


POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO



POTIGUAR CONSTRUTORA


Caraúbas, 2026

1.^a versão


	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

SUMÁRIO

1. Apresentação e Objetivos.....	3
2. Abrangência.....	3
3. Glossário.....	4
PARTE I – PRIVACIDADE E PROTEÇÃO DE DADOS.....	5
4. Princípios do Tratamento de Dados.....	5
4.1 Princípios Gerais (Art. 6.º LGPD).....	5
4.2 Bases Legais para o Tratamento.....	6
4.3 Dados Sensíveis.....	7
4.4 Transferências Internacionais.....	7
5. Direitos dos Titulares.....	7
5.1 Informações ao Titular.....	7
5.2 Exercício de Direitos.....	8
6. Subcontratação de Operadores.....	8
7. Incidentes e Notificação à ANPD.....	9
PARTE II – SEGURANÇA DA INFORMAÇÃO.....	9
8. Classificação da Informação.....	9
9. Diretrizes de Uso de Recursos de TI.....	10
9.1 Dispositivos e Equipamentos.....	10
9.2 E-mail e Comunicações Corporativas.....	11
9.3 Internet e Redes Sociais.....	11
9.4 Armazenamento e Backup.....	11
9.5 Segurança Física.....	12
PARTE III – GESTÃO DE ACESSOS.....	12
10. Princípios da Gestão de Acessos.....	12
11. Ciclo de Vida dos Acessos.....	13
11.1 Concessão.....	13
11.2 Revisão Periódica.....	13
11.3 Revogação.....	14
12. Perfis de Acesso.....	14
13. Credenciais e Senhas.....	15

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

14. Acessos Privilegiados e de Terceiros.....	15
Acessos Privilegiados.....	15
Acessos de Terceiros.....	16
15. Auditoria e Monitoramento.....	16
16. Governança e Responsabilidades.....	17
Alta Direção.....	17
DPO (Encarregado de Dados).....	17
Comitê de Integridade.....	17
Área de TI.....	18
Gestores de Área.....	18
Colaboradores e Terceiros.....	18
17. Registro de Reclamações.....	18
18. Sanções.....	19

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	


1. Apresentação e Objetivos

A informação é um dos ativos mais estratégicos da Potiguar Construtora – desde dados de projetos e contratos até informações pessoais de colaboradores, clientes e parceiros. Protegê-la com eficiência é tanto uma obrigação legal quanto um compromisso ético da empresa com todos os que confiam a ela seus dados.

Esta Política consolida, em um único documento, as diretrizes de privacidade, proteção de dados e segurança da informação da Potiguar Construtora, estruturadas em três partes complementares:

- Parte I – Privacidade e Proteção de Dados: regras de coleta, uso, armazenamento e compartilhamento de dados pessoais, em conformidade com a LGPD (Lei n.º 13.709/2018);
- Parte II – Segurança da Informação: diretrizes para uso seguro de sistemas, dispositivos e ambientes físicos, alinhadas às normas ISO 27001 e ISO 27002;
- Parte III – Gestão de Acessos: regras para concessão, revisão e revogação de acessos a sistemas e dados, aplicando o princípio do menor privilégio.

Esta Política integra o Programa de Integridade da Potiguar Construtora e deve ser lida em conjunto com o Código de Ética e Conduta e as demais políticas da empresa.

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

2. Abrangência

Esta Política aplica-se a todos os colaboradores, estagiários, aprendizes, diretores, prestadores de serviço, consultores e terceiros que tratem dados pessoais ou acessem sistemas, informações ou infraestrutura da Potiguar Construtora – nos ambientes físicos da empresa ou em trabalho remoto. Abrange dados de colaboradores, candidatos, clientes, fornecedores e parceiros, em processos automatizados ou manuais.


3. Glossário

LGPD	<i>Lei Geral de Proteção de Dados Pessoais – Lei n.º 13.709, de 14 de agosto de 2018.</i>
-------------	---

Dado Pessoal	<i>Qualquer informação relacionada a pessoa natural identificada ou identificável.</i>
---------------------	--

Dado Sensível	<i>Dado referente a origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, saúde, vida sexual, dado genético ou biométrico vinculado a pessoa natural.</i>
----------------------	--

Titular	<i>A pessoa natural a quem os dados se referem – colaborador, cliente, fornecedor ou candidato.</i>
----------------	---

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

Controlador	<i>Pessoa natural ou jurídica que decide sobre as finalidades e meios do tratamento dos dados pessoais.</i>
--------------------	---


Operador	<i>Pessoa natural ou jurídica que realiza o tratamento de dados em nome do Controlador.</i>
-----------------	---

Tratamento	<i>Toda operação sobre dados pessoais: coleta, uso, armazenamento, compartilhamento, eliminação, entre outras.</i>
-------------------	--

DPO	<i>Encarregado de Dados (Data Protection Officer): coordena a conformidade com esta Política e atua como canal com titulares e com a ANPD.</i>
------------	--

ANPD	<i>Autoridade Nacional de Proteção de Dados – órgão público responsável por fiscalizar o cumprimento da LGPD.</i>
-------------	---

Incidente de Segurança	<i>Evento que comprometa ou ameace a confidencialidade, integridade ou disponibilidade de dados ou sistemas da empresa.</i>
-------------------------------	---

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	


PARTE I – PRIVACIDADE E PROTEÇÃO DE DADOS

4. Princípios do Tratamento de Dados

4.1 Princípios Gerais (Art. 6.º LGPD)

Todo tratamento de dados pessoais realizado pela Potiguar Construtora observa os seguintes princípios:

- Finalidade: coleta apenas para propósitos específicos, explícitos e legítimos;
- Adequação: tratamento compatível com as finalidades informadas ao titular;
- Necessidade: limitação ao mínimo indispensável para a realização das finalidades;
- Livre acesso: consulta facilitada ao titular sobre seus dados e o tratamento realizado;
- Qualidade: exatidão, clareza e atualização dos dados tratados;
- Transparência: informações claras e acessíveis sobre o tratamento;
- Segurança: medidas técnicas e administrativas contra acessos não autorizados;
- Prevenção: ações para evitar danos decorrentes do tratamento;
- Não discriminação: vedação ao uso de dados para fins discriminatórios ilícitos;
- Responsabilização: capacidade de demonstrar conformidade com a LGPD.

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

4.2 Bases Legais para o Tratamento

O tratamento de dados pessoais só ocorre quando amparado por uma das seguintes bases legais previstas na LGPD:


- Consentimento inequívoco do titular;
- Cumprimento de obrigação legal ou regulatória;
- Execução de contrato ou procedimentos preliminares a pedido do titular;
- Exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Proteção da vida ou incolumidade física do titular ou de terceiros;
- Interesses legítimos do controlador, desde que não prevaleçam sobre direitos fundamentais do titular.

4.3 Dados Sensíveis

O tratamento de dados sensíveis só é admitido nas hipóteses do Art. 11 da LGPD, incluindo consentimento específico e destacado do titular, cumprimento de obrigação legal, proteção da vida e prevenção de fraudes. A empresa adota controles adicionais para esse tipo de dado, incluindo restrição de acesso, criptografia e registro de tratamentos realizados.

4.4 Transferências Internacionais

Transferências de dados pessoais para fora do Brasil só são admitidas quando o país destinatário oferecer grau de proteção adequado (conforme avaliação da ANPD) ou quando a empresa demonstrar que o operador internacional cumpre os princípios e direitos previstos na LGPD.

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

5. Direitos dos Titulares

5.1 Informações ao Titular


No momento da coleta – ou antes do início do tratamento – o titular recebe informações sobre: identidade do controlador, finalidade e base legal do tratamento, destinatários dos dados, prazo de retenção e como exercer seus direitos. Essas informações constam nos contratos, formulários e canais oficiais da empresa.

5.2 Exercício de Direitos

Os titulares podem exercer, a qualquer tempo, os direitos previstos na LGPD:

- Confirmação da existência de tratamento;
- Acesso, correção e atualização dos dados;
- Anonimização, bloqueio ou eliminação de dados desnecessários;
- Portabilidade a outro fornecedor, mediante requisição expressa;
- Informação sobre compartilhamento com terceiros;
- Revogação do consentimento, a qualquer momento.

As solicitações são respondidas em até 15 dias úteis, com retorno inicial ao titular em até 5 dias úteis. Canais: ouvidoria@potiguarconstrutora.com.br e <https://www.potiguarconstrutora.com/>.

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	


6. Subcontratação de Operadores

Quando o tratamento for realizado por operador em nome da Potiguar Construtora, a empresa seleciona subcontratados que adotem medidas técnicas e organizacionais equivalentes às previstas nesta Política. A contratação é formalizada por escrito, especificando que o operador atuará apenas conforme as instruções da empresa e sob sua supervisão.

7. Incidentes e Notificação à ANPD

Ao identificar um incidente de segurança envolvendo dados pessoais, o colaborador deve:

1. Notificar imediatamente o DPO e o Comitê de Integridade;
2. O DPO aciona o Plano de Tratamento de Incidentes e coordena a contenção;
3. A ANPD é notificada sem demora injustificada após a ciência do incidente;
4. A comunicação à ANPD deve conter: natureza dos dados afetados, titulares impactados, medidas adotadas e motivos de eventual demora;
5. Os titulares afetados são informados quando o incidente puder causar risco ou dano relevante.

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

PARTE II – SEGURANÇA DA INFORMAÇÃO

8. Classificação da Informação


As informações da Potiguar Construtora são classificadas conforme sua sensibilidade:

CONFIDENCIAL	<i>Acesso restrito a pessoas expressamente autorizadas. Exemplos: dados pessoais sensíveis, estratégia corporativa, contratos não públicos, resultados financeiros, segredos de engenharia. Requer registro de acesso.</i>
---------------------	--

INTERNA	<i>Uso interno, sem divulgação externa. Exemplos: comunicados internos, procedimentos operacionais, dados de projetos em andamento. Acesso restrito a colaboradores.</i>
----------------	--

PÚBLICA	<i>Aprovada para divulgação externa. Exemplos: releases, material de marketing, publicações institucionais. Compartilhamento livre, respeitada a aprovação institucional.</i>
----------------	---

Em caso de dúvida sobre a classificação, trate a informação como Confidencial até obter orientação do DPO ou do Comitê de Integridade.

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

9. Diretrizes de Uso de Recursos de TI

9.1 Dispositivos e Equipamentos


- Dispositivos corporativos são de uso profissional; uso pessoal eventual e moderado é tolerado desde que não comprometa a segurança;
- Dispositivos pessoais só acessam sistemas da empresa mediante autorização e controles equivalentes;
- Perda ou roubo deve ser comunicado imediatamente ao Comitê de Integridade e à área de TI;
- Todos os dispositivos devem ter senha de bloqueio e criptografia habilitadas.

9.2 E-mail e Comunicações Corporativas

- E-mail e mensagens corporativas são ferramentas de trabalho e devem ser usadas com responsabilidade;
- É vedado o envio de informações confidenciais por canais não autorizados ou a destinatários externos sem justificativa;
- Mensagens suspeitas (*phishing*) devem ser reportadas sem clicar em links ou abrir anexos.

9.3 Internet e Redes Sociais

- O acesso à internet pela rede corporativa é monitorado e deve se limitar a atividades profissionais;
- É vedado o acesso a sites com conteúdo ilícito, pornográfico ou que violem direitos autorais;

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

• Informações confidenciais ou dados de projetos não devem ser divulgados em redes sociais, mesmo aparentemente de forma inofensiva.

9.4 Armazenamento e *Backup*

• Informações confidenciais devem ser armazenadas nos servidores e sistemas autorizados pela empresa;

É vedado o armazenamento em serviços de nuvem pessoal ou dispositivos não autorizados;

• A empresa mantém rotina de backup periódico de dados críticos, testada regularmente;

• Documentos físicos confidenciais devem ser guardados em locais seguros e descartados com fragmentadoras.


9.5 Segurança Física

• Controle de acesso físico às instalações por crachás, senhas ou biometria;

• Visitantes devem ser identificados, registrados e acompanhados por colaborador da empresa;

• Política de mesa limpa: documentos confidenciais não devem ser deixados expostos ao sair do posto;

• As instalações contam com monitoramento por câmeras, nos termos da legislação vigente.

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

PARTE III – GESTÃO DE ACESSOS


10. Princípios da Gestão de Acessos

Menor Privilégio	<i>Cada usuário acessa apenas os recursos estritamente necessários ao desempenho de suas funções.</i>
-------------------------	---

Segregação de Funções	<i>Funções incompatíveis – como autorizar e executar pagamentos – devem ser atribuídas a usuários distintos.</i>
------------------------------	--

Rastreabilidade	<i>Todo acesso a sistemas e dados críticos é registrado em log auditável, com identificação do usuário, data, hora e ação.</i>
------------------------	--

Responsabilidade Individual	<i>Credenciais são pessoais e intransferíveis. O compartilhamento de senha é vedado e sujeita o infrator a sanções.</i>
------------------------------------	---

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

11. Ciclo de Vida dos Acessos

11.1 Concessão

- O gestor da área solicita formalmente os acessos necessários ao perfil da função, via formulário específico;
- A área de TI valida a solicitação, verifica a adequação do perfil e provisiona os acessos;
- O colaborador ou terceiro recebe credenciais individuais e assina Termo de Ciência e Responsabilidade;
- Acessos a dados confidenciais ou sistemas críticos exigem aprovação adicional do Comitê de Integridade.


11.2 Revisão Periódica

- Revisão semestral de todos os acessos, conduzida pela área de TI com apoio dos gestores;
- Revisão imediata em caso de mudança de cargo, função ou área;
- Acessos privilegiados revisados trimestralmente;
- Acessos identificados como desnecessários devem ser imediatamente revogados.

11.3 Revogação

A revogação deve ocorrer de forma imediata nos seguintes eventos:

- Desligamento ou rescisão contratual – no próprio dia;
- Encerramento ou suspensão de contrato com terceiro;
- Mudança de função que torne o acesso desnecessário;


	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

- Suspeita ou confirmação de uso indevido de credenciais;
- Determinação do Comitê de Integridade em processo de investigação.

O RH e os gestores têm a obrigação de comunicar à área de TI os eventos que exigem revogação imediata.

12. Perfis de Acesso

Perfil	Descrição	Exemplos
Operacional	Acesso básico para execução do cargo	Ponto, e-mail, intranet
Técnico	Acesso a sistemas e dados da função	ERP (módulos da área), pastas de projeto
Gestão	Acesso ampliado para supervisores	Relatórios gerenciais, aprovação de fluxos
Administrativo	Acesso a dados financeiros e pessoais	RH, financeiro, contabilidade
Privilegiado	Acesso total a sistemas críticos e infraestrutura	Administradores de sistema, DBA
Terceiro	Acesso temporário restrito ao escopo do contrato	Sistemas específicos do projeto

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	


13. Credenciais e Senhas

- Senhas com no mínimo 10 caracteres, combinando maiúsculas, minúsculas, números e caracteres especiais;
- Troca obrigatória a cada 90 dias ou imediatamente após suspeita de comprometimento;
- É absolutamente proibido compartilhar senhas – mesmo quando solicitado por gestor ou TI;
- Sistemas críticos devem adotar autenticação multifator (MFA);
- Contas compartilhadas, quando indispensáveis, devem ter acesso gerenciado pela área de TI.

14. Acessos Privilegiados e de Terceiros

Acessos Privilegiados

- Concedidos apenas a colaboradores com necessidade técnica comprovada e aprovação do Comitê de Integridade;
- Toda ação com credenciais privilegiadas é registrada em log auditável;
- Cada administrador deve ter conta cotidiana separada da conta privilegiada;
- Sessões remotas privilegiadas utilizam canais criptografados e são monitoradas quando tecnicamente possível.

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

Acessos de Terceiros


- Acesso formalmente solicitado pelo gestor responsável pela contratação;
- Terceiros assinam Termo de Confidencialidade antes do primeiro acesso;
- Credenciais individuais – nunca compartilhadas com a equipe interna;
- Acesso revogado imediatamente ao término do contrato;
- Acessos a dados confidenciais exigem aprovação prévia do Comitê de Integridade e do DPO.

15. Auditoria e Monitoramento

A empresa deverá manter logs de acesso a sistemas e dados críticos. Os registros:

- Identificam usuário, data, hora, ação realizada e recurso acessado;
- São protegidos contra alteração ou exclusão pelos próprios usuários;
- São retidos por no mínimo 12 meses;
- São analisados periodicamente em busca de padrões anômalos ou suspeitos.

Acessos fora do horário habitual, tentativas repetidas negadas ou volumes incomuns de dados devem gerar alertas e ser investigados.

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

16. Governança e Responsabilidades

Alta Direção


- Aprovar e patrocinar esta Política, garantindo os recursos necessários à sua implementação;
- Promover a cultura de privacidade e segurança como valor organizacional.

DPO (Encarregado de Dados)

- Coordenar a conformidade com esta Política e com a LGPD;
- Receber e responder comunicações de titulares e da ANPD;
- Notificar a ANPD e os titulares em caso de incidentes;
- Elaborar e manter atualizados o RIPD e o Inventário de Dados.

Comitê de Integridade

- Aprovar concessões de acesso a dados confidenciais e sistemas críticos;
- Supervisionar o cumprimento desta Política e propor melhorias;
- Coordenar a resposta a incidentes de segurança e de proteção de dados.

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

Área de TI

- Provisionar, gerenciar e revogar acessos conforme solicitações aprovadas;
- Manter logs de acesso atualizados e disponíveis para auditoria;
- Monitorar acessos privilegiados e emitir alertas sobre comportamentos anômalos.

Gestores de Área


- Solicitar formalmente os acessos necessários para suas equipes;
- Comunicar imediatamente à área de TI qualquer mudança de função ou desligamento;
- Garantir que terceiros sob sua gestão assinem os termos de confidencialidade exigidos.

Colaboradores e Terceiros

- Proteger credenciais e não compartilhá-las;
- Utilizar acessos e sistemas apenas para finalidades profissionais;
- Reportar imediatamente qualquer suspeita de uso indevido, vazamento ou incidente.

17. Registro de Reclamações

A Potiguar Construtora disponibiliza os seguintes canais para reclamações sobre privacidade e segurança da informação:

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

• Sítio eletrônico: <https://www.potiguarconstrutora.com/>

• ANPD: www.gov.br/anpd


18. Sanções

O descumprimento desta Política sujeita o infrator às sanções disciplinares previstas no Código de Ética e Conduta da Potiguar Construtora, proporcionais à gravidade da conduta – de advertência à rescisão por justa causa. Terceiros infratores podem ter seus contratos rescindidos imediatamente. Em casos de violação grave da LGPD ou de outros diplomas legais, a empresa adotará as medidas legais cabíveis, incluindo comunicação às autoridades competentes.

19. Histórico de aprovação e alterações

Data de aprovação: 14/05/2026

N.º DA REVISÃO	DATA	ATUALIZAÇÃO REALIZADA	RESPONSÁVEL	ATA VINCULADA
–	–	–	–	–

	POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO	CÓDIGO	
		VERSÃO	1
		DATA INICIAL	14/05/2026
		DATA DE REVISÃO	

MEMBROS TITULARES – ASSINATURAS



Wesley de Araújo Santos
Diretor Administrativo - Grupo Potiguar
CRA-RN Nº 20-08326

Assinado digitalmente na ZapSign por
Wesley Araujo Santos
Data: 15/05/2026 08:49:19.815 (UTC-0300)

Wesley Araujo Santos

Gerente Administrativo



Assinado digitalmente na ZapSign por
Marcos Paulo Peitl Silva
Data: 15/05/2026 08:34:39.863 (UTC-0300)

Marcos Paulo Peitl Silva

Advogado



Assinado digitalmente na ZapSign por
Luiz Henrique de Almeida Costa
Data: 15/05/2026 09:39:32.620 (UTC-0300)

Luiz Henrique de Almeida Costa

Contador



Assinado digitalmente na ZapSign por
Ricardo Lyra Shelman de Souza
Data: 15/05/2026 08:57:25.789 (UTC-0300)

Ricardo Lyra Shelman de Souza

Gestor de Suprimentos



Assinado digitalmente na ZapSign por
Roseane Pereira Gomes
Data: 15/05/2026 08:30:04.393 (UTC-0300)

Roseane Pereira Gomes

Engenheira Civil

Relatório de Assinaturas

Datas e horários em UTC-0300 (America/Sao_Paulo)

Última atualização em 15 Maio 2026, 09:39:33

Status: Assinado

Documento: POLÍTICA DE PRIVACIDADE, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO.Pdf

Número: f2b0f31b-9a84-4161-86a7-3fc2d0c8b29f







Data da criação: 15 Maio 2026, 08:22:44

Hash do documento original (SHA256): 03a3c8cf8fa4b523bc59f2721cee46b2cfe6c76cd29331e14c414cce05386af8



Assinaturas

5 de 5 Assinaturas

<p>Assinado  via ZapSign by Truora</p> <p>LUIZ HENRIQUE DE ALMEIDA COSTA</p> <p>Data e hora da assinatura: 15/05/2026 09:39:32 Token: edbc224c-ff56-4a51-abe5-a46cf269f913</p>	<p>Assinatura</p>  <p>Luiz Henrique de Almeida Costa</p>
<p>Pontos de autenticação: Telefone: 5584991345027 E-mail: luizhenrique@potipedras.com.br</p>	<p>Localização aproximada: -5.875000, -35.335399 IP: 191.6.253.176 Dispositivo: Mozilla/5.0 (iPhone; CPU iPhone OS 18_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/26.3 Mobile/15E148 Safari/604.1</p>
<p>Assinado  via ZapSign by Truora</p> <p>WESLEY ARAUJO SANTOS</p> <p>Data e hora da assinatura: 15/05/2026 08:49:19 Token: 01d02361-0311-4e07-b4cb-44188583e103</p>	<p>Assinatura</p>  <p>Wesley Araujo Santos</p>
<p>Pontos de autenticação: Telefone: 5584998280048 E-mail: wesley@potiguarconstrutora.com.br</p>	<p>Localização aproximada: -5.856100, -35.352300 IP: 191.6.253.176 Dispositivo: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/148.0.0.0 Safari/537.36 Edg/148.0.0.0</p>
<p>Assinado  via ZapSign by Truora</p> <p>ROSEANE PEREIRA GOMES</p> <p>Data e hora da assinatura: 15/05/2026 08:30:04 Token: 4933e398-810e-4216-abf6-0cb406495b87</p>	<p>Assinatura</p>  <p>Roseane Pereira Gomes</p>
<p>Pontos de autenticação: Telefone: 5584988365446 E-mail: roseane.gomes@britapotiguar.com.br</p>	<p>IP: 191.6.253.176 Dispositivo: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/148.0.0.0 Safari/537.36 Edg/148.0.0.0</p>

INTEGRIDADE CERTIFICADA - ICP-BRASIL

Assinaturas eletrônicas e físicas têm igual validade legal, conforme MP 2.200-2/2001 e Lei 14.063/2020.

[Confirme a integridade do documento aqui.](#)







Este Log é exclusivo e parte integrante do documento número f2b0f31b-9a84-4161-86a7-3fc2d0c8b29f, segundo os [Termos de Uso da ZapSign](#), disponíveis em zapsign.com.br

Relatório de Assinaturas

Datas e horários em UTC-0300 (America/Sao_Paulo)

Última atualização em 15 Maio 2026, 09:39:33

<p>Assinado  via ZapSign by Truora</p> <p>MARCOS PAULO PEITL SILVA Data e hora da assinatura: 15/05/2026 08:34:39 Token: d05d0a55-fda3-4134-85d5-f8c37488676f</p>	<p>Assinatura</p>  <p>Marcos Paulo Peitl Silva</p>
<p>Pontos de autenticação: Telefone: 5584999286769 E-mail: marcos@pgm.adv.br</p>	<p>Localização aproximada: -5.874619, -35.334651 IP: 191.6.253.176 Dispositivo: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/148.0.0.0 Mobile Safari/537.36</p>
<p>Assinado  via ZapSign by Truora</p> <p>RICARDO LYRA SHELMAN DE SOUZA Data e hora da assinatura: 15/05/2026 08:57:25 Token: d7311405-f9a3-4789-a903-a132fb54c39b</p>	<p>Assinatura</p>  <p>Ricardo Lyra Shelman de Souza</p>
<p>Pontos de autenticação: Telefone: 5584999878055 E-mail: ricardo.shelman@britapotiguar.com.br</p>	<p>IP: 191.6.253.176 Dispositivo: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/148.0.0.0 Safari/537.36</p>

INTEGRIDADE CERTIFICADA - ICP-BRASIL

Assinaturas eletrônicas e físicas têm igual validade legal, conforme MP 2.200-2/2001 e Lei 14.063/2020.

[Confirme a integridade do documento aqui.](#)



Este Log é exclusivo e parte integrante do documento número f2b0f31b-9a84-4161-86a7-3fc2d0c8b29f, segundo os [Termos de Uso da ZapSign](#), disponíveis em zapsign.com.br