# PROGRAMA DE CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

## PORTAL CABOCO

O Programa de Conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) do Portal Caboco será estruturado como um instrumento institucional, jurídico, administrativo e operacional, destinado a estabelecer regras, responsabilidades, procedimentos e controles para garantir a proteção dos dados pessoais tratados pela organização.

O documento considera os dados empresariais informados, o Alvará de Localização e Funcionamento da Prefeitura de Manaus e a indicação de Nilson Barroso Belém como responsável pela segurança dos dados pessoais coletados e armazenados.

### 1. Identificação da organização

Com base no Alvará de Localização e Funcionamento apresentado (página 1), foram identificadas as seguintes informações:

ALVARA.pdf

| Identificação | Informação |
|---|---|
| Razão social | Aline Luana Vieira Belém |
| Nome fantasia | Agência Assessoria Caboco |
| CNPJ | 35.417.162/0001-04 |
| Inscrição municipal | 44909701 |
| Município | Manaus – AM |

| | |
|---|---|
| Atividade autorizada | Portais, provedores de conteúdo e outros serviços de informação na internet |
| CNAE | 6319-4/00.01 |
| Endereço cadastral | Rua Prof. Heloísa Monteiro, nº 75, Flores, Manaus/AM |
| Portal institucional | https://portalcaboco.com.br/ |
| Responsável pela segurança dos dados | Nilson Barroso Belém |

Observação: A indicação de Nilson Barroso Belém como responsável pela segurança da informação não significa, automaticamente, que ele seja o encarregado pelo tratamento de dados pessoais (DPO) formalmente designado nos termos da LGPD. Essa atribuição deverá ser expressamente definida pela organização.

**2. Apresentação e finalidade do programa**

O Portal Caboco, mantido pela empresa Aline Luana Vieira Belém, nome fantasia Agência Assessoria Caboco, reconhece a importância da privacidade e da proteção dos dados pessoais como elementos fundamentais para o exercício de suas atividades na internet.

Considerando sua atividade econômica autorizada, relacionada à operação de portais, provedores de conteúdo e serviços de informação na internet, a organização estabelece este Programa de Conformidade com a LGPD para orientar o tratamento adequado dos dados pessoais de:

- Usuários e visitantes do Portal Caboco;
- Leitores e consumidores de conteúdo;
- Pessoas que estabeleçam contato por meio dos canais digitais;
- Colaboradores, prestadores de serviços e parceiros;
- Representantes de empresas e instituições que mantenham relacionamento com o portal;
- Outras pessoas naturais cujos dados sejam tratados no desenvolvimento das atividades da organização.

O programa tem como objetivos:

1. Assegurar o cumprimento da Lei nº 13.709/2018 (LGPD).
2. Identificar e controlar os dados pessoais coletados, utilizados, armazenados e compartilhados.
3. Garantir transparência aos titulares sobre o tratamento de seus dados.
4. Estabelecer procedimentos de segurança da informação.
5. Prevenir acessos não autorizados, vazamentos, perdas e utilização indevida de informações.
6. Definir responsabilidades dos agentes envolvidos no tratamento de dados.
7. Estabelecer procedimentos para atendimento aos direitos dos titulares.
8. Criar mecanismos de monitoramento, avaliação e melhoria contínua.

**3. Fundamentação legal**

O programa observa especialmente:

- Constituição Federal de 1988, especialmente o direito à intimidade, à vida privada e à proteção de dados pessoais.
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.
- Lei nº 12.965/2014 – Marco Civil da Internet.
- Decreto nº 8.771/2016, que regulamenta o Marco Civil da Internet.
- Regulamentações e orientações da Autoridade Nacional de Proteção de Dados (ANPD).
- Regulamento de Comunicação de Incidente de Segurança da ANPD.
- Demais normas aplicáveis à atividade de tratamento de dados pessoais.

**4. Governança e responsabilidades**

A governança de proteção de dados será organizada de modo a estabelecer responsabilidades institucionais e operacionais.

4.1. Controladora dos dados pessoais

A pessoa jurídica identificada neste programa será responsável pelas decisões referentes ao tratamento dos dados pessoais realizados no âmbito das atividades do Portal Caboco, na condição de controladora, quando efetivamente determinar as finalidades e os meios do tratamento.

4.2. Responsável pela segurança dos dados

Responsável indicado

Nilson Barroso Belém

Compete ao responsável pela segurança dos dados coletados e armazenados:

- Coordenar a implementação das medidas de segurança da informação.
- Supervisionar os mecanismos de proteção dos bancos de dados.
- Controlar e acompanhar os níveis de acesso aos sistemas.
- Orientar colaboradores e prestadores de serviços sobre boas práticas de segurança.
- Acompanhar a realização de cópias de segurança (backups).
- Monitorar vulnerabilidades e riscos tecnológicos.
- Apoiar a identificação, contenção e tratamento de incidentes de segurança.
- Manter registros das ocorrências e das providências adotadas.
- Recomendar melhorias nos procedimentos técnicos e administrativos.
- Apoiar a realização de avaliações periódicas de riscos.

4.3. Encarregado pelo tratamento de dados pessoais

A organização deverá formalizar a designação de um encarregado pelo tratamento de dados pessoais, observando o artigo 41 da LGPD e a regulamentação aplicável da ANPD.

O encarregado será o canal de comunicação entre a organização, os titulares dos dados e a ANPD.

Caso Nilson Barroso Belém também venha a exercer essa função, deverá existir designação formal, definição de atribuições e divulgação dos seus canais de contato.

4.4. Colaboradores e prestadores de serviços

Todos os colaboradores e prestadores que tenham acesso a dados pessoais deverão:

- Utilizar as informações exclusivamente para finalidades autorizadas.
- Manter sigilo sobre as informações acessadas.
- Não compartilhar credenciais de acesso.
- Respeitar as políticas internas de segurança.
- Comunicar imediatamente situações suspeitas ou incidentes.
- Participar das orientações e capacitações sobre proteção de dados.

**5. Mapeamento das operações de tratamento de dados**

O Portal Caboco deverá manter um inventário atualizado das operações de tratamento de dados pessoais.

Esse inventário deverá contemplar, no mínimo, as seguintes categorias:

| Operação | Dados potencialmente envolvidos |
|---|---|

| | |
|---|---|
| Navegação no portal | Endereço IP, registros de acesso e informações técnicas |
| Formulários de contato | Nome, e-mail, telefone e mensagem |
| Comunicação com leitores | Dados de identificação e contato |
| Cookies e tecnologias similares | Identificadores, preferências e dados de navegação |
| Gestão administrativa | Dados de colaboradores e prestadores |
| Relacionamento comercial | Dados de representantes e contatos empresariais |
| Segurança da plataforma | Logs, registros de autenticação e eventos de segurança |

Importante: A tabela representa operações potenciais que devem ser verificadas. Não constitui confirmação de que todos esses dados sejam efetivamente coletados pelo Portal Caboco. O levantamento técnico deverá confirmar cada operação, sua finalidade, seus sistemas e seus fornecedores.

Para cada operação identificada, deverá ser documentado:

- Categoria dos dados pessoais;
- Finalidade do tratamento;
- Base legal correspondente;
- Origem dos dados;
- Sistemas e ambientes de armazenamento;
- Pessoas ou organizações com acesso;
- Compartilhamentos realizados;
- Prazo de conservação;
- Procedimento de eliminação;
- Medidas de segurança aplicadas.

**6. Princípios para o tratamento dos dados pessoais**

O Portal Caboco adotará os princípios previstos no artigo 6º da LGPD:

1. Finalidade: utilização dos dados para propósitos legítimos, específicos e informados.
2. Adequação: compatibilidade do tratamento com as finalidades comunicadas.
3. Necessidade: coleta apenas dos dados indispensáveis.
4. Livre acesso: disponibilização de informações sobre o tratamento.
5. Qualidade dos dados: manutenção de informações corretas e atualizadas.
6. Transparência: comunicação clara sobre as práticas de tratamento.
7. Segurança: utilização de medidas técnicas e administrativas de proteção.
8. Prevenção: adoção de medidas para evitar danos.
9. Não discriminação: proibição de tratamento discriminatório ilícito ou abusivo.
10. Responsabilização e prestação de contas: demonstração da efetividade das medidas adotadas.

**7. Bases legais para o tratamento**

O Portal Caboco deverá identificar e documentar a hipótese legal que autoriza cada operação de tratamento, conforme os artigos 7º e 11 da LGPD, quando aplicáveis.

As bases legais potencialmente pertinentes incluem:

- Consentimento do titular;
- Cumprimento de obrigação legal ou regulatória;
- Execução de contrato ou procedimentos preliminares;
- Exercício regular de direitos;
- Legítimo interesse, mediante avaliação de necessidade, proporcionalidade e salvaguardas;
- Proteção da vida ou da incolumidade física, nas situações legalmente previstas.

O consentimento não deverá ser utilizado como autorização genérica para qualquer tratamento. Cada finalidade deverá possuir uma justificativa jurídica adequada.

Dados pessoais sensíveis, quando eventualmente tratados, exigirão observância das hipóteses específicas do artigo 11 da LGPD.

**8. Política de privacidade e transparência**

O Portal Caboco deverá disponibilizar uma Política de Privacidade em local de fácil acesso no site.

Essa política deverá informar:

- Quem é o controlador dos dados;
- Quais dados pessoais são coletados;
- Por que os dados são tratados;
- Quais são as bases legais utilizadas;
- Como ocorre o armazenamento;
- Com quem os dados podem ser compartilhados;
- Quais são os prazos de conservação;

- Como funcionam os cookies;
- Quais são os direitos dos titulares;
- Como solicitar acesso, correção ou eliminação dos dados;
- Como entrar em contato com o encarregado;
- Como a organização trata incidentes de segurança.

A política deverá corresponder às práticas efetivamente adotadas, evitando declarações genéricas ou promessas de segurança que não possam ser demonstradas.

**9. Política de cookies**

O Portal Caboco deverá realizar levantamento das tecnologias utilizadas para armazenamento ou acesso a informações nos dispositivos dos visitantes.

Os cookies deverão ser classificados, conforme sua finalidade, em:

- Estritamente necessários;
- Funcionais;
- Analíticos ou estatísticos;
- Publicitários ou de marketing.

Quando aplicável, deverá ser disponibilizado mecanismo de gerenciamento de preferências, permitindo ao visitante aceitar ou rejeitar cookies não necessários, sem prejuízo do funcionamento dos recursos essenciais.

A organização deverá documentar os fornecedores envolvidos, as informações coletadas e eventuais transferências internacionais.

**10. Segurança da informação e proteção dos dados**

A segurança dos dados pessoais será coordenada por Nilson Barroso Belém, mediante implementação e acompanhamento de controles técnicos e administrativos compatíveis com os riscos das operações.

As medidas mínimas previstas são:

10.1. Controle de acesso

- Contas individuais para usuários autorizados.
- Senhas fortes e exclusivas.
- Autenticação multifator sempre que disponível.
- Restrição de privilégios conforme a necessidade de cada função.
- Revisão periódica dos usuários autorizados.

10.2. Proteção tecnológica

- Atualização periódica do sistema de gerenciamento do portal.
- Atualização de plugins, temas e componentes.
- Utilização de conexões protegidas por HTTPS.

- Proteção contra códigos maliciosos e acessos indevidos.
- Monitoramento de vulnerabilidades.
- Utilização de firewall e mecanismos de proteção compatíveis com a infraestrutura.

10.3. Armazenamento e backups

- Armazenamento em ambientes controlados.
- Cópias de segurança periódicas.
- Proteção dos arquivos de backup.
- Testes de restauração.
- Restrição de acesso às cópias de segurança.

10.4. Segurança administrativa

- Termos de confidencialidade.
- Orientação dos colaboradores.
- Procedimentos para compartilhamento de informações.
- Controle de equipamentos e dispositivos.
- Descarte seguro de documentos e arquivos digitais.

10.5. Monitoramento

- Registro de eventos relevantes.
- Identificação de atividades suspeitas.
- Acompanhamento de tentativas de acesso indevido.
- Registro de ações corretivas e preventivas.

**11. Compartilhamento de dados pessoais**

O compartilhamento de dados pessoais deverá ocorrer exclusivamente quando houver finalidade legítima e fundamento jurídico adequado.

Poderão existir relações com:

- Empresas de hospedagem de sites;
- Fornecedores de infraestrutura tecnológica;
- Prestadores de serviços de manutenção;
- Ferramentas de análise de tráfego;
- Serviços de comunicação;
- Plataformas de publicidade;
- Outros operadores envolvidos nas atividades do portal.

Os fornecedores que atuarem como operadores deverão receber instruções documentadas e assumir obrigações contratuais de confidencialidade e segurança.

A organização deverá verificar a localização dos servidores, os subprocessadores utilizados e a existência de transferências internacionais de dados, observando os artigos 33 a 36 da LGPD e a regulamentação da ANPD.

**12. Direitos dos titulares dos dados pessoais**

O Portal Caboco deverá disponibilizar mecanismos para que os titulares possam exercer os direitos previstos no artigo 18 da LGPD.

Entre eles:

- Confirmação da existência de tratamento;
- Acesso aos dados pessoais;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários ou tratados em desconformidade;
- Portabilidade, quando regulamentada e aplicável;
- Eliminação dos dados tratados com consentimento, ressalvadas as hipóteses legais de conservação;
- Informação sobre compartilhamento;
- Informação sobre a possibilidade de não fornecer consentimento;
- Revogação do consentimento;
- Revisão de decisões tomadas unicamente com base em tratamento automatizado, nos termos da legislação.

As solicitações deverão ser recebidas, registradas, analisadas e respondidas dentro dos prazos legais aplicáveis.

**13. Gestão de incidentes de segurança**

A organização estabelecerá um procedimento formal para identificação, comunicação, contenção, investigação e resolução de incidentes envolvendo dados pessoais.

São exemplos de incidentes:

- Acesso não autorizado;
- Vazamento de informações;
- Roubo ou perda de equipamentos;
- Exclusão acidental de dados;
- Ataques cibernéticos;
- Comprometimento de credenciais;
- Alteração indevida de informações;
- Indisponibilidade de sistemas com impacto sobre dados pessoais.

Fluxo de resposta:

1. Identificação e registro da ocorrência.
2. Comunicação imediata ao responsável pela segurança, Nilson Barroso Belém.
3. Avaliação da natureza e extensão do incidente.
4. Adoção de medidas de contenção.
5. Preservação de evidências.
6. Avaliação dos riscos e possíveis danos aos titulares.
7. Comunicação à direção da organização.

8. Avaliação da necessidade de comunicação à ANPD e aos titulares.
9. Implementação de medidas corretivas.
10. Registro do incidente e elaboração de relatório conclusivo.

A comunicação à ANPD e aos titulares deverá observar a regulamentação vigente, inclusive o prazo de três dias úteis previsto na Resolução CD/ANPD nº 15/2024, quando o incidente atender aos critérios de comunicação.

**14. Retenção e descarte de dados**

Os dados pessoais não deverão ser mantidos indefinidamente.

A organização estabelecerá uma tabela de temporalidade documental e digital, considerando:

- Finalidade da coleta;
- Necessidade operacional;
- Obrigações legais e regulatórias;
- Exercício regular de direitos;
- Prazos prescricionais aplicáveis;
- Necessidade de manutenção de registros de acesso.

Após o encerramento da finalidade, os dados deverão ser eliminados ou anonimizados, ressalvadas as hipóteses legais de conservação previstas no artigo 16 da LGPD.

O descarte deverá ocorrer de maneira segura, inclusive em backups e sistemas de terceiros, conforme as possibilidades técnicas e os prazos documentados.

**15. Treinamento e conscientização**

O Portal Caboco deverá promover ações de conscientização e capacitação para as pessoas que participem do tratamento de dados pessoais.

Os treinamentos deverão abordar:

- Conceitos fundamentais da LGPD;
- Responsabilidades dos agentes de tratamento;
- Proteção de senhas e credenciais;
- Prevenção de phishing;
- Segurança na utilização de e-mails;
- Compartilhamento seguro de informações;
- Tratamento de solicitações dos titulares;
- Identificação e comunicação de incidentes.

As capacitações deverão ser registradas, com identificação dos participantes, datas e conteúdos abordados.

**16. Avaliação de riscos e conformidade**

A organização deverá realizar avaliações periódicas dos riscos relacionados ao tratamento de dados pessoais.

| Risco identificado | Impacto potencial | Medida preventiva |
|---|---|---|
| Acesso não autorizado | Exposição de dados | Controle de acesso e autenticação |
| Vazamento de dados | Danos aos titulares e sanções | Monitoramento e criptografia |
| Ataques cibernéticos | Comprometimento do portal | Atualizações e proteção tecnológica |
| Perda de informações | Indisponibilidade de dados | Backups e testes de restauração |
| Compartilhamento indevido | Violação da privacidade | Controle contratual e autorização |
| Coleta excessiva | Tratamento desnecessário | Minimização dos dados |
| Ausência de transparência | Prejuízo aos direitos dos titulares | Política de privacidade |
| Falhas de fornecedores | Exposição de informações | Avaliação de operadores |

A avaliação deverá considerar probabilidade, impacto, medidas existentes e risco residual.

Quando necessário, deverá ser elaborado Relatório de Impacto à Proteção de Dados Pessoais (RIPD), especialmente em operações que possam representar alto risco aos direitos e liberdades dos titulares.

**17. Plano de implementação do programa**

A implementação será dividida em cinco etapas.

1. Etapa 1 – Diagnóstico e levantamento
   Prazo sugerido: primeiros 15 dias.
   - Identificação dos dados coletados.
   - Levantamento dos sistemas utilizados.
   - Identificação de fornecedores.
   - Mapeamento dos fluxos de informações.
   - Avaliação preliminar de riscos.
2. Etapa 2 – Adequação documental
   Prazo sugerido: dias 16 a 30.
   - Aprovação da Política de Privacidade.
   - Elaboração da Política de Segurança da Informação.
   - Formalização das responsabilidades.
   - Elaboração dos termos de confidencialidade.
   - Definição dos procedimentos para titulares.
3. Etapa 3 – Adequação tecnológica
   Prazo sugerido: dias 31 a 60.
   - Revisão dos acessos.
   - Implementação dos controles de segurança.
   - Revisão dos backups.
   - Adequação dos mecanismos de cookies.
   - Verificação dos contratos com fornecedores.
4. Etapa 4 – Capacitação e operacionalização
   Prazo sugerido: dias 61 a 75.
   - Treinamento dos envolvidos.
   - Implantação dos procedimentos de atendimento.
   - Simulação de incidentes.
   - Registro das evidências de conformidade.
5. Etapa 5 – Monitoramento e melhoria contínua
   Prazo sugerido: dias 76 a 90 e continuamente.
   - Auditoria interna.
   - Revisão do inventário de dados.
   - Avaliação dos controles.
   - Correção de não conformidades.
   - Emissão de relatórios de acompanhamento.

Cronograma proposto, sujeito à disponibilidade de recursos e à complexidade efetiva da infraestrutura do Portal Caboco.

**18. Indicadores de conformidade**

Para acompanhar a efetividade do programa, serão utilizados indicadores de desempenho:

| Indicador | Meta proposta |
|---|---|
| Operações de tratamento mapeadas | 100% |
| Sistemas com acessos revisados | 100% |
| Fornecedores críticos avaliados | 100% |
| Colaboradores envolvidos capacitados | 100% |
| Solicitações de titulares registradas | 100% |
| Backups submetidos a testes periódicos | 100% do cronograma |
| Incidentes registrados e avaliados | 100% |
| Políticas e procedimentos revisados | Anualmente |

Os indicadores deverão ser acompanhados pelo responsável pela segurança dos dados e apresentados à administração.

**19. Documentos complementares obrigatórios para a implantação**

Para que o programa seja efetivamente operacional, deverão ser elaborados e mantidos os seguintes documentos:

1. Política de Privacidade do Portal Caboco.
2. Política de Segurança da Informação.
3. Política de Cookies.
4. Registro das Operações de Tratamento de Dados Pessoais (ROPA).
5. Matriz de Riscos de Proteção de Dados.

6. Termo de Confidencialidade e Responsabilidade.
7. Procedimento de Atendimento aos Direitos dos Titulares.
8. Plano de Resposta a Incidentes de Segurança.
9. Plano de Backup e Recuperação de Dados.
10. Termos e cláusulas de proteção de dados para fornecedores.
11. Registro de treinamentos e capacitações.
12. Relatório de Auditoria e Monitoramento da LGPD.

**20. Monitoramento, revisão e atualização**

O Programa de Conformidade com a LGPD deverá ser revisado, no mínimo, anualmente ou sempre que ocorrerem mudanças relevantes:

- Na estrutura organizacional;
- Nas atividades desenvolvidas;
- Nas tecnologias utilizadas;
- Nos sistemas de armazenamento;
- Nos fornecedores contratados;
- Nas operações de tratamento;
- Na legislação ou regulamentação aplicável.

O responsável pela segurança deverá acompanhar a implementação das medidas, registrar as evidências e recomendar ações de melhoria.

A administração da empresa deverá assegurar os recursos necessários para a manutenção do programa.

**21. Aprovação institucional**

O presente Programa de Conformidade com a Lei Geral de Proteção de Dados Pessoais estabelece as diretrizes institucionais para a proteção dos dados pessoais tratados no âmbito das atividades do Portal Caboco.

Sua implementação deverá ser acompanhada pela administração da empresa e pelo responsável pela segurança dos dados, observando os princípios da transparência, segurança, prevenção, responsabilização e prestação de contas.

Manaus, 28 de Outubro de 2026.

**CONTROLADORA**

**ALINE LUANA VIEIRA BELÉM**

Nome fantasia: Agência Assessoria Caboco

CNPJ: 35.417.162/0001-04

Assinatura: _____

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

Nome: _____

E-mail institucional: _____

Assinatura: _____

ALINE LUANA VIEIRA BELÉM
CNPJ: 35.417.162/0001-04

DIRETORA ADMINISTRATIVA