Guia de Revisão: Segurança da Informação, LGPD e Ouvidoria Pública

Este guia foi elaborado para servir como material de apoio técnico e prático aos servidores públicos na implementação de diretrizes de conformidade, segurança e transparência. A governança de dados não deve ser vista como um obstáculo burocrático, mas como um processo contínuo de melhoria da gestão e proteção do cidadão.

1. Fundamentos da Segurança da Informação no Setor Público

A segurança da informação baseia-se em uma mudança de cultura organizacional. Medidas técnicas são fundamentais, mas o comportamento humano é o elo principal da proteção.

Ações de Baixo Custo e Alto Impacto:

- **Bloqueio de Tela:** Bloquear a estação de trabalho sempre que se ausentar, mesmo que por poucos minutos.
- **Política de Mesa e Tela Limpa:** Não deixar documentos com dados sensíveis expostos sobre a mesa ao final do expediente ou arquivos visíveis para passantes.
- **Gestão de Rascunhos:** Evitar o uso de impressões descartadas como rascunho sem verificar se há dados pessoais ou sigilosos no verso.
- **Conscientização Cultural (O Lembrete do Post-it):** Uma técnica eficaz e discreta é o uso de pequenos lembretes. Ao notar uma mesa desarrumada ou tela desbloqueada, deixe um bilhete amigável: *"A LGPD mandou lembranças :)"*. Isso cria cultura sem gerar constrangimento ou punição imediata.
- **O "Sonho de Consumo" (Pen Test):** O Teste de Intrusão (Penetration Test) é o nível mais alto de maturidade. Embora seja o objetivo ideal para testar vulnerabilidades, reconhecemos que seu alto custo e a necessidade de profissionais altamente especializados o tornam, por enquanto, um projeto de longo prazo para muitos municípios.

Componentes Essenciais de uma Política de Segurança da Informação (PSI)

Componente	Descrição e Ações Necessárias
Backup e Restore	Definir periodicidade e realizar testes de recuperação. Não basta salvar os dados; é preciso garantir que o *restore* funcione em caso de crise.

Antivírus e Proteção	Pilar fundamental da segurança. Deve estar sempre ativo, centralizado e atualizado em todas as estações de trabalho.
Criptografia	Implementar obrigatoriamente no transporte de dados (nuvem) e em arquivos sensíveis para garantir que, em caso de interceptação, a informação seja ilegível.
Atualização de Software	Realizar atualizações de sistemas e aplicativos assim que disponíveis. Elas corrigem brechas críticas que são as principais portas de entrada para ataques.
Gestão de Crises (Plano B)	Estabelecer um plano para ataques de *Ransomware*. Saber quem acionar e quais processos são críticos permite decidir de forma objetiva, sem o desespero do momento do ataque.

---

2. Implementação da LGPD na Gestão Pública

A adequação à Lei Geral de Proteção de Dados exige transparência e a organização dos fluxos de dados internos.

Portal da Privacidade

Todo órgão deve possuir um espaço centralizado em seu site oficial para a comunicação com os titulares de dados. **Itens Obrigatórios:**

- **Identificação do Encarregado (DPO):** Nome completo da pessoa física designada por portaria.
- **Substituto:** Identificação de quem assume as funções em faltas ou afastamentos.
- **Canal de Contato:** E-mail direto ou formulário específico para requisição de direitos.

Inventário de Dados (Metodologia 5W2H)

O mapeamento deve ser feito de forma incremental (ex: um processo por semana). O template abaixo é baseado no modelo validado pela **Secretaria de Governo Digital e aprovado pela ANPD**, garantindo conformidade com o padrão nacional.

Processo (What)	Dados Coletados (Who)	Onde Armazena (Where)	Como Coleta (How)	Finalidade (Why)	Base Legal - Art. 6º	Retenção (When)
Contratação de RH	Nome, CPF, Endereço, Currículo	Servidor Local / Nuvem	E-mail e Físico	Processo seletivo e admissão	Obrigação Legal / Execução de Contrato	Vigência do contrato + 5 anos

Gestão de Riscos e Terceiros

- **ISO 31.000:** Aplicada para classificar riscos de forma objetiva entre **Baixo, Médio e Alto**.
- **RIPD (Relatório de Impacto):** Documento obrigatório para processos que apresentem riscos elevados à liberdade civil e aos direitos fundamentais.
- **Due Diligence:** Ao contratar softwares ou serviços (terceiros), verifique:
    1. **Segregação de acessos:** O fornecedor garante que apenas pessoas autorizadas vejam os dados?
    2. **Políticas de Backup:** Como o terceiro protege os dados do órgão em caso de falha deles?
    3. **Criptografia em Nuvem:** Os dados trafegam e residem de forma criptografada?

---

3. Auditoria e Governança de Dados

A governança só é perene se for institucionalizada. O monitoramento contínuo evita que a conformidade se perca em trocas de gestão.

- **Padrões Internacionais:** A utilização das normas **ISO 27001** (Segurança) e **ISO 27701** (Privacidade) serve como o norte técnico para auditorias internas e externas.
- **Periodicidade:** Recomenda-se auditoria anual. Uma estratégia prática para evitar sobrecarga é auditar um departamento diferente a cada dois meses, criando um ciclo de monitoramento constante.
- **O Compromisso Público:** A publicação de manuais de conduta e a "Palavra do Presidente/Prefeito" no site oficial são vitais. No setor público, o compromisso que não é público "morre" quando o servidor responsável se aposenta ou quando a gestão política muda. A publicidade garante a longevidade da política de dados.
- **A Ouvidoria como Sensor:** O canal de ouvidoria funciona como um "sensor" para a auditoria, indicando quais setores apresentam mais falhas ou reclamações, direcionando o foco dos auditores.

---

4. Ouvidoria Pública: Canal de Controle e Cidadania

A Ouvidoria é o elo de mediação e o instrumento que garante a participação social e a melhoria contínua dos serviços.

Quadro Comparativo de Transparência

Tipo de Transparência	Descrição	Exemplos Práticos
Ativa	Divulgação espontânea e obrigatória pelo órgão.	Portal da Transparência, dados orçamentários, índices de vacinação (CME).
Passiva	Informação fornecida após provocação do cidadão.	Pedidos via e-SIC, manifestações de Ouvidoria.

Legislação e Ferramentas

- **Normas:** Constituição Federal, Lei nº 13.460/2017 (Direitos do Usuário) e Lei nº 12.527/2011 (LAI).
- **Fala.BR:** Plataforma da CGU que permite adesão municipal simplificada via termo de compromisso.

O Perfil do Ouvidor e Segurança Jurídica

O ouvidor deve atuar com **empatia, mediação e conciliação**. É um papel de "ponte", sem lado político.

- **Independência:** Recomenda-se o uso de servidores efetivos para evitar retaliações em denúncias contra a gestão de turno.
- **Estágio Probatório:** Conforme o **Acórdão 3450 do TCE**, é permitido que servidores em **estágio probatório** assumam funções gratificadas e cargos de confiança, como o de Ouvidor, garantindo segurança jurídica para a designação desses profissionais.

---

5. Tipos de Manifestações e Prazos

O cidadão possui cinco formas de interagir com o canal:

1. **Denúncia:** Relato de ilícitos ou irregularidades.

2. **Reclamação:** Insatisfação com o serviço prestado.
3. **Sugestão:** Ideia para melhoria do serviço.
4. **Elogio:** Reconhecimento (ferramenta de motivação interna).
5. **Solicitação de Providências:** Pedidos práticos (ex: roçada de terreno, troca de lâmpada).

Risco de Identificação do Denunciante: A proteção ao sigilo vai além de omitir o nome. Em municípios pequenos ou departamentos específicos, a identificação pode ocorrer por **estilometria (padrões de escrita)** ou **padrões de voz** em áudios de WhatsApp. O ouvidor deve ter o cuidado técnico de transcrever ou resumir o teor da denúncia para que a forma de expressão original do cidadão não revele sua identidade aos investigados.

---

6. Inovação: Inteligência Artificial na Transparência Pública

A tecnologia de IA está transformando o controle social e a fiscalização:

- **Detecção de Fraudes:** Ferramentas de IA já apresentam um índice de **89% de eficácia na identificação de indícios de desvio de verbas**.
- **Lançamento Próximo:** Uma dessas ferramentas poderosas de auditoria de dados públicos está prevista para ser **lançada publicamente até o meio deste ano**.
- **Acessibilidade:** O uso de bots integrados ao WhatsApp, que permitem o envio de áudios, democratiza o acesso para cidadãos com baixa escolaridade, garantindo que a ouvidoria seja um canal de inclusão.

---

7. Checklist de Adequação para o Servidor

Ao retornar ao seu órgão, verifique os seguintes itens de conformidade:

- [ ] **Senhas:** Atualizar senhas de sistemas a cada 90 ou 180 dias (mínimo de 8 caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos).
- [ ] **Cookies:** Verificar se o site oficial possui o "cardápio de cookies" para aceite do usuário.
- [ ] **Mapeamento:** Realizar o inventário de pelo menos **um processo de trabalho por semana** utilizando o 5W2H.
- [ ] **DPO:** Garantir que o nome e contato do Encarregado de Dados estejam visíveis no portal.
- [ ] **Mesa Limpa:** Implementar a rotina de organizar a estação de trabalho e bloquear a tela ao final do expediente.
- [ ] **Ouvidoria:** Verificar se as respostas às manifestações estão sendo dadas com clareza e dentro do prazo, evitando que o canal se torne um "repositório de pendências".