

6. POLÍTICA DE SEGURANÇA DE DADOS

1. OBJETIVO

Esta política estabelece as diretrizes e responsabilidades para a **proteção, integridade, confidencialidade e disponibilidade dos dados pessoais e sensíveis** tratados pela empresa Simone Yagui, garantindo a conformidade com a **Lei Geral de Proteção de Dados Pessoais (LGPD)** e promovendo um ambiente seguro para a gestão das informações dos clientes.

2. ABRANGÊNCIA

Esta política se aplica a **todos os dados coletados, armazenados, acessados ou processados** no contexto das atividades da empresa, abrangendo:

- Dados cadastrais (nome, telefone, e-mail, endereço);
 - Dados sensíveis (informações espirituais, terapêuticas, emocionais, energéticas);
 - Registros de atendimento, agendamento e compras;
 - Informações comerciais e operacionais;
 - Ambientes digitais (sistema de gestão, loja virtual, WhatsApp, redes sociais) e físicos (documentos impressos);
 - Dispositivos utilizados pela titular e por colaboradores.
-

3. PRINCÍPIOS NORTEADORES

A segurança de dados será garantida com base nos seguintes princípios:

- **Confidencialidade:** apenas pessoas autorizadas podem acessar os dados;
 - **Integridade:** os dados devem ser mantidos corretos, íntegros e atualizados;
 - **Disponibilidade:** as informações devem estar acessíveis somente quando necessário;
 - **Minimização:** coleta e uso restritos aos dados essenciais;
 - **Prevenção:** adoção de práticas que evitem incidentes de segurança.
-

4. RESPONSABILIDADES

4.1. Da Titular / Encarregada de Dados (Simone Yagui):

- Garantir a implementação e o cumprimento desta política;
- Controlar o acesso aos sistemas e ferramentas utilizadas;
- Supervisionar os backups, atualizações e armazenamento seguro das informações;
- Treinar colaboradores sobre as práticas de segurança e privacidade;
- Responder por incidentes de segurança e notificar os titulares, quando necessário;
- Monitorar riscos e revisar esta política periodicamente.

4.2. Dos Colaboradores (funcionários ou prestadores de serviço):

- **Manter sigilo absoluto** sobre todos os dados e informações acessadas;
- Utilizar os dados pessoais dos clientes **somente quando autorizado e para finalidades específicas** da empresa;
- Manter **senhas protegidas** e nunca compartilhá-las com terceiros;
- Utilizar dispositivos (celulares, notebooks) com **trava de tela, antivírus e atualizações em dia**;
- **Evitar o uso de redes públicas ou não seguras** para acessar informações da empresa;
- **Não armazenar dados sensíveis fora dos sistemas autorizados** (ex: salvar fichas em arquivos pessoais ou nuvem particular);
- Reportar imediatamente à titular qualquer suspeita de vazamento, falha de segurança ou uso indevido de informações;
- Seguir a Política de Impressão e as orientações sobre descarte de documentos físicos;
- **Assinar termo de confidencialidade** e cumprir as demais políticas internas relacionadas à LGPD.

5. DIRETRIZES DE SEGURANÇA

5.1. Controle de Acesso

- O acesso aos dados será concedido apenas conforme a necessidade da função.
- A titular centraliza o controle e autorização de acesso aos sistemas sensíveis.

5.2. Segurança dos Dispositivos

- Todos os dispositivos utilizados devem estar protegidos por senha, bloqueio automático e antivírus;
- É proibido o uso de dispositivos de terceiros não autorizados para atividades da empresa.

5.3. Ambientes de Armazenamento

- Dados digitais devem ser armazenados em sistemas com login seguro e backup em nuvem confiável;
- Armazenamento local em pastas deve ser temporário, com criptografia ou proteção de acesso.

5.4. Transmissão de Dados

- O envio de informações sensíveis por WhatsApp, e-mail ou redes sociais só pode ser feito com autorização da titular e consentimento do cliente.

5.5. Descarte de Dados

- Documentos físicos devem ser descartados com trituração ou inutilização;
- Arquivos digitais devem ser apagados de forma segura após a perda de finalidade.

6. INCIDENTES DE SEGURANÇA

- Qualquer vazamento, perda, acesso indevido ou suspeita de incidente deve ser reportada imediatamente à titular;
- Será realizada análise do impacto e das providências necessárias, incluindo notificação aos titulares e registros do incidente.

7. MONITORAMENTO E REVISÃO

- A titular revisará esta política **anualmente** ou sempre que houver mudança nos processos ou tecnologia utilizada;
- A empresa manterá registro de atualizações, treinamentos e controles aplicados.

8. DISPOSIÇÕES FINAIS

O descumprimento desta política por parte de colaboradores poderá acarretar **advertência, desligamento, responsabilização cível e/ou penal**, conforme a gravidade da infração e a legislação vigente.

A Política de Segurança de Dados é parte integrante do compromisso da empresa Simone Yagui com a ética, o respeito aos seus clientes e a conformidade legal. Todos os envolvidos devem agir com responsabilidade, zelo e sigilo no tratamento de dados pessoais.

E, por estarem de pleno acordo, firmam o presente instrumento .

Campina Grande – PB, ____ de _____ de 2025.

Simone Yagui

Titular e Encarregada de Dados

[Nome do(a) Colaborador(a)]

CPF: [preencher]