PREFEITURA MUNICIPAL DE PEDERNEIRAS

PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão 1.0
2025

SUMÁRIO

1. INTRODUÇÃO

A Política de Segurança da Informação (PSI), também conhecida como PSI, é um guia essencial que estabelece as diretrizes e práticas corporativas da Prefeitura Municipal de Pederneiras (PMP) para proteger os ativos de informação e reduzir a exposição à responsabilidade legal de todos os seus usuários, como violações de segurança. É obrigatório que esta política seja estritamente seguida e implementada em todas as Secretarias, setores áreas e órgãos subordinados a PMP.

A PSI apresentada tem suas bases alicerçadas nas recomendações preconizadas pelas normas ABNT NBR ISO/IEC 27002:2005 e ISO/IEC 27001. Essas normas são amplamente reconhecidas como um código de boas práticas para a gestão da segurança da informação em escala global. Além disso, a política é também fundamentada no Marco Civil da Internet e nas normas estabelecidas pela Lei Geral de Proteção de Dados (LGPD).

Para fortalecer a segurança da infraestrutura tecnológica que suporta os serviços públicos, esta política visa orientar os servidores da PMP sobre a utilização responsável dos ativos de tecnologia da informação disponibilizados.

2. OBJETIVO

A Política de Segurança da Informação (PSI) municipal estabelece diretrizes e normas para todas as áreas da administração pública, buscando mitigar riscos, garantir a continuidade das operações e proteger contra ameaças diversas, em conformidade com os princípios de autenticidade e legalidade das informações. A implementação deste documento tem como objetivo promover um comportamento ético na utilização de recursos de TI, adotando novas metodologias de trabalho com práticas preventivas para reduzir ameaças e vulnerabilidades.

Além disso, a Prefeitura Municipal de Pederneiras (PMP) estabelece diretrizes específicas para a gestão de riscos, a continuidade dos serviços de TI e a classificação adequada das informações institucionais, conforme estabelecido no Plano de Gestão de Riscos (Anexo III), no Plano de Continuidade e Recuperação de Desastres (Anexo IV), na Política de Classificação da Informação (Anexo V) e na Política de Uso de Criptografia (Anexo VI), garantindo a identificação e tratamento adequado dos riscos associados aos ativos de TI, a continuidade das áreas de negócio, a correta classificação e proteção da integridade das informações armazenadas e transmitidas.

Adicionalmente, destaca-se que está em desenvolvimento e implementação do **Arquivo Público Municipal**, que será responsável por regulamentar, com maior profundidade, a classificação e a guarda de documentos oficiais, garantindo conformidade com normativas arquivísticas e de segurança da informação.

A PSI também busca estabelecer o controle de níveis de acesso de fornecedores externos a sistemas, gerenciar os acessos de colaboradores em equipamentos remotos, garantir a segurança em dispositivos e supervisionar atividades vinculadas à TI. Estas ações visam seguir padrões de comportamento relacionados à segurança da informação, adequados às necessidades do serviço público, proporcionando proteção legal à PMP e aos indivíduos envolvidos, além de melhorar a eficiência na gestão de recursos, proteger

equipamentos e ferramentas de trabalho, reduzir gastos e aprimorar o atendimento aos munícipes, bem como a produtividade dos colaboradores.

3. PRINCÍPIOS

Este documento estabelece padrões comportamentais e princípios básicos relacionados à segurança da informação, que devem ser considerados:

a) Autenticidade: os dados devem ser certificados quanto à sua origem, evitando modificações ao longo do processo. Exemplos de ferramentas incluem biometria e certificado digital;

b) Confidencialidade: o acesso aos dados deve ser restrito a indivíduos, entidades ou órgãos autorizados. Criptografia é um exemplo de ferramenta para garantir a confidencialidade;

c) Disponibilidade: os dados e recursos devem estar disponíveis sempre que necessários para órgãos, indivíduos, entidades ou sistemas autorizados. Exemplos de ferramentas incluem backup, firewall e nobreak;

d) Integridade: os ativos de informação devem estar protegidos contra alterações não autorizadas ou acidentais. Assinatura digital é um exemplo de ferramenta para garantir a integridade dos dados.

4. DIRETRIZES E REQUISITOS

Essas diretrizes são aplicáveis a todos os colaboradores, incluindo funcionários, indivíduos físicos ou jurídicos que tenham acesso a dados ou informações do município por qualquer meio. O escopo abrange a Governança de TI, visando impulsionar melhorias nos sistemas de informação e na gestão municipal, mantendo e otimizando processos, garantindo a segurança das informações e comunicações.

Para assegurar a consistência, é fundamental seguir as diretrizes abaixo como referência:

a) Propriedade da Informação

- Qualquer informação gerada ou recebida pelos colaboradores no curso de suas atividades profissionais para a PMP é considerada propriedade desta instituição. As exceções devem ser claramente definidas e formalizadas por meio de contrato entre as partes.

b) Segurança da Informação

- A preservação da segurança da informação, por meio da análise de vulnerabilidades e mitigação de riscos, é essencial para a manutenção dos serviços e a proteção da instituição. Para isso, devem ser seguidas as diretrizes estabelecidas no Plano de Gestão de Riscos (Anexo III), no Plano de Continuidade e Recuperação de Desastres (Anexo IV) e na Política de Classificação da Informação (Anexo V), garantindo um processo estruturado para identificar, analisar, avaliar e tratar os riscos à segurança

da informação, assim como restaurar os serviços essenciais em caso de falhas ou incidentes e classificar corretamente as informações institucionais.

c) Acesso Autorizado

- Os usuários devem ser autorizados a acessar apenas as informações essenciais para a execução de suas funções. É crucial evitar a disseminação de dados, mídias e informações consideradas confidenciais, assim como a exposição de materiais impressos em locais de fácil acesso.

d) Conformidade Legal

- As aquisições, recebimento de equipamentos e contratação de serviços de TI devem estar em conformidade com as leis vigentes, sendo supervisionados pela Coordenadoria de Tecnologia da Informação – CTI para garantir especificações e verificações adequadas.

e) Monitoramento

- Os ambientes nos setores administrativos da Prefeitura, assim como sistemas de gestão, redes e computadores, podem ser monitorados sem aviso prévio, com o intuito de garantir a preservação da segurança dos dados da instituição.

f) Gerenciamento de Equipamentos

- Os equipamentos podem ser retirados, desativados para fins de manutenção, sujeitos a auditoria ou realocados conforme as necessidades e padrões da instituição, sem aviso prévio.

g) Atualização da PSI

- A Política de Segurança da Informação (PSI) será periodicamente atualizada e revisada, considerando o surgimento constante de ameaças cibernéticas e propostas de melhoria em sistemas, além de mudanças comportamentais e fatores relevantes.

h) Conhecimento e Cumprimento

- É dever de cada colaborador permanecer ciente e informado sobre os procedimentos e normas desta política, buscando esclarecimentos junto à CTI sempre que surgirem dúvidas relacionadas ao uso de recursos de TI.

i) Responsabilidade

- A responsabilidade pela segurança da informação deve ser comunicada durante a fase de contratação dos servidores, acompanhada de orientações sobre os procedimentos de segurança e uso adequado dos ativos para mitigar riscos. Todos os colaboradores devem ter acesso e conhecimento desta política.

j) Comunicação de Incidentes

- Incidentes que impactem a segurança da informação devem ser comunicados imediatamente à CTI.

k) Requisitos de Segurança em Projetos

- Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados durante a fase de levantamento de escopo de um projeto ou sistema. Estes requisitos devem ser justificados, acordados, documentados, implementados e testados ao longo da fase de execução.

l) Responsabilidade e Consequências

- A PMP isenta-se de responsabilidade por uso indevido, negligente ou imprudente de recursos e serviços concedidos aos colaboradores, reservando o direito de analisar dados e indícios com o propósito de obter elementos probatórios para investigações, bem como de adotar as medidas legais cabíveis.

m) Implementação e Conformidade

- A implementação da PSI na PMP ocorrerá por meio de procedimentos específicos obrigatórios para todos os colaboradores, independentemente de cargo ou função, assim como de vínculo empregatício ou prestação de serviço. O descumprimento dos requisitos expostos nessa PSI sujeitará o usuário a medidas administrativas e legais conforme as regras internas da instituição.

5. RESPONSABILIDADES ESPECÍFICAS

5.1 Dos Colaboradores

a) Definição de Colaborador

- O termo "colaborador" engloba toda pessoa física, seja contratada por meio de concurso público, processo seletivo, comissão, estágio, menor aprendiz ou terceiros que prestem serviços à Prefeitura Municipal acessando os recursos de TI dentro ou fora da instituição.

b) Responsabilidades do Colaborador

- Cada colaborador é inteiramente responsável por qualquer prejuízo ou dano causado à Prefeitura Municipal e/ou a terceiros devido à não conformidade com as diretrizes e normas estabelecidas.
- É imperativo que zelem pelo patrimônio público e utilizem adequadamente as ferramentas e recursos necessárias ao desempenho de suas funções.

c) Adesão às Normas de Segurança

- É obrigatório ler, compreender e aderir integralmente aos termos estabelecidos na Política de Segurança da Informação – PSI, assim como às demais normas e procedimentos de segurança em vigor.
- É necessário assinar o Termo de Responsabilidade e Confidencialidade da Prefeitura, formalizando o conhecimento e aceitação plena das disposições contidas nesta Política de Segurança da Informação, juntamente com as demais normas e procedimentos de segurança, assumindo total responsabilidade pelo seu cumprimento.

d) Procedimentos de Desligamento

- Em caso de desligamento, é fundamental manter o sigilo e confidencialidade das informações.
- Se aplicável, devolver as ferramentas utilizadas em bom estado de conservação.

5.2 Dos Gestores

a) Conduta Ética

- É dever do gestor adotar uma conduta ética exemplar em relação à segurança da informação, servindo como modelo para os colaboradores sob sua supervisão.

b) Termo de Responsabilidade e Confidencialidade

- O gestor deve requerer a assinatura do Termo de Responsabilidade e Confidencialidade pelos colaboradores, comprometendo-se a seguir as normas estabelecidas e a manter sigilo sobre os ativos de informação da PMP, mesmo após o desligamento.

c) Procedimentos de Contratação

- Na contratação de novos colaboradores, o gestor deve abrir um chamado na plataforma *Help Desk* para solicitar a criação de usuário, indicando o setor e quais os recursos de rede o novo colaborador terá acesso, bem como os Sistemas de Gestão indicando quais privilégios de acesso serão necessários. Antes de conceder o acesso, é fundamental que o gestor solicite a assinatura do Termo de Responsabilidade e Confidencialidade por parte dos colaboradores, para anexar ao chamado.

5.3 Da Diretoria de Gestão de Pessoas

a) Comunicação de Desligamentos

- Todos os desligamentos são processados pela Diretoria de Gestão de Pessoas da Secretaria Municipal de Administração, sendo sua responsabilidade comunicar à CTI sobre todas as rescisões. Essa comunicação visa garantir que as credenciais de acesso aos sistemas, contas de e-mail institucional e demais recursos computacionais dos usuários sejam desativados devidamente.

b) Comunicação de Transferência

- Todas as transferências de colaboradores de seu local de trabalho atual para outro são processadas pela Diretoria de Gestão de Pessoas da Secretaria Municipal de Administração, sendo sua responsabilidade comunicar à CTI sobre essas ocorrências. Essa comunicação visa garantir que as credenciais de acesso aos sistemas, contas de e-mail institucional e demais recursos computacionais dos usuários sejam atualizados devidamente, não permitindo acesso a documentos e informações do local de trabalho anterior.

c) Arquivamento de Documentos

- A Secretaria deve arquivar o Termo de Responsabilidade e Confidencialidade assinados pelos colaboradores em suas respectivas pastas (prontuários).

5.4 Da Coordenadoria de Tecnologia da Informação

A Coordenadoria de Tecnologia da Informação – CTI possui atribuições específicas relacionadas à segurança da informação e à gestão de tecnologia na PMP. Suas responsabilidades incluem:

a) Administração e Coordenação de Projetos

- Administrar, planejar, dimensionar e coordenar a execução de projetos e ações de tecnologia da informação, seguindo as diretrizes estabelecidas.

b) Implementação de Ajustes e Atualizações

- Implementar ajustes e realizar atualizações nas ferramentas e dispositivos, seguindo os requisitos de segurança estipulados na PSI.

c) Bloqueio de Acesso

- Assegurar, mediante solicitação formal do Setor de Recursos Humanos, o bloqueio imediato do acesso de usuários em casos de desligamento da empresa ou outras situações que demandem medidas restritivas.

d) Controle e Auditoria

- Adotar mecanismos de controle que permitam auditoria e investigações por meio de registros (logs).
- Garantir a segurança de sistemas com acesso externo, destinados ao público, contra ataques ou possíveis problemas de disponibilidade.

e) Atribuição de Responsabilidades e Conrole de Acessos

- Associar cada usuário de recursos de TI ou dispositivo de acesso a um responsável identificável como pessoa física.
- Atribuir responsabilidades específicas para usuários individuais e para usuários de terceiros.
- Dividir as funções administrativas e operacionais para limitar ao mínimo necessário as autorizações de cada indivíduo.
- Eliminar ou reduzir a presença de pessoas com capacidade de excluir registros e trilhas de auditoria de suas próprias ações.

f) Segurança de Backup

- Preservar cópias seguras e testadas dos sistemas e dados em locais distintos, com acesso restrito.

g) Desenvolvimento de Propostas e Metodologias

- Desenvolver propostas para metodologias e processos direcionados à segurança da informação, incluindo avaliação de riscos e implementação de medidas de mitigação.

h) Disseminação da PSI

- Disseminar e divulgar as versões da Política de Segurança da Informação.

i) Monitoramento e Avaliação

- Monitorar o ambiente de TI de maneira abrangente, produzindo indicadores e registros relativos a diversos aspectos, como utilização da capacidade instalada, tempo de resposta, períodos de inacessibilidade, ocorrências de segurança e atividades dos colaboradores.

6. MONITORAMENTO E AUDITORIA

Com o objetivo de assegurar o cumprimento das diretrizes mencionadas nesta Política de Segurança da Informação (PSI) e minimizar os riscos operacionais, a Prefeitura Municipal de Pederneiras (PMP) adota processos contínuos de monitoramento e auditoria, conforme definido no Plano de Gestão de Riscos (Anexo III), no Plano de Continuidade e Recuperação de Desastres (Anexo IV) e na Política de Classificação da Informação (Anexo V).

a) Implementação de Sistemas de Supervisão

- Implementar sistemas de supervisão em estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou sem fio, elementos de rede e demais recursos computacionais. As informações produzidas por esses sistemas poderão ser utilizadas para identificar usuários, bem como os acessos efetuados e o conteúdo manipulado.

b) Divulgação de Informações

- Tornar divulgadas as informações obtidas pelos sistemas de supervisão e auditoria, quando exigido por via judicial ou mediante solicitação de autoridades superiores.

c) Inspeções Físicas

- Realizar, a qualquer momento, inspeções físicas nas máquinas de propriedade da instituição.

d) Implementação de Sistemas de Salvaguarda

- Implementar sistemas de salvaguarda, tanto preventivos quanto detectáveis, a fim de garantir a segurança das informações e dos perímetros de acesso.

Essas medidas têm como objetivo garantir a segurança da informação e o cumprimento das políticas estabelecidas, protegendo os ativos da Prefeitura Municipal de Pederneiras contra ameaças internas e externas.

7. CONTROLE DE ACESSO

7.1 Acesso Lógico

O acesso lógico refere-se à entrada em sistemas, redes e recursos computacionais que demandem credenciais de identificação, como login, autorizando o colaborador a utilizar determinadas ferramentas da organização.

Normas, Diretrizes e Procedimentos

a) Proibição de Compartilhamento de Credenciais

- **É estritamente proibido compartilhar credenciais de acesso**. A responsabilidade perante a Prefeitura Municipal e a legislação (código penal art. 307 – falsa identidade), em caso de incidentes, recairá sobre os colaboradores que descumprirem esta diretriz.

b) Critérios de Responsabilidade

- Todos os colaboradores devem seguir os critérios de responsabilidade sobre o uso dos dispositivos de identificação.

c) Solicitação de Permissões de Acesso

- A solicitação de permissões de acesso a sistemas, redes, ativos e a criação de usuários deve ser feita pelo gestor da pasta por meio de um chamado na plataforma *Help Desk*, detalhando os dados do colaborador como nome, CPF, setor e quais os recursos de rede e privilégios de sistemas serão necessários.

d) Assinatura do Termo de Responsabilidade e Confidencialidade

- O colaborador (usuário) deverá assinar o Termo de Responsabilidade e Confidencialidade, conforme Anexo I, que será arquivado em seu prontuário no Setor de Recursos Humanos da Secretaria de Administração.

e) Restrição de Acesso

- O acesso aos recursos de TI são restritos àqueles disponíveis para a Secretaria a qual o Colaborador está lotado. Acesso ou privilérios de acessos a recursos de outra Secretaria deverão ser aprovados pelos respectivos Secretários.

f) Definição de Privilégios

- Os privilégios concedidos devem estar alinhados com as necessidades específicas das funções desempenhadas pelo usuário.

g) Padrões de Senhas

- As senhas não devem conter dados pessoais, como nome, sobrenome, data de nascimento, e não devem ser constituídas de combinações óbvias de teclado. Elas devem seguir critérios mínimos de segurança, incluindo:

  – comprimento de no mínimo 7 caracteres;

  – com ao menos 1 letra maiúscula;

  – com ao menos 1 letra minúscula;

  – com ao menos 1 número;

– com ao menos 1 caracter especial (@, #, $, %, &).

h) Renovação de Senhas

- As senhas devem ser renovadas a cada 180 (cento e oitenta) dias, e as 12 (doze) senhas anteriores não podem ser reutilizadas. Em caso de esquecimento, perda ou suspeita de acesso não autorizado por terceiros, os usuários devem solicitar imediatamente a emissão de uma nova senha através de chamado na plataforma *Help Desk*.

i) Bloqueio de Conta

- Após 5 (cinco) tentativas de acesso malsucedidas, a conta do usuário será automaticamente bloqueada. Para solicitar o desbloqueio, o usuário deve abrir um chamado na plataforma Help Desk ou, na impossibilidade, entrar em contato com a Coordenadoria de Tecnologia da Informação (CTI).

j) Manutenção de Registros

- Os servidores da CTI não mantêm registro das senhas e não têm meios para conhecer ou identificar as senhas dos Colaboradores.

k) Registro de Acessos

- Qualquer ação realizada mediante o uso das credenciais pessoais é de responsabilidade exclusiva do respectivo usuário.

l) Desligamento de Colaboradores

- No momento em que um usuário for desligado do quadro de colaboradores da PMP, a pedido ou não, o Setor de Recursos Humanos deve comunicar imediatamente essa informação à CTI para que as devidas medidas sejam tomadas. Todos os acessos devem ser prontamente bloqueados quando se tornarem desnecessários.

m) Comunicação de Acessos Suspeitos

- A detecção de acessos desconhecidos ou a suspeita de acessos ilegítimos aos recursos de TI devem ser prontamente comunicados ao gestor competente e a CTI para que sejam tomadas as devidas providências.

n) Acesso Remoto

- O acesso remoto aos ativos só será permitido mediante a prévia autorização do gestor competente e da CTI. Colaboradores devem solicitar esse acesso, identificando-se e fornecendo informações detalhadas sobre o recurso necessário, o motivo, o local e o período de utilização. Tais solicitações devem ser conduzidas por meios seguros, garantindo a integridade e legitimidade da atividade.

o) Acesso de Administrador

- O acesso com o perfil de administrador aos recursos de TI é restrito, exclusivamente a CTI, não sendo possível o compartilhamento deste perfil de acesso a nenhum Colaborador fora da equipe da CTI.

- O acesso ao perfil de administrador dos recursos de TI é exclusivo da CTI, sendo expressamente proibido o compartilhamento desse perfil com qualquer colaborador fora da equipe.

7.2 Acesso Físico

O acesso físico refere-se ao ingresso a infraestrutura do *Datacenter*, que é o local onde são mantidos em operação constante todos os computadores centrais e os principais recursos computacionais da instituição. A entrada neste local deve ser estritamente limitada e controlada, visado reforçar a segurança e garantir o funcionamento eficiente e seguro do *Datacenter*.

Normas, Diretrizes e Procedimentos

a) Acesso restrito

- Apenas colaboradores da Coordenadoria de Tecnologia da Informação (CTI) têm permissão para acessar a infraestrutura do *Datacenter*.

b) Supervisão obrigatória

- Todo acesso deve ser supervisionado por um membro da equipe da CTI.

c) Fechadura biométrica

- A sala do datacenter deve ser mantida permanentemente fechada com uma fechadura biométrica para prevenir acesso não autorizado.

d) Controle de temperatura

- A temperatura do *Datacenter* deve ser cuidadosamente controlada para evitar superaquecimento dos equipamentos.

e) Registro de Acessos

- Todos os acessos ao Datacenter devem ser registrados, incluindo data, hora e identidade dos visitantes autorizados.

f) Proibição de Equipamentos Pessoais

- Não é permitido o uso de dispositivos eletrônicos pessoais dentro do Datacenter para evitar riscos de segurança e interferências operacionais.

g) Sistema de Monitoramento

- O ambiente deve contar com câmeras de segurança para monitoramento contínuo e gravação dos acessos.

h) Plano de Contingência

- Deve existir um plano de contingência em caso de falhas elétricas, incêndios ou outros incidentes que possam comprometer a segurança e a operação dos sistemas.

i) Controle de Material e Ferramentas

- A entrada e saída de materiais, peças e ferramentas no Datacenter deve ser documentada e autorizada previamente.

8. ASSINATURA ELETRÔNICA

Os documentos digitais produzidos pela Prefeitura Municipal de Pederneiras devem ter sua autenticidade e integridade garantidas por meio de assinatura eletrônica. Documentos com assinatura digital têm validade equiparada à de documentos assinados fisicamente, conforme regulamentado pelo Decreto Federal nº 10.543, de 13/11/2020 (alterado pelo Decreto Federal nº 10.900/2021).

A assinatura eletrônica ocorre por meio de:

a) Assinatura eletrônica simples
   - Permite identificar o signatário e associar seus dados a outros em formato eletrônico.

b) Assinatura eletrônica avançada
   - Utiliza certificados não emitidos pela ICP-Brasil ou outros meios aceitos pelas partes para comprovar autoria e integridade de documentos eletrônicos, como a assinatura GOV.BR.

c) Assinatura eletrônica qualificada
   - Utiliza certificado digital ICP-Brasil (infraestrutura de Chaves Públicas Brasileira).

A prática de atos assinados eletronicamente implica a aceitação das normas regulamentares sobre o assunto. A assinatura eletrônica é de uso pessoal e intransferível, sendo de responsabilidade do titular sua guarda e sigilo. A utilização indevida da assinatura eletrônica individual será de responsabilidade exclusiva do titular.

9. INTERNET

Normas para o uso ético e profissional dos recursos de internet na PMP:

a) Acesso e monitoramento
   - Todo acesso, envio, recebimento ou produção de informação na internet está sujeito ao controle, auditoria e divulgação;
   - A PMP reserva o direito de monitorar e registrar todas as interações na rede, incluindo o volume de trafego e endereços de web (http:// e https://) visitados.

b) Propriedade e bloqueio
   - Os dispositivos, tecnologia e serviços para conexão à internet são propriedade da instituição;
   - A PMP pode analisar e, quando necessário, bloquear arquivos, sites, e-mails, domínios ou aplicativos na rede/internet, gravados localmente ou em áreas privadas da rede.

c) Uso proibido

- É estritamente proibido o uso de recursos computacionais, serviços e ativos de informação para propósitos ilegais ou em desacordo com esta política de uso, que resulte em danos, desativação, sobrecarga ou prejuízo a qualquer área, serviço ou conteúdo, assim como interfira no uso e na participação dos colaboradores;
- Qualquer colaborador que realizar modificações nos parâmetros de segurança dos recursos computacionais da rede interna sem o devido credenciamento e autorização da CTI será considerado infrator, e os riscos relacionados serão comunicados ao colaborador e ao gestor correspondente;
- O uso de recursos computacionais para atividades ilícitas sujeitará o infrator a ações administrativas e penalidades conforme processos civil e criminal, com a instituição colaborando ativamente com as autoridades competentes.

d) Segurança de dados

- Dados confidenciais devem ser armazenados nas pastas designadas para cada setor;
- É responsabilidade do colaborador assegurar que os dados confidenciais sejam armazenados exclusivamente nas pastas designadas para cada setor, evitando o uso de pastas publicas, como “PREFEITURA”, que se presta exclusivamente para transferência de momentânea de documentos.

e) Restrições de acesso

- Não é permitido tentar obter acesso não autorizado a qualquer área, serviço e conteúdo dos sistemas ou redes de computadores conectados, seja por ações mal-intencionadas, corrupção de credenciais ou outros meios;
- É proibida a utilização de proxies, incluindo aplicativos, endereços, sites, extensões de navegador ou qualquer outro meio que possa interferir nas políticas de segurança da informação.

f) Uso adequado

- O colaborador deve utilizar e acessar a rede, internet e/ou e-mail institucional exclusivamente para fins profissionais, voltados à execução e desempenho dos objetivos da Administração Pública. Qualquer uso fora desses propósitos poderá ser interrompido sem aviso prévio ao colaborador. Os gestores podem requerer a CTI, o bloqueio e a limitação do acesso dos colaboradores, mediante chamado no sistema *Help Desk*.

g) Restrições de conteúdo

- Está estritamente proibida a utilização dos recursos computacionais e de comunicação da Administração Pública, bem como a exposição, armazenamento, distribuição, edição e gravação de conteúdo das categorias de sites abaixo:
  - ✓ Conteúdo com teor sexual explícito, especialmente relacionado à proteção da infância, ou qualquer material contrário a princípios éticos e morais;
  - ✓ Conteúdo impróprio, ofensivo, preconceituoso ou discriminatório;
  - ✓ Apologia à violência, terrorismo ou uso de drogas;

- ✓ Violação de direitos autorais (pirataria);
- ✓ Práticas fraudulentas de qualquer natureza;
- ✓ Compartilhamento de arquivos não relacionados às atividades da Prefeitura sem autorização do superior hierárquico.

- Estão igualmente proibidos acessos a sites de streaming, séries, filmes, vídeos e arquivos de entretenimento, tais como Netflix, HBO Max, Disney Plus, Youtube e/ou similares, exceto em atividades relacionadas a necessidade da Administração Pública mediante autorização do gestor da Secretaria.

h) Responsabilidades

- A utilização de qualquer recurso computacional da PMP para atividades ilegais constitui motivo para investigação interna por meio de sindicância ou PAD (processo administrativo disciplinar). A Administração Pública cooperará ativamente com as autoridades policiais ou judiciais em tais casos.

i) Proibições e restrições adicionais

- É proibido o uso dos recursos computacionais da PMP para a propagação deliberada de vírus, *worms*, cavalos de Tróia, spam, assédio de qualquer natureza, perturbação ou programas de controle de outros computadores;
- É proibida a utilização de jogos, inclusive os onlines;
- É proibido o acesso a softwares ponto a ponto, tais como Kazaa, uTorrent e similares;
- Os colaboradores não estão autorizados, em hipótese alguma, a utilizar os recursos computacionais da PMP para efetuar o *download* ou distribuição não autorizada de *software*;
- É expressamente proibido o uso, instalação, cópia ou distribuição de *softwares* que possuam direitos autorais, marca registrada ou patente na internet, sem a devida aquisição legal. Qualquer *software* não autorizado será excluído pela CTI;
- É expressamente proibido ao colaborador compartilhar informações confidenciais da Administração Pública em fóruns de discussão, conversas, plataformas de mensagens, e-mails, chamadas telefônicas, redes sociais, WhatsApp, entre outros, seja a divulgação intencional ou acidental, e em caso de descumprimento estará sujeito às sanções determinadas por lei, processos internos e/ou conforme a legislação vigente, incluindo responsabilidade criminal ou civil;
- É proibido realizar o *upload* de qualquer *software* licenciado à PMP ou de dados pertencentes à Prefeitura para parceiros e clientes sem expressa autorização do responsável pelo *software* ou pelos dados.

j) Uso de imagens

- Apenas colaboradores autorizados podem copiar, capturar, imprimir ou enviar imagens da tela para terceiros, desde que observem a norma interna de uso de imagens, a Lei de Direitos Autorais e demais dispositivos legais vigentes que garantam a proteção da imagem.

k) Manifestação oficial

- Somente os colaboradores autorizados a representar a PMP nos meios de comunicação podem se manifestar, seja por e-mail, entrevista online, podcast, documento físico, entre outros.

l) Transferência de programas

- É proibida a transferência de programas, aplicativos, softwares, de quaisquer natureza, inclusive jogos e similares para a rede interna da Administração Pública sem autorização específica do gestor.

m) Download restrito

- É proibido o *download* de arquivos com extensões como .exe, .mp3, .wav, .bat, .com, .sys, .scr, .ppt, .mpeg, .avi, .rmvb, .d11, e de programas de entretenimento ou jogos, a menos que sejam essenciais para o desempenho das atividades relacionadas à função do colaborador. Neste caso o colaborador deve apresentar a necessidade ao gestor competente que poderá fazer a solicitação ao CTI através do chamado no *Help Desk*.

n) Confidencialidade

- É proibido ao colaborador divulgar, fora do ambiente profissional ou institucional, qualquer informação ou fato do qual tenha conhecimento em razão de suas atribuições, salvo quando autorizado por decisão legal ou judicial competente.

o) Notícias

- Com o objetivo de manter os colaboradores bem informados, a Administração Pública permite o acesso a sites ou serviços de notícias, desde que essa atividade não prejudique a largura de banda da rede nem interfira no andamento das atividades. É fundamental que os colaboradores estejam cientes e sigam os termos estabelecidos nesta política de uso.

p) Relato de exceções

- Qualquer exceção ou situação não prevista deve ser prontamente comunicada ao gestor responsável pelo colaborador.

Essas normas visam garantir o uso seguro e responsável da internet, preservando a segurança e integridade dos dados da Prefeitura Municipal de Pederneiras.

10. E-MAIL INSTITUCIONAL

O e-mail institucional deve ser utilizado exclusivamente para atividades relacionadas às funções do colaborador, estando sujeito à supervisão do gestor imediato.

As contas de e-mail são criadas com tamanho padrão, para uso individual e intransferível, vinculadas à pessoa física, com acesso restrito mediante autenticação por senha pessoal.

Listas de distribuição consistem em agrupamentos de endereços de e-mail de pessoas físicas reunidos sob um único endereço eletrônico. Mensagens enviadas a esse endereço são automaticamente encaminhadas a todos os integrantes do grupo.

Esse recurso é frequentemente utilizado para representar setores, secretarias, programas, equipes de trabalho, conselhos, entre outros grupos organizacionais.

É de responsabilidade dos gestores das áreas garantir que as listas de distribuição de e-mail estejam sempre atualizadas, refletindo com precisão a composição atual das equipes, setores ou grupos de trabalho. A manutenção correta dessas listas é fundamental para assegurar a confidencialidade, a integridade e a entrega adequada das informações institucionais, evitando o envio indevido de mensagens a destinatários não autorizados ou desvinculados da função.

O uso do e-mail não confere prerrogativas ou autoridade para conceder acesso a terceiros, pois envolve informações pertencentes à PMP.

Diretrizes para o correto emprego da ferramenta de e-mail:

a) Segurança da Credencial

- Os colaboradores são responsáveis por manter suas credenciais seguras e fechar a conta quando não estiver em uso.

b) Recebimento de Spam

- Recomenda-se excluir mensagens de spam ou de remetentes desconhecidos para prevenir infecções por vírus.

c) Assinatura Padrão

- As mensagens devem conter na assinatura padronizada as seguintes infromações:
  - ✓ Nome do colaborador;
  - ✓ Setor de atuação;
  - ✓ Nome da instituição, Prefeitura Municipal de Pederneiras;
  - ✓ Número(s) de telefone;
  - ✓ Endereço de correio eletrônico.

d) Proibições de Uso

- É terminantemente proibido aos colaboradores o uso do e-mail institucional da PMP para:
  - ✓ Enviar mensagens não solicitadas para múltiplos destinatários, exceto quando relacionadas ao uso legítimo da instituição;
  - ✓ Enviar mensagens utilizando o endereço de e-mail de outro usuário ou setor, ou ainda, utilizar endereços de correio eletrônico não autorizados;
  - ✓ Transmitir mensagens eletrônicas que possam tornar seu remetente, a PMP ou suas unidades vulneráveis a ações civis ou criminais;
  - ✓ Divulgar quaisquer informações não autorizadas da instituição como documentos, dados de sistemas, ou até de terceiros como imagens de tela e

afins sem a devida autorização expressa e formal concedida pelo proprietário desse ativo de informação;

- ✓ Falsificar informações de endereçamento, adulterar cabeçalhos com o intuito de ocultar a identidade de remetentes e/ou destinatários, visando evitar as penalidades previstas;
- ✓ Registrar-se em plataformas de entretenimento, comércio online e receber propagandas, assim como para divulgar anúncios publicitários, mensagens encadeadas, vírus, conteúdos prejudiciais, conteúdos ofensivos, obscenos, pornográficos ou que violem qualquer norma legal;
- ✓ Apagar mensagens relevantes de correio eletrônico durante qualquer auditoria ou investigação envolvendo setores e colaboradores da PMP;
- ✓ Entre outros usos não autorizados.

e) Anexos e Links

- Evitar abrir arquivos anexos de remetentes desconhecidos ou inesperados e relatar imediatamente qualquer ocorrência à CTI.

f) Conteúdo Proibido

- Não é permitido enviar mensagens que:
  - ✓ contenham ameaças cibernéticas, como spam, bombardeio de e-mails e vírus de computador;
  - ✓ incluam arquivos com código executável, com extensões que representem riscos à segurança, tais como: .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf, ou equivalentes;
  - ✓ tenham o propósito de obter acesso não autorizado a outro computador, servidor ou rede;
  - ✓ busquem interromper serviços, servidores ou redes de computadores por meio de métodos ilícitos;
  - ✓ tenham a intenção de burlar sistemas de segurança;
  - ✓ visem vigiar ou assediar outros usuários;
  - ✓ tenham como objetivo acessar informações confidenciais sem a explícita autorização do proprietário;
  - ✓ procurem acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
  - ✓ incluam imagens criptografadas ou mascaradas de qualquer forma.

g) Conteúdo Inapropriado

- Não é permitido enviar mensagens que:
  - ✓ possuam conteúdo considerado impróprio, obsceno ou ilegal;

- ✓ tenham caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, religioso entre outros;
- ✓ contenham materiais preconceituosos ou discriminatórios baseada em orientação sexual, raça, gênero, incapacidade física ou mental ou outras situações protegidas;
- ✓ manifestações de apreço ou desapreço a políticos locais ou nacionais (propaganda política);
- ✓ incluam material protegido por direitos autorais sem a permissão explícita do detentor dos direitos.

O uso do e-mail institucional deve seguir estritamente as diretrizes mencionadas para garantir a segurança da informação e o cumprimento das normas da PMP.

11. ESTAÇÕES DE TRABALHO E RECURSOS TECNOLÓGICOS

Todo colaborador é responsável por aderir às diretrizes para o uso e preservação dos ativos de TI, garantindo a integridade do patrimônio público.

Os ativos de TI devem ser usados exclusivamente como ferramentas de trabalho para as atividades designadas.

Diretrizes para o correto emprego da ferramenta de e-mail:

a) Armazenamento de Arquivos

- Os arquivos e pastas contendo os conteúdos considerados importantes pela Secretaria devem ser armazenados no Servidor de Arquivos administrado pela CTI, garantindo a realização de cópias de segurança (backup). Arquivos salvos localmente, ou seja, no disco rígido da estação de trabalho, não são respaldados, sendo de responsabilidade do colaborador em caso de perda ou danos.

b) Uso da Pasta “PREFEITURA”

- A pasta do Servidor de Arquivos denominada “PREFEITURA” é compartilhada por todos os usuários conectados à rede, o que a torna suscetível a modificações ou exclusões sem garantias de segurança;
- Portanto, é altamente desaconselhado utilizá-la como meio de armazenamento permanente, devendo ser reservada **exclusivamente** para transferência de arquivos temporários, entre os colaboradores;
- É responsabilidade do colaborador assegurar que dados confidenciais e sensíveis sejam armazenados exclusivamente nas pastas designadas para cada setor, evitando a pasta “'PREFEITURA'”;
- A CTI realizará regularmente a limpeza da pasta “'PREFEITURA'” para garantir a confidencialidade das informações e otimizar o uso dos recursos computacionais.

c) Documentos Digitalizados

- Todos os documentos digitalizados deverão ser transferidos para a pasta de rede da Secretaria ou Setor, caso haja a necessidade de salvá-los permanentemente, pois arquivos salvos localmente, ou seja, no disco rígido da estação de trabalho, não são respaldados, podendo ser sobrepostos ou apagados acidentalmente.

d) Segurança da Estação de Trabalho

- É fundamental que, ao se ausentar da estação de trabalho, o colaborador remova suas credenciais de acesso, realizando a desautenticação – *logoff* no computador.

e) Comunicação em Caso de Incidentes

- Em caso de furtos, roubos ou extravios de ativos, é necessário comunicar imediatamente a CTI e ao gestor da Secretaria para que seja lavrado um Boletim de Ocorrência visando à apuração dos fatos.

f) Restrições de Uso

- Não é permitida a colocação de adesivos, propagandas ou imãs em equipamentos. Apenas etiquetas de identificação ou patrimônio são autorizadas;
- É estritamente proibido armazenar arquivos pessoais (fotos, vídeos, documentos) nos equipamentos do município;
- É expressamente proibido o uso de impressoras de repartições públicas para a impressão de documentos pessoais;
- Não é permitido o uso de equipamentos de TI por pessoas sem vínculo com a PMP, exceto nos casos específicos de equipamentos destinados a essa função;
- A utilização de pendrives, mídias removíveis e outras fontes externas devem restringir-se exclusivamente à execução de atividades de trabalho.

g) Manutenção e Configuração

- A execução de qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação está proibida sem o conhecimento prévio e a supervisão de um colaborador da CTI, ou designado por este. Para testes, os responsáveis devem solicitar autorização antecipada à CTI, assumindo plena responsabilidade jurídica e técnica pelas ações realizadas.

h) Segurança dos Equipamentos

- É requisito essencial que os computadores estejam equipados com versões atualizadas do sistema operacional e do software antivírus, devidamente instaladas e ativadas de forma permanente, cabendo ao colaborador a atualização, especialmente, do sistema operacional. No caso de suspeita de vírus ou problemas na funcionalidade, o colaborador deve contatar a CTI, registrando um chamado no *Help Desk*;
- O colaborador é incumbido de manter a configuração do equipamento fornecido pela CTI, aderindo aos controles de segurança estabelecidos pela Política de Segurança da Informação e pelas normas específicas da instituição. Nesse contexto, assume a responsabilidade como custodiante de informações;

- É fundamental que os equipamentos mantenham, de forma segura, registros de eventos que incluam a identificação dos usuários, datas e horários de acesso;
- É obrigatório comunicar a CTI toda movimentação de ativos de TI primeiramente, a fim de avaliar a viabilidade e prevenir possíveis deteriorações financeiras e físicas no patrimônio público.

i) Controle de Acesso

- É estritamente proibido que colaboradores da PMP e/ou titulares de contas privilegiadas realizem a execução de comandos ou programas que possam causar sobrecarga nos serviços da rede corporativa, exceto com o acompanhamento prévio da CTI;
- Os colaboradores têm a responsabilidade de comunicar a CTI qualquer identificação de dispositivo desconhecido conectado ao seu computador.

j) Senhas Padrão

- Todas as senhas padrão dos ativos tecnológicos recém adquiridos devem ser alteradas imediatamente após configuração e operacionalização do equipamento.

k) Proibição – Acesso Não Autorizado

- É proibido tentar ou obter acesso não autorizado a outros computadores, servidores ou redes;
- É vedada a manipulação de sistemas de segurança;
- É expressamente proibido acessar informações confidenciais sem a autorização explícita do proprietário;
- Não é permitido monitorar secretamente outras pessoas por meio de dispositivos eletrônicos ou softwares;
- Está terminantemente proibida a interrupção de serviços, servidores ou redes de computadores por métodos ilícitos ou não autorizados.

l) Demais proibições

- É estritamente vedado utilizar qualquer recurso tecnológico para cometer ou participar de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedagem de pornografia, material racista ou qualquer conteúdo que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública não é permitida.

O cumprimento dessas diretrizes é fundamental para garantir a segurança da informação e o adequado funcionamento dos ativos de TI da PMP.

12. DISPOSITIVOS MÓVEIS

Com o objetivo de otimizar a mobilidade e a troca de informações entre seus colaboradores, a Prefeitura Municipal de Pederneiras (PMP) autoriza o uso de dispositivos móveis, considerando como tal todo dispositivo eletrônico dotado de funcionalidades de mobilidade, pertencente à instituição, como notebooks, smartphones, tablets, drives portáteis e dispositivos semelhantes a estes.

Esta norma visa estabelecer diretrizes para a manipulação, prevenção e responsabilidade no uso de dispositivos móveis, sendo aplicável a todos os colaboradores que façam uso desses equipamentos.

Diretrizes para o correto uso dos dispositivos móveis são:

a) Inspeções

- A PMP reserva o direito de realizar inspeções a qualquer momento, especialmente se necessário para manutenções de segurança.

b) Confidencialidade

- O colaborador compromete-se a não utilizar, revelar ou compartilhar, de forma alguma, qualquer informação, seja ela confidencial ou não, à qual tenha acesso em decorrência de suas responsabilidades na PMP, mesmo após o término de seu vínculo com a instituição.

c) Senha de bloqueio

- É obrigatório que o colaborador empregue senhas de bloqueio automático por inatividade em seus dispositivos móveis.

d) Modificação de configuração

- A modificação da configuração dos sistemas operacionais dos dispositivos não será permitida, a menos que haja comunicação prévia e autorização da área responsável, sob supervisão, assistência ou presença de um colaborador da CTI.

e) Programas e aplicativos

- É responsabilidade do colaborador garantir que não mantenha ou utilize programas e aplicativos sem relação direta com suas funções ou não autorizados.

f) Reprodução não autorizada

- Qualquer reprodução não autorizada dos softwares ou seus dados instalados nos dispositivos móveis fornecidos pela instituição será considerada uso inadequado do equipamento e uma infração legal aos direitos autorais do fabricante.

g) Furto ou roubo

- Em caso de furto ou roubo de um dispositivo móvel fornecido pela PMP, é incumbência do colaborador notificar prontamente seu gestor imediato e a CTI, buscar auxílio das autoridades policiais e registrar um boletim de ocorrência (B.O.) o mais rápido possível.

h) Riscos associados

- O colaborador deve ter plena ciência de que a utilização inadequada do dispositivo móvel implicará na aceitação de todos os riscos associados à sua má utilização, sendo o único responsável por quaisquer danos à PMP ou a terceiros.

i) Saída de equipamento

- O colaborador será responsável por qualquer equipamento pertencente à Prefeitura Municipal que estiver sob sua guarda, que seja utilizado dentro de suas dependências ou fora dela.

j) Equipamentos portáteis pessoais

- A utilização de equipamentos portáteis, tais como smartphones, tablets e notebooks, que não tenham sido fornecidos pela instituição ao colaborador, não será autorizada para uso e conexão na rede corporativa.

k) Acesso à rede sem fio

- Para obter acesso à rede sem fio, o gestor da Secretaria ou unidade precisa preencher a solicitação de inclusão de usuários na rede, conforme descrito no anexo III. Ressalta-se que esta rede deve ser utilizada exclusivamente para fins relacionados ao serviço da PMP e que todos os acessos são registrados e monitorados.

13. TRATAMENTO DE DADOS

As informações confidenciais e/ou sigilosas presentes em documentos impressos devem passar pelo processo de fragmentação antes de serem descartadas, garantindo assim a segurança e confidencialidade dos dados. Somente após essa medida de segurança, os documentos poderão ser eliminados de forma apropriada, evitando possíveis vazamentos ou acesso não autorizado.

O tratamento de dados deve seguir rigorosamente as diretrizes estabelecidas na Política de Proteção de Dados Pessoais da instituição, em conformidade com as disposições do Decreto nº 1.732/2022, que regulamenta a política de proteção de dados no âmbito do Município de Pederneiras, e as normas da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018 - LGPD). Essas medidas visam assegurar a privacidade e integridade das informações, além de garantir o cumprimento das normativas legais vigentes.

14. BACKUP

A PMP possui implementada uma política de backup como parte integrante de suas medidas de segurança da informação. Esta política assegura a preservação e a recuperação eficiente de dados em casos de incidentes, garantindo a continuidade operacional sem perdas significativas. Todos os colaboradores são orientados a seguir as diretrizes estabelecidas nesta política, assegurando a integridade e a disponibilidade dos dados críticos da instituição.

A estratégia de backup está alinhada ao Plano de Continuidade e Recuperação de Desastres (Anexo IV), garantindo que os procedimentos de restauração sejam eficazes e bem documentados. Para detalhes específicos, consulte o documento completo da Política de Backup e as diretrizes estabelecidas no Plano de Continuidade e Recuperação de Desastres.

15. ABREVIAÇÕES E TERMOS

ABNT – Associação Brasileira de Normas Técnicas

BO – Boletim de Ocorrência

CTI – Coordenadoria de Tecnologia da Informação

ICP – Infraestrutura de Chaves Públicas

ISO – *International Organization for Standardization*

LGPD – Lei Geral de Proteção dos Dados

NBR – Norma Brasileira

PAD – Processo Administrativo Disciplinar

PMP – Prefeitura Municipal de Pederneiras

PSI – Política de Segurança da Informação

TI – Tecnologia da Informação

Ativo. Em TI, os ativos referem-se a qualquer recurso que tenha valor para uma organização. Isso pode incluir hardware, software, dados, redes, entre outros.

Ativo físico. São os componentes tangíveis de um sistema de TI, como servidores, computadores, notebooks, impressoras, roteadores, dispositivos de armazenamento, cabos de rede, *Switches*, entre outros. Esses ativos podem ser tocados e manipulados fisicamente.

Ativo lógico. Referem-se aos componentes intangíveis de um sistema de TI, como software, sistemas operacionais, aplicativos, bancos de dados e algoritmos, dados não estruturados (e-mails, planilhas, documentos de texto etc). Esses ativos são essenciais para o funcionamento do sistema, mas não podem ser tocados fisicamente.

Colaborador. Servidores contratados por concurso público, processo seletivo (temporários), comissionados, estágiários, menor aprendiz (mirins), prestadores de serviço pessoa jurídica ou não, que realize atividades dentro da Prefeitura ou fora dela – remotamente.

Correio eletrônico/E-mail – Serviço utilizado para a troca de mensagens, podendo ou não fazer uso dos recursos da Internet. Também conhecido como e-mail.

Credencial de acesso. Conjunto de login e senha capazes de identificar um usuário.

Download – Consiste na obtenção de uma cópia, no computador local, de um arquivo originalmente armazenado em um computador remoto ou em uma rede (internet).

Estação de trabalho. Conjunto de equipamentos e seus sistemas operacionais utilizados pelos colaboradores para acesso à internet, ao sistema de arquivos ou aos demais sistemas

institucionais. Tipicamente compreendem: computador e monitor, notebook, tablet ou smartphone com seus respectivos softwares.

Gestor – Refere-se a qualquer pessoa responsável por Secretarias ou setores municipais. Na Prefeitura, incluem-se secretários, supervisores, coordenadores, encarregados, dentre outros responsáveis nomeados.

Hardware – Compreende o microcomputador e seus componentes internos, como processador, memórias, unidades de disco, leitores/gravadores de CD/DVD, incluindo periféricos como monitores, teclado, mouse, impressoras e outros. Abrange ainda dispositivos portáteis como notebooks, tablets, celulares, equipamentos de rede e servidores.

***Help Desk*.** Plataforma pela qual podem ser solicitados ao CTI: reparos de ativos, instalações e ações referentes às credenciais de acesso.

Internet – É o conjunto global de computadores interligados em uma rede de abrangência mundial, comunicando-se por meio de protocolos específicos.

Log – São registros que têm o propósito de descrever eventos relacionados ao funcionamento e à utilização dos sistemas pelos colaboradores, assim como interações com outros softwares.

Pastas compartilhadas. Pastas que estão armazenadas nos servidores de arquivos e são compartilhadas entre diferentes estações de trabalho sejam elas do mesmo setor ou não.

Pastas de Setor. Pastas compartilhadas com acesso permitido às estações de trabalho de um setor.

Pastas de Secretaria. Pastas compartilhadas com acesso permitido às estações de trabalho da mesma secretaria ou de setores correlatos

Pasta Pública. Pastas compartilhadas com acesso permitido a todas asestações de trabalho da instituição.

Ponto de Acesso sem Fio. Equipamento que é ou desempenha função de acesso sem fio à rede local.

Rede cabeada. Sistema que interliga equipamentos utilizando cabos de par trançado ou fibras ópticas.

Rede local. Conjunto de recursos compartilhados através dos servidores de rede, switches e estações de trabalho nos quais circulam as informações corporativas da Prefeitura.

Rede sem fio. Sistema que interliga equipamentos com transmissão através de ondas eletromagnéticas.

Site – Um sítio, conhecido como site, website ou web site, refere-se a uma coleção de páginas web, ou seja, documentos acessíveis pela Internet.

Software – Refere-se às instruções, programas e dados associados utilizados durante a operação do sistema.

Upload – Consiste na transmissão de dados de um sistema de computador para outro através de uma rede (internet).

Usuário externo. Indivíduo que não faz parte do quadro de colaboradores da Prefeitura, mas acessa recursos de TI disponíveis a este perfil.

16. ANEXOS

ANEXO I - TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

ANEXO II - SOLICITAÇÃO DA INCLUSÃO DE USUÁRIOS NA REDE WIFI

ANEXO III - MODELO DO PLANO DE GESTÃO DE RISCOS

ANEXO IV - MODELO DO PLANO DE CONTINUIDADE E RECUPERAÇÃO DE DESASTRES

ANEXO V - MODELO DE POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

ANEXO VI - MODELO DE POLÍTICA DE USO DE CRIPTOGRAFIA

ANEXO I

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

IDENTIFICAÇÃO:

Nome Completo:	
CPF:	**Secretaria:**
Local de trabalho:	**Cel. para contato:**

Pelo presente instrumento e em razão de meu vínculo com a PREFEITURA MUNICIPAL DE PEDERNEIRAS, firmo o presente TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE, mediante as estipulações consignadas neste instrumento.

DECLARO QUE:

1. Tenho conhecimento e acesso à Política de Segurança da Informação (PSI), bem como às demais normas de Segurança da Informação necessárias ao meu trabalho, as quais estão disponíveis para consulta e/ou impressão no website da PREFEITURA MUNICIPAL DE PEDERNEIRAS. Li na íntegra e recebi cópia digital disponível no link https://web.pederneiras.sp.gov.br/tecnologia-da-informacao/psi-menu, tomando conhecimento e ciência de suas diretrizes.

2. Compreendi completamente os termos, diretrizes, conceitos e condições de uso da Política de Segurança da Informação (PSI), bem como das demais normas de Segurança da Informação necessárias ao meu trabalho. Comprometo-me a cumprir integralmente as diretrizes constantes em tais documentos.

3. Estou ciente e concordo que tanto os ativos de informação quanto a infraestrutura tecnológica da PREFEITURA MUNICIPAL DE PEDERNEIRAS poderão ser utilizados somente para fins exclusivamente profissionais e relacionados ao cumprimento de minhas atribuições neste órgão.

4. Estou ciente de que é realizado o monitoramento de todos os acessos e comunicações ocorridos através da infraestrutura tecnológica da PREFEITURA MUNICIPAL DE PEDERNEIRAS.

5. Estou ciente de que as violações da Política de Segurança da Informação (PSI), bem como das demais normas de Segurança da Informação, são passíveis de sanções e punições, podendo incorrer em responsabilização legal nas esferas administrativa, civil e penal, nos termos da legislação em vigor.

6. Reconheço que, se necessário, o uso de assinatura eletrônica (engloba-se certificado digital) é de minha responsabilidade, incluindo a posse, a proteção e os devidos cuidados associados. Compreendo que a assinatura eletrônica é pessoal e intransferível, sendo estritamente proibidos empréstimos ou transferências a terceiros.

7. Comprometo-me a não revelar fatos ou informações de qualquer natureza aos quais tenha conhecimento e/ou acesso por força das minhas atribuições, mesmo após o encerramento do contrato de trabalho com a PREFEITURA MUNICIPAL DE PEDERNEIRAS.

SOLICITO AS CREDENCIAIS DE ACESSO:

Por meio deste, solicito formalmente a implementação de minhas credenciais de acesso aos recursos de rede e sistemas de gestão utilizados por minha unidade **assinalados abaixo**. Assumo total responsabilidade pelo acesso às informações, comprometendo-me a utilizá-las de maneira profissional e adequada. Estou ciente de que todas as ações (inclusão, alteração, consulta e exclusão) realizadas nos sistemas com minhas credenciais serão de minha inteira responsabilidade.

São necessários ao desempenho de minhas atribuições os recursos assinalados **X** abaixo:

a) RECURSOS DE REDE

	Conta de Usário de Domínio (login no computador)
	Conta de e-mail
	Acesso ao Servidor de Arquivos (somente usuários do Paço Municipal)

b) SISTEMAS DE GESTÃO

	Administração de Aquisições Públicas, Estoque, Suprimentos e Patrimônio (SMARam)
	Administração de Cemitérios (SMARit)
	Administração de Frotas (SMARfr)
	Administração de Recursos Humanos (SMARrh)
	Administração Orçamentária e Financeira (SMARcp)
	Administração Tributária (SMARtb)
	Atendimento ao Munícipe, Controle de Processos e Protocolo (SMARsa)
	Consigo – Sistema de Empréstimos Consignados (Montreal)
	Controle Interno (SMARci)
	Diário Oficial Municipal (P&P Colibri)
	DPOnet – Leis Proteção de Dados (DPOnet)
	Gestão de Assitência Social (Jungle Consultoria)
	Gestão de Frequência de Ponto Eletrônico (Insight)
	Gestão de Saúde Municipal (RKM)
	Gestão Educacional (Empresarial)
	Leis Municipais (Liz Serviços Online)
	Portal da Transparência e Serviços Online (Prefeitura)

	Portal de Transparência e Acesso à informação (SMARpt)
	SEI Cidades (Prodesp)
	Sistema de Gestão de Atendimento – SGA (Prefeitura)
	Web Site Oficial (Instar)

Prefeitura Municipal de Pederneiras, ___ de _____ de _____.

_____
Assinatura do Colaborador/Terceirizado

_____
Assinatura do Gestor Responsável **com Carimbo ou nome legível**

ANEXO II

SOLICITAÇÃO DE INCLUSÃO DE USUÁRIOS NA REDE WIFI

Venho por meio desta solicitar a inclusão dos seguintes colaboradores para acesso à rede WiFi da Prefeitura.

Secretaria/Setor: _____

Nome	CPF

Justificativa para fins profissionais:

Declaro estar ciente que todo acesso à rede estará sendo registrado e monitorado, e que a rede WiFi só deve ser utilizada para fins relacionados ao serviço da Prefeitura.

Prefeitura Municipal de Pederneiras, ___ de _____ de _____.

_____

Assinatura do Gestor Responsável **com Carimbo ou nome legível**

ANEXO III

PLANO DE GESTÃO DE RISCOS

1. OBJETIVO

O presente plano tem como objetivo estabelecer um processo sistemático de identificação, análise, avaliação, tratamento e monitoramento dos riscos relacionados à segurança da informação na Prefeitura Municipal de Pederneiras (PMP). O objetivo é garantir a proteção dos ativos de informação contra ameaças internas e externas, mitigar vulnerabilidades e assegurar a continuidade dos serviços públicos.

2. ESCOPO

O plano aplica-se a todos os ativos de informação da PMP, incluindo dados, sistemas, infraestrutura de TI, colaboradores, prestadores de serviço e qualquer entidade que tenha acesso às informações institucionais, sejam elas armazenadas, processadas ou transmitidas.

3. METODOLOGIA DE GESTÃO DE RISCOS

A gestão de riscos seguirá o ciclo estabelecido na norma ISO/IEC 27005, abrangendo:

3.1 Identificação de Riscos

Os riscos serão identificados a partir dos seguintes elementos:

- **Ativos de informação**: Dados, sistemas, dispositivos, redes e serviços de TI.
- **Ameaças**: Ataques cibernéticos, vazamento de informações, falhas humanas, desastres naturais, entre outros.
- **Vulnerabilidades**: Sistemas desatualizados, acessos indevidos, senhas fracas, falta de backups, etc.

3.2 Análise de Riscos

Cada risco identificado será analisado com base em:

- **Impacto**: Consequências caso o risco se materialize (baixo, médio ou alto).
- **Probabilidade**: Chances de ocorrência (raro, possível ou frequente).
- **Classificação do Risco**: Matriz de risco que cruza impacto e probabilidade para definir a criticidade.

3.3 Avaliação de Riscos

Os riscos serão priorizados de acordo com sua classificação:

- **Crítico**: Exige ação imediata.

- **Alto**: Requer medidas corretivas rápidas.
- **Médio**: Precisa de monitoramento e possíveis ações preventivas.
- **Baixo**: Pode ser aceito ou mitigado.

3.4 Tratamento de Riscos

Para cada risco identificado, será definido um plano de ação que pode envolver:

- **Eliminação**: Remover a causa do risco.
- **Mitigação**: Reduzir impacto e/ou probabilidade.
- **Transferência**: Contratação de seguros ou serviços terceiros.
- **Aceitação**: Quando o custo da redução é maior que o impacto esperado.

4. CRITÉRIOS DE ACEITAÇÃO DE RISCOS

Os riscos que forem classificados como "médio" ou "baixo" podem ser aceitos caso o custo da mitigação seja superior ao dano potencial. Para riscos "altos" e "críticos", a aceitação só poderá ser realizada mediante aprovação formal da Coordenadoria de Tecnologia da Informação (CTI).

5. RESPONSABILIDADES

- **Coordenadoria de Tecnologia da Informação (CTI)**: Responsável por implementar, monitorar e revisar o plano.
- **Secretaria Municipal de Administração**: Apoiar a implantação e garantir o cumprimento das diretrizes.
- **Colaboradores e gestores**: Seguir as diretrizes, reportar incidentes e participar de treinamentos.

6. MONITORAMENTO E REVISÃO DOS RISCOS

A gestão de riscos será revisada periodicamente para garantir sua eficiência. O monitoramento incluirá:

- **Auditorias regulares** nos sistemas e processos.
- **Análise de incidentes passados** para melhoria contínua.
- **Revisão do plano a cada 24 meses** ou quando houver mudanças significativas no ambiente de TI.

Este plano entra em vigor a partir de sua aprovação pela Secretária Municipal de Administração e deve ser revisado e atualizado periodicamente a cada 2 anos ou a qualquer tempo conforme necessário.

ANEXO IV

PLANO DE CONTINUIDADE E RECUPERAÇÃO DE DESASTRES

1. OBJETIVO

Este plano tem como objetivo garantir a continuidade das operações e a recuperação eficiente dos serviços de tecnologia da informação (TI) da Prefeitura Municipal de Pederneiras (PMP) em caso de falhas, desastres naturais, ataques cibernéticos ou outros incidentes que possam comprometer a disponibilidade dos sistemas e dados.

2. ESCOPO

O plano aplica-se a todos os sistemas, redes, bancos de dados, servidores, estações de trabalho e serviços de TI essenciais para a continuidade das operações da PMP. Também abrange procedimentos a serem seguidos por colaboradores, gestores e pela Coordenadoria de Tecnologia da Informação (CTI).

3. PRINCÍPIOS DA CONTINUIDADE DE NEGÓCIOS

- **Disponibilidade**: Garantia de acesso aos sistemas e dados essenciais.
- **Redução de Impacto**: Minimização dos efeitos adversos em caso de incidentes.
- **Rapidez na Recuperação**: Procedimentos claros para restaurar os serviços.
- **Segurança da Informação**: Proteção contra acessos não autorizados e corrupção de dados.

4. CENÁRIOS DE RISCO

Os seguintes cenários foram identificados como ameaças potenciais aos serviços de TI:

1. **Falhas de Hardware**: Defeitos em servidores, discos rígidos, switches ou equipamentos críticos.
2. **Ataques Cibernéticos**: Malware, ransomware, phishing, DDoS, invasões.
3. **Desastres Naturais**: Enchentes, incêndios, quedas de energia prolongadas.
4. **Erro Humano**: Exclusão acidental de dados, configuração incorreta de sistemas.
5. **Falhas de Software**: Bugs em sistemas críticos, corrupção de arquivos.

5. ESTRATÉGIAS DE CONTINUIDADE E RECUPERAÇÃO

5.1 Medidas Preventivas

- Implementação de backups diários e semanais.
- Uso de servidores redundantes e espelhamento de dados.
- Atualização regular de software e aplicação de patches de segurança.
- Treinamento periódico para colaboradores sobre boas práticas de segurança.
- Monitoramento contínuo de redes e sistemas para identificação de ameaças.

5.2 Procedimentos de Resposta a Incidentes

1. **Detecção do Incidente**: Identificação de falha ou ataque.
2. **Isolamento**: Contenção do incidente para evitar propagação.
3. **Avaliação de Impacto**: Análise do dano e dos serviços afetados.
4. **Ação Corretiva**: Implementação de soluções para restaurar serviços.
5. **Registro e Análise**: Documentação do incidente e medidas adotadas.

5.3 Recuperação de Sistemas e Dados

- **Backup e Restauração**: Procedimentos de recuperação de dados armazenados.
- **Ativação de Ambientes Alternativos**: Uso de servidores de contingência.
- **Revalidação de Credenciais**: Reinicialização de acessos e senhas comprometidas.

6. RESPONSABILIDADES

- **Coordenadoria de Tecnologia da Informação (CTI)**: Coordena e executa os planos de continuidade e recuperação.
- **Secretaria de Administração**: Garante suporte institucional e comunicação com órgãos superiores.
- **Colaboradores**: Devem seguir os protocolos estabelecidos e relatar incidentes imediatamente.

7. MONITORAMENTO E TESTES

- Testes semestrais de recuperação de dados.
- Simulações anuais de resposta a incidentes.
- Revisão e atualização do plano a cada 24 meses ou conforme necessidade.

Este plano entra em vigor a partir da aprovação do PSI – Política de Segurança da Informação pela Secretária Municipal de Administração e deve ser revisado e atualizado periodicamente em conjunto com o PSI a cada 2 anos ou a qualquer tempo conforme necessário.

ANEXO V

POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

1. OBJETIVO

A presente Política de Classificação da Informação tem como objetivo estabelecer diretrizes para a classificação, manuseio, armazenamento e compartilhamento das informações da Prefeitura Municipal de Pederneiras (PMP). Essa classificação visa garantir a proteção adequada dos dados institucionais, prevenindo acessos indevidos, vazamentos e uso inadequado das informações. Além disso, o **Arquivo Público Municipal**, atualmente em desenvolvimento e implementação, será responsável por regulamentar, com maior profundidade, a classificação e a guarda de documentos oficiais, garantindo conformidade com normativas arquivísticas e de segurança da informação.

2. ESCOPO

Esta política se aplica a todos os servidores, colaboradores, prestadores de serviço e qualquer pessoa que tenha acesso às informações da PMP, independentemente do meio em que as informações estejam armazenadas ou transmitidas. O **Arquivo Público Municipal** também atuará como instância de referência para diretrizes adicionais sobre a gestão documental e o tempo de retenção de documentos.

3. CATEGORIAS DE CLASSIFICAÇÃO DA INFORMAÇÃO

As informações institucionais serão classificadas em quatro categorias principais:

3.1 Pública

- Pode ser divulgada livremente, sem causar impactos negativos à administração.
- **Exemplos:** comunicados oficiais, informações em sites institucionais, editais públicos.

3.2 Restrita

- Destinada ao uso interno da PMP, podendo ser compartilhada com terceiros mediante autorização.
- O compartilhamento não autorizado pode causar transtornos administrativos.
- **Exemplos:** relatórios internos, processos administrativos, registros de reuniões.

3.3 Confidencial

- Acesso limitado a pessoas autorizadas.
- O vazamento pode causar impactos institucionais significativos.
- **Exemplos:** dados financeiros, contratos, informações pessoais de servidores e munícipes.

3.4 Secreta

- Altamente sensível, com acesso estritamente controlado.
- O vazamento pode comprometer a segurança da instituição.
- **Exemplos:** credenciais de sistemas críticos, investigações sigilosas, informações estratégicas.

4. DIRETRIZES DE CONTROLE

Cada categoria de informação deve seguir as diretrizes abaixo:

Categoria	Controle de Acesso	Armazenamento	Transmissão Segura	Tempo de Retenção
Pública	Livre	Qualquer meio	Sem restrição	Permanente
Restrita	Somente internos	Servidores internos	E-mail institucional	5 anos
Confidencial	Apenas autorizados	Criptografado	VPN ou e-mail criptografado	10 anos
Secreta	Estritamente controlado	Ambiente seguro e criptografado	Transmissão manual ou segura	Tempo indefinido

5. IMPLEMENTAÇÃO E MONITORAMENTO

- **Treinamento:** Todos os colaboradores serão treinados sobre a aplicação da classificação de informações.
- **Marcas visuais:** Documentos devem ser identificados com etiquetas indicando sua classificação.
- **Auditoria:** Revisões periódicas serão realizadas para garantir a conformidade com esta política.
- **Sanções:** O descumprimento das diretrizes desta política pode resultar em medidas administrativas e legais.

6. REVISÃO DA POLÍTICA

Esta política entra em vigor a partir da aprovação do PSI – Política de Segurança da Informação pela Secretária Municipal de Administração e deve ser revisado e atualizado, adicionalmente, conforme avançar a implementação do Arquivo Público Municipal e periodicamente em conjunto com o PSI a cada 2 anos ou a qualquer tempo conforme necessário.

ANEXO VI

PLANO DE USO DE CRIPTOGRAFIA

1. OBJETIVO

Esta política estabelece diretrizes para o uso de criptografia na Prefeitura Municipal de Pederneiras (PMP), garantindo a proteção da integridade, confidencialidade e autenticidade das informações armazenadas e transmitidas.

2. ESCOPO

Aplica-se a todos os servidores, prestadores de serviço, sistemas, bancos de dados, redes e comunicações da PMP, abrangendo o armazenamento, transmissão e autenticação de informações.

3. DIRETRIZES PARA USO DE CRIPTOGRAFIA

A criptografia deve ser aplicada nos seguintes cenários:

3.1 Proteção de Dados Sensíveis e Confidenciais

- Dados classificados como **Confidenciais** ou **Secretos** devem ser armazenados com criptografia AES-256.
- Credenciais de autenticação e informações de login devem ser protegidas com hashing seguro (PBKDF2, bcrypt ou Argon2).

3.2 Transmissão Segura de Informações

- Todas as comunicações eletrônicas que envolvem informações sensíveis devem utilizar **TLS 1.2 ou superior**.
- O acesso remoto aos sistemas da PMP deve ser feito exclusivamente via **VPN segura**.

3.3 Proteção de Arquivos e Backups

- Backups contendo dados sigilosos devem ser armazenados com **criptografia AES-256**.
- Os backups devem ser protegidos contra acesso não autorizado e mantidos em local seguro.

3.4 Assinatura Digital e Autenticação

- Documentos oficiais devem ser assinados eletronicamente utilizando **certificados digitais ICP-Brasil**.
- A autenticação em sistemas críticos deve utilizar múltiplos fatores (MFA/2FA).

4. ALGORITMOS E PADRÕES RECOMENDADOS

Uso	Algoritmo	Observações
Criptografia de dados	AES-256	Para bancos de dados e arquivos sigilosos
Criptografia de comunicação	TLS 1.2 ou superior	Para transmissão segura de dados
Assinatura digital	RSA 2048 ou ECC-256	Para autenticação e validação de documentos
Hashing de senhas	PBKDF2, bcrypt ou Argon2	Para armazenamento seguro de senhas

5. GERENCIAMENTO DE CHAVES CRIPTOGRÁFICAS

- As chaves devem ser armazenadas em **Hardware Security Modules (HSM)** ou repositórios protegidos.
- O acesso às chaves deve ser restrito a **usuários autorizados** da Coordenadoria de Tecnologia da Informação (CTI).
- As chaves devem ser renovadas periodicamente e alteradas imediatamente em caso de comprometimento.

6. RESPONSABILIDADES

- **Coordenadoria de Tecnologia da Informação (CTI):** Implementar, monitorar e garantir a conformidade com esta política.
- **Gestores e Colaboradores:** Utilizar corretamente os sistemas e tecnologias criptográficas.
- **Secretaria Municipal de Administração:** Apoiar na adoção de assinaturas digitais e medidas de segurança.

7. MONITORAMENTO E REVISÃO

- Auditorias periódicas serão realizadas para garantir a conformidade com esta política.
- Esta política será revisada anualmente ou sempre que houver necessidade de atualizações tecnológicas.

Esta política entra em vigor a partir da aprovação do PSI – Política de Segurança da Informação pela Secretária Municipal de Administração e deve ser revisado e atualizado periodicamente em conjunto com o PSI a cada 2 anos ou a qualquer tempo conforme necessário.