

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Município de Pompeia

"Protegendo dados, pessoas e sistemas em conformidade com a LGPD e boas práticas de segurança."

Secretaria Municipal de Tecnologia da Informação

2025



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

ÍNDICE

1. Introdução e Objetivo
2. Abrangência
3. Base Legal e Referências
4. Definições e Glossário
5. Princípios da Segurança da Informação
6. Governança e Estrutura Organizacional
 - 6.1 Comitê de Segurança da Informação (CSI)
 - 6.2 Encarregado pela LGPD (DPO)
 - 6.3 Equipe de Tecnologia da Informação
7. Obrigações dos Colaboradores
8. Classificação da Informação
9. Controle de Segurança
 - 9.1 Políticas de Acesso
 - 9.2 Gestão de Ativos
 - 9.3 Segurança Física
 - 9.4 Segurança de Rede
 - 9.5 Backup e Recuperação
 - 9.6 Atualizações e Patch Management
 - 9.7 Terceiros e Fornecedores
 - 9.8 Uso da Tecnologia
 - 9.9 Teletrabalho e BYOD
10. Mesa Limpa e Tela Protegida
11. Gestão de Incidentes de Segurança
 - 11.1 Definição de Incidente



/PrefPompeia



@prefpompeiaoficial



www.pompeia.sp.gov.br

CNPJ: 44.483.444/0001-09



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1

CEP 17.580-053 Fone (14)3405-1500

11.2 Fluxo de Resposta (Anexo H)

11.3 Prazos (PGPD)

12. Conscientização e Treinamento

13. Auditoria e Melhoria Contínua

14. Penalidades

15. Anexos

16. Disposições Finais

17. Aprovação

Política de Segurança da Informação Município de Pompeia

1. Introdução e Objetivo

A Política de Segurança da Informação (PSI) do Município de Pompeia define as diretrizes para proteção de dados, informações e ativos tecnológicos, assegurando confidencialidade, disponibilidade, rastreabilidade e conformidade Legal. Esta política estabelece responsabilidade de servidores, estagiários, prestadores de serviços e fornecedores.

Protegendo ativos de informação contra ameaças internas e externas, em conformidade com a legislação vigente, especialmente a LGPD (Lei. N. 13.709/2018)

2. Abrangência

Este plano aplica-se a:

- Todos os servidores públicos (efetivos, comissionados e terceirizados);
- Sistema de Informação (interno e externos);
- Infraestrutura de Tecnologia da Informação (servidores, redes, dispositivos móveis, nuvem, etc);
- Dados pessoais e sensíveis de cidadãos, servidores e parceiros;
- Processos administrativos que envolvam tratamento de dados.



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

Ou seja, aplica-se a todos os órgãos de forma direta ou indireta que utilizem ou tenham acesso a informações, sistemas e recursos tecnológicos do Município de Pompeia, seja de forma presencial ou remota.

3. Base Legal e Referências

- Lei n. 13.709/2018 - LGPD;
- ISO/IEC 27001:2022 - Requisitos para Sistemas de Gestão de Segurança da Informação (SGSI);
- Política Nacional de Segurança da Informação (PNSI).

4. Definições e Glossário

Ativo: qualquer recurso de informação (físico ou lógico);

Anonimização: técnica que retira a possibilidade de identificar um indivíduo;

BYOD: Bring Your Own Device, uso de dispositivo pessoais para fins profissionais;

Criptografia: técnica de proteção de dados por meio de algoritmos que tornam a informação ilegível sem chave apropriada;

Dado Pessoal: Informação relacionada a pessoa natural identificada ou identificável;

Dado Pessoal Sensível: origem racial, saúde, convicção religiosa, opinião política, biometria, etc;

Engenharia Social: manipulação psicológica de pessoas para obter informações confidenciais ou acesso a sistemas;

Incidente de Segurança: evento que comprometa ou ameace dados, sistemas ou serviços;



/PrefPompeia



@prefpompeiaoficial



www.pompeia.sp.gov.br

CNPJ: 44.483.444/0001-09



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

Logs: registros eletrônicos que armazenam atividades de sistemas, usuários e aplicações para auditoria e rastreabilidade;

Pseudonimização: técnica que substitui informações que identificam diretamente um titular por outros identificadores artificiais, reduzindo risco de exposição;

Phishing: técnica de fraude eletrônica que induz usuários a fornecer sensíveis por meio de mensagens falsas;

Teletrabalho: execução de atividades fora das dependências físicas da Prefeitura;

VPN: Rede privada virtual para acesso remoto seguro.

5. Princípios da Segurança da Informação

- **Confidencialidade:** Garantir que as informações sejam acessadas apenas por pessoas autorizadas;
- **Integridade:** Assegurar que as informações não sejam alteradas indevidamente;
- **Disponibilidade:** Assegurar que informações estejam acessíveis quando necessárias;
- **Rastreabilidade:** Assegurar registro das ações e acessos realizados;
- **Conformidade:** Aderência à LGPD, Marco Civil da Internet e demais normas;
- **Responsabilidade:** Cada servidor é responsável pelo uso adequado dos ativos de informação.



/PrefPompeia



@prefpompeiaoficial



www.pompeia.sp.gov.br

CNPJ: 44.483.444/0001-09



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

6. Governança e Estrutura Organizacional

6.1. Comitê de Segurança da Informação (CSI)

- Composição: Prefeito (ou representante), Secretário de Administração, Secretário de Tecnologia da Informação, Encarregado de Proteção de Dados (DPO) e representante Jurídico.
- Atribuições: Aprovar políticas, analisar incidente graves, revisar o PSI anualmente.

6.2. Encarregado pela LGPD (DPO - Data Protection Officer)

- Nomeado oficialmente conforme art. 41 da LGPD;
- Atua como ponto focal entre a Prefeitura, titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

6.3. Equipe de Tecnologia da Informação

- Responsável pela implementação técnica dos controles, monitoramento, resposta a incidentes e treinamentos.

7. Obrigações dos Colaboradores

- Respeitar confidencialidade das informações, inclusive após desligamento;
- Proteger senhas e credenciais de acesso;
- Comunicar incidentes imediatamente à TI e ao DPO;
- Não Compartilhar dados pessoais ou confidenciais sem autorização;
- Cumprir normas de uso de e-mail, internet e softwares.



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

8. Classificação da Informação

Nível	Descrição	Exemplo
Público	Informações de acesso livre	Editais, Leis municipais
Interno	Uso restrito a servidores	Processos administrativos internos
Confidencial	Dados sensíveis ou restritos	Dados pessoais, contratos, laudos médicos
Reservado	Informações críticas à segurança	Senhas de sistemas, plano de contingência, plano de backup

9. Controle de Segurança (Baseado na ISO 27001)

9.1. Políticas de Acesso

- Controle de acesso baseado no princípio do menor privilégio
- Autenticação forte (senhas complexas + MFA onde possível)
- Revogação imediata de acessos ao término de vínculo

9.2. Gestão de Ativos

- Inventário atualizado de hardware, software e dados
- Rotulagem de ativos conforme classificação da informação

9.3. Segurança Física

- Controle de acesso físico a salas de servidores e estações de trabalho;



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

- Câmeras de vigilância (monitoramento) e registros de entrada/saída.

9.4. Segurança de Rede

- Firewall, segmentação de rede, IDS/IPS;
- Wi-Fi corporativo segregado do público;
- Criptografia de dados em trânsito (TLS 1.2+).

9.5. Backup e recuperação

- Backups diários críticos, semanais gerais;
- Testes de restauração trimestrais;
- Armazenamento off-site ou em nuvem segura;
- Plano de contingência contra ransomware e falhas críticas.

9.6. Atualizações e Patch Management

- Política de atualização obrigatórias de sistemas e software;
- Vulnerabilidade críticas corrigidas em até 72h;
- Proibição de software piratas ou não autorizados, apenas software licenciados e homologados;
- Auditorias periódicas em estações e servidores.

9.7. Terceiros e Fornecedores

- Cláusulas de segurança e LGPD em contratos;
- Avaliação de riscos antes de integração de sistemas de terceiros.

9.8. Uso da Tecnologia

- Senhas fortes (mínimo 7 caracteres, troca a cada 90 dias, 2FA);



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

- Internet e e-mail: uso exclusivo institucional;
- Proibido spam, phishing, correntes e sites ilícitos;
- Computadores e notebooks: uso exclusivo institucional; somente softwares licenciados;
- Cloud computing: apenas em provedores homologados;
- Mensageria: WhatsApp/Telegram dentre outros, apenas com autorização, respeitando confidencialidade.

9.9. Teletrabalho e BYOD

- Uso de VPN obrigatório para acesso remoto.
- Antivírus e firewall sempre atualizados e licenciados.
- Proibição de uso de redes Wi-Fi abertas.
- BYOD permitindo apenas com criptografia, software licenciados e Antivírus ativo.
- Responsabilidade do usuário pela segurança dos dados em seu dispositivo.

10. Mesa Limpa e Tela Protegida

- Documentos sensíveis não devem ser deixados sobre mesas.
- Computadores devem bloquear a tela após 10 minutos de inatividade.

11. Gestão de Incidentes de Segurança

11.1. Definição de Incidente

Qualquer evento que comprometa a segurança da informação (exemplo: vazamento de dados, ransomware, acesso não autorizado).



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

11.2. Fluxo de Resposta (Anexo H)

- 1 - Detecção;
- 2 - Notificação ao DPO/CSI;
- 3 - Contenção;
- 4 - Investigação;
- 5 - Recuperação;
- 6 - Comunicação aos órgãos competentes (se necessário à ANPD/Titulares);
- 7 - Lições aprendidas.

11.3. Prazos (PGPD)

Notificação à ANPD em até 72 horas após confirmação do incidente, se houver risco aos titulares.

Todos os incidentes devem ser reportados à Secretaria Municipal de Tecnologia da Informação e ao DPO de imediato ao incidente.

12. Conscientização e Treinamento

Treinamento obrigatório anual para todos os servidores sobre:

- LGPD;
- Phishing e engenharia social;
- Uso seguro de senhas;
- Procedimentos em caso de incidente;
- Simulações de ataques (ex.: e-mails falsos de phishing) semestralmente.



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

13. Auditoria e melhoria Contínua

- Auditorias internas semestrais ou anuais de conformidade com o PSI;
- Revisão a cada 2 anos do plano pelo Comitê de Segurança;
- Indicadores de desempenho (ex.: número de incidentes, tempo de resposta, % de servidores treinados).

14. Penalidades

O descumprimento das disposições da Política de Segurança da Informação – PSI sujeitará o responsável às sanções administrativas, civis e penais previstas na legislação vigente, observados o contraditório e a ampla defesa, quando cabíveis.

O desconhecimento da política não será aceito como justificativa.

15. Anexos

- Anexo A: Termo de Confidencialidade para servidores;
- Anexo B: Termos de responsabilidade do Usuário;
- Anexo C: Formulário de Notificação de Incidente;
- Anexo D: Lista de Sistemas Críticos e Classificação de Dados;
- Anexo E: Fluxo de resposta de incidentes;
- Anexo F: Guia de Boas Práticas de Teletrabalho.

16. Disposições Finais



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

Esta PSI entra em vigor na data de sua publicação oficial e deve estar disponível no site da Prefeitura de Pompeia. Todos os colaboradores deverão assinar termo de ciência e compromisso. Será revisada a cada 2 anos ou quando houver mudanças legais ou tecnológicas exigirem.

Esta política revoga disposições anteriores sobre segurança da informação no âmbito da Prefeitura Municipal de Pompeia.

Pompeia, 29 de dezembro de 2025.

JOSÉ STEVERSON AGUILAR FERREIRA

Secretário Municipal de Tecnologia da Informação

DIOGO MONTEFUSCO CESHIM SILVA

Prefeito Municipal de Pompeia



/PrefPompeia



@prefpompeiaoficial



www.pompeia.sp.gov.br

CNPJ: 44.483.444/0001-09

ANEXO A:

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

1. Identificação do Servidor

Nome completo: [Nome completo do servidor]

Matrícula: [Número de matrícula]

Cargo/Função: [Cargo ou função exercida]

Setor/Departamento: [Nome do setor ou departamento]

Eu, [Nome completo do servidor], portador(a) do RG nº [Número do RG] e CPF nº [Número do CPF], servidor(a) da Prefeitura Municipal de Pompeia e Autarquias, declaro, para os devidos fins, ter conhecimento da Política de Segurança da Informação (PSI) desta instituição e assumo as seguintes responsabilidades:

2. Do Compromisso de Confidencialidade

Comprometo-me a manter o mais absoluto sigilo e confidencialidade sobre todas as informações e dados aos quais tiver acesso durante o exercício de minhas funções, independentemente da forma de armazenamento (física ou digital). Isso inclui, mas não se limita a:

- Dados pessoais e informações de cidadãos, nos termos da Lei Geral de Proteção de Dados (LGPD).
- Informações estratégicas, financeiras, administrativas ou operacionais da instituição, exceto o que é permitido por Lei.
- Documentos, processos, fluxogramas, códigos-fonte e quaisquer outros materiais sigilosos.



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

3. Das Obrigações e Proibições

O meu compromisso de sigilo abrange as seguintes obrigações e proibições:

- Não divulgar, repassar ou dar conhecimento a terceiros, sem autorização expressa, das informações confidenciais a que tive acesso.
- Não utilizar as informações confidenciais para benefício próprio ou de terceiros, seja de forma direta ou indireta.
- Não efetuar cópias, gravações ou reproduções de documentos ou informações confidenciais, a menos que seja estritamente necessário para o desempenho da função e com a devida autorização.
- Utilizar os ativos de informação (equipamentos, sistemas, redes) da Prefeitura Municipal de Pompeia exclusivamente para fins de serviço, respeitando a legislação vigente e as normas internas.
- Proteger os acessos e credenciais (senhas, logins), sendo o único responsável por seu uso indevido.

4. Da Permanência da Obrigação

A obrigação de confidencialidade e sigilo permanecerá válida e em pleno vigor mesmo após o encerramento das minhas funções na Prefeitura Municipal de Pompeia.

5. Das Sanções

Estou ciente de que o descumprimento deste termo, bem como de quaisquer regras da Política de Segurança da Informação, sujeitará o servidor às sanções administrativas, civis e penais cabíveis, conforme a legislação aplicável. A Prefeitura Municipal de Pompeia poderá apurar a quebra do sigilo em processo administrativo regular.

6. Do Conhecimento e Assinatura

Declaro que li e compreendi integralmente este Termo de Responsabilidade e Confidencialidade, estando ciente de todas as suas cláusulas e obrigações.

Pompeia, _____ de _____ de _____

[Nome completo do servidor]

CPF: [Número do CPF]



/PrefPompeia



@prefpompeiaoficial



www.pompeia.sp.gov.br

CNPJ: 44.483.444/0001-09

ANEXO B:

TERMO DE RESPONSABILIDADE DO USUÁRIO DE TECNOLOGIA DA INFORMAÇÃO

1. Identificação do Usuário

Nome completo: [Nome completo do usuário]

Matrícula/ID: [Número de matrícula ou identificação]

Cargo/Função: [Cargo ou função exercida]

Setor/Departamento: [Nome do setor ou departamento]

Eu, [Nome completo do usuário], inscrito(a) no CPF sob nº [Número do CPF], declaro estar ciente da Política de Segurança da Informação da Prefeitura Municipal de Pompeia e, ao utilizar os recursos de tecnologia da informação, assumo as seguintes responsabilidades:

2. Acesso e Senhas

- Manter a confidencialidade das minhas credenciais de acesso (usuário e senha), que são pessoais e intransferíveis.
- Não compartilhar credenciais sob nenhuma circunstância.
- Comunicar imediatamente à área de TI qualquer suspeita de comprometimento de senha ou incidente de segurança.
- Bloquear ou encerrar a sessão da estação de trabalho sempre que me ausentar.

3. Uso de Equipamentos e Sistemas

- Utilizar os equipamentos, sistemas e softwares da Prefeitura exclusivamente para fins institucionais.



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

- Não instalar ou utilizar softwares, aplicativos ou dispositivos sem autorização prévia da área de TI.
- Zelar pela integridade e conservação dos equipamentos sob minha responsabilidade.
- Comunicar imediatamente qualquer dano, defeito, perda, furto ou roubo de equipamentos.
- Reconhecer que, em caso de mau uso, negligência ou uso inadequado, poderei ser responsabilizado(a) pela reparação ou substituição do bem.

4. Navegação, Dados e Informação

- Utilizar a internet e a rede institucional de forma responsável, não acessando sites ilícitos, de jogos, pornografia, ou que possam comprometer a segurança.
- Não realizar download, instalação ou distribuição de arquivos ilegais, piratas ou maliciosos.
- Zelar pela proteção de dados pessoais e informações sigilosas em conformidade com a LGPD.
- Garantir o correto armazenamento e tratamento das informações, evitando sua exposição ou acesso não autorizado.
- Observar e cumprir as normas de backup e guarda de dados definidas pela Prefeitura Municipal de Pompeia.

5. Comunicação e E-mail Corporativo

- Utilizar o e-mail e demais meios de comunicação corporativos de forma ética e profissional.
- Não enviar mensagens ofensivas, discriminatórias, correntes, propagandas não autorizadas ou informações sigilosas sem a devida permissão.



/PrefPompeia



@prefpompeiaoficial



www.pompeia.sp.gov.br

CNPJ: 44.483.444/0001-09



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

- Reconhecer que o uso dos recursos de TI poderá ser monitorado para fins de auditoria e segurança, em conformidade com a legislação vigente.

6. Responsabilidade e Penalidades

- Estou ciente de que o uso inadequado dos recursos de TI poderá resultar em sanções disciplinares, administrativas, civis e/ou criminais, conforme previsto na legislação e normas internas.
- Reconheço que a violação deste termo ou da Política de Segurança da Informação poderá configurar falta grave e acarretar responsabilização funcional e judicial.

7. Ciência e Assinatura

Declaro que li, compreendi e estou de acordo com os termos do presente documento, comprometendo-me a cumpri-lo integralmente.

Pompeia, _____ de _____ de _____

[Nome completo do usuário]

CPF: [Número do CPF]



/PrefPompeia



@prefpompeiaoficial



www.pompeia.sp.gov.br

CNPJ: 44.483.444/0001-09



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

ANEXO C:

FORMULÁRIO SIMPLIFICADO DE NOTIFICAÇÃO DE INCIDENTE

1. Dados Gerais

- Data da ocorrência: _____
- Hora: _____
- Local/Setor: _____
- Responsável pelo registro: _____

2. Tipo de Incidente (assinale o que se aplica)

- ☐ Acesso não autorizado
- ☐ Vazamento de dados
- ☐ Perda de informação
- ☐ Infecção por malware
- ☐ Falha de sistema
- ☐ Outro: _____

3. Descrição do Incidente

4. Impacto Identificado

- Sistemas/serviços afetados: _____
- Dados pessoais envolvidos: ☐ Sim ☐ Não ☐ A avaliar
- Risco ao titular (conforme LGPD): ☐ Alto ☐ Médio ☐ Baixo

5. Ações Imediatas Adotadas

6. Responsáveis pela Ação

- Responsável técnico (TI): _____
- Responsável pelo setor: _____
- DPO/Encarregado de Dados: _____

7. Encerramento

- Data de encerramento: _____
- Observações finais: _____



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1

CEP 17.580-053 Fone (14)3405-1500

8. Assinaturas

Responsável pelo registro: _____ Data: ____/____/____

Responsável técnico (TI): _____ Data: ____/____/____

DPO/Encarregado de Dados: _____ Data: ____/____/____

9. Orientações:

- Este formulário deve ser preenchido **imediatamente após a detecção** de qualquer incidente de segurança da informação.
- Deve ser encaminhado a **Secretaria de Tecnologia da Informação** e ao **Encarregado de Dados (DPO)**.
- Incidentes que envolvam **dados pessoais** devem seguir o fluxo de comunicação e notificação conforme previsto na **LGPD** e no **Plano de Resposta a Incidentes da Prefeitura**.



/PrefPompeia



@prefpompeiaoficial



www.pompeia.sp.gov.br

CNPJ: 44.483.444/0001-09

ANEXO D:

Lista de Sistemas Críticos e Classificação da Informação

1. Objetivo

Este anexo define os sistemas de informação considerados críticos para a continuidade das operações da Prefeitura de Pompeia, bem como a classificação dos dados por eles tratados ou armazenados, de acordo com o nível de confidencialidade, integridade e disponibilidade (CID).

2. Classificação das Informações

A classificação baseia-se no grau de sensibilidade e impacto em caso de incidente de segurança, conforme Política de Segurança da Informação.

Nível de Classificação	Descrição	Exemplos de Dados
Público	Informações que podem ser divulgadas sem restrições.	Informações institucionais, releases de imprensa, editais, publicações oficiais.
Interno	Informações de uso interno, cuja divulgação indevida teria baixo impacto negativo.	Manuais de procedimentos, fluxos internos, organogramas.
Confidencial	Informações sensíveis, cuja divulgação não autorizada causaria impacto financeiro, operacional, legal ou de imagem.	Dados pessoais (LGPD), contratos, relatórios financeiros, planos estratégicos.
Restrito / Secreto	Informações de alto sigilo, cuja exposição traria danos graves à organização ou à segurança pública.	Dados de investigações, credenciais administrativas, senhas-mestras, chaves criptográficas, informações de segurança.



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

3. Inventário e Classificação dos Sistemas Críticos

A tabela a seguir apresenta os sistemas institucionais e sua classificação quanto à criticidade e aos tipos de dados tratados.

ID do Sistema	Nome do Sistema / Aplicação	Descrição / Função	Responsável / Proprietário	Nível de Criticidade (Negócio)	Classificação dos Dados Processados
SIS001	Sistema ERP (Gestão Pública / Financeira/RH/Contratos e Compras)	Gestão de finanças, orçamento, patrimônio, RH, almoxarifado e compras.	Departamento Financeiro, Recursos Humanos, Compras e Contrato	Crítico (Alto)	Confidencial / Restrito
SIS002	Servidor de E-mail Corporativo	Comunicação institucional interna e externa.	Secretaria de TI	Alto	Interno / Confidencial
SIS003	Website (Portal) Institucional	Portal de informações públicas e serviços ao cidadão.	Secretarias de TI e Comunicação	Baixo (Não Crítico)	Público
SIS004	Sistema de Protocolo e Documentos (SEI)	Registro e tramitação de processos eletrônicos e documentos oficiais.	Secretaria Administrativa/ Gabinete	Crítico (Alto)	Confidencial/ Público
SIS005	Banco de Dados de Contribuintes (Tributário)	Cadastro de contribuintes, arrecadação e débitos municipais.	Departamento de Rendas / Tributação	Crítico (Alto)	Confidencial / Restrito
SIS006	Sistema de Saúde (e-SUS / PEC)	Prontuários eletrônicos e	Secretaria de Saúde (DHS)	Crítico (Alto)	Confidencial / Restrito



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

		informações de pacientes.			
SIS007	Sistema de Backup Corporativo	Armazena cópias de segurança dos dados institucionais	Secretaria de TI	Crítico (Alto)	Vários (herda a classificação dos sistemas backups)
SIS008	Sistema de Videomonitorame nto Urbano	Câmeras públicas, gravações e controle de acesso.	Secretaria de TI	Crítico (Alto)	Restrito
SIS009	Sistema de Acesso ao Servidor (Active Directy)	Libera acesso aos computadores na rede	Secretaria de TI	Crítico (Alto)	Restrito
SIS010	Sistema de Segurança e Monitoramento da Infraestrutura de rede	Regras de segurança e monitoramento de equipamentos e acesso a rede.	Secretaria de TI	Crítico (Alto)	Restrito
SIS011	Sistema PABX Virtual	Concentra todos os ramais da Administração	Secretaria de TI	Crítico (Alto)	Público/Interno
SIS012	Sistema de Protocolo Físico (Legado)	Gestão de documentos e processos físicos.	Secretaria Administrativa/Ga binete	Médio	Interno / Confidencial
SIS013	Sistema de Gestão Escolar	Dados de alunos, notas, frequência e servidores da educação.	Secretaria de Educação	Alto	Confidencial



**CIDADE DE
POMPEIA**

PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1
CEP 17.580-053 Fone (14)3405-1500

SIS014	Sistema de Gestão Social	Dados de Beneficiados em relação projetos, programas, políticas e ações Sociais	Fundo Social/ Secretaria de Desenvolvimento Econômico e Social	Alto	Interno/ Confidencial
--------	--------------------------	---	--	------	--------------------------

4. Diretrizes Adicionais

- **Revisão:** Este anexo deve ser revisado a cada 2 anos ou sempre que houver alterações significativas nos sistemas ou nos tipos de dados tratados.
- **Controles de Segurança:** Devem ser aplicados controles técnicos e administrativos compatíveis com o nível de criticidade e classificação dos dados, incluindo backups, controles de acesso, registros de log e criptografia.
- **Responsabilidades:** Cada sistema deve possuir um proprietário responsável pela segurança, atualização e conformidade de suas informações.
- **Auditoria e Monitoramento:** O Secretaria de TI deve manter monitoramento contínuo dos sistemas críticos e gerar relatórios de conformidade e disponibilidade.



**CIDADE DE
POMPEIA**

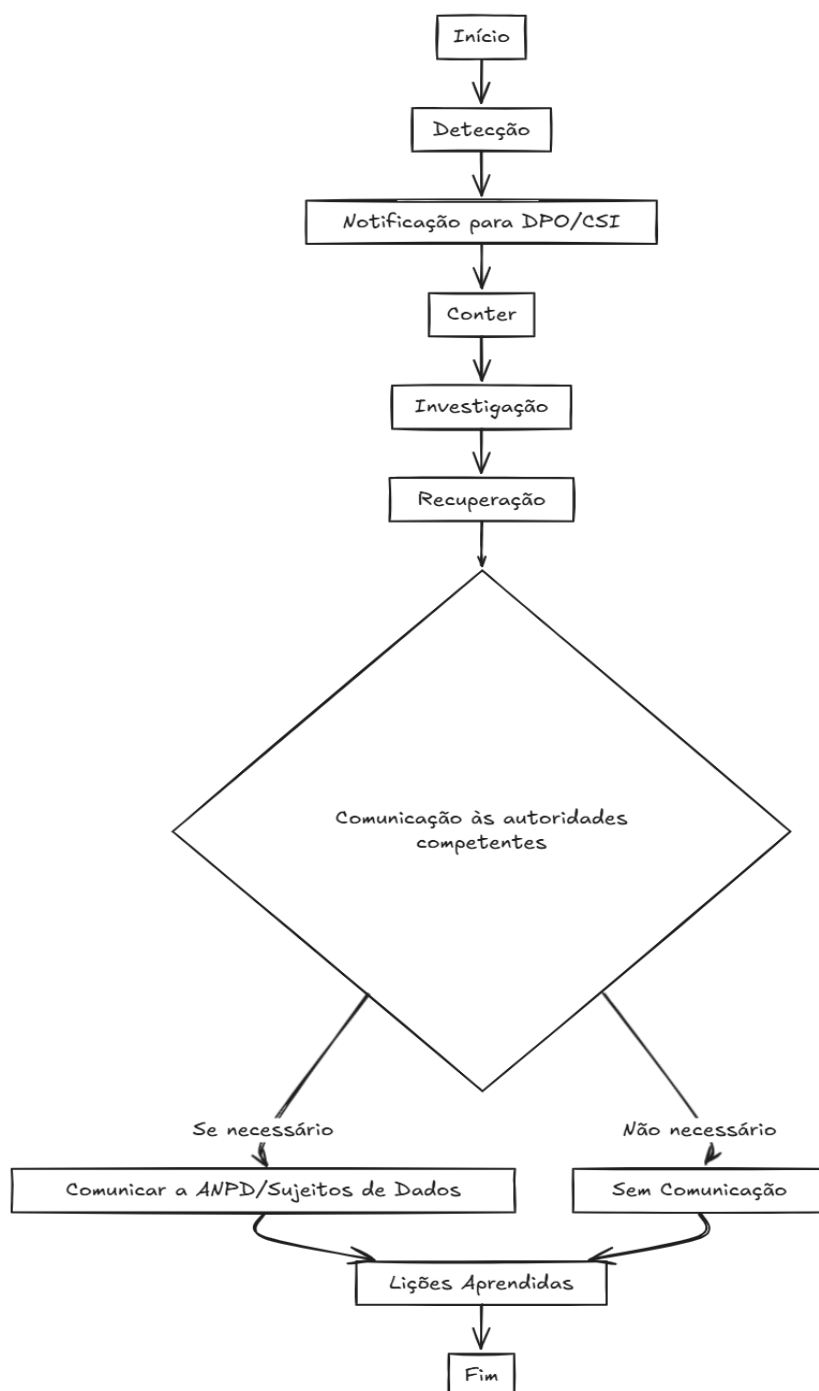
PREFEITURA MUNICIPAL DE POMPEIA

Rua Dr. José de Moura Resende, 572 – Caixa Postal nº 1

CEP 17.580-053 Fone (14)3405-1500

ANEXO E:

Fluxo de resposta de incidentes



/PrefPompeia



@prefpompeiaoficial



www.pompeia.sp.gov.br

CNPJ: 44.483.444/0001-09