PREFEITURA DE
Peruíbe
www.peruibe.sp.gov.br

PSI

Plano de Segurança da Informação

Departamento de Tecnologia e Gestão da Informação
Secretaria Municipal de Planejamento

Prefeitura Municipal da Estância Balneária de Peruíbe
Rua Nilo Soares Ferreira, 50
(13) 3451.1000

SUMÁRIO

Histórico de Versões e Revisões

Versão	Data	Tipo	Resumo	Responsável
1.0	**20/12/2025**	**Criação**	**Versão Inicial do PSI**	**Rodrigo Campos**

Prefeito
Felipe Antonio Colaço Bernardo

Vice-prefeito
Alexandre Tamer Júnior

Secretário de Planejamento
Elias Abdalla Neto

Secretário de Assuntos Jurídicos
Paulo Renato Passos de Carvalho Pereira

Equipe de Estudo e Elaboração

Rodrigo Rogério Campos — **DTGI | Secretaria de Planejamento**
Jorge Nunes da Silva Neto — **DTGI | Secretaria de Planejamento**
Lucas Cortezzi Marques — **Departamento de Normatização | SAJ**

1. APRESENTAÇÃO

A Política de Segurança da Informação (PSI) da Prefeitura Municipal da Estância Balneária de Peruíbe estabelece os princípios, diretrizes e responsabilidades institucionais voltados à proteção das informações, dos sistemas e dos ativos de Tecnologia da Informação e Comunicações, reconhecendo a informação como ativo estratégico essencial ao funcionamento da Administração Pública.

A crescente digitalização dos serviços públicos, a centralização de informações em sistemas informatizados e a ampliação do uso de plataformas digitais para atendimento ao cidadão tornaram a Administração Pública altamente dependente de ambientes digitais confiáveis, íntegros e disponíveis. Nesse contexto, falhas de segurança da informação podem comprometer não apenas a operação administrativa, mas também a continuidade dos serviços públicos essenciais, a proteção de dados pessoais, a confiança da sociedade e a própria imagem institucional do Município.

A Administração Pública Municipal está exposta a um cenário crescente de ameaças cibernéticas, que incluem ataques a sistemas, indisponibilidade de serviços, sequestro de dados (ransomware), vazamento de informações sensíveis, comprometimento de credenciais e uso indevido de dados públicos e pessoais. Esses riscos são potencializados pela complexidade dos ambientes tecnológicos, pela interconexão entre sistemas e pela necessidade de acesso remoto e compartilhado às informações.

Destaca-se, ainda, o alto risco associado às técnicas de engenharia social, atualmente consideradas um dos principais vetores de incidentes de segurança da informação. Ataques baseados em manipulação psicológica, como phishing, fraudes por e-mail, mensagens falsas, ligações telefônicas fraudulentas e uso indevido de identidade institucional, exploram vulnerabilidades humanas e organizacionais, independentemente do nível de proteção tecnológica existente.

Nesse cenário, a Segurança da Informação deixa de ser apenas uma questão técnica e passa a ser um tema institucional, estratégico e transversal, envolvendo pessoas, processos, tecnologia e governança.

Esta Política está integrada ao Plano Diretor de Tecnologia da Informação e Comunicações (PDTIC) 2026–2029, constituindo instrumento normativo essencial para a gestão de riscos, proteção da informação, continuidade dos serviços públicos e conformidade legal, especialmente no que se refere à Lei Geral de Proteção de Dados Pessoais (LGPD) e às boas práticas de governança exigidas pelos órgãos de controle.

2. OBJETIVOS

A Política de Segurança da Informação tem como objetivo estabelecer um marco institucional de proteção das informações e dos ativos digitais, assegurando que o uso da Tecnologia da Informação e Comunicações ocorra de forma segura, responsável, controlada e alinhada ao interesse público.

São objetivos específicos desta Política:

I. proteger as informações institucionais contra acessos não autorizados, perdas, alterações indevidas e indisponibilidades;

II. reduzir os riscos associados a incidentes de cibersegurança, incluindo ataques externos, falhas internas e ações maliciosas ou acidentais;

III. mitigar os riscos decorrentes de engenharia social, conscientizando usuários e estabelecendo controles institucionais adequados;

IV. garantir a continuidade dos serviços públicos digitais, minimizando impactos operacionais e institucionais;

V. assegurar a conformidade legal, especialmente com a LGPD, preservando os direitos dos titulares de dados;

VI. estabelecer responsabilidades claras quanto ao uso, à proteção e ao tratamento das informações;

VII. fortalecer a governança da Tecnologia da Informação e Comunicações, contribuindo para o controle interno, a transparência e a prestação de contas.

3. ABRANGÊNCIA

A presente Política de Segurança da Informação (PSI) aplica-se a toda a Administração Pública Municipal Direta da Estância Balneária de Peruíbe, abrangendo órgãos, secretarias, departamentos, unidades administrativas e demais estruturas que utilizem informações, sistemas ou recursos de Tecnologia da Informação e Comunicações sob responsabilidade do Município.

Estão sujeitos ao cumprimento desta Política:

I. todos os servidores públicos municipais, efetivos, comissionados ou temporários;
II. estagiários, bolsistas e demais colaboradores que utilizem recursos de Tecnologia da Informação e Comunicações da Prefeitura;
III. prestadores de serviços, empresas terceirizadas, consultores e fornecedores, sempre que tenham acesso, físico ou lógico, a informações, sistemas, redes, equipamentos ou ativos de TIC do Município;

IV. quaisquer outras pessoas físicas ou jurídicas que, a qualquer título, utilizem ou tenham acesso a recursos de Tecnologia da Informação e Comunicações da Administração Pública Municipal.

A Política abrange todos os ativos de informação e de TIC, independentemente do meio ou formato, incluindo, mas não se limitando a:

- informações digitais, impressas ou verbais de caráter institucional;
- sistemas de informação e aplicações corporativas;
- bases de dados e repositórios de informações;
- infraestrutura tecnológica, redes, servidores, estações de trabalho e dispositivos móveis;
- serviços digitais, incluindo o correio eletrônico institucional de implementação própria;
- ambientes físicos relacionados à Tecnologia da Informação e Comunicações.

O cumprimento desta Política é obrigatório, constituindo condição para a utilização dos recursos de Tecnologia da Informação e Comunicações do Município, devendo ser observada em conjunto com as normas, procedimentos e orientações complementares que venham a ser instituídas.

4. REFERÊNCIAS E ALINHAMENTOS

A Política de Segurança da Informação (PSI) da Prefeitura Municipal da Estância Balneária de Peruíbe foi elaborada em conformidade com o arcabouço legal, normativo e de boas práticas aplicáveis à Administração Pública, observando os princípios da legalidade, da eficiência, da transparência, da governança e do controle.

Constituem referências e alinhamentos para a presente Política, entre outros:

4.1 Referências Legais e Normativas

I. Constituição da República Federativa do Brasil de 1988, especialmente os princípios que regem a Administração Pública;

II. Lei nº 12.527, de 2011 (Lei de Acesso à Informação – LAI), no que se refere à transparência ativa e passiva, à proteção das informações e à responsabilidade no tratamento da informação pública;

III. Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que dispõe sobre o tratamento de dados pessoais, a proteção dos direitos dos titulares e a segurança no tratamento das informações;

IV. Lei nº 14.133, de 2021 (Lei de Licitações e Contratos Administrativos), especialmente quanto às exigências de planejamento, governança, gestão de riscos e responsabilidades contratuais relacionadas à Tecnologia da Informação e Comunicações;

V. Lei Municipal nº 2.834, de 2006, que dispõe sobre a reorganização do sistema administrativo municipal da Estância Balneária de Peruíbe, instituindo o Departamento de Tecnologia e Gestão da Informação (DTGI).

4.2 Alinhamento Institucional e de Governança

A presente Política está alinhada:

I. ao Plano Diretor de Tecnologia da Informação e Comunicações (PDTIC) 2026–2029, constituindo instrumento normativo complementar para a gestão de riscos, segurança da informação e continuidade dos serviços digitais;

II. às diretrizes do Planejamento Institucional do Município, apoiando a modernização administrativa, a transformação digital e a proteção das informações públicas;

III. às boas práticas de governança da Tecnologia da Informação e Comunicações aplicáveis à Administração Pública, conforme orientações dos órgãos de controle.

4.3 Referenciais de Boas Práticas

Para a estruturação das diretrizes de segurança da informação, foram considerados, como referência, os princípios e conceitos da família de normas ISO/IEC 27000, especialmente no que se refere à:

- gestão de riscos de segurança da informação;
- proteção da confidencialidade, integridade e disponibilidade das informações;
- definição de controles proporcionais ao contexto institucional;
- abordagem integrada envolvendo pessoas, processos e tecnologia.

O uso desses referenciais não implica adoção obrigatória de certificações formais, mas orienta a adoção de práticas reconhecidas, adequadas à realidade e à capacidade institucional do Município.

Por meio dessas referências e alinhamentos, a Política de Segurança da Informação assegura conformidade legal, coerência institucional e aderência às boas práticas de governança, fortalecendo a proteção dos ativos informacionais da Prefeitura Municipal da Estância Balneária de Peruíbe.

5. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação no âmbito da Prefeitura Municipal da Estância Balneária de Peruíbe será orientada por princípios que assegurem a proteção adequada das informações institucionais, a continuidade dos serviços públicos e a redução dos riscos digitais, considerando a realidade operacional e a capacidade institucional do Município.

Os princípios a seguir estabelecidos constituem a base para a definição de normas, procedimentos e controles de segurança da informação, devendo ser observados por todos os usuários e responsáveis pelos recursos de Tecnologia da Informação e Comunicações.

5.1 Confidencialidade

As informações institucionais devem ser protegidas contra acessos não autorizados, assegurando que somente pessoas devidamente autorizadas tenham acesso às informações necessárias ao desempenho de suas atribuições.

A confidencialidade é essencial para a proteção de dados pessoais, informações sensíveis, dados estratégicos e demais informações cujo uso indevido possa causar prejuízos à Administração Pública Municipal ou aos cidadãos.

5.2 Integridade

As informações devem ser protegidas contra alterações indevidas, intencionais ou acidentais, garantindo sua exatidão, confiabilidade e completude.

A integridade das informações é fundamental para a tomada de decisão administrativa, para a execução de políticas públicas e para a credibilidade dos serviços prestados pelo Município.

5.3 Disponibilidade

Os sistemas, serviços e informações institucionais devem estar disponíveis sempre que necessários para o exercício das atividades administrativas e para a prestação dos serviços públicos.

A indisponibilidade de sistemas críticos pode comprometer a continuidade dos serviços essenciais, impactando diretamente a Administração e a população, devendo ser tratada como risco institucional relevante.

5.4 Necessidade de Conhecer

O acesso às informações deve ser concedido exclusivamente às pessoas que necessitam delas para o desempenho de suas funções institucionais, reduzindo a exposição desnecessária e o risco de uso indevido.

Esse princípio contribui para a redução da superfície de ataque e para a mitigação de riscos associados a falhas humanas e incidentes de segurança.

5.5 Mínimo Privilégio

Usuários, sistemas e processos devem possuir apenas os privilégios estritamente necessários para o cumprimento de suas atribuições, evitando acessos excessivos ou permanentes sem justificativa.

A aplicação do princípio do mínimo privilégio reduz significativamente os impactos de incidentes de segurança, inclusive aqueles decorrentes de engenharia social ou comprometimento de credenciais.

5.6 Rastreabilidade e Auditoria

As ações relevantes realizadas sobre sistemas e informações institucionais devem ser registradas de forma adequada, permitindo o monitoramento, a auditoria e a responsabilização quando necessário.

A rastreabilidade contribui para a detecção de incidentes, para a apuração de responsabilidades e para o atendimento às exigências de controle interno e externo.

5.7 Responsabilização e Cultura de Segurança

Todos os usuários dos recursos de Tecnologia da Informação e Comunicações são responsáveis pelo uso adequado das informações e dos sistemas sob sua responsabilidade.

A Segurança da Informação depende não apenas de controles técnicos, mas também da conscientização e do comportamento dos usuários, sendo fundamental a promoção de uma cultura institucional de segurança digital, com atenção especial aos riscos de engenharia social, fraudes digitais e uso indevido de identidade institucional.

6. PAPÉIS E RESPONSABILIDADES

A efetividade da Política de Segurança da Informação (PSI) depende da definição clara de papéis e responsabilidades, assegurando que a proteção das informações e dos ativos de Tecnologia da Informação e Comunicações seja tratada de forma institucional, coordenada e integrada.

As responsabilidades descritas a seguir não substituem atribuições legais ou regimentais, mas complementam-nas no âmbito da segurança da informação.

6.1 Departamento de Tecnologia e Gestão da Informação (DTGI)

Compete ao Departamento de Tecnologia e Gestão da Informação (DTGI):

I. coordenar a implementação, a manutenção e a revisão periódica da Política de Segurança da Informação;
II. definir, orientar e apoiar a adoção de controles técnicos e organizacionais de segurança da informação;
III. administrar os acessos a sistemas, redes, serviços e recursos de Tecnologia da Informação e Comunicações;
IV. monitorar, registrar e apoiar o tratamento de incidentes de segurança da informação;
V. apoiar a gestão de riscos de segurança da informação, em consonância com o PDTIC;
VI. promover ações de orientação e conscientização em segurança da informação;
VII. apoiar auditorias, controles internos e demandas dos órgãos de controle relacionadas à segurança da informação.

6.2 Gestores das Unidades Administrativas

Compete aos gestores das unidades administrativas:

I. zelar pelo cumprimento desta Política no âmbito de suas respectivas unidades;
II. comunicar ao DTGI as necessidades de concessão, alteração ou revogação de acessos aos recursos de TIC;
III. apoiar a correta utilização das informações e dos sistemas sob sua responsabilidade;
IV. incentivar a observância das boas práticas de segurança da informação pelos servidores e colaboradores;
V. comunicar prontamente incidentes ou suspeitas de falhas de segurança da informação.

6.3 Usuários dos Recursos de Tecnologia da Informação e Comunicações

Compete aos usuários:

I. utilizar os recursos de Tecnologia da Informação e Comunicações exclusivamente para fins institucionais;
II. proteger suas credenciais de acesso, mantendo sigilo sobre senhas e informações de autenticação;
III. observar as diretrizes desta Política e das normas complementares;
IV. adotar comportamento preventivo quanto a riscos de cibersegurança e engenharia social;
V. comunicar imediatamente ao DTGI qualquer incidente, suspeita de comprometimento ou uso indevido de informações ou sistemas.

6.4 Terceirizados, Prestadores de Serviços e Fornecedores

Os prestadores de serviços, empresas terceirizadas, consultores e fornecedores que tenham acesso a recursos de Tecnologia da Informação e Comunicações deverão:

I. cumprir integralmente esta Política e as normas complementares aplicáveis;
II. utilizar acessos exclusivamente para a execução dos serviços contratados;
III. manter sigilo sobre as informações às quais tenham acesso;
IV. assinar termo de responsabilidade e confidencialidade, quando aplicável;

V. submeter-se às regras de controle, monitoramento e auditoria estabelecidas pela Administração Municipal.

6.5 Responsabilidade Institucional Compartilhada

A segurança da informação é responsabilidade compartilhada, envolvendo gestores, usuários, áreas técnicas e prestadores de serviços, devendo ser tratada como elemento essencial para a proteção institucional, a continuidade dos serviços públicos e a mitigação de riscos digitais.

7. CLASSIFICAÇÃO E TRATAMENTO DAS INFORMAÇÕES

A correta classificação e o tratamento adequado da informação são fundamentais para a proteção dos ativos informacionais do Município de Peruíbe, para a mitigação de riscos de segurança da informação e para o cumprimento das obrigações legais e institucionais, especialmente aquelas relacionadas à proteção de dados pessoais.

As informações produzidas, recebidas, armazenadas ou tratadas no âmbito da Administração Pública Municipal deverão ser classificadas de acordo com seu grau de sensibilidade, considerando o impacto potencial decorrente de seu acesso não autorizado, alteração indevida ou indisponibilidade.

7.1 Classificação da Informação

Para fins desta Política, as informações serão classificadas, no mínimo, nas seguintes categorias:

I. Informação Pública
Informações destinadas à divulgação pública ou cujo acesso é garantido por lei, observadas as restrições legais e a proteção de dados pessoais.

II. Informação de Uso Interno
Informações destinadas ao uso interno da Administração Pública Municipal, cujo acesso deve ser restrito aos servidores, colaboradores e terceiros autorizados, conforme a necessidade de conhecer.

III. Informação Confidencial
Informações cujo acesso não autorizado possa causar prejuízos institucionais, legais, financeiros ou à privacidade dos cidadãos, incluindo dados pessoais sensíveis, informações estratégicas, credenciais de acesso e dados protegidos por sigilo legal.

A classificação da informação deverá considerar, sempre que aplicável, as disposições da Lei de Acesso à Informação (LAI) e da Lei Geral de Proteção de Dados Pessoais (LGPD).

7.2 Tratamento da Informação

O tratamento das informações deverá observar sua classificação, aplicando-se controles proporcionais ao nível de sensibilidade, incluindo, entre outros:

I. restrições de acesso conforme a necessidade de conhecer e o princípio do mínimo privilégio;
II. cuidados no armazenamento, transmissão e compartilhamento das informações;
III. proteção contra cópia, alteração ou divulgação não autorizada;
IV. adoção de medidas para evitar perda ou indisponibilidade das informações;
V. descarte adequado das informações, conforme normas aplicáveis.

7.3 Responsabilidades quanto à Classificação e Tratamento

Os gestores das unidades administrativas são responsáveis por orientar a correta classificação das informações sob sua responsabilidade, em articulação com o DTGI, quando necessário.

Os usuários são responsáveis por tratar as informações de acordo com sua classificação, adotando comportamento preventivo e observando as diretrizes desta Política e das normas complementares.

7.4 Normas Complementares

O detalhamento dos procedimentos de classificação, rotulagem, armazenamento, compartilhamento, retenção e descarte das informações será estabelecido em normas complementares, a serem elaboradas e atualizadas conforme a maturidade institucional e as necessidades do Município.

8. GESTÃO DE RISCO E INCIDENTES DE SI

A gestão de riscos e de incidentes de segurança da informação constitui elemento essencial da governança da Tecnologia da Informação e Comunicações no Município de Peruíbe, tendo por finalidade identificar, avaliar, tratar e monitorar os riscos que possam comprometer a confidencialidade, a integridade e a disponibilidade das informações e dos serviços públicos digitais.

Considerando a criticidade dos sistemas e serviços digitais municipais e a crescente exposição a ameaças cibernéticas, a gestão de riscos de segurança da informação deve ser tratada de forma estruturada, contínua e integrada aos processos de planejamento, operação e controle da Administração Pública Municipal.

8.1 Gestão de Riscos de Segurança da Informação

A gestão de riscos de segurança da informação reconhecerá que nenhum ambiente digital é isento de riscos, devendo adotar abordagem proporcional à realidade institucional e à capacidade operacional do Município.

A identificação e a avaliação dos riscos deverão considerar, entre outros aspectos:

I. indisponibilidade de sistemas e serviços digitais críticos;
II. ataques cibernéticos externos, incluindo malware e ransomware;

III. exploração de vulnerabilidades técnicas e organizacionais;
IV. falhas humanas e uso inadequado dos recursos de TIC;
V. riscos decorrentes de engenharia social, como phishing, fraudes digitais e comprometimento de credenciais;
VI. riscos associados a terceiros e prestadores de serviços;
VII. impactos legais e institucionais relacionados à proteção de dados pessoais.

Os riscos identificados deverão ser priorizados conforme seu impacto e probabilidade, podendo ser tratados por meio de ações de mitigação, aceitação, transferência ou eliminação, conforme avaliação institucional.

8.2 Integração com a Governança e o PDTIC

A gestão de riscos de segurança da informação está integrada ao Plano Diretor de Tecnologia da Informação e Comunicações (PDTIC) e ao ciclo de governança da TIC, sendo objeto de acompanhamento nas revisões semestrais, com registro formal das análises e das decisões adotadas.

Essa integração assegura coerência entre o planejamento estratégico, a gestão de riscos e a execução das ações de Tecnologia da Informação e Comunicações.

8.3 Incidentes de Segurança da Informação

Considera-se incidente de segurança da informação qualquer evento que comprometa, ou possa comprometer, a confidencialidade, a integridade ou a disponibilidade das informações ou dos sistemas, incluindo tentativas de acesso não autorizado, falhas de sistemas, vazamento de informações e incidentes decorrentes de engenharia social.

Os incidentes de segurança da informação deverão ser:

I. comunicados imediatamente ao Departamento de Tecnologia e Gestão da Informação (DTGI);
II. registrados de forma adequada para fins de controle, análise e auditoria;
III. tratados com prioridade compatível com sua criticidade e impacto;
IV. objeto de ações corretivas e preventivas, visando evitar recorrências.

O detalhamento dos procedimentos de resposta, comunicação e tratamento de incidentes será estabelecido em norma complementar, observando a legislação vigente e as diretrizes desta Política.

8.4 Importância Institucional da Gestão de Incidentes

Os incidentes de segurança da informação devem ser tratados como eventos institucionais relevantes, podendo gerar impactos operacionais, legais, financeiros e reputacionais para o Município.

A pronta comunicação e o tratamento adequado dos incidentes são fundamentais para:

- reduzir danos e indisponibilidades;
- proteger dados pessoais e informações sensíveis;
- garantir a continuidade dos serviços públicos;
- produzir evidências para controle interno e externo;
- fortalecer a governança e a maturidade institucional em segurança da informação.

9. CONTROLES MÍNIMOS DE SEGURANÇA DA INFORMAÇÃO

A Prefeitura Municipal da Estância Balneária de Peruíbe adotará controles mínimos de segurança da informação, de natureza organizacional, técnica e procedimental, com o objetivo de reduzir riscos, proteger os ativos informacionais e assegurar a continuidade dos serviços públicos digitais, de forma proporcional à realidade institucional do Município.

Os controles mínimos estabelecidos nesta Política definem obrigações institucionais, cabendo o detalhamento técnico e operacional a normas e procedimentos complementares, sob coordenação do Departamento de Tecnologia e Gestão da Informação (DTGI).

9.1 Controle de Acessos

O acesso aos sistemas, redes, serviços e informações institucionais deverá observar:

I. concessão de acessos mediante autorização formal e compatível com as atribuições do usuário;
II. aplicação dos princípios da necessidade de conhecer e do mínimo privilégio;
III. uso de credenciais individuais e intransferíveis;
IV. revisão periódica dos acessos concedidos;
V. revogação tempestiva de acessos em casos de desligamento, mudança de função ou término de contrato.

9.2 Uso de Credenciais e Autenticação

Os usuários são responsáveis pela proteção de suas credenciais de acesso, devendo:

I. manter sigilo sobre senhas e demais informações de autenticação;
II. evitar o compartilhamento de credenciais;
III. adotar práticas seguras de autenticação, conforme orientações institucionais;
IV. estar atentos a tentativas de engenharia social voltadas à obtenção indevida de credenciais.

9.3 Uso do Correio Eletrônico Institucional

O correio eletrônico institucional oficial do Município de Peruíbe constitui o meio formal e autorizado para a realização de comunicações institucionais, administrativas e operacionais no âmbito da Administração Pública Municipal.

É obrigatória a utilização do e-mail institucional fornecido e gerenciado pelo Município para a troca de informações relacionadas às atividades funcionais, à gestão administrativa, à comunicação entre unidades e ao relacionamento institucional com cidadãos, fornecedores e demais entes públicos.

Não é autorizada a realização de comunicação institucional por meio de:

I. contas pessoais de e-mail;
II. serviços de correio eletrônico fornecidos por outras empresas ou plataformas externas, ainda que de uso gratuito;
III. contas de e-mail não gerenciadas ou não controladas pela Administração Municipal.

Essa restrição tem por finalidade:

- assegurar a segurança da informação;
- preservar a integridade, rastreabilidade e arquivamento das comunicações institucionais;
- reduzir riscos de vazamento de informações e de engenharia social;
- garantir conformidade com a legislação vigente e com os princípios da Administração Pública.

Os usuários deverão adotar cuidados redobrados na abertura de mensagens, links e anexos recebidos, especialmente diante de tentativas de phishing, fraudes digitais e uso indevido de identidade institucional, comunicando imediatamente ao DTGI qualquer suspeita de incidente de segurança.

9.4 Uso da Internet e dos Recursos de Rede

O uso da internet e dos recursos de rede no âmbito da Administração Pública Municipal deverá ocorrer exclusivamente por meio da infraestrutura institucional oficialmente disponibilizada e gerenciada pelo Município, observando as diretrizes de segurança da informação e de governança de TIC.

É vedada a utilização, para fins institucionais:

I. de acessos à internet residencial ou particular, ainda que de servidores ou colaboradores;
II. de conexões não homologadas ou não controladas pelo Departamento de Tecnologia e Gestão da Informação (DTGI);
III. de equipamentos de rede de classe residencial, tais como roteadores, modems, pontos de acesso ou dispositivos similares não destinados a uso corporativo.

A utilização de acessos ou equipamentos não institucionais expõe o Município a riscos elevados de cibersegurança, incluindo:

- ausência de controles adequados de segurança;
- falhas de atualização e correção de vulnerabilidades;
- impossibilidade de monitoramento e rastreabilidade;
- maior exposição a ataques cibernéticos e incidentes de engenharia social;
- comprometimento da confidencialidade, integridade e disponibilidade das informações.

O acesso aos sistemas e serviços digitais deverá ocorrer exclusivamente por meio da infraestrutura de rede oficial do Município, observando-se as orientações técnicas e de segurança emitidas pelo DTGI.

O uso dos recursos de internet e de rede poderá ser monitorado para fins de segurança, controle, auditoria e conformidade, respeitada a legislação vigente e as diretrizes desta Política.

9.5 Proteção de Equipamentos e Infraestrutura

Os equipamentos, servidores, estações de trabalho e demais ativos de TIC deverão ser utilizados de forma adequada, protegidos contra acesso não autorizado, danos físicos e uso indevido.

A proteção da infraestrutura tecnológica é essencial para a continuidade dos serviços públicos digitais e para a mitigação de riscos operacionais e institucionais.

9.6 Backup e Recuperação de Informações

A proteção das informações institucionais é responsabilidade compartilhada, cabendo tanto à Administração Municipal quanto aos usuários dos recursos de Tecnologia da Informação e Comunicações adotar medidas adequadas para evitar perdas, danos ou indisponibilidades de dados.

Compete ao usuário utilizador zelar pela guarda, organização e proteção dos dados e arquivos salvos em seu computador funcional, observando as orientações institucionais quanto ao uso adequado dos recursos de TIC.

Os usuários deverão:

I. adotar práticas responsáveis no armazenamento de arquivos e informações institucionais;
II. evitar o armazenamento exclusivo de informações relevantes em mídias locais sem proteção ou redundância;

III. observar as orientações do Departamento de Tecnologia e Gestão da Informação (DTGI) quanto aos locais adequados para armazenamento de dados institucionais;
IV. comunicar ao DTGI situações de perda, corrupção ou comprometimento de dados sob sua responsabilidade.

As rotinas institucionais de backup existentes, têm por objetivo reduzir riscos sistêmicos e apoiar a recuperação de serviços, não substituindo a responsabilidade individual do usuário quanto à guarda e proteção dos dados e arquivos sob sua custódia.

O detalhamento dos procedimentos de backup, armazenamento institucional e recuperação de informações será estabelecido em normas e orientações complementares, considerando a criticidade das informações e a capacidade operacional do Município.

9.7 Registro e Monitoramento de Eventos

Os eventos relevantes relacionados à segurança da informação poderão ser registrados e monitorados, com a finalidade de:

I. identificar incidentes e tentativas de acesso indevido;
II. apoiar investigações e auditorias;
III. fortalecer o controle interno e a governança da TIC.

9.8 Normas Complementares

O detalhamento dos controles técnicos e operacionais será definido por meio de normas e procedimentos complementares, que poderão abranger, entre outros temas, controle de acessos, uso aceitável dos recursos de TIC, gestão de backups, resposta a incidentes e segurança de terceiros.

10. CONSCIENTIZAÇÃO E CULTURA DE SEGURANÇA DA INFORMAÇÃO

A conscientização e a promoção de uma cultura institucional de segurança da informação são reconhecidas como elementos essenciais para a efetividade desta Política, considerando que o fator humano constitui um dos principais vetores de risco em ambientes digitais.

A Administração Pública Municipal reconhece que controles técnicos, por si só, não são suficientes para garantir a segurança da informação, sendo indispensável o engajamento consciente dos usuários na adoção de práticas seguras e responsáveis no uso dos recursos de Tecnologia da Informação e Comunicações.

10.1 Cultura Institucional de Segurança da Informação

A segurança da informação deve ser incorporada à rotina administrativa e à cultura organizacional, sendo tratada como responsabilidade institucional permanente e compartilhada.

Nesse contexto, todos os usuários dos recursos de TIC devem atuar de forma preventiva, ética e responsável, adotando comportamentos que reduzam riscos e contribuam para a proteção das informações e dos serviços públicos digitais.

10.2 Conscientização quanto à Cibersegurança e Engenharia Social

As ações de conscientização deverão priorizar a prevenção a riscos relacionados à cibersegurança, com destaque para as ameaças decorrentes de engenharia social, incluindo, entre outras:

I. tentativas de phishing e fraudes por e-mail;
II. mensagens eletrônicas ou comunicações falsas utilizando identidade institucional;
III. solicitações indevidas de credenciais, informações sensíveis ou dados pessoais;
IV. links e anexos maliciosos;
V. abordagens fraudulentas por telefone ou outros meios de comunicação.

Os usuários deverão adotar postura crítica e cautelosa diante de comunicações suspeitas, comunicando imediatamente ao Departamento de Tecnologia e Gestão da Informação (DTGI) quaisquer indícios de tentativa de fraude ou incidente de segurança da informação.

10.3 Ações de Orientação e Capacitação

A Administração Municipal, por meio do DTGI, poderá promover ações de orientação e capacitação, compatíveis com a realidade institucional, tais como:

- divulgação de orientações e comunicados de segurança;
- campanhas internas de conscientização;
- materiais educativos sobre boas práticas de segurança digital;
- orientações específicas para novos servidores, estagiários e terceirizados.

As ações de conscientização têm caráter preventivo e educativo, visando reduzir riscos, fortalecer a cultura de segurança da informação e apoiar a continuidade dos serviços públicos.

10.4 Responsabilidade dos Usuários

Cada usuário é responsável por contribuir para a segurança da informação, observando as diretrizes desta Política, das normas complementares e das orientações institucionais.

A negligência, o desconhecimento ou o descumprimento das diretrizes de segurança da informação podem expor o Município a riscos significativos, devendo ser tratados com a devida seriedade institucional.

11. MONITORAMENTO, AUDITORIA E CONFORMIDADE

O monitoramento, a auditoria e a conformidade constituem elementos essenciais para assegurar a efetividade da Política de Segurança da Informação (PSI), permitindo o acompanhamento contínuo do cumprimento de suas diretrizes, a identificação de fragilidades e a adoção de medidas corretivas e preventivas.

A Administração Pública Municipal adotará práticas de monitoramento e controle compatíveis com sua realidade institucional, respeitando os princípios da legalidade, proporcionalidade, transparência e proteção de dados pessoais.

11.1 Monitoramento da Segurança da Informação

O uso dos recursos de Tecnologia da Informação e Comunicações poderá ser monitorado para fins de segurança da informação, prevenção de incidentes, controle e conformidade normativa, observada a legislação vigente.

O monitoramento tem por finalidade:

I. identificar tentativas de acesso não autorizado;
II. detectar incidentes de segurança da informação;
III. apoiar a gestão de riscos e a continuidade dos serviços;
IV. produzir evidências para controle interno e externo;
V. subsidiar ações corretivas e preventivas.

As atividades de monitoramento não têm caráter de vigilância pessoal, devendo ser realizadas de forma impessoal, técnica e justificada, exclusivamente para fins institucionais.

11.2 Auditoria e Controle

A Política de Segurança da Informação e as normas complementares poderão ser objeto de auditorias internas, verificações de conformidade e avaliações promovidas pela Administração Municipal ou por órgãos de controle competentes.

As auditorias poderão abranger, entre outros aspectos:

I. cumprimento das diretrizes da Política;
II. existência de controles mínimos de segurança da informação;
III. registro e tratamento de incidentes;
IV. gestão de acessos e credenciais;
V. conformidade com a legislação aplicável, especialmente a LGPD.

O DTGI deverá apoiar as ações de auditoria e controle, fornecendo informações, registros e evidências necessárias.

11.3 Conformidade Legal e Normativa

O cumprimento desta Política visa assegurar a conformidade legal e normativa no tratamento das informações e no uso dos recursos de Tecnologia da Informação e Comunicações, reduzindo riscos legais, institucionais e reputacionais para o Município.

As diretrizes da PSI devem ser observadas em conjunto com:

- legislação vigente;
- normativos internos do Município;
- cláusulas contratuais aplicáveis a prestadores de serviços;
- orientações e determinações dos órgãos de controle.

11.4 Ações Corretivas e Melhoria Contínua

As não conformidades identificadas por meio de monitoramento, auditoria ou análise de incidentes deverão ser tratadas de forma adequada, com a adoção de ações corretivas e preventivas proporcionais à gravidade e ao impacto identificado.

A Política de Segurança da Informação será continuamente aprimorada, com base nos resultados do monitoramento, das auditorias e das revisões periódicas, fortalecendo a maturidade institucional em segurança da informação e cibersegurança.

12. SANÇÕES E MEDIDAS DISCIPLINARES

O descumprimento das diretrizes estabelecidas nesta Política de Segurança da Informação (PSI), bem como das normas e procedimentos complementares dela decorrentes, poderá ensejar a adoção de medidas administrativas, disciplinares ou contratuais, conforme a natureza da infração, a gravidade do fato e a legislação vigente.

As sanções e medidas disciplinares têm por finalidade proteger o interesse público, prevenir recorrências, mitigar riscos institucionais e reforçar a responsabilidade no uso dos recursos de Tecnologia da Informação e Comunicações, não se confundindo com ações de caráter meramente punitivo.

12.1 Aplicação das Medidas

A aplicação de medidas decorrentes do descumprimento desta Política observará:

I. os princípios da legalidade, razoabilidade e proporcionalidade;
II. o direito ao contraditório e à ampla defesa, quando aplicável;
III. a legislação estatutária, trabalhista e contratual vigente;

IV. os normativos internos da Administração Pública Municipal.

12.2 Medidas Administrativas

Sem prejuízo de outras medidas cabíveis, poderão ser adotadas, conforme o caso:

I. orientação formal ao usuário;
II. suspensão temporária de acessos a sistemas ou recursos de TIC;
III. revogação de privilégios de acesso incompatíveis com a função exercida;
IV. comunicação à chefia imediata ou à autoridade competente.

12.3 Responsabilização de Terceirizados

Os prestadores de serviços, empresas terceirizadas e fornecedores que descumprirem esta Política ou utilizarem indevidamente os recursos de TIC poderão sofrer as sanções previstas nos instrumentos contratuais, sem prejuízo de outras medidas legais cabíveis.

12.4 Responsabilidade Legal

O descumprimento das diretrizes de segurança da informação poderá, conforme o caso, ensejar responsabilização civil, administrativa ou penal, especialmente quando resultar em danos à Administração Pública, aos cidadãos ou em violação à legislação vigente, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD).

13. VIGÊNCIA, REVISÃO E CONTROLE DE VERSÕES

A presente Política de Segurança da Informação (PSI) entra em vigor na data de sua aprovação pela autoridade competente e terá vigência por prazo indeterminado, mantendo-se válida enquanto não for formalmente revisada ou substituída.

A adoção de vigência por prazo indeterminado reflete o caráter permanente, institucional e contínuo da segurança da informação, reconhecendo que a proteção dos ativos informacionais e dos serviços digitais não se limita a ciclos de planejamento específicos.

13.1 Revisão da Política

A Política de Segurança da Informação deverá ser revisada periodicamente, no mínimo de forma semestral, ou sempre que ocorrerem mudanças relevantes, tais como:

I. alterações significativas no ambiente tecnológico;
II. ocorrência de incidentes relevantes de segurança da informação;
III. mudanças legais ou normativas aplicáveis;
IV. reestruturações administrativas que impactem a governança de TIC;
V. recomendações de auditorias ou dos órgãos de controle.

As revisões serão coordenadas pelo Departamento de Tecnologia e Gestão da Informação (DTGI), podendo contar com a participação de outras áreas administrativas, conforme a natureza das alterações propostas.

13.2 Controle de Versões

Todas as versões da Política de Segurança da Informação deverão ser formalmente registradas, assegurando rastreabilidade, transparência e evidências de governança.

O controle de versões deverá contemplar, no mínimo:

I. identificação da versão do documento;
II. data de aprovação e de vigência da versão;
III. descrição resumida das alterações realizadas;
IV. responsáveis pela revisão;
V. instância de aprovação.

As versões anteriores deverão ser preservadas para fins de histórico, controle e auditoria.

13.3 Publicação e Divulgação

A versão vigente da Política de Segurança da Informação deverá ser amplamente divulgada no âmbito da Administração Pública Municipal, garantindo o conhecimento de suas diretrizes por servidores, colaboradores e terceiros abrangidos.

A divulgação observará as diretrizes de segurança da informação e de proteção de dados pessoais, assegurando o acesso às informações necessárias ao cumprimento desta Política.