilhado, ele deverá ser responsabilizado.

9.6 É proibido o compartilhamento de login para funções de administração de sistemas/rede.

9.7 Serão distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas, mediante a apresentação de documento pessoal, bem como identificação da Prefeitura Municipal de Paranaguá. Este processo será realizado na portaria do edifício, e só terá o acesso as áreas restritas mediante autorização expressa.

9.8 Todo acesso de terceiros as áreas sensíveis e críticas, são acompanhadas pelo responsável do setor, desde a sua entrada até a sua saída.

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

9.10 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.

9.11 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 do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

9.12 Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato (via telelefone) com o Departamento de Tecnologia da Informação para regularização.

9.13 Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

9.14 A senha deve seguir um nível de criticidade mínima, contendo no minimo 8 caracteres, com letras maiusculas, minusculas, números e caracteres especiais (!, @, #, ...).

9.15 Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico do Departamento de Tecnologia da Informação.

9.16 Caso o servidor (concursado/comissionado) esqueça sua senha, poderá acessar o Link (http://senha.paranagua.pr.gov.br) para a geração de uma nova senha, e/ou ele deverá requisitar formalmente (Via GLPI) a troca ou comparecer pessoalmente ao Departamento de Tecnologia da Informação para cadastrar uma nova senha.

9.17 A periodicidade máxima para troca das senhas é 90 (sessenta) dias, não podendo ser repetidas as últimas 3 senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 45 dias.

9.18 Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum servidor (concursados/comissionados) for exonerado ou realocado de entidade, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia de Informação, a fim de que essa providência

seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

ARTIGO DÉCIMO - COMPUTADORES E RECURSOS TECNOLÓGICOS

10.1 Os equipamentos disponíveis aos servidores (concursados/comissionados) são de propriedade da Prefeitura Municipal de Paranaguá, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da Prefeitura Municipal de Paranaguá, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

10.2 A Prefeitura Municipal de Paranaguá, na qualidade de proprietário das estações de trabalho, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

10.3 É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do Departamento de Tecnologia da Informação, ou de quem este determinar.

10.4 Todas as atualizações e correções de segurança (patches) do sistema operacional ou aplicativos dos Servidores, somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois disponibilizadas no ambiente de produção.

10.5 No caso de ser identificado um patch crítico, será dado a prioridade pela equipe responsável para que seja aplicado as devidas diretrizes, levando em consideração o tempo disponível para tal.

10.6 Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro.

10.7 **Arquivos pessoais** e/ou não pertinentes ao negócio (**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, poderão ser excluídos sem aviso prévio.

10.8 Documentos imprescindíveis para as atividades dos servidores (concursados/comissionados) da Prefeitura Municipal de Paranaguá deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), **não terão backup** e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

10.9 Os servidores (concursados/comissionados) 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 Departamento de Tecnologia de Informação.

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

10.10.1. Os servidores (concursados/comissionados) devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;

10.10.2. 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 Tecnologia da Informação ou por terceiros devidamente contratados para o serviço;

10.10.3. 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 no GLPI. 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;

10.10.4. O servidor (concursado/comissionado) deverá manter as configurações do equipamento disponibilizado pela Prefeitura Municipal de Paranaguá, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação (PSI), assumindo a responsabilidade como custodiante de informações;

10.10.5. Todos os recursos tecnológicos adquiridos pela Prefeitura Municipal de Paranaguá devem ter imediatamente suas senhas padrões (default) alteradas;

10.10.6. Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos servidores (concursados / comissionados), datas e horários de acesso;

10.11 Situações em que é proibido o uso de computadores e recursos tecnológicos da Prefeitura Municipal de Paranaguá:

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

10.11.2. Burlar quaisquer sistemas de segurança;

10.11.3. Acessar informações confidenciais sem explícita autorização do proprietário;

10.11.4. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares;

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

10.11.6. 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;

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

10.11.8. Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional;

ARTIGO DÉCIMO PRIMEIRO - DISPOSITIVOS MÓVEIS

11.1 A Prefeitura Municipal de Paranaguá deseja facilitar a mobilidade e o fluxo de informações entre seus servidores (concursados /comissionados), permitindo o uso destes dispositivos, desde que não infrinjam as regras descritas nesta política.

11.2 Quando se descreve "dispositivos móveis" entende-se qualquer equipamento eletrônico com atribuições de mobilidade, aprovados ou não pela Superintendência do Departamento de Tecnologia da Informação, como por exemplo, notebooks, smartphones, pendrives, câmeras fotográficas, entre outros.

11.3 Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os servidores (concursados/comissionados) que utilizem tais equipamentos.

11.4 Em ambiente de alocação da Prefeitura Municipal de Paranaguá, o servidor (concursado/comissionado) deverá responsabilizar-se em não utilizar quaisquer dispositivos, programas e/ou aplicativos que não tenham sido autorizados via Oficio para um técnico, analista e/ou Superintendência do Departamento de Tecnologia da Informação.

11.5 A utilização não autorizada de quaisquer dispositivos, programas e/ou aplicativos que não tenham sido autorizados pelo Departamento de Tecnologia da Informação, constituirá como uma violação do **ITEM 11.4**, caracterizando-se como uma infração legal prevista na **Lei 9.609/1998**

11.6 O servidor (concursados/comissionados) deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a Prefeitura Municipal de Paranaguá e/ou a terceiros.

11.7 O servidor (concursados/comissionados) que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da Prefeitura Municipal de Paranaguá deverá submeter previamente tais equipamentos ao processo de autorização da Departamento de Tecnologia da Informação.

ARTIGO DÉCIMO SEGUNDO - DATACENTER

12.1 Todo acesso ao Datacenter pelo sistema (on-line), deverá ser registrado (usuário, data e hora e IP de acesso) mediante software próprio.

12.2 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.

12.3 No caso de exoneração e/ou realocação para outra entidade servidores (concursados/comissionados) que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação e da lista de servidores (concursados / comissionado) autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter.

12.4 A administração dos Servidores, Máquinas virtuais e ativos de Rede desta municipalidade é de responsabilidade exclusiva dos Administradores de Rede, Diretor de Infraestrutura e Segurança e o Superintendente do Departamento de Tecnologia da Informação, sendo expressantemente vedado o acesso aos Servidores, Máquinas virtuais e ativos de Rede por outros servidores e cargos comissionados.

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

12.6 Devido a criticidade do ambiente de Datacenter, a manutenção (Limpeza, realocação, padronização dos Racks, entre outros) preventiva dos Servidores, assim como a manutenção dos Racks de Rede (manutenção das NBR14565, TIA/EIA 568, ISO/IEC 11801, ABNT NBR16665, ...), deve ser realizado pelos Administradores de Rede e Diretor de Infraestrutura e Segurança do Departamento de Tecnologia de Informação.

ARTIGO DÉCIMO TERCEIRO - TRILHAS DE AUDITORIA

13.1 As trilhas de auditoria (logs) são monitoradas e gravadas diariamente, sendo analisadas a cada 15 dias, gerando um relatório que será apresentado ao Comitê de Segurança da Informação, e aprovados por todos os membros.

13.2 Após a aprovação do relatório, as trilhas são arquivadas e segregadas de maneira física e logica, por um período de até 5 anos. Os relatórios aprovados pelo como Comitê de Segurança da Informação são devidamente arquivados.

ARTIGO DÉCIMO QUARTO - BACKUP

14.1 Todos os backups devem ser automáticos por sistemas de agendamento (realizados no minimo uma vez ao dia) automatizados 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.

14.2 Os backups poderão ser armazenados em dispositivos de storage dedicados, tais como SAN (Storage Area Network) ou NAS (Network Attached Storage), que oferecem maior flexibilidade, escalabilidade e eficiência no armazenamento e recuperação de dados. Esses dispositivos devem atender aos seguintes requisitos:

- Localização em ambientes seguros, climatizados e com acesso restrito.
- Implementação de redundância de dados, utilizando tecnologias como RAID ou equivalentes, para maior segurança contra falhas.

14.3 Os servidores (concursados/comissionados) 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.

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

14.5 Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

14.6 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.

14.7 Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade.

14.8 Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis.

14.9 Testes de restauração (restore) de backup devem ser executados por seus responsáveis, aproximadamente a cada 30 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.

ARTIGO DÉCIMO QUINTO – NORMAS COMPLEMENTARES

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

15.1.1. NC 01 - Política de Controle de Acesso;
15.1.2. NC 02 - Política de Publicações no Portal do Município
15.1.3. NC 03 - Política para uso de Serviço de Nuvem - Cloud
15.1.4. NC 04 - Política do Sistema de Circuito Fechado de Televisão (CFTV)
15.1.5. NC 05 - Administração do Sistema de Controle de Acesso de Pessoas
15.1.6. NC 06 - Política de Administração de Servidores/Datacenter

ARTIGO DÉCIMO SEXTO - DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Prefeitura Municipal de Paranaguá, sendo que todas as práticas que ameaçam a segurança da informação serão tratadas com a aplicação de ações disciplinares, desde uma advertência verbal, processo administrativo Disciplinar, podendo chegar até a exoneração, levando em consideração os fatores como: função exercida pelo servidor (concursado/comissionado), período da ocorrência, local, horário e prejuízo real ou potencial causado à Prefeitura Municipal de Paranaguá, e seus contribuintes e fornecedores, ou seja, é importante considerar a natureza pública e o compromisso com os princípios éticos e legais pela Prefeitura Municipal de Paranaguá.

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. Todo cadastramento de conta de acesso à rede da Prefeitura Municipal de Paranaguá deve ser formalizado mediante solicitação via ofício e protocolado, assinado pelo Secretário da pasta do requerente e endereçada aos Administradores de Rede lotados no Departamento de Tecnologia da Informação.

2.2. Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário aos quais as informações estão vinculadas;

2.3. A base de dados de senhas deve ser armazenada com criptografia;

2.4. 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;

2.5. 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.

2.6. 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;

2.7. As contas com alto privilégio de administração de rede deve 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.

2.8. A administração dos servidores e máquinas virtuais desta municipalidade é de responsabilidade exclusiva dos Administradores de Rede, Diretor de infraestrutura e Superintendente do Departamento de Tecnologia da Informação, sendo expressamente vedado o acesso por outros servidores.

2.9. 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, Diretor de infraestrutura e Superintendente 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.

1.4. O acesso remoto aos recursos da Prefeitura Municipal de Paranaguá, é estritamente controlado e limitado à equipe responsável pela Administração de Redes, Suporte de Técnico, Diretor de Infraestrutura e Superintendente do Departamento de Tecnologia da Informação (concursados/comissionados). 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 Prefeitura Municipal de Paranaguá.

1.5. Qualquer tentativa não autorizada de acesso remoto será prontamente detectada e tratada de acordo com os procedimentos de segurança estabelecidos e acionando os meios legais para apuração.

1.6. Além do acesso remoto restrito à equipe designada, a utilização de máquinas virtuais (VMs) e Docker nas instalações da Prefeitura Municipal de Paranaguá, 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 Tecnologia da Informação. Apenas os Administradores de Redes, Diretor de Infraestrutura e Superintendente do Departamento de Tecnologia da Informação (concursados/comissionados), são autorizados a criar e gerenciar VMs e Docker, garantindo a integridade e a segurança dos sistemas virtuais.

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:

4.2.1. 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:

4.3.1. Manter em sigilo sua senha de acesso as bases de dados;

4.3.2. 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:

4.4.1. Deverá ser firmado Termo de Responsabilidade, pela Prefeitura Municipal de Paranaguá e a entidade interessada, sobre as informações que deverão ser compartilhadas.

4.4.2. 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.

4.4.3. 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:

4.5.1. 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.

4.5.2. 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.

4.5.3. 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

5.1.1. Os controles de acesso físico visam restringir o acesso aos equipamentos de Tecnologia da Informação;

5.1.2. O acesso ao Datacenter somente poderá ser feito por pessoas autorizadas pelos Administradores de Rede, Diretor de Infraestrutura e Superintendente do Departamento de Tecnologia a Informação (concursados / comissionados), que são os responsáveis pelo Datacenter;

5.1.3. 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;

5.1.4. 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;

5.1.5. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto famígero ou inflamável;

NC 02 – 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 sítio 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 a autorização 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 03 – Política para uso de Serviço de Nuvem – Cloud (DriveLocal)

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 Servidor (concursado/comissionado);

NC 04 – Política do sistema de Circuito Fechado de Televisão (CFTV)

1. OBJETIVO

Esta normativa visa estabelecer diretrizes claras e procedimentos para a administração segura e eficaz do Sistema de CFTV (Circuito Fechado de TV ou VMS – Vídeo Management System), administrado pelo Departamento de Tecnologia da Informação da Prefeitura Municipal de Paranaguá e a Contratada para fornecer o serviço, 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 do Sistema de Circuito Fechado de Televisão (CFTV) serão de exclusividade dos técnicos especializados em TI do Departamento de Tecnologia da Informação da Prefeitura de Paranaguá. 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 Circuito Fechado de Televisão (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 Em conformidade com a LGPD:

As imagens captadas pelo sistema de Circuito Fechado de Televisão (CFTV) serão utilizadas exclusivamente para fins de segurança patrimonial, proteção de pessoas e prevenção de incidentes, em conformidade com os princípios da Lei Geral de Proteção de Dados (LGPD). ***Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).***

NC 05 – 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 06 – 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, Diretor de infraestrutura e Superintendente do Departamento de Tecnologia da Informação. 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, Diretor de Infraestrutura e Superintendente do Departamento de Tecnologia da Informação, que são servidores públicos (concursados/comissionados) 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, Diretor de Infraestrutura e Superintendente do Departamento de Tecnologia da Informação, sejam eles servidores concursados ou comissionados. 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, Diretor de Infraestrutura e Superintendente do Departamento de Tecnologia da Informação (concursados/comissionados), 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, Diretor de Infraestrutura e Superintendente do Departamento de Tecnologia da Informação (concursados/comissionados), 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 Administradores de Rede, Diretor de Infraestrutura e Superintendente do Departamento de Tecnologia da Informação (concursados/comissionados), 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 pelo Comitê de Segurança da Informação, 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 ao Comitê de Segurança da Informação, enfatizando a manutenção da segurança da informação.

Esta política reafirma o compromisso da Prefeitura Municipal de Paranaguá, 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.

**Revogam-se todas as publicações de PSI – Politica de Segurança da Informação até esta data.*

Paranaguá, 15 de Abril de 2025.

Adriano Ramos
Prefeito Municipal de Paranaguá

Thiago Themanski Campos
Secretário Municipal de Governo

Rafael Carneiro Sacoman
Superintendente Especial de Tecnologia da Informação

Aline Abalem Stahlschimidt
Presidente do Comitê de Revisão e Governança da Segurança da Informação