PSI – Política de Segurança da Informação

Versão 01

Setembro 2025

Histórico de Versões

Versão	Data	Comentários	Autor
1.0	08/10/2025		Benedito Braz

Sumário

1 - INTRODUÇÃO

A Prefeitura do Município de Queluz, por meio do Departamento de Tecnologia da Informação, é responsável pela gestão, manutenção, sustentação, modernização e segurança da infraestrutura tecnológica que suporta as atividades administrativas e operacionais de todas as Secretarias e unidades organizacionais do Município. Compete à área de Tecnologia da Informação garantir a disponibilidade, desempenho, integridade e continuidade dos sistemas corporativos, serviços digitais, redes de comunicação, bancos de dados e demais ativos tecnológicos, assegurando o pleno funcionamento dos processos institucionais e a eficiência na prestação dos serviços públicos. Além disso, cabe ao setor promover a evolução tecnológica do ambiente computacional municipal, implementar boas práticas de governança, fortalecer os mecanismos de segurança da informação e estabelecer padrões que assegurem a proteção dos dados e a continuidade operacional da administração pública. É necessário garantir a disponibilidade, integridade, confidencialidade e rastreabilidade das informações produzidas e armazenadas pelas Secretarias, Departamentos, Escolas, Hospital Municipal, Unidades Básicas de Saúde, Sistemas de Videomonitoramento e demais Unidades Funcionais, independentemente de estarem hospedadas em infraestrutura local ou em ambientes computacionais em nuvem.

Nesse contexto, reconhece-se que os recursos tecnológicos constituem ativos estratégicos para o funcionamento da administração pública, sendo imprescindível a implantação de mecanismos contínuos de gestão, proteção e monitoramento, capazes de reduzir riscos operacionais, indisponibilidades, perdas de dados e incidentes de segurança que possam comprometer a continuidade dos serviços públicos prestados ao cidadão.

Visando à modernização da infraestrutura tecnológica municipal, existe ainda a perspectiva de implantação e ampliação de uma rede corporativa interligada por meio de fibra óptica entre todos os setores, Secretarias e unidades administrativas da Prefeitura, permitindo a centralização do acesso aos serviços de tecnologia, otimização da gestão dos ativos computacionais, padronização dos ambientes, fortalecimento dos controles internos, aplicação uniforme das políticas de segurança da informação e maior eficiência operacional na administração dos recursos tecnológicos do Município.

Diante desse cenário, a presente Política de Segurança da Informação (PSI) estabelece diretrizes, responsabilidades, procedimentos e controles voltados à proteção dos ativos de informação do Município, tendo como fundamento as melhores práticas internacionais de governança, gestão de riscos e segurança da informação, especialmente as recomendações previstas nas normas **ISO/IEC 27001:2022** (Sistema de Gestão de Segurança da Informação), **ISO/IEC 27002:2022** (Controles de Segurança da Informação), **ISO 31000:2018** (Gestão de Riscos), além de observar os princípios estabelecidos pelo **Marco Civil da**

Internet – Lei nº 12.965/2014, pela **Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018)** e demais legislações aplicáveis à administração pública.

Assim, a PSI passa a nortear os processos de implementação operação, monitoramento, revisão e melhoria contínua dos controles de segurança, promovendo o fortalecimento da governança de Tecnologia da Informação e a mitigação permanente dos riscos institucionais. Considerando a constante evolução tecnológica, normativa e das ameaças cibernéticas, esta Política deverá ser periodicamente revisada e atualizada, assegurando sua aderência às necessidades estratégicas do Município, aos requisitos legais vigentes e às boas práticas internacionais de segurança da informação.

2 - Objetivo

A presente Política de Segurança da Informação (PSI) tem por objetivo estabelecer diretrizes, processos, procedimentos, controles e normas aplicáveis a toda a Administração Pública Municipal, visando fortalecer a governança da Tecnologia da Informação, mitigar riscos operacionais e cibernéticos, assegurar a continuidade dos serviços públicos e proteger os ativos institucionais, especialmente as informações produzidas, processadas, armazenadas ou compartilhadas pela Administração, independentemente do meio utilizado, físico ou digital.

A PSI busca ainda promover padrões de segurança voltados à preservação da disponibilidade, integridade, confidencialidade e autenticidade das informações, reduzindo vulnerabilidades e prevenindo incidentes que possam comprometer a infraestrutura tecnológica, os sistemas corporativos, os processos administrativos e a prestação dos serviços públicos.

Com a implementação desta Política, espera-se fortalecer a cultura organizacional de segurança da informação e incentivar o comportamento ético, responsável e consciente na utilização dos recursos tecnológicos disponibilizados pela Prefeitura de Queluz, minimizando ocorrências que possam resultar em danos operacionais, financeiros, legais ou reputacionais ao Município, aos agentes públicos, fornecedores, prestadores de serviço, usuários dos sistemas e demais partes relacionadas.

3 - Padrões Comportamentais

Novos padrões comportamentais foram fixados observando, quando aplicáveis, as diretrizes e regramentos da Lei Geral de Processamento de Dados - LGPD (Lei nº 13.709, de 14 de agosto de 2018) bem como da Instrução Normativa SEADM nº 03, de 23 de dezembro de 2025:

3.1. Disponibilidade: As informações e recursos deverão estar disponíveis sempre que necessários para qualquer indivíduo, órgão ou sistemas autorizados naquilo que prevê.

3.2. Integridade: Garantia que os ativos de informação estejam protegidos e não sejam alterados de forma não autorizada ou acidental.

3.3. Confidencialidade: Acesso as informações somente de indivíduos, órgãos e entidades autorizadas.

3.4. Autenticidade: As informações deverão ser certificadas com relação a sua origem evitando mutações ao longo do processo.

3.5. Atualidade: Deverão ocorrer atualizações periódicas dos procedimentos e normas para manutenção da qualidade e segurança dos serviços.

3.6. Aplicabilidade: Todos processos de trabalhos deverão ser integrados e aplicados de maneira funcional obedecendo as normas de segurança.

3.7. Clareza: Não poderá existir dúvidas relacionadas às responsabilidades, normas, procedimentos e direitos de cada envolvido.

3.8. Conhecimento: Deverão ser desenvolvidos materiais informativos e capacitações periódicas dos servidores acerca da Segurança da Informação.

3.9. Simplicidade: A segurança deverá ser realizada de maneira simples, eficaz e objetiva de forma a evitar erros.

3.10. Privilégios: Os recursos disponíveis deverão ser necessários para um bom desempenho das atividades evitando acesso a recursos não condizentes às funções.

3.11. Auditoria: Qualquer tipo de processo poderá ser auditado e suas informações rastreáveis através de log.

3.12. Resiliência: Deverá ter a capacidade de recuperação rápida em caso de desastre ou perda de informações.

3.13. Redundância: Em caso de falhas um outro controle assume o papel evitando transtornos por falta de disponibilidade.

3.14. Legalidade: Garantia de que as informações estão de acordo com legislação vigente.

3.15. Irretratabilidade: Capacidade de garantir que o autor de uma transação ou alteração em sistema não possa negar a sua autoria, mediante a existência de registos de auditoria (logs) e assinaturas digitais.

IMPORTANTE: As diretrizes estabelecidas pela PSI são de cumprimento obrigatório, sem exceções, a toda a Administração Direta e aos agentes que

utilizam ou geram as informações, devendo todos permanecerem atualizados quanto aos termos da PSI, seus processos e procedimentos.

4 – Diretrizes

Buscando promover melhorias nos sistemas de informação e gestão municipal, além de manter e otimizar os processos e procedimentos garantindo a segurança das informações e das comunicações, fixam-se as seguintes diretrizes de cumprimento obrigatório:

4.1. A Segurança da Informação, através da análise de vulnerabilidades e da mitigação de riscos deverá ser preservada e constantemente incentivada visando a manutenção dos serviços e a proteção da Prefeitura do Município de Queluz.

4.2. Os servidores e demais agentes terão acesso somente às informações que se fazem necessárias para o efetivo desempenho suas funções e atribuições.

4.3. Todo incidente que potencialmente afete a Segurança da Informação deverá ser imediatamente e formalmente reportado à chefia imediata.

4.4. A Prefeitura do Município de Queluz se reserva ao direito de a qualquer tempo analisar dados e evidências para obtenção de provas com a finalidade de instruir processos investigatórios de natureza administrativa, civil ou criminal além de outras medidas legalmente possíveis.

4.5. Toda e qualquer aquisição e recebimento de equipamentos bem como as contratações de serviços e sistemas condizentes com a Tecnologia da Informação somente ocorrerão após a análise e formal manifestação técnica devidamente apreciada pelo Departamento de Tecnologia da Informação.

4.6. Todos os servidores e demais agentes que direta ou indiretamente utilizam ou geram as informações da Prefeitura do Município de Queluz restam cientes de que os ambientes da Prefeitura bem como os sistemas de gestão, redes e computadores poderão ser monitorados ou gravados sem aviso prévio visando a manutenção da Segurança da Informação.

4.7. Equipamentos poderão ser removidos ou desligados para manutenção, auditoria ou mesmo realocados de acordo com as necessidades e sem aviso prévio.

4.8. É dever de cada servidor se manter ciente e atualizado sobre os procedimentos e normas desta Política buscando informações junto a DTI sempre que houver dúvidas quanto ao uso de recursos da Tecnologia da Informação.

5 - Responsabilidades e Atribuições Específicas

5.1. Departamento de Tecnologia da Informação – DTI:

a) Rever, atualizar e aprovar periodicamente a PSI;

b) Realizar configurações, atualizações, instalações de ferramentas adequadas para o desempenho das funções em todos equipamentos com base nos requisitos de segurança estabelecidos e mediante software licenciado ou *open source*;

c) Em caso de manutenção, troca de equipamentos ou usuários, garantir a integridade das informações;

d) Em caso de desligamento do servidor ou usuário, realizar o bloqueio de contas e credenciais tão logo seja comunicado;

e) Garantir e promover aos servidores e usuários em conjunto com as Secretarias o conhecimento de ameaças e da Segurança da Informação desenvolvendo e disponibilizando cartilhas, tutoriais e materiais informativos de maneira periódica ou conforme a necessidade;

f) Avaliar periodicamente a eficácia dos controles de segurança, bem como alertar sobre casos de engenharia social e fraudes quando identificadas bem como manter sempre atualizados os dispositivos de segurança e os sistemas de acordo com surgimento de novas tecnologias;

g) Implantar mecanismos de controle que permitam auditoria e investigações através de logs. Sistemas com acesso externo (disponibilizados ao público) deverão ter atenção especial contra ataques ou problemas de disponibilidade;

h) Manter em pleno funcionamento e execução ferramentas de monitoramento de ativos, fazer inserção ou configuração de novos e exclusão de obsoletos ou problemáticos;

i) Manter cópias seguras e testadas dos sistemas e dados em locais diferentes e com acesso restrito;

j) Criar perfis de acessos com privilégios de usuário, não possibilitando, ou suspendendo sempre que necessário, o acesso a recursos de servidores e usuários não autorizados;

k) Reavaliar as liberações e permissões de acesso concedidas cancelando aquelas que não forem mais necessárias;

l) Constantemente analisar o ambiente para identificação de possíveis riscos e mitigação dos mesmos;

m) Criar, estruturar, gerenciar e prover a conexão entre as redes de dados da Prefeitura do Município de Queluz.

5.2. Secretarias e demais Unidades Organizacionais e Funcionais:

a) Cumprir e fazer cumprir a PSI assegurando que suas equipes possuam o acesso e conhecimento de seus termos;

b) Sugerir procedimentos de Segurança da Informação relacionados às suas áreas;

c) Comunicar imediatamente ao DTI quando da verificação de violação de Segurança da Informação.

5.3. Departamento de Pessoal:

a) Comunicar a DTI sempre que ocorra o ingresso e desligamento (efetivo ou temporário) de servidores para fins de inserção ou desligamento de credenciais de acesso a sistemas, plataformas, redes, ambientes, e-mails, etc.

5.4. Servidores e demais agentes e usuários:

a) Cabe aos servidores cumprirem as determinações legais que regem o funcionalismo público, devendo manter sigilo e a confidencialidade das informações que detém ou deteve;

b) Em caso de desligamento (exoneração, demissão ou afastamento temporário) os equipamentos utilizados no desempenho de suas funções deverão ser devolvidos mediante recibo;

c) Serão responsáveis por qualquer tipo de dano que sofrer ou causar em decorrência do não cumprimento das normas e diretrizes da PSI, seja à Prefeitura do Município de Queluz, seja a terceiros;

d) Deverão relatar imediatamente à chefia imediata qualquer incidente de segurança que tenha conhecimento ou até mesmo a suspeita de sua ocorrência.

6 - Normas Gerais de Controle e Acesso

6.1. Monitoramento e Auditoria do Ambiente:

a) As estações de trabalho, servidores de dados, equipamentos móveis bem como qualquer outro relacionado à Tecnologia da Informação poderão ser monitorados visando a correlação entre usuário, equipamento, atribuições e acessos;

b) A qualquer tempo o DTI poderá promover inspeções físicas nos equipamentos;

c) O DTI poderá instalar sistemas e softwares de proteção, preventivos e detectáveis visando garantir a efetiva Segurança da Informação.

6.2. Acesso Lógico:

O acesso lógico aos sistemas e bases de dados municipais será concedido exclusivamente mediante identificação única e pessoal, sendo vedado o partilhamento de credenciais sob qualquer pretexto:

a) O usuário deverá ter privilégio de acordo com as necessidades de suas funções;

b) O acesso remoto a ativos só é permitido mediante autorização prévia do DTI. Os usuários deverão solicitar o acesso, se identificando, informando o motivo, o local e período de utilização, mediante meios seguros para tal atividade;

c) A criação de conta de e-mail institucional (correio eletrônico) deve ser solicitada através do gestor da Unidade Organizacional ou Funcional, por meio apropriado e definido pelo DTI assim como também para a permissão de acesso a sistemas, redes e ativos;

d) As credenciais de acesso (senhas) são criadas de maneira provisório pela DTI, cabendo ao usuário a troca por uma credencial forte e pessoal imediatamente após o primeiro login observando necessariamente critérios mínimos e obrigatórios que devem ser seguidos;

e) As credenciais deverão ser trocadas periodicamente para garantia de segurança. Em caso de esquecimento ou perda, deve-se solicitar uma nova imediatamente;

f) Acessos desconhecidos ou suspeita de acessos aos recursos da Tecnologia da Informação devem ser informados com urgência ao setor para providências.

6.3. Acesso à Infraestrutura:

O acesso às dependências das salas destinadas à infraestrutura é restrito aos servidores lotados no DTI, devendo as salas permanecerem constantemente trancadas para evitar acessos indevidos e o risco à Segurança da Informação.

6.4. Acesso à Rede e Recursos:

O acesso à rede e aos recursos é liberado como condição de uso. As áreas, serviços e conteúdos institucionais não poderão ser usados para quaisquer propósitos proibidos por esta PSI, evitando-se assim danificar, desativar, sobrecarregar, prejudicar qualquer área, serviço ou conteúdo ou interferir no uso e participação de qualquer um dos demais usuários.

6.5. Internet e Intranet:

As regras aqui definidas visam o desenvolvimento de um comportamento ético, profissional e acima de tudo seguro para a utilização da internet e da intranet. Para tanto:

a) Qualquer informação acessada, transmitida, recebida ou produzida na internet e/ou na intranet está sujeita a divulgação e auditoria;

b) Os equipamentos, tecnologia e serviços fornecidos para acesso à internet são de propriedade ou uso da Prefeitura do Município de Queluz, que pode analisar e se entender necessário através da DTI, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede ou internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta PSI;

c) A Prefeitura do Município de Queluz, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer servidor, colaborador ou usuário, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao agente e chefia imediata. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes;

d) Não é permitida o acesso e a navegação em sites pertencentes às categorias abaixo, e tampouco a exposição, o armazenamento, a distribuição, a edição, a gravação através do uso dos recursos computacionais e de comunicação:

i. Material sexualmente explícito e, ainda, material contrário a moral ou aos bons costumes;

ii. Material de conteúdo impróprio, ofensivo, preconceituoso ou discriminatório;

iii. Apologia à violência ou ao terrorismo;

iv. Apologia às drogas;

v. Violação de direito autoral (pirataria);

vi. Execução de quaisquer tipos ou formas de fraudes;

vii. Sites de relacionamentos e bate-papo;

viii. Sites de séries, filmes, TV, vídeos streamings e arquivos de entretenimento, exceto em atividades relacionadas ao setor e mediante prévia e expressa autorização;

ix. Compartilhamento de arquivos estranhos às atividades da Administração Pública.

e) Não é permitida a troca ou compartilhamento de arquivos de vídeo ou música;

f) É proibida a transferência ou download de qualquer tipo de programa, jogo ou similares com as extenções .exe, .mp3, .wav, .bat, .com, .sys, .scr, .ppt, .mpeg, .avi, .rmvb, .dll entre outras que permitam a execução de scripts ou alteração de sistema, sem a prévia autorização da DTI;

g) É proibido o uso de jogos, inclusive os da Internet (online);

h) É proibida o acesso e consequente uso de equipamentos de informática pessoais (notebooks, tablets, etc.) na rede de dados municipal;

i) Celulares e smartphones de servidores poderão ter acesso à rede de dados da Prefeitura do Município de Queluz desde que previamente cadastrados pela DTI;

j) Não é permitido o acesso à internet por meio de proxy não autorizado pela DTI;

k) A Intranet será alimentada por informações produzidas pela Administração Direta seguindo, no que couber, os mesmos critérios aplicados para a internet.

6.6. Da Manifestação Pública e Compartilhamento:

a) Somente os servidores autorizados pela Administração poderão copiar, captar, imprimir ou enviar prints ou imagens de tela para terceiros, em atendimento às atribuições que desempenhar, às normas internas e aos dispositivos legais;

b) É proibida a divulgação ou o compartilhamento de informações da área administrativa, imagem de tela de sistemas, documentos e afins, em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo, comunicadores instantâneos ou qualquer outra tecnologia correlata.

7. E-mail Institucional (Correio eletrônico):

O uso do correio eletrônico fornecido e gerido pela Prefeitura do Município de Queluz através da DTI é exclusivo para fins "corporativos" e relacionados às atividades do servidor e usuário conforme as atribuições legalmente definidas. É vedado o uso do correio eletrônico para fins pessoais.

a) As mensagens de correio eletrônico institucional deverão incluir obrigatoriamente a assinatura padronizada pela Secretaria de Comunicação contendo nome completo, cargo, secretaria e telefone de contacto institucional, visando a identidade visual e a fidedignidade da comunicação oficial.

8. Computadores, Dispositivos Portáteis e Recursos Tecnológicos:

A Prefeitura do Município de Queluz detém a propriedade dos equipamentos fornecidos aos seus servidores, sendo-lhe reservado o direito de, a qualquer tempo, inspecionar local ou remotamente qualquer equipamento, cabendo a cada servidor utilizá-los e manuseá-los corretamente para as atividades e atribuições que lhe competem, bem como:

a) Os arquivos devem ser armazenados no servidor de arquivos indicado pela DTI para a possibilidade de cópia de segurança evitando-se o armazenamento local (disco rígido da estação de trabalho);

b) Para a manutenção dos computadores e outros equipamentos da Tecnologia da Informação, é necessária a abertura de chamado pela Unidade junto a DTI, restando vedada qualquer ação, por qualquer pessoa estranha a ela;

c) A violação de lacre de segurança instalado pela DTI em qualquer equipamento configura ato manifestamente atentatório à PSI e às normas de conduta, ensejando a instauração do competente procedimento administrativo disciplinar em desfavor do autor da ação;

d) Somente a DTI está autorizado a configurar rede, roteadores, switches e alterar endereços de rede IPs bem como adicionar, modificar e remover ativos;

e) Utilização de pendrives, mídias removíveis e outras fontes externas deverão ser utilizadas somente para fins de execução de atividades de trabalho mediante expressa autorização da chefia imediata;

f) Não é permitido o armazenamento de arquivos pessoais (fotos, vídeos, documentos) em equipamentos da Prefeitura;

g) É proibido o uso das impressoras das Unidades para impressões de documentos pessoais.

9. Backup:

A implantação de política de backup assegura que no caso de algum incidente a Prefeitura do Município de Queluz consiga restaurar dados em sua totalidade sem transtornos ou danos às informações. Para tanto, alguns procedimentos são primordiais:

a) Todo sistema deve possuir cópia de dados para que em caso de uma eventual indisponibilidade possa ser restaurado com impactos mínimos;

b) Os backups devem ser automatizados por sistemas de agendamento para que sejam executados, preferencialmente, fora do horário comercial, períodos em que há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas;

c) Os backups são armazenados e devidamente identificados em localizações diferentes da estrutura da Prefeitura, com controle de segurança, de acesso restrito e climatizado;

d) Testes de restauração bem como integridade dos dados devem ser periodicamente executados em locais diferentes dos originais (evitando sobreposição) para garantia que as informações se mantenham preservadas e as rotinas funcionais;

e) Mídias de armazenamento devem ser monitoradas e substituídas de acordo com prazo especificado pelo fabricante;

f) Sempre haverá redundância de equipamentos para substituição em caso de emergência;

g) Os procedimentos de configuração, administração, armazenamento e restauração de backup devem ser de conhecimento de pelo menos dois funcionários treinados e formalmente autorizados para este fim.

10 - Referências

1. BRASIL. Marco Civil da Internet. Lei 12.965/14.

2. ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. ABNT, 2013.

3. ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. ABNT, 2013.

4. ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO 31000 – Gestão de Riscos – Diretrizes. ABNT, 2018.

Benedito Braz dos Santos

Analista de Tecnologia da Informação