PREFEITURA MUNICIPAL DA ESTANCIA CLIMATICA DE CAMPOS NOVOS PAULISTA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Setor Responsável:

Divisão de Tecnologia da Informação (TI)
Prefeitura Municipal de Campos Novos Paulista – SP

Endereço:

Prefeitura Municipal de Campos Novos Paulista
Rua Edgard Bonini (DENGO), 492, Centro,
Campos Novos Paulista – SP | CEP: 19960-000
Telefone: (14) 3476-1144 | Site: www.camposnovospaulista.sp.gov.br | e-mail: ti@camposnovospaulista.sp.gov.br

PREFEITURA MUNICIPAL DE CAMPOS NOVOS PAULISTA

Divisão de Tecnologia da Informação (TI)

Histórico de Versões

Data	Versão	Descrição	Autor
26/06/2025	1.0	Primeira versão do documento	

SUMÁRIO

1. OBJETIVO

Estabelecer diretrizes, normas e procedimentos para garantir a proteção dos ativos de informação, a privacidade dos dados e a segurança da infraestrutura tecnológica da Prefeitura Municipal de Campos Novos Paulista, em conformidade com a Lei Geral de Proteção de Dados (LGPD) e as boas práticas de segurança da informação.

2. INTRODUÇÃO

I. De acordo com a norma ISO 27002, a informação é considerada um ativo valioso, sujeito a riscos decorrentes de ameaças, tanto acidentais quanto intencionais, uma vez que processos, sistemas, redes e pessoas possuem vulnerabilidades inerentes. Nesse contexto, a Prefeitura Municipal de Campos Novos Paulista, em conjunto com eventuais parceiros, é responsável pelo armazenamento, processamento e gestão de informações de diversos setores da administração pública, seja em Data Centers locais ou em ambientes de computação em nuvem (Cloud).

II. Diante disso, torna-se essencial garantir que essas informações sejam devidamente processadas, armazenadas e protegidas contra ameaças e riscos. A segurança da informação depende da implementação de um conjunto adequado de controles, aliados a políticas, procedimentos, processos, estruturas organizacionais, além de recursos tecnológicos, como softwares e hardwares.

III. É importante destacar que a conectividade — seja direta ou indireta, temporária ou permanente — proporciona inúmeros benefícios, mas também expõe os ativos de informação a riscos significativos, exigindo uma abordagem rigorosa quanto à proteção desses dados.

IV. Neste cenário, a Política de Segurança da Informação (PSI) tem como objetivo estabelecer as diretrizes, os limites e os princípios que norteiam a proteção das informações institucionais, além de definir as responsabilidades legais de todos os colaboradores, usuários e setores da administração pública direta e indireta.

V. Por fim, a PSI visa padronizar normas e procedimentos obrigatórios, com o propósito de orientar o comportamento dos envolvidos e assegurar a

confidencialidade, integridade e disponibilidade das informações sob a responsabilidade da Prefeitura Municipal de Campos Novos Paulista.

3. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO – PSI

> "O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um minuto interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos".
>
> ABNT NBR ISO/IEC 27002:2013

3.1 Objetivo

Visa estabelecer diretrizes, princípios e normas para a proteção das informações tratadas pela Prefeitura Municipal de Campos Novos Paulista, a fim de garantir a confidencialidade, integridade e disponibilidade dos dados, em conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e demais normas aplicáveis.

3.2 Divulgação

A Política de Segurança da Informação (PSI) será amplamente divulgada a todos os colaboradores da Prefeitura Municipal de Campos Novos Paulista, abrangendo tanto a administração direta quanto a indireta. O documento ficará disponível de forma acessível, permitindo sua consulta a qualquer momento pelos colaboradores.

No momento da admissão de novos colaboradores que, por suas funções, tenham acesso à rede corporativa, computadores, internet e/ou e-mail institucional da Prefeitura, será obrigatória a entrega de uma cópia da PSI, seja em formato físico e/ou digital.

Os novos colaboradores deverão realizar a leitura completa da política e, na sequência, formalizar sua ciência e concordância por meio da assinatura do **"Termo de Responsabilidade de Uso e Segurança da Informação"**, instrumento que assegura o compromisso individual com o cumprimento das normas e diretrizes estabelecidas.

Essa medida constitui um dos principais mecanismos de conscientização, orientação e garantia da plena divulgação da política no ambiente organizacional.

3.3 Princípios

A segurança da informação será guiada pelos seguintes princípios:

I. **Confidencialidade**: Garantir que a informação seja acessível apenas a pessoas autorizadas;
II. **Integridade**: Preservar a exatidão e completude das informações;
III. **Disponibilidade**: Assegurar que as informações estejam acessíveis sempre que necessário;
IV. **Responsabilidade**: Cada agente público é responsável pelo tratamento ético e seguro da informação;
V. **Legalidade**: O tratamento de informações deve observar a LGPD e outras normas legais.

4. RESPONSABILIDADES

4.1 Dos Colaboradores

É considerado **colaborador** toda pessoa física que exerça atividades em nome da Prefeitura Municipal de Campos Novos Paulista, seja por meio de vínculo efetivo (concurso público), contratação temporária, prestação de serviços (individual ou por intermédio de pessoa jurídica), bem como ocupantes de cargos em comissão, funções de confiança ou qualquer outro tipo de vínculo funcional ou contratual, atuando dentro ou fora das dependências da Prefeitura.

- **Servidores e Colaboradores:** Devem cumprir integralmente esta política, zelar pelas boas práticas e relatar qualquer irregularidade.
- **TI Municipal:** Responsável pela implementação de soluções técnicas de segurança e suporte aos usuários.
- **Controladoria e Encarregado (DPO):** Monitorar a conformidade com a LGPD e promover ações corretivas quando necessário.
- **Comitê LGPD:** Acompanhar a evolução das práticas e revisar esta política periodicamente.

É dever de todos os colaboradores:

- Cumprir integralmente as diretrizes estabelecidas na Política de Segurança da Informação (PSI);
- Buscar orientação junto ao gestor imediato sempre que houver dúvidas relacionadas à segurança da informação;
- Proteger as informações institucionais contra acesso, alteração, destruição ou divulgação não autorizada;
- Garantir que os recursos tecnológicos disponibilizados sejam utilizados exclusivamente para os fins institucionais autorizados pela Prefeitura Municipal de Campos Novos Paulista;
- Observar e cumprir rigorosamente as legislações e normas relacionadas à propriedade intelectual;
- Zelar pelo sigilo e confidencialidade das informações, evitando qualquer tipo de compartilhamento indevido;
- Comunicar de forma imediata à área de Tecnologia da Informação qualquer ocorrência de descumprimento, suspeita ou violação das normas previstas nesta política.

4.2 Dos Gestores

Consideram-se **gestores** o Prefeito Municipal, os Secretários Municipais, Chefes de Divisão e demais ocupantes de cargos em comissão que possuam atribuições de gestão dentro da Prefeitura Municipal de Campos Novos Paulista.

Compete aos gestores:

- Atuar como modelo de conduta, mantendo uma postura ética e exemplar no cumprimento e na promoção das práticas de segurança da informação;
- Assegurar que todos os colaboradores sob sua gestão tenham pleno conhecimento da Política de Segurança da Informação (PSI) e sejam responsabilizados pelo seu cumprimento;
- Promover a divulgação, orientação e acompanhamento do cumprimento desta política em suas respectivas áreas;
- Identificar eventuais desvios, não conformidades ou violações relacionadas à segurança da informação e adotar, prontamente, as medidas corretivas cabíveis;
- Adaptar processos, procedimentos, fluxos de trabalho e sistemas sob sua responsabilidade, alinhando-os às diretrizes estabelecidas na PSI;
- Avaliar, aprovar e propor melhorias contínuas nos termos, controles, processos e demais dispositivos previstos nesta política, garantindo sua efetividade e aderência às necessidades institucionais.

4.3 Da Área de Tecnologia da Informação

5. SOBRE O E-MAIL INSTITUCIONAL

O uso do correio eletrônico institucional da Prefeitura Municipal de Campos Novos Paulista é estritamente destinado a fins corporativos, sendo utilizado exclusivamente para atividades relacionadas às funções e atribuições do colaborador no exercício de suas atividades na Prefeitura.

Fica expressamente **proibido**:

- O uso do e-mail institucional para assuntos de caráter pessoal, particular ou que não estejam diretamente relacionados às atividades da Prefeitura;
- Da mesma forma, é vedado o uso de e-mails pessoais e particulares para a realização de atividades vinculadas às funções exercidas na Prefeitura Municipal de Campos Novos Paulista.

Essa medida visa garantir a segurança da informação, a rastreabilidade das comunicações institucionais e a conformidade com as normas internas e legais aplicáveis.

É terminantemente **proibido**, no uso do correio eletrônico institucional e demais meios eletrônicos da Prefeitura Municipal de Campos Novos Paulista, as seguintes práticas:

- Enviar mensagens sem autorização utilizando o endereço eletrônico do seu departamento ou se passando por outra pessoa, bem como utilizar indevidamente o nome, identidade ou endereço de e-mail de terceiros;
- Enviar qualquer tipo de mensagem que possa expor o remetente, a Prefeitura Municipal de Campos Novos Paulista ou qualquer de suas unidades e servidores a responsabilidades cíveis, criminais, administrativas ou éticas;
- Produzir, transmitir, replicar ou divulgar mensagens contendo ameaças eletrônicas, tais como: *spam*, *e-mail bombing*, propagação de vírus, *malware*, *ransomware*, *worms*, entre outros conteúdos maliciosos;
- Enviar, compartilhar ou disponibilizar arquivos com extensões potencialmente perigosas, como: .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf ou quaisquer outros arquivos que possam representar risco à segurança da informação e dos sistemas institucionais;
- Produzir, transmitir ou divulgar qualquer mensagem, conteúdo ou ação que tenha por finalidade, ou que resulte, na interrupção, degradação ou indisponibilidade de serviços, servidores ou redes de computadores da Prefeitura, seja por métodos ilícitos, maliciosos ou não autorizados;
- Executar qualquer ação eletrônica que, de forma intencional, busque contornar, burlar ou violar sistemas, mecanismos ou controles de segurança da informação;
- Produzir, transmitir ou divulgar mensagens de qualquer natureza que contenham conteúdo ofensivo, calunioso, difamatório, injurioso, degradante, discriminatório, violento, ameaçador, pornográfico, obsceno, ou qualquer outro que atente contra a moral, os bons costumes, a legislação vigente ou que possa gerar danos à imagem institucional da Prefeitura.

- Mensagens que contenham informações sensíveis, sigilosas ou restritas devem ser enviadas utilizando ferramentas de criptografia ponta a ponta ou criptografia de anexos.

5.1 Sobre Hardware, Internet e Outros

É terminantemente proibido:

- Conectar dispositivos pessoais (notebooks, celulares, pendrives, HDs externos) às redes, computadores e sistemas da Prefeitura sem autorização prévia e formal;
- Alterar configurações dos computadores, impressoras, roteadores, switches ou qualquer equipamento de TI sem autorização da área técnica;
- Desconectar ou desligar equipamentos críticos (servidores, nobreaks, roteadores, firewall) sem motivo operacional e sem conhecimento da TI;
- Movimentar equipamentos de TI (computadores, notebooks, impressoras) de um setor para outro sem autorização formal da área responsável;
- Executar arquivos de origem desconhecida;
- Acessar links suspeitos recebidos por e-mail, mensagens instantâneas ou SMS;
- Instalar extensões, plugins ou complementos nos navegadores sem autorização da TI;
- Desabilitar, remover ou ignorar alertas de antivírus, firewall ou ferramentas de proteção.

5.2 Serviços de Streaming, Comunicação Instantânea e Redes Sociais

- Fica Proibido a utilização de serviços de streaming (rádios online, canais de Transmissão, *Twitch*, *Youtube*, *Tiktok*, *Spotify*), Redes Sociais (*Facebook*, Instagram e similares).
- A utilização de serviços de streaming (rádios online, canais de transmissão e similares), plataformas de comunicação instantânea (como *WhatsApp, Skype, Teams*, entre outros) e redes sociais (*Facebook, LinkedIn, Instagram* e afins) será, em regra, restrita. No entanto, poderá ser autorizada de forma excepcional, desde que haja solicitação formal e aprovação prévia dos

responsáveis pela segurança da informação da respectiva Secretaria, Órgão Municipal, e a autoridade máxima no município (Prefeito em exercício). em conformidade com as diretrizes estabelecidas no item 5.4 desta política.

5.3 Fica a cargo do Departamento de "TI"

- Fazer utilização de filtros de acesso à internet que atuam de forma automática e preventiva. Esses filtros têm como objetivo restringir e bloquear a navegação ou o acesso a sites cujo conteúdo seja considerado inadequado, ilícito ou prejudicial, incluindo, mas não se limitando a: pornografia, apologia ou incentivo ao uso de drogas, pedofilia, qualquer forma de racismo, discriminação, discurso de ódio, violência, extremismo ou qualquer outro conteúdo que possa comprometer a segurança, a integridade da rede corporativa, os ativos de informação e a imagem institucional da Prefeitura;
- Apresentar relatórios do sistema de filtros de acessos periódicos aos usuários que eventualmente navegam ou utilizam recursos da instituição como computadores, e-mail, ou a internet indevidamente;
- Apresentar à autoridade máxima qualquer indício de conduta criminosa ou que possa ser prejudicial para a administração pública ou de terceiros, para que sejam tomadas ações administrativas cabíveis.

5.4 Requerimento para solicitação de acessos a sites específicos

- Caso haja a necessidade de acesso a alguma plataforma especifica não autorizada (como exemplo o departamento de comunicação com redes sociais da administração), deverão solicitar a liberação do acesso via formulário **"FASA – Formulário de Acesso a Sites Autorizados"(Anexo I),** onde depois de preenchido com o nome do solicitante, e o superior direto da pasta, e enviado ao Departamento Municipal de T.I (ti@camposnovospaulista.sp.gov.br), e o mesmo será encaminhado e apresentado ao prefeito para ser avaliado e autorizado, em conformidade com as diretrizes estabelecidas no item 3.4 desta política.

5.5. Utilização de Serviços em Regime de Exceção

A utilização de serviços de streaming (rádios online, canais de transmissão, plataformas de vídeo), redes sociais (*Facebook, Instagram, LinkedIn, TikTok* e similares), ferramentas de comunicação instantânea (*WhatsApp Web, Telegram Web, Skype, Teams, Zoom* e outros), bem como quaisquer serviços online que não sejam diretamente relacionados às atividades da Prefeitura, **é, por padrão, restrita e bloqueada**, visando preservar a segurança da informação, garantir a disponibilidade da rede e priorizar o uso dos recursos tecnológicos para fins institucionais.

5.5.1 Critérios para Autorização

No entanto, poderá ser autorizada a utilização desses serviços **em caráter excepcional**, desde que atendidos os seguintes critérios:

1. **Justificativa formal:** A solicitação deverá conter uma descrição clara da necessidade funcional, demonstrando que o uso está diretamente relacionado às atividades institucionais do setor, projeto ou ação específica;
2. **Análise técnica:** A área de Tecnologia da Informação (TI) realizará uma análise técnica dos riscos, avaliando impacto na segurança, na integridade dos dados e na disponibilidade da rede;
3. **Autorização formal:** A liberação deverá ser aprovada pelos responsáveis pela segurança da informação, conjuntamente com o gestor da Secretaria ou Órgão solicitante;
4. **Prazo definido:** A permissão deverá ter um prazo de validade pré-estabelecido. Caso haja necessidade de prorrogação, uma nova solicitação formal deverá ser realizada;
5. **Registro e controle:** Toda autorização concedida será devidamente documentada, registrando setor, usuário(s), serviços liberados, período de uso e justificativa;
6. **Monitoramento:** O uso autorizado será monitorado para garantir que se mantenha dentro dos parâmetros definidos e não gere riscos à segurança da informação ou impactos na infraestrutura;

7. **Revogação:** A qualquer tempo, a Prefeitura Municipal de Campos Novos Paulista poderá revogar a autorização caso sejam identificados riscos, mau uso, desvio de finalidade ou impacto na rede e nos serviços.

Exemplos de Situações em que o uso pode ser autorizado:

- Divulgação de ações institucionais em redes sociais, quando executada pelo setor de comunicação da Prefeitura;
- Utilização de plataformas de comunicação instantânea (como WhatsApp Web ou Teams) para interação direta com munícipes, em projetos específicos, eventos, ações de atendimento remoto, reuniões internas da administração, audiências entre outros;
- Transmissões de eventos oficiais, sessões públicas, audiências ou campanhas, via plataformas de streaming.

6. SENHAS

As senhas são a primeira linha de defesa contra acessos não autorizados a sistemas e informações. A criação e gestão de senhas seguras são cruciais para a proteção de dados pessoais e a conformidade com a LGPD, que exige a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (Art. 46 da LGPD).

6.1 Criação de Senhas Fortes

Todos os colaboradores são responsáveis por criar e manter senhas fortes para todas as contas e sistemas corporativos. Uma senha forte deve:

- Ter no mínimo 12 caracteres;
- Conter uma combinação de letras maiúsculas e minúsculas;
- Incluir números e caracteres especiais (ex: !, @, #, $, %, ^, &, *);

- Não conter informações pessoais óbvias (nome, data de nascimento, etc.) ou sequências fáceis de adivinhar (ex: "123456", "senha");
- Ser única para cada sistema ou serviço, evitando a reutilização de senhas.

6.2. Gestão e Proteção de Senhas

A gestão adequada das senhas é tão importante quanto a sua criação. As seguintes práticas são obrigatórias:

- Confidencialidade: Nunca compartilhe suas senhas com ninguém, nem mesmo com colegas, superiores ou equipes de suporte técnico. A senha é de uso pessoal e intransferível;
- Armazenamento Seguro: Não anote senhas em locais visíveis ou de fácil acesso (ex: post-its, cadernos na mesa). Recomenda-se o uso de gerenciadores de senhas aprovados pela instituição, se disponíveis;
- Alteração Periódica: Altere suas senhas regularmente, conforme a política de segurança da informação da instituição ou sempre que houver suspeita de comprometimento.
- Bloqueio de Contas: Em caso de múltiplas tentativas falhas de login, as contas serão bloqueadas para proteger contra ataques de força bruta. O colaborador deverá seguir o procedimento de desbloqueio estabelecido;
- Notificação de Suspeita: Qualquer atividade suspeita relacionada à sua conta ou senha deve ser imediatamente reportada ao setor de Tecnologia da Informação (TI) ou ao Encarregado de Dados (DPO).

O uso de acessos, com identificação de outra pessoa, constitui crime tipificado no Código Penal Brasileiro (art. 307 – Falsidade Ideológica).

6.3. Autenticação de Múltiplos Fatores (MFA)

Sempre que disponível, a autenticação de múltiplos fatores (MFA) deve ser ativada e utilizada. O MFA adiciona uma camada extra de segurança, exigindo uma segunda forma de verificação (ex: código enviado para o celular, biometria) além da senha, dificultando o

acesso indevido mesmo que a senha seja comprometida. A implementação do MFA é uma medida técnica robusta que contribui significativamente para a segurança dos dados pessoais, conforme exigido pela LGPD.

7. EQUIPAMENTOS

Os equipamentos utilizados para o desempenho das atividades laborais, sejam eles de propriedade da instituição ou pessoais (no caso de política BYOD - Bring Your Own Device, se aplicável), são pontos críticos para a segurança da informação e a proteção de dados pessoais. A LGPD exige que sejam adotadas medidas de segurança para proteger os dados tratados nesses equipamentos. O uso inadequado ou a falta de proteção podem levar a vazamentos de dados e sérias consequências para a instituição e para os titulares dos dados.

7.1. Uso e Manutenção de Equipamentos Corporativos

Todos os equipamentos fornecidos pela instituição (computadores, notebooks, tablets, smartphones, etc.) devem ser utilizados exclusivamente para fins profissionais e de acordo com as políticas internas. As seguintes diretrizes devem ser seguidas:

- Acesso Controlado: Mantenha os equipamentos sempre protegidos por senhas fortes e ative o bloqueio automático de tela após um curto período de inatividade;
- Software Autorizado: Instale e utilize apenas softwares e aplicativos autorizados pela área de TI. A instalação de programas não autorizados pode comprometer a segurança do equipamento e dos dados;
- Atualizações de Segurança: Mantenha o sistema operacional, antivírus e demais softwares sempre atualizados. As atualizações corrigem vulnerabilidades de segurança que podem ser exploradas por cibercriminosos;
- Antivírus e Firewall: Certifique-se de que o software antivírus e o firewall estejam sempre ativos e atualizados nos equipamentos;
- Não Compartilhamento: Não compartilhe equipamentos corporativos com pessoas não autorizadas, incluindo familiares e amigos;
- Relato de Problemas: Qualquer mau funcionamento, perda, roubo ou suspeita de infecção por malware deve ser imediatamente reportado ao setor de TI.

7.2. Proteção de Dados em Equipamentos

A proteção dos dados armazenados e processados nos equipamentos é fundamental para a conformidade com a LGPD. As seguintes práticas são obrigatórias:

- Armazenamento Seguro: Armazene dados pessoais apenas em locais designados e seguros (ex: servidores da instituição, sistemas em nuvem autorizados). Evite armazenar dados pessoais diretamente no disco rígido local do equipamento, a menos que seja estritamente necessário e temporário;
- Criptografia: Sempre que possível e aplicável, utilize a criptografia para proteger dados sensíveis armazenados em discos rígidos, pendrives ou outros dispositivos de armazenamento;
- Backup: Certifique-se de que os dados importantes estejam sendo regularmente copiados e armazenados de forma segura, conforme as políticas de backup da instituição. Isso garante a disponibilidade dos dados em caso de falha do equipamento;
- Descarte Seguro: Ao descartar equipamentos ou mídias de armazenamento, siga os procedimentos de descarte seguro da instituição para garantir que os dados sejam irrecuperáveis. Nunca descarte equipamentos contendo dados pessoais no lixo comum.

7.3. Uso de Equipamentos Pessoais (BYOD)

Caso a instituição adote uma política de BYOD, o uso de equipamentos pessoais para fins profissionais deve seguir diretrizes específicas para garantir a segurança dos dados:

- Acordo de Uso: O colaborador deve assinar um termo de responsabilidade e concordância com as políticas de segurança da informação da instituição;
- Segregação de Dados: Mantenha os dados corporativos e pessoais segregados. Utilize perfis de usuário separados ou soluções de virtualização, se fornecidas pela TI;
- Medidas de Segurança: Os equipamentos pessoais utilizados para fins profissionais devem possuir as mesmas medidas de segurança exigidas para os equipamentos corporativos (senhas fortes, antivírus, firewall, atualizações);

- Acesso Remoto Seguro: O acesso a sistemas e redes corporativas a partir de equipamentos pessoais deve ser feito exclusivamente através de conexões seguras (VPN - Virtual Private Network) fornecidas pela instituição;
- Remoção de Dados: Em caso de desligamento do colaborador ou término da política BYOD, todos os dados corporativos devem ser removidos de forma segura do equipamento pessoal, conforme orientação da TI;
- Dispositivos Removíveis: Em caso de desligamento do colaborador todos os dispositivos removíveis que contenham dados da instituição devem ser entregues para a administração para recolhimento e remoção dos dados pertencentes a instituição.

8. DISPOSITIVOS PORTÁTEIS

Dispositivos portáteis, como pendrives, discos externos, smartphones e tablets, são ferramentas úteis para o trabalho, mas representam um risco significativo para a segurança da informação e a proteção de dados pessoais se não forem utilizados corretamente. A facilidade de perda ou roubo desses dispositivos, aliada à grande capacidade de armazenamento, pode resultar em vazamentos de dados massivos e graves violações da LGPD. É imperativo que todos os colaboradores sigam as diretrizes abaixo para mitigar esses riscos.

8.1. Uso de Dispositivos Portáteis

- Minimização do Uso: Utilize dispositivos portáteis apenas quando estritamente necessário para o desempenho de suas funções. Priorize o armazenamento e o compartilhamento de dados através dos sistemas e redes corporativas seguras;
- Dispositivos Aprovados: Utilize apenas dispositivos portáteis aprovados e, se possível, fornecidos pela instituição. Dispositivos pessoais devem seguir as diretrizes da política de BYOD (se aplicável) e ter as medidas de segurança adequadas;
- Conexão Segura: Ao conectar dispositivos portáteis a computadores corporativos, certifique-se de que o sistema operacional e o antivírus estejam atualizados e que o dispositivo seja verificado em busca de malware;

- Evitar Conexões em Computadores Não Confiáveis: Não conecte dispositivos portáteis da instituição a computadores públicos ou não confiáveis (ex: cibercafés, computadores de terceiros).

8.2. Proteção de Dados em Dispositivos Portáteis

A proteção dos dados armazenados em dispositivos portáteis é crucial para evitar perdas e acessos não autorizados:

- Criptografia: Todos os dispositivos portáteis que armazenam dados pessoais ou informações confidenciais da instituição devem ser criptografados. A criptografia é uma medida técnica essencial para proteger os dados em caso de perda ou roubo do dispositivo;
- Senhas Fortes: Proteja o acesso aos dispositivos portáteis com senhas fortes, PINs ou biometria. Ative o bloqueio automático após um curto período de inatividade;
- Armazenamento Mínimo: Armazene o mínimo de dados pessoais possível em dispositivos portáteis. Transfira os dados para os sistemas corporativos seguros assim que a tarefa for concluída;
- Não Armazenar Dados Sensíveis: Evite armazenar dados pessoais sensíveis (saúde, religião, orientação sexual, etc.) em dispositivos portáteis, a menos que seja absolutamente necessário e com a devida criptografia e autorização.

8.3. Perda ou Roubo de Dispositivos Portáteis

- A perda ou roubo de um dispositivo portátil contendo dados da instituição é um incidente de segurança grave e deve ser tratado com urgência;
- Reporte Imediato: Em caso de perda, roubo ou extravio de qualquer dispositivo portátil da instituição ou pessoal que contenha dados corporativos, o incidente deve ser reportado imediatamente ao setor de TI e ao Encarregado de Dados (DPO);
- Ação Remota: Se o dispositivo possuir recursos de localização e limpeza remota, a TI deverá ser acionada para tentar localizar e apagar os dados remotamente, minimizando o risco de vazamento;

- Investigação: Todos os incidentes de perda ou roubo serão investigados para determinar a extensão do impacto e as medidas corretivas necessárias, incluindo a notificação aos titulares dos dados e à ANPD, se aplicável, conforme o Art. 48 da LGPD.

9. USO DA REDE

O uso adequado da rede de computadores da instituição é fundamental para garantir a segurança da informação e a proteção dos dados pessoais. A rede é a espinha dorsal da comunicação e do acesso à informação, e seu uso indevido pode expor a instituição a ataques cibernéticos, vazamentos de dados e outras ameaças que comprometem a conformidade com a LGPD. Todos os colaboradores devem aderir às seguintes diretrizes ao utilizar a rede interna e externa da instituição.

9.1. Acesso à Rede

- Acesso Autorizado: O acesso à rede da instituição é restrito a colaboradores autorizados e deve ser feito utilizando credenciais pessoais e intransferíveis;
- Rede Wi-Fi Corporativa: Utilize a rede Wi-Fi corporativa para acesso à internet e sistemas internos. Evite o uso de redes Wi-Fi públicas ou não seguras para acessar informações confidenciais ou dados pessoais;
- Rede de Convidados: Se houver uma rede de convidados, ela deve ser utilizada apenas por visitantes e para fins específicos, sem acesso a recursos internos da rede corporativa;
- VPN (Virtual Private Network): Para acesso remoto à rede corporativa, é obrigatório o uso da VPN fornecida pela instituição. A VPN garante que a comunicação seja criptografada e segura, protegendo os dados em trânsito;

9.2. Navegação na Internet e E-mail

A navegação na internet e o uso de e-mail são atividades rotineiras que exigem atenção redobrada para evitar riscos à segurança e à privacidade:

- Sites Confiáveis: Acesse apenas sites confiáveis e evite clicar em links suspeitos ou de origem desconhecida. Phishing e sites maliciosos são vetores comuns de ataques;
- Downloads: Faça downloads apenas de fontes confiáveis e autorizadas. Tenha cautela com anexos de e-mail e arquivos executáveis;
- Conteúdo Inapropriado: É proibido o acesso, download ou compartilhamento de conteúdo ilegal, ofensivo, discriminatório ou pornográfico utilizando os recursos de rede da instituição;
- E-mail Corporativo: O e-mail corporativo deve ser utilizado para fins profissionais. Evite o envio de dados pessoais sensíveis por e-mail sem criptografia ou outras medidas de segurança adequadas. Tenha cuidado ao enviar e-mails para múltiplos destinatários, utilizando a opção Cco (Com Cópia Oculta) quando necessário para proteger a privacidade dos endereços;
- Anexos: Verifique sempre a procedência de anexos de e-mail antes de abri-los, especialmente se forem de remetentes desconhecidos ou contiverem extensões suspeitas.

9.3. Redes Sociais e Aplicativos de Mensagens

O uso de redes sociais e aplicativos de mensagens no ambiente de trabalho deve ser feito com responsabilidade e atenção à segurança da informação:

- Uso Pessoal vs. Profissional: Mantenha a distinção entre o uso pessoal e profissional das redes sociais. Evite discutir assuntos confidenciais ou dados pessoais da instituição em plataformas públicas;
- Informações Confidenciais: Nunca compartilhe informações confidenciais, dados pessoais de terceiros ou informações estratégicas da instituição em redes sociais ou aplicativos de mensagens;
- Configurações de Privacidade: Mantenha as configurações de privacidade de suas contas pessoais nas redes sociais sempre atualizadas e restritivas;
- Aplicativos de Mensagens: Utilize aplicativos de mensagens aprovados pela instituição para comunicação profissional. Tenha cautela ao compartilhar dados pessoais ou confidenciais por esses meios, mesmo em grupos fechados.

9.4. Monitoramento da Rede

A instituição reserva-se o direito de monitorar o uso da rede, incluindo o tráfego de internet, e-mails e acesso a sistemas, para fins de segurança, conformidade legal e auditoria. Este monitoramento será realizado em conformidade com a legislação vigente e com o devido respeito à privacidade dos colaboradores, visando exclusivamente a proteção dos ativos da instituição e dos dados pessoais sob sua guarda.

10. AUDITORIA

Tem por objetivo garantir o controle, a rastreabilidade e a integridade das atividades realizadas nos sistemas, redes e equipamentos da Prefeitura Municipal de Campos Novos Paulista, possibilitando a detecção de incidentes, fraudes, acessos indevidos e o cumprimento das normas estabelecidas nesta Política de Segurança da Informação (PSI) e na legislação vigente.

10.1 Diretrizes Gerais de Auditoria

Todas as ações realizadas por usuários nos sistemas, dispositivos e rede da Prefeitura poderão ser **monitoradas e registradas** por meio de ferramentas de auditoria e controle de logs.

O monitoramento poderá abranger:

- Acessos a sistemas, horários e usuários logados;
- Tráfego de rede;
- Uso de email institucional;
- Alterações em dados ou configurações;
- Dispositivos Móveis conectados à rede;
- Servidores;
- Atividades em estações de trabalho.

Os Registros de auditoria poderão ser utilizados para identificar violações à PSI; investigar incidentes de segurança; atender a obrigações legais, administrativas ou judiciais; Auxiliar na melhoria contínua dos controles internos.

Os dados de auditoria serão armazenados em ambientes seguros e com acesso restrito, obedecendo aos princípios de confidencialidade, integridade e disponibilidade.

10.2 Transparência e Legalidade

- As atividades de auditoria não visam expor ou fiscalizar aspectos pessoais dos funcionários da administração, mas sim garantir a conformidade com o uso adequado dos ativos institucionais;
- As informações coletadas serão utilizadas apenas para uso interno, exceto em casos de: Requisições Judiciais; Processos administrativos; Demandas do Ministério Público; Demandas do Tribunal e contas do Estado de São Paulo; ou solicitação formal de algum gestor.

- Consequências para caso os registros de auditoria revelem uso indevido dos recursos, tentativas de fraudes, violação de dados, ou qualquer desvio de conduta, poderão ser adotadas as seguintes medidas: Notificação e Advertência formal; Suspensão ou bloqueio de acessos; abertura de processos administrativo disciplinar (PAD); Comunicação às autoridades competentes, quando aplicável (ANPD); Adoção de medidas corretivas ou preventivas.

11. LGPD – LEI GERAL DE PROTEÇÃO DE DADOS

A Prefeitura Municipal de Campos Novos Paulista, por meio desta Política de Segurança da Informação (PSI), adota e reforça seu compromisso com a proteção dos dados pessoais, em consonância com a **Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD)**.

Faz parte dos princípios desta política assegurar que os dados pessoais coletados, armazenados, processados e compartilhados sejam tratados de forma lícita, transparente, segura e restrita às finalidades institucionais da administração pública municipal.

- Finalidade, adequação e necessidade no tratamento de dados pessoais;
- Transparência com os titulares dos dados;
- Garantia de segurança, integridade e confidencialidade das informações;
- Prevenção contra incidentes de segurança e vazamento de dados;
- Responsabilização e prestação de contas no tratamento de dados.

11.1. Solicitações de Titulares de Dados Pessoais

Para garantir os direitos dos titulares de dados pessoais (como acesso, correção, exclusão, anonimização ou portabilidade de dados), a Prefeitura disponibiliza um processo formal para registro, análise e resposta a essas solicitações.

O procedimento deverá ser realizado por meio de formulário próprio denominado **"Formulário de Atendimento ao Titular de Dados Pessoais – LGPD"**, disponível em anexo a esta PSI (Anexo II).

Todas as solicitações serão tratadas pela área responsável pela proteção de dados da Prefeitura, respeitando os prazos legais e os fluxos internos estabelecidos.

11.2. Responsabilidade dos Colaboradores

É responsabilidade de todos os colaboradores:

- Respeitar a confidencialidade dos dados pessoais acessados no exercício de suas funções;
- Não compartilhar, divulgar ou tratar dados pessoais sem a devida autorização ou finalidade legítima;
- Comunicar imediatamente à área de Tecnologia da Informação ou ao Encarregado de Dados (DPO) qualquer incidente de segurança envolvendo dados pessoais.

12. VIOLAÇÕES E SANÇÕES

O descumprimento das normas, diretrizes e responsabilidades previstas nesta Política de Segurança da Informação (PSI) constitui **violação às regras administrativas da Prefeitura Municipal de Campos Novos Paulista** e poderá acarretar medidas disciplinares, civis e/ou penais, conforme a natureza e gravidade da infração.

12.1 Considera-se violação à PSI, entre outras condutas

- Uso indevido de equipamentos, sistemas, redes, e-mail ou internet para fins pessoais ou ilícitos;
- Divulgação ou compartilhamento não autorizado de informações institucionais ou dados pessoais;
- Acesso não autorizado a sistemas, informações, arquivos ou dispositivos;
- Instalação de softwares não autorizados ou com licenças irregulares;
- Compartilhamento de senhas, credenciais ou uso de identidade de terceiros;
- Ocultação de incidentes de segurança ou falhas que comprometam os ativos de informação.
- Qualquer tentativa de burlar os mecanismos de controle, monitoramento ou segurança da informação.

12.2 - Classificação das Violações

As violações poderão ser classificadas em:

- **Leves**: uso indevido sem prejuízos diretos ou sem recorrência;
- **Médias**: condutas repetidas, com risco à segurança ou à imagem institucional;
- **Graves**: atos intencionais, com prejuízo comprovado à Prefeitura, violação de dados pessoais, quebra de sigilo, vazamento de informações, sabotagem, ou acesso não autorizado a informações críticas.

12.3 - Sanções Possíveis

De acordo com as legislações vigentse e o Estatuto dos Servidores Públicos Municipais de lei numero **522/2011,** de 8 de fevereiro de 2011, poderão ser aplicadas as seguintes sanções:

- Advertência verbal ou escrita;
- Suspensão temporária de acesso a sistemas e recursos tecnológicos;
- Responsabilização administrativa, civil e/ou criminal;
- Abertura de processo administrativo disciplinar (PAD);
- Demissão por justa causa (nos casos mais graves ou reincidentes);
- Rescisão de contrato ou descredenciamento (para prestadores de serviço ou terceiros).

12.4 - Responsabilidade e Fiscalização

- Cabe à área de Tecnologia da Informação (TI),e aos gestores de cada Diretoria zelar pelo cumprimento desta política e registrar, comunicar e tratar os incidentes ou violações detectadas;
- Toda denúncia ou constatação de violação será apurada com garantia de contraditório e ampla defesa, nos termos da legislação aplicável.

CONCLUSÃO

A presente Política de Segurança da Informação (PSI) da Prefeitura Municipal de Campos Novos Paulista estabelece um conjunto de diretrizes, normas e responsabilidades que visam garantir a proteção dos ativos de informação, a continuidade dos serviços públicos, o uso ético e responsável dos recursos tecnológicos e o cumprimento das legislações vigentes, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD).

Mais do que um conjunto de regras, esta política representa um compromisso institucional com a integridade, confidencialidade e disponibilidade das informações que sustentam as atividades da Administração Pública Municipal. A adesão consciente e colaborativa de todos os servidores, colaboradores, gestores e parceiros é essencial para a eficácia das medidas estabelecidas, assegurando um ambiente seguro, transparente e alinhado às boas práticas de governança e segurança da informação.

A atualização contínua deste documento, bem como a capacitação dos usuários e a adequação tecnológica da infraestrutura municipal, são pilares fundamentais para a consolidação de uma cultura de segurança, privacidade e responsabilidade digital na Prefeitura de Campos Novos Paulista.

REFERÊNCIA BIBLIOGRÁFICA E LEGISLAÇÃO APLICÁVEL

Lei Federal 8159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);

Lei Federal 9610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral);

Lei Federal 9279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes);

Lei Federal 3129, de 14 de outubro de 1982 (Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial);

Lei Municipal nº

Lei Federal 10406, de 10 de janeiro de 2002 (Institui o Código Civil);

Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código

Penal);

Lei Federal 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências).

Lei n°. 10.406, de 10 de janeiro de 2022. Institui o Código Civil Brasileiro.

ANEXO - I

FASA – Formulário de Acesso a Sites Autorizados

Instruções:

Este formulário deve ser preenchido pelo solicitante sempre que houver necessidade de acesso a plataformas específicas não autorizadas na rede padrão, conforme diretrizes da política de segurança da informação (item 3.4). Após preenchimento, o formulário deve ser enviado ao Departamento Municipal de T.I pelo e-mail ti@camposnovospaulista.sp.gov.br para análise e encaminhamento ao prefeito para autorização.

Dados do Solicitante

- Nome completo:
- Cargo:
- Departamento/Setor:
- E-mail institucional:
- Telefone para contato:

Detalhes do Acesso Solicitado

- Site ou plataforma a ser acessada:
- URL (endereço do site):
- Justificativa para a solicitação:

Para uso do Departamento Municipal de T.I

- Recebido em:
- Análise preliminar:
- Encaminhamento para autorização do prefeito:
- Data do encaminhamento:

Decisão do Prefeito

- Acesso autorizado: ( ) Sim ( ) Não
- Observações:
- Assinatura do prefeito:
- Data:

ANEXO - II

Formulário de Atendimento ao Titular de Dados Pessoais – LGPD

Identificação do Solicitante

- Nome Completo: _____
- CPF: _____
- Telefone: _____
- E-mail: _____
- Endereço Completo: _____

Tipo de Solicitação

( ) Confirmação da existência de tratamento de dados pessoais
( ) Acesso aos dados pessoais tratados
( ) Correção de dados incompletos, inexatos ou desatualizados
( ) Anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos
( ) Portabilidade dos dados para outro fornecedor
( ) Revogação de consentimento para o tratamento de dados
( ) Informações sobre uso compartilhado de dados com terceiros
( ) Outras (especificar): _____

Descrição da Solicitação

Descreva detalhadamente a informação ou providência desejada:

_____

_____

_____

_____

_____

Documentos Anexados (se necessário)

( ) Cópia do RG ou documento de identificação com foto
( ) Outros (especificar): _____

Prazo e Forma de Resposta

Prazo para resposta: até 15 dias úteis após a data de protocolo.
Forma preferencial de resposta:

( ) E-mail
( )
Correio
( ) Retirada presencial no setor de protocolo

Termo de Ciência

Declaro estar ciente de que o atendimento à minha solicitação será realizado conforme os prazos e limites estabelecidos pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

Assinatura do Solicitante: _____

Data: __/_/20_____

Observações Importantes:

- **O prazo de 15 dias úteis começa a contar a partir da data de protocolo desta ficha.**
- **Caso seja necessária uma extensão de prazo, o solicitante será informado.**
- **Informações adicionais podem ser solicitadas ao titular, caso necessário, para o processamento da solicitação.**