

## ANEXO D – CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÕES SIGILOSAS

### 1. Finalidade e Abrangência

1.1. O presente Anexo estabelece os critérios, procedimentos, controles e níveis de classificação das Informações Sigilosas e Informações Sensíveis tratadas no âmbito da Oportunidade de Negócio SMARTSAMP, Confidencialidade e Informações Sigilosas deste Contrato.

1.2. Este Anexo aplica-se a toda e qualquer informação:

- I – técnica, operacional, institucional, estratégica ou comercial;
- II – decorrente de atividades da ON;
- III – compartilhada entre as PARCEIRAS;
- IV – produzida por qualquer PARCEIRA na execução da ON;
- V – oriunda de órgãos da Administração Pública Municipal.

1.3. A classificação aqui prevista não se aplica a Dados Pessoais, cujo tratamento é regido exclusivamente pela Cláusula 8 e pelo Anexo A – Tratamento de Dados Pessoais.

### 2. Definições Complementares

2.1. Informação: qualquer dado, artefato, documento, registro, arquivo, código, rotina, relatório, metadado, log, estrutura lógica, modelo ou especificação relacionado à ON.

2.2. Autoridade Classificadora: órgão ou profissional designado pela governança da ON para classificar, revisar e reclassificar informações.

2.3. Sistema Crítico: componente tecnológico cuja indisponibilidade, violação ou modificação possa comprometer a continuidade operacional da ON ou serviços municipais.

2.4. Incidente de Segurança de Informação: qualquer evento que resulte ou possa resultar em acesso, uso, alteração, destruição, divulgação ou perda de informação classificada.

2.5. Cadeia de Custódia da Informação: conjunto de registros que permitem rastrear quem acessou, alterou, transportou, analisou ou descarregou determinada informação classificada.

### 3. Níveis de Classificação da Informação



As Informações tratadas no âmbito da ON serão classificadas em um dos seguintes níveis:

### 3.1. Nível 1 – PÚBLICA

Informações destinadas à divulgação ampla, cujo acesso não acarreta risco à segurança municipal, à operação da ON ou aos interesses das PARCEIRAS.

Exemplos:

informações publicadas em portais oficiais;

manuals públicos;

material promocional autorizado.

### 3.2. Nível 2 – RESTRITA

Informações cujo acesso indevido pode gerar risco operacional moderado, prejuízo institucional ou comprometer processos internos.

Exemplos:

atas de reuniões da governança;

relatórios de avanço da ON;

especificações de módulos não sensíveis;

documentação de APIs não críticas.

Regras principais:

acesso mediante autorização;

proibida cópia para dispositivos pessoais;

armazenamento em ambientes controlados.

### 3.3. Nível 3 – CONFIDENCIAL

Informações cujo acesso indevido pode causar prejuízo relevante, afetar negociações,



comprometer a segurança tecnológica da solução ou gerar impacto jurídico/institucional.

Exemplos:

diagramas internos da arquitetura;

documentação de integrações com sistemas legados;

regras de negócio sensíveis;

dados territoriais que possam revelar vulnerabilidades de serviços públicos.

Regras principais:

acesso apenas para equipes designadas;

obrigatoriedade de criptografia em repouso e trânsito;

registro em cadeia de custódia.

#### 3.4. Nível 4 – ALTAMENTE CONFIDENCIAL / CRÍTICA

Informações estratégicas cujo acesso indevido pode causar:

risco à segurança urbana;

paralisação de serviços essenciais;

violação de sistemas críticos;

impactos severos à Administração Pública e às PARCEIRAS.

Exemplos:

chaves criptográficas mestras;

diagramas de segurança;

credenciais privilegiadas;

mapas de infraestrutura crítica;

lógica interna de módulos sensíveis do SMARTSAMPA.

Regras principais:

acesso restrito e nominal;

dupla autenticação e criptografia forte;

vedação de transporte fora do ambiente institucional;

políticas de segregação rígida;

monitoramento contínuo.

#### 4. Procedimentos de Classificação

4.1. Toda informação criada, recebida ou modificada no âmbito da ON deverá ser avaliada quanto ao nível de classificação, de acordo com:

- I – sensibilidade;
- II – criticidade tecnológica;
- III – impacto à política pública;
- IV – risco jurídico ou reputacional;
- V – potencial de exploração externa.

4.2. A classificação será feita pela Autoridade Classificadora, podendo ser revista pela governança da ON.

4.3. É obrigatória a aplicação de identificadores visuais, digitais e metadados que indiquem o nível de classificação da informação.

#### 5. Acesso a Informações Classificadas

5.1. O acesso obedecerá aos critérios de:

- I – “need to know”;
- II – aprovação formal da governança;
- III – trilhas de auditoria;
- IV – mecanismos de autenticação forte.

5.2. Todos os acessos deverão ser registrados, permitindo rastreabilidade completa.

5.3. O compartilhamento externo exigirá:

- a) justificativa formal;
- b) registro em cadeia de custódia;
- c) termo de confidencialidade;
- d) criptografia ponta a ponta.

## 6. Armazenamento e Transporte

### 6.1. Informações classificadas devem ser armazenadas exclusivamente em:

- I – ambientes institucionais aprovados;
- II – infraestruturas gerenciadas conforme a Cláusula 8;
- III – sistemas controlados pela governança da ON.

### 6.2. Proibições expressas:

uso de dispositivos pessoais;

envio por e-mail não institucional;

armazenamento em serviços de nuvem não autorizados;

transporte em mídias físicas sem autorização.

### 6.3. O transporte físico ou digital de informação classificada deve sempre:

ser criptografado;

ter registro de origem e destino;

ser realizado por pessoa autorizada.

## 7. Retenção, Conservação e Descarte

### 7.1. Os prazos de retenção serão definidos:

- I – pelo PNO;
- II – por exigência legal;
- III – por deliberação da governança;
- IV – por criticidade do módulo da solução.

### 7.2. O descarte seguro deve incluir:

sobrescrita;

destruição física controlada;

logs de eliminação;

relatório de auditoria.

## 8. Incidentes de Segurança Relacionados a Informações Classificadas

8.1. Qualquer incidente envolvendo informação classificada deve ser comunicado:

- I – imediatamente;
- II – com nível detalhado de impacto;
- III – com descrição da informação afetada;
- IV – com plano de mitigação.

8.2. Incidentes envolvendo Informação Altamente Confidencial são considerados críticos e exigem:

- a) acionamento emergencial da governança;
- b) comunicação à alta administração (quando aplicável);
- c) relatório circunstanciado;
- d) revisão de controles.

## 9. Auditoria e Monitoramento

9.1. A governança da ON poderá realizar auditorias:

- I – periódicas;
- II – extraordinárias;
- III – temáticas (arquitetura, credenciais, acessos, logs).

9.2. As PARCEIRAS devem possibilitar o acesso a:

- a) registros de acesso;
- b) cadeia de custódia;
- c) relatórios de incidentes;
- d) evidências de conformidade.

## 10. Responsabilidades Específicas das PARCEIRAS

10.1. PRODAM deverá fornecer diretrizes, requisitos e padrões de segurança aplicáveis à ON.

## 10.2. A PARCEIRA deverá:

- I – adotar medidas compatíveis com a criticidade da informação;
- II – segregar ambientes;
- III – manter controles de identidade e acesso;
- IV – atender às normas internas da PRODAM.

## 11. Atualização e Evolução do Anexo

### 11.1. Este Anexo poderá ser atualizado:

- I – por deliberação da governança da ON;
- II – mediante alteração tecnológica significativa;
- III – por mudança no ciclo de vida do SMARTSAMPÁ;
- IV – por demanda de órgãos de controle ou normativos internos.

11.2. Versões atualizadas substituem automaticamente as anteriores, desde que registradas no processo administrativo da ON.

1.1. O presente Anexo detalha as obrigações operacionais, procedimentos, controles e instrumentos necessários para o adequado tratamento de Dados Pessoais e Dados Pessoais Sensíveis no âmbito da Oportunidade de Negócio SMARTSAMPÁ, em complemento direto à Cláusula 8 – Proteção de Dados e Segurança da Informação deste Contrato.

1.2. Este Anexo deve ser interpretado como extensão técnica da Cláusula 8, não criando regimes paralelos, mas especificando como tais obrigações serão executadas, documentadas e auditadas.

## 2. Papéis e Responsabilidades:

2.1. As PARCEIRAS reconhecem que os papéis de Controlador, Operador e Suboperador serão definidos caso a caso, conforme já previsto na Cláusula 8, especialmente em seu item 8.3, respeitando:

- I – a finalidade do tratamento;
- II – o ente responsável pela política pública ou serviço;
- III – o instrumento jurídico firmado com o Cliente;
- IV – os fluxos descritos no PNO.

2.2. Para fins operacionais, fica estabelecido que:

- a) quando o tratamento decorrer de política pública municipal, o órgão público é, em regra, o Controlador;
- b) a PRODAM atuará preferencialmente como Operadora;
- c) a PARCEIRA atuará como Operadora ou Suboperadora, conforme o fluxo documental aprovado pela governança.

2.3. A definição final dos papéis será sempre registrada:

- I – no PNO;
- II – no contrato específico com Clientes (quando houver);
- III – no processo administrativo da ON.

### 3. Categorias de Dados e Finalidades:

3.1. As categorias de dados tratadas no âmbito da SMARTSAMPa serão aquelas estritamente necessárias para:

- I – execução de políticas públicas relacionadas ao território, mobilidade, eventos urbanos, atendimento digital e demais serviços integrados;
- II – operação do ecossistema digital SMARTSAMPa;
- III – funcionalidades previstas no PNO ou instrumento correlato.

3.2. Cada fluxo relevante de dados deverá conter:

- a) descrição da categoria de dados pessoais tratada;
- b) finalidade específica;
- c) base legal aplicável (item 8.4 da Cláusula 8);
- d) indicação do operador responsável;
- e) prazo de retenção;
- f) critérios de eliminação ou anonimização.

3.3. O registro desses fluxos ocorrerá nos mapas de tratamento da ON e ficará disponível para consulta pela governança.

### 4. Bases Legais:

4.1. As bases legais previstas no item 8.4 da Cláusula 8 serão aplicadas conforme cada operação, devendo constar nos documentos:

- I – PNO (versão vigente);
- II – Plano de Governança;
- III – instrumentos firmados com Clientes.

4.2. A mudança de base legal motivada por alteração de finalidade deverá ser previamente submetida à governança da ON.

#### 5. Direitos dos Titulares (Complemento ao item 8.5)

5.1. Em cumprimento ao item 8.5 da Cláusula 8, cada PARCEIRA deverá manter mecanismos para atender, de forma rastreável, solicitações de titulares relativas a confirmação de tratamento, acesso, correção, anonimização, revogação de consentimento (quando aplicável), informação sobre compartilhamento, portabilidade (quando cabível).

5.2. O ponto de contato principal com o titular será o órgão público Controlador. PRODAM e PARCEIRA prestarão suporte operacional mediante procedimentos definidos no PNO.

#### 6. Compartilhamento de Dados:

6.1. Como complemento ao item 8.6, todo compartilhamento de dados pessoais com terceiros deverá:

- I – ter base legal válida;
- II – ser documentado no processo administrativo;
- III – ser amparado por cláusulas contratuais equivalentes às deste Anexo e da Cláusula 8;
- IV – estar previsto no PNO ou instrumento com o Cliente.

6.2. Operações que envolvam subcontratados exigem:

- a) assinatura de Termo de Confidencialidade;
- b) aceite das políticas de segurança da PRODAM;
- c) aceite deste Anexo e da Cláusula 8.

#### 7. Segurança da Informação:

7.1. Os controles previstos no item 8.7 serão detalhados operacionalmente:

- I – no Plano de Governança da ON;
- II – nos controles de acesso à solução SMARTSAMPA;
- III – nos procedimentos de criptografia, autenticação, segregação e rastreabilidade;
- IV – nos requisitos de proteção de dados territoriais e urbanos sensíveis.

7.2. A PARCEIRA compromete-se a implementar controles compatíveis com:

- a) normas internas de segurança da PRODAM;
- b) políticas de classificação de informação;
- c) requisitos específicos do módulo da solução.

## 8. Incidentes de Segurança:

8.1. Incidentes descritos no item 8.8 deverão ser comunicados por escrito à outra PARCEIRA:

- I – imediatamente, em até 24 horas após a ciência;
- II – com informações suficientes para avaliação preliminar;
- III – com atualização contínua até o encerramento do incidente.

8.2. A governança da ON será responsável por:

- a) qualificar o impacto;
- b) indicar medidas de mitigação;
- c) decidir sobre comunicações obrigatórias à ANPD e titulares;
- d) registrar todo o fluxo no processo administrativo.

## 9. Retenção e Eliminação de Dados:

9.1. Os prazos de retenção definidos no item 8.9 serão detalhados conforme:

- I – contrato com Cliente;
- II – legislação aplicável à política pública correlata;
- III – requisitos do módulo da solução.

9.2. A eliminação ou anonimização deve:

- a) ocorrer de forma segura;
- b) ser documentada;
- c) ser aprovada pela governança.

## 10. Transferência Internacional de Dados:

10.1. Qualquer operação tratada no item 8.10 exigirá:

- I – avaliação de risco;
- II – cláusulas contratuais específicas;
- III – garantia de nível adequado de proteção;
- IV – registro formal no processo administrativo da ON.



## 11. Encarregado (DPO) e Comunicação:

11.1. PRODAM e PARCEIRA deverão manter seus Encarregados atualizados no processo administrativo da ON.

11.2. As comunicações relacionadas a direitos de titulares, incidentes e avaliações de risco ocorrerão:

- I – preferencialmente pelo SEI;
- II – por e-mail institucional, quando necessário;
- III – com rastreabilidade garantida.

## 12. Atualizações:

12.1. As atualizações previstas no item 8.12 serão incorporadas mediante:

- I – deliberação da governança;
- II – termo aditivo, quando necessário;
- III – registro no processo da ON;
- IV – comunicação às áreas técnicas envolvidas.