



Política de Proteção de Dados Pessoais (PPDP)

Versão 1.3

Santa Rosa, Brasil, Fevereiro de 2026

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS - PPDP

DIREÇÃO EXECUTIVA

Alexandre Luis Machado

Eliseu Marafiga

COORDENAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Fernando Krein Pinheiro

COMITÊ DE PRIVACIDADE E PROTEÇÃO DE DADOS

Fernando Krein Pinheiro

Rodrigo Krein Pinheiro

Bruno Lopes

Aline Pereira de Oliveira

Silmar Parodes

Ricardo Leidemer

Lucas Berg

Lucas Frisk

Bruno Borges

Tanize Itermann

Andreia Becker Ferreira

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS - DPO

Fernando Krein Pinheiro

Equipe Técnica de Elaboração

Fernando Krein Pinheiro

Ricardo Leidemer

Douglas Acosta

Marcus Volkweis

Equipe Revisora

Lucas Laiber

Laura Bikoski

Histórico de versões

Data	Versão	Descrição	Autor
20/01/2025	1.0	Início da fase de implementação	Fernando Pinheiro
11/02/2026	1.1	Inclusão do Item 10.5 sobre Mensageria	Fernando Pinheiro
19/02/2026	1.2	Revisão geral de escrita e reforços de aderência ANPD (RCIS), Cookies, Legítimo Interesse, DPO, SLAs e evidências	Fernando Pinheiro
20/02/2026	1.3	Reforço de art. 41, art. 9, RCIS, LI, RIPD, cookies, terceiros e evidências	Fernando Pinheiro

1. OBJETIVO	6
1.1 Finalidade da Política	6
1.2 Alinhamento com os Objetivos Estratégicos do Negócio	6
1.3 Dados Pessoais como Ativo Estratégico	6
1.4 Estrutura e Hierarquia dos Documentos	6
1.5 Identificação do Controlador e do Encarregado (DPO)	7
2. ESCOPO E ABRANGÊNCIA	8
2.1 Abrangência Organizacional	8
2.2 Aplicabilidade a Colaboradores, Terceiros e Parceiros	8
2.3 Titulares de Dados	8
2.4 Meios e Ambientes	8
2.5 Papel da Brphonia como Agente de Tratamento	9
2.6 Exclusões e Exceções Formais	9
3. MARCOS REGULATÓRIOS E REFERÊNCIAS	10
3.1 Leis e Decretos	10
3.2 Normas e Frameworks	10
3.3 Regulamentação Setorial	10
3.4 Guias e Regulamentos da ANPD	11
4. CONCEITOS E DEFINIÇÕES	11
5. PRINCÍPIOS DE PROTEÇÃO DE DADOS	12
6. GOVERNANÇA DE PROTEÇÃO DE DADOS, PRIVACIDADE E PAPÉIS	13
6.1 Diretoria Executiva	13
6.2 Encarregado pelo Tratamento de Dados Pessoais (DPO)	13
6.3 Gestores de Área	14
6.4 TI, Infraestrutura e Redes	15
6.5 Colaboradores, Prestadores e Parceiros	15
7. GESTÃO DE RISCOS DE PRIVACIDADE, ROPA E RIPD	15
7.1 Registros de Operações de Tratamento (ROPA)	15
7.2 Análise de Risco e Relatório de Impacto à Proteção de Dados (RIPD)	16
7.3 Privacidade por Design e por Padrão	17
7.4 Sistema de Gestão de Proteção de Dados Pessoais (SGPDP/PIMS)	18
8. CLASSIFICAÇÃO E CATEGORIAS DE DADOS PESSOAIS E TITULARES	19
8.1 Clientes	19
8.2 Colaboradores e Candidatos	19
8.3 Filhos de Colaboradores (Crianças e Adolescentes)	20
8.4 Fornecedores, Prestadores e Parceiros	21
9. BASES LEGAIS E FINALIDADES	21
9.1 Legítimo Interesse	22
9.2 Consentimento e Revogação	23
10. CICLO DE VIDA DOS DADOS PESSOAIS	24
10.1 Coleta	24
10.2 Uso, Acesso e Compartilhamento Interno	24
10.3 Compartilhamento com Terceiros	24
10.4 Retenção, Anonimização e Eliminação	25

10.5	Uso de Canais de Comunicação e Mensageria Digital	26
11.	DADOS SENSÍVEIS E DE CRIANÇAS/ADOLESCENTES	26
12.	COOKIES E TECNOLOGIAS DE RASTREAMENTO	27
13.	TRANSFERÊNCIAS INTERNACIONAIS DE DADOS	28
14.	SISTEMAS AUTOMATIZADOS, PERFILHAMENTO E INTELIGÊNCIA ARTIFICIAL	29
15.	DIREITOS DOS TITULARES E CANAIS DE ATENDIMENTO	30
15.1	Canais de Atendimento	31
15.2	Prazos, Portabilidade e Evidências	32
16.	GESTÃO DE TERCEIROS, OPERADORES E CO-CONTROLADORES	32
17.	SEGURANÇA DA INFORMAÇÃO APLICADA À PROTEÇÃO DE DADOS	33
18.	GESTÃO DE INCIDENTES E VAZAMENTOS	34
19.	TREINAMENTO, CONSCIENTIZAÇÃO E CULTURA DE PRIVACIDADE	35
20.	CONFORMIDADE, AUDITORIA E MELHORIA CONTÍNUA	35
21.	EXCEÇÕES À POLÍTICA	36
21.1	Processo Formal de Exceções	36
21.2	Aprovação e Registro	37
21.3	Revisão Periódica das Exceções	37
22.	REVISÃO, ATUALIZAÇÃO E VIGÊNCIA DA POLÍTICA	37
22.1	Periodicidade de Revisão	37
22.2	Controle de Versões	37
22.3	Vigência	38

1. OBJETIVO

1.1 Finalidade da Política

Esta Política de Proteção de Dados Pessoais (PPDP) tem por finalidade estabelecer princípios, diretrizes, responsabilidades e requisitos mínimos para o tratamento de dados pessoais pela Brphonia, assegurando proteção adequada aos dados e conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e demais normas aplicáveis.

1.2 Alinhamento com os Objetivos Estratégicos do Negócio

A PPDP está alinhada aos objetivos estratégicos e à governança corporativa da Brphonia, contribuindo para:

- a confiança de clientes, colaboradores, fornecedores, parceiros e reguladores;
- a continuidade, disponibilidade e confiabilidade dos serviços de telecomunicações e conectividade;
- a mitigação de riscos legais, regulatórios, financeiros e reputacionais decorrentes do tratamento de dados pessoais.

1.3 Dados Pessoais como Ativo Estratégico

A Brphonia reconhece que os dados pessoais sob sua responsabilidade constituem ativos estratégicos, devendo ser:

- protegidos contra acesso não autorizado, uso indevido, alteração, perda, destruição ou divulgação indevida;
- tratados de forma ética, transparente, segura e proporcional às finalidades para as quais foram coletados.

1.4 Estrutura e Hierarquia dos Documentos

Esta PPDP é um documento de nível estratégico, que se desdobra em:

- Normas Corporativas de Privacidade e Proteção de Dados;
- Procedimentos Operacionais Padrão (POPs);
- Documentos públicos complementares, como Avisos/Notas de Privacidade e Política de Cookies;
- Tabela de Retenção de Dados Pessoais.

Em caso de conflito entre documentos internos, aplica-se o seguinte:

1. Prevalecem sempre as leis e regulamentos aplicáveis (LGPD, Marco Civil da Internet, normas setoriais etc.).
2. Entre a Política de Segurança da Informação e Cibersegurança (PSI), esta PPDP e demais normas internas, **prevalecerá a norma que garantir maior proteção aos direitos dos titulares de dados pessoais**, em consonância com os princípios da LGPD.
3. Normas, POPs, Tabela de Retenção, Política de Cookies, Avisos de Privacidade e demais documentos correlatos devem ser interpretados de forma compatível com esta PPDP e com a legislação vigente, não podendo reduzir o nível de proteção aqui estabelecido.

1.5 Identificação do Controlador e do Encarregado (DPO)

Para fins desta Política:

- **Controlador**
 - Razão social: Brphonia Provedor IP LTDA
 - CNPJ: 10.431.131.0001/87
 - Endereço: Av. Santa Cruz, 572, Centro, Santa Rosa - RS
- **Encarregado pelo Tratamento de Dados Pessoais (DPO)**
 - Nome: Fernando Krein Pinheiro
 - E-mail institucional para contato: dpo.privacidade@brphonia.com.br
 - Canal eletrônico adicional: <https://politicas.brphonia.com.br>

A identidade e os canais de contato do Encarregado da Brphonia são divulgados publicamente, em atendimento ao art. 41, §1º da LGPD, por meio de:

- página de Privacidade/Proteção de Dados no site institucional;
 - Avisos/Notas de Privacidade de clientes, colaboradores, candidatos e demais titulares;
 - outras comunicações oficiais, conforme necessário.
-

2. ESCOPO E ABRANGÊNCIA

2.1 Abrangência Organizacional

Esta Política aplica-se a todas as unidades organizacionais, áreas de negócio, subsidiárias, filiais, controladas e demais estruturas sob responsabilidade da Brphonia, no território nacional ou no exterior, sempre que houver tratamento de dados pessoais.

2.2 Aplicabilidade a Colaboradores, Terceiros e Parceiros

A PPDP é de cumprimento obrigatório por:

- colaboradores, estagiários, aprendizes, sócios e administradores;
- prestadores de serviços, consultores, fornecedores, parceiros e operadores que tratem dados pessoais em nome da Brphonia;
- qualquer pessoa que, por função, contrato ou vínculo, acesse ou participe de decisões relacionadas ao tratamento de dados pessoais sob responsabilidade da Brphonia.

2.3 Titulares de Dados

Esta Política abrange o tratamento de dados pessoais de:

- clientes pessoa física e representantes de clientes pessoa jurídica;
- colaboradores, ex-colaboradores, candidatos, estagiários e aprendizes;
- filhos de colaboradores (crianças e adolescentes) para fins de concessão de benefícios;
- representantes de fornecedores, parceiros e demais terceiros;
- quaisquer outras pessoas naturais cujos dados sejam tratados no contexto das atividades da Brphonia.

2.4 Meios e Ambientes

O disposto nesta PPDP aplica-se aos dados pessoais tratados:

- em sistemas, aplicações, bancos de dados, serviços em nuvem, redes e dispositivos;
- em e-mails corporativos, ferramentas de colaboração, sistemas de mensagens autorizados e mídias removíveis;
- em documentos físicos, formulários, contratos, relatórios, gravações de áudio e vídeo;

- em registros técnicos, logs, trilhas de auditoria e demais evidências geradas.

2.5 Papel da Brphonia como Agente de Tratamento

- A Brphonia atua predominantemente como **controladora** de dados pessoais.
- Em situações específicas, definidas contratualmente, poderá atuar como **operadora**, realizando tratamento em nome de outro controlador.
- Não sendo considerada agente de pequeno porte, a Brphonia compromete-se a:
 - manter Registros das Operações de Tratamento (ROPA) abrangentes e atualizados;
 - elaborar Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) nas hipóteses previstas em lei e recomendadas pela ANPD.

2.6 Exclusões e Exceções Formais

Exceções à PPDP:

- devem ser solicitadas formalmente, com justificativa e análise de risco;
- exigem aprovação mínima do Encarregado (DPO) e do gestor da área, podendo envolver a Diretoria Executiva de acordo com a matriz interna de aprovação;
- devem possuir prazo de validade definido, com definição de controles compensatórios e registro em repositório específico.

As exceções seguem o processo corporativo de gestão de riscos e exceções estabelecido na PSI, e estão sujeitas à revisão periódica.

3. MARCOS REGULATÓRIOS E REFERÊNCIAS

3.1 Leis e Decretos

A PPDP está fundamentada na legislação brasileira aplicável à proteção de dados, privacidade e sigilo de informações, em especial:

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Constituição Federal;
- Código Civil e Código de Defesa do Consumidor;

- Consolidação das Leis do Trabalho (CLT) e normas trabalhistas e previdenciárias;
- Legislação fiscal e Tributária aplicável;
- Lei nº 12.965/2014 – Marco Civil da Internet e seu decreto regulamentador;

3.2 Normas e Frameworks

Como referência técnica, a Brphonia adota, entre outras:

- Política de Segurança da Informação e Cibersegurança (PSI) da Brphonia;
- Normas ISO/IEC 27001 e 27002;
- Norma ISO/IEC 27701;
- CIS Controls v8 e seu Guia Complementar de Privacidade.

3.3 Regulamentação Setorial

No contexto de telecomunicações e conectividade, a Brphonia observa:

- Normas, resoluções e regulamentos da Agência Nacional de Telecomunicações (Anatel);
- Regras específicas sobre qualidade, atendimento, faturamento, guarda de registros e sigilo de comunicações, quando aplicáveis;

3.4 Guias e Regulamentos da ANPD

Na interpretação e aplicação desta PPDP, a Brphonia considera, entre outros:

- Guia de Atuação do Encarregado pelo Tratamento de Dados Pessoais;
- Guia Orientativo sobre Cookies e Proteção de Dados Pessoais;
- Guia sobre Legítimo Interesse;
- Guias e fascículos sobre segurança da informação, incidentes e vazamento de dados;
- Orientações sobre tratamento de dados de crianças e adolescentes;
- Regulamento de Comunicação de Incidentes de Segurança (RCIS), incluindo prazos e requisitos de notificação à ANPD.

4. CONCEITOS E DEFINIÇÕES

Aplicam-se, dentre outras, as definições a seguir:

- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável.
- **Dado pessoal sensível:** dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.
- **Titular:** pessoa natural a quem se referem os dados pessoais.
- **Tratamento:** toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração.
- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- **Encarregado pelo Tratamento de Dados Pessoais (DPO):** pessoa indicada pela Brphonia para atuar como canal de comunicação entre o controlador, os titulares e a ANPD e apoiar a conformidade com a LGPD.
- **Incidente de segurança com dados pessoais:** evento adverso, confirmado ou sob suspeita, relacionado a violação de segurança que resulte em destruição, perda, alteração, divulgação ou acesso não autorizado a dados pessoais.
- **Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
- **Pseudonimização:** tratamento de dados pessoais por meio do qual estes perdem, temporária ou parcialmente, a possibilidade de associação direta a um titular, sem que se tornem irreversivelmente anônimos, mediante substituição de identificadores por pseudônimos.
- **Decisão automatizada:** decisão tomada exclusivamente com base em tratamento automatizado de dados pessoais, que afete os interesses do titular.
- **Inteligência Artificial (IA):** sistemas ou modelos computacionais que, por meio de algoritmos, técnicas estatísticas ou aprendizado de máquina, analisam dados e realizam tarefas como previsão, classificação, recomendação ou tomada de decisão

envolvendo dados pessoais.

5. PRINCÍPIOS DE PROTEÇÃO DE DADOS

As operações de tratamento de dados pessoais realizadas pela Brphonia devem observar, no mínimo, os princípios previstos na LGPD:

- finalidade;
- adequação;
- necessidade;
- livre acesso;
- qualidade dos dados;
- transparência;
- segurança;
- prevenção;
- não discriminação;
- responsabilização e prestação de contas.

A Brphonia adota, adicionalmente:

- **privacidade desde a concepção (privacy by design)**, incorporando requisitos de proteção de dados desde o planejamento de processos, sistemas, serviços e contratos;
- **privacidade por padrão (privacy by default)**, configurando processos e sistemas para que, por padrão, coletem, utilizem e disponibilizem apenas o mínimo necessário de dados pessoais.

Como parte da responsabilização e prestação de contas, a Brphonia manterá registros formais que demonstrem a análise de aderência de cada operação de tratamento aos princípios do art. 6º da LGPD, integrando essa avaliação ao ROPA, aos RIPDs e a outros documentos de governança de privacidade.

6. GOVERNANÇA DE PROTEÇÃO DE DADOS, PRIVACIDADE E PAPÉIS

6.1 Diretoria Executiva

Compete à Diretoria Executiva:

- aprovar esta PPDP e os documentos correlatos;
- assegurar recursos adequados à implantação do programa de privacidade;
- apoiar e patrocinar institucionalmente a atuação do Encarregado (DPO) e do Comitê de Privacidade;
- acompanhar indicadores e relatórios relevantes de proteção de dados;
- avaliar periodicamente a eficácia do Sistema de Gestão de Proteção de Dados Pessoais (SGPDP).

6.2 Encarregado pelo Tratamento de Dados Pessoais (DPO)

Compete ao Encarregado (DPO):

- atuar como canal de comunicação entre a Brphonia, os titulares e a ANPD;
- orientar colaboradores e terceiros sobre as práticas de proteção de dados pessoais;
- receber comunicações da ANPD e adotar providências;
- apoiar a elaboração, revisão e manutenção do ROPA e dos RIPDs;
- apoiar a gestão de incidentes envolvendo dados pessoais;
- apoiar treinamentos e ações de conscientização;
- monitorar o cumprimento da LGPD, desta PPDP, da PSI e dos demais normativos relacionados à privacidade.

Para garantir a independência e mitigar conflitos de interesse:

- o DPO possui **linha de reporte direto à Diretoria Executiva**, podendo levar recomendações e pareceres sem necessidade de validação prévia de outras áreas;
- a Brphonia compromete-se a garantir que o DPO não receba instruções quanto ao conteúdo de seus pareceres sobre conformidade com a LGPD e as normas desta PPDP;

- possíveis conflitos de interesse decorrentes de acumulação de funções (por exemplo, DPO e Cordenação de Segurança da Informação) serão avaliados ao menos uma vez ao ano pelo Comitê de Privacidade, com registro formal das conclusões e das medidas de mitigação;
- em avaliações críticas, auditorias internas de privacidade ou decisões de maior impacto, poderá ser envolvido profissional ou consultoria independente, especialmente quando houver risco de conflito de interesses;
- o DPO terá acesso aos recursos necessários (informações, apoio técnico, tempo e orçamento proporcional) para o desempenho de suas funções.

6.3 Gestores de Área

Compete aos gestores de área:

- mapear e manter atualizados os tratamentos de dados pessoais sob sua responsabilidade;
- assegurar o registro desses tratamentos no ROPA;
- garantir que novos projetos, produtos, serviços e sistemas apliquem privacidade by design e by default;
- apoiar a elaboração de RIPDs, quando exigidos;
- implementar e acompanhar planos de ação de privacidade em suas áreas;
- disseminar e fazer cumprir normas e POPs de proteção de dados em suas equipes.

6.4 TI, Infraestrutura e Redes

Compete às áreas de TI, Infraestrutura e Redes:

- implementar e manter os controles técnicos definidos na PSI e nesta PPDP;
- adotar práticas de Gestão de Identidades e Acessos (IAM) e de arquitetura Zero Trust;
- proteger ativos core de rede e sistemas críticos associados à prestação de serviços;
- garantir a geração, integridade e retenção de logs relevantes para segurança e privacidade;

- apoiar a análise de riscos de privacidade em sistemas, integrações e projetos de tecnologia;
- apoiar a resposta a incidentes de segurança e a produção de evidências.

6.5 Colaboradores, Prestadores e Parceiros

Todos os colaboradores, prestadores e parceiros que tenham acesso a dados pessoais devem:

- conhecer e cumprir esta PPDP, a PSI e as normas e POPs correlatos;
 - tratar dados pessoais apenas quando necessário e autorizado;
 - proteger os dados contra acesso não autorizado, uso indevido, vazamento ou destruição indevida;
 - comunicar imediatamente qualquer suspeita ou ocorrência de incidente envolvendo dados pessoais pelos canais internos definidos.
-

7. GESTÃO DE RISCOS DE PRIVACIDADE, ROPA E RIPD

7.1 Registros de Operações de Tratamento (ROPA)

A Brphonia manterá ROPA atualizado, contemplando, para cada operação de tratamento:

- finalidades do tratamento;
- categorias de titulares;
- categorias de dados pessoais (incluindo dados sensíveis e dados de crianças/adolescentes, quando houver);
- bases legais utilizadas;
- categorias de destinatários e compartilhamentos, inclusive transferências internacionais;
- prazos de retenção, em consonância com a Tabela de Retenção de Dados Pessoais;
- medidas de segurança e controles aplicáveis, incluindo pseudonimização, quando utilizada;

- indicação de existência de RIPD associado;
- indicação e referência ao teste de legítimo interesse, quando esta base legal for empregada.

O ROPA:

- será mantido em **repositório central** sob responsabilidade conjunta do DPO e dos gestores de área;
- terá responsáveis (owners) claramente definidos para cada operação de tratamento;
- será atualizado, no mínimo, trimestralmente para operações de maior risco e anualmente para as demais, ou sempre que houver mudanças relevantes nas finalidades, tecnologias ou bases legais;
- integrará o Sistema de Gestão de Proteção de Dados Pessoais e estará disponível para auditorias internas, externas e para solicitações da ANPD.

7.2 Análise de Risco e Relatório de Impacto à Proteção de Dados (RIPD)

Será obrigatória a elaboração de RIPD, entre outros casos:

- tratamento em larga escala de dados pessoais sensíveis;
- uso de biometria para identificação ou autenticação;
- tratamento de dados de crianças e adolescentes em contextos de maior risco;
- monitoramento sistemático de áreas acessíveis ao público ou de tráfego de rede associado a perfis de usuários;
- decisões automatizadas que produzam efeitos relevantes sobre os titulares;
- projetos que envolvam uso intensivo de Inteligência Artificial em análise, classificação ou recomendação envolvendo dados pessoais;
- implantação de novos sistemas ou integrações que ampliem significativamente a escala, volume ou sensibilidade dos dados tratados.

RIPDs adicionais poderão ser elaborados sempre que o DPO, o Comitê de Privacidade ou a Diretoria entenderem necessário.

O RIPD deverá descrever:

- as operações de tratamento, finalidades e bases legais;
- a avaliação de necessidade e proporcionalidade;
- os riscos aos titulares e sua probabilidade e impacto;
- as medidas de mitigação e salvaguardas técnicas e organizacionais;
- o plano de monitoramento e revisão.

Os RIPDs:

- serão registrados em repositório próprio, com controle de versões e indicação de responsáveis;
- terão sua elaboração e revisão integradas à metodologia corporativa de gestão de riscos (ERM);
- serão revisados periodicamente, especialmente quando houver alterações relevantes no tratamento, na legislação ou nas orientações da ANPD.

7.3 Privacidade por Design e por Padrão

Projetos, produtos, serviços, sistemas, integrações e contratos envolvendo dados pessoais deverão:

- considerar requisitos de privacidade e proteção de dados desde a concepção;
- utilizar configurações padrão que minimizem a coleta, o uso e o compartilhamento de dados pessoais;
- priorizar, sempre que possível, o uso de dados anonimizados ou pseudonimizados;
- prever mecanismos de gestão de consentimento e preferências de titulares;
- incluir desde o início a definição de ciclos de vida e prazos de retenção, conforme Tabela de Retenção;
- envolver o DPO e o Comitê de Privacidade em avaliações de impacto, quando cabível.

Todo novo projeto ou alteração relevante que envolva tratamento de dados pessoais classificados como de **alto risco** deverá:

- ser submetido previamente à avaliação do DPO, antes da fase de implantação;

- somente avançar para etapas de desenvolvimento ou produção após consideração dos riscos de privacidade e, quando aplicável, aprovação de RIPD ou Relatório de Impacto específico.

7.4 Sistema de Gestão de Proteção de Dados Pessoais (SGPDP/PIMS)

A Brphonia mantém um **Sistema de Gestão de Proteção de Dados Pessoais (SGPDP)**, alinhado à ISO/IEC 27701 e integrado ao Sistema de Gestão de Segurança da Informação (SGSI), que engloba:

- esta PPDP, normas e POPs de privacidade;
- ROPA, RIPDs e LIAs;
- Tabela de Retenção de Dados Pessoais;
- registros de consentimentos e preferências;
- evidências de atendimento a titulares, treinamentos e auditorias;
- processos de gestão de terceiros e transferências internacionais.

O SGPDP:

- terá escopo, objetivos mensuráveis, indicadores e responsáveis definidos;
- contemplará critérios de risco de privacidade e critérios de aceitação de risco aprovados pela Diretoria;
- contará com ciclo de auditorias internas de privacidade, com frequência mínima bienal, escopo definido e independência adequada;
- será objeto de revisão periódica pela Diretoria Executiva, com base em relatórios do DPO e do Comitê de Privacidade.

8. CLASSIFICAÇÃO E CATEGORIAS DE DADOS PESSOAIS E TITULARES

8.1 Clientes

A Brphonia trata, dentre outros, os seguintes dados de clientes:

- identificação e contato: nome completo, RG, CPF, CNPJ (quando aplicável), data de nascimento, endereço, telefone fixo e celular, e-mail;

- dados contratuais e de relacionamento: número de contrato, código de cadastro de cliente, histórico de atendimentos e protocolos;
- dados financeiros: informações bancárias para cobrança, débito em conta e estorno, quando aplicável;
- dados técnicos de rede e de serviço, tais como:
 - código de conexão à internet;
 - endereços IP;
 - endereços MAC de roteadores, ONUs e demais equipamentos de cliente;
 - usuário e senha de conexão PPPoE;
 - usuário e senha de rede sem fio;
 - usuário e senha de acesso ao roteador Wi-Fi, quando aplicável.

Esses dados técnicos constituem dados pessoais na medida em que permitem a identificação ou associação a um titular e às suas atividades na rede, recebendo proteção reforçada, em alinhamento com a PSI, com o Marco Civil da Internet e com a regulamentação da Anatel.

8.2 Colaboradores e Candidatos

Entre os dados de colaboradores e candidatos, incluem-se:

- identificação e contato: nome, RG, CPF, data de nascimento, endereço, telefone, e-mail, filiação, estado civil, grau de instrução, foto 3x4;
- dados funcionais e contratuais: matrícula interna, cargo, histórico profissional, número da CTPS, PIS/PASEP, CNH, código de cadastro de colaborador, código de contrato de trabalho;
- dados bancários para pagamento de salários e benefícios;
- dados sensíveis: informações de saúde ocupacional (exames admissionais e periódicos), biometria (quando utilizada), raça/cor, placa de veículo associada a colaborador, quando estritamente necessário;
- dados de recrutamento e seleção: currículos, testes, avaliações e registros de entrevistas;

- dados de acesso lógico e físico: credenciais de sistemas, registros de acesso a ambientes, logs de autenticação.

8.3 Filhos de Colaboradores (Crianças e Adolescentes)

Para concessão de benefícios (creche, auxílio educacional, plano de saúde e correlatos), poderão ser tratados:

- nome;
- data de nascimento;
- RG e CPF (quando houver);
- informações constantes da carteira de vacinação ou laudos médicos estritamente necessários à concessão do benefício.

O tratamento observará sempre o melhor interesse da criança e do adolescente, bem como os seguintes requisitos:

- quando exigível, o tratamento de dados de crianças dependerá de consentimento específico e em destaque, dado por pelo menos um dos pais ou responsável legal;
- serão adotados esforços razoáveis para verificar que o consentimento foi fornecido por responsável legítimo;
- serão mantidas informações públicas e acessíveis sobre o tratamento de dados de crianças e adolescentes, por meio de Avisos de Privacidade e outros canais adequados.

Dados de filhos de colaboradores usados para benefícios serão coletados no mínimo necessário, com prazos de retenção definidos na Tabela de Retenção e controles de acesso restritos.

8.4 Fornecedores, Prestadores e Parceiros

Os dados pessoais tratados de fornecedores, prestadores e parceiros podem incluir:

- dados pessoais de representantes: nome, RG, CPF, cargo, função;
- dados de contato: endereço comercial, telefone, e-mail;
- dados bancários e fiscais necessários à contratação e pagamentos;
- dados de acesso a sistemas e instalações, quando aplicáveis.

9. BASES LEGAIS E FINALIDADES

As operações de tratamento realizadas pela Brphonia observarão as hipóteses legais previstas na LGPD, destacando-se:

- cumprimento de obrigação legal ou regulatória;
- execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular seja parte;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- proteção da vida ou da incolumidade física do titular ou de terceiro;
- tutela da saúde, em procedimento realizado por profissionais ou serviços de saúde, quando aplicável;
- legítimo interesse do controlador ou de terceiro, respeitados os direitos e liberdades fundamentais do titular;
- consentimento do titular, quando aplicável.

As finalidades de tratamento incluem, entre outras:

- prestação e suporte de serviços de telecomunicações e conectividade;
- gestão de contratos, faturamento, cobrança e relacionamento com clientes;
- gestão de pessoas (colaboradores e candidatos) e cumprimento de obrigações trabalhistas, previdenciárias e fiscais;
- atendimento a exigências legais e regulatórias;
- segurança da informação, monitoramento de redes, prevenção a fraudes e controle de acessos;
- melhoria de produtos, serviços e processos, inclusive mediante análises estatísticas, preferencialmente com dados anonimizados;
- ações de comunicação e marketing, respeitadas as preferências e bases legais adequadas.

Para cada operação de tratamento, será mantida, no ROPA, a vinculação explícita entre:

- finalidades;
- bases legais;
- categorias de dados e de titulares;
- categorias de destinatários (incluindo terceiros e transferências internacionais);
- critérios de retenção.

9.1 Legítimo Interesse

Quando utilizar o legítimo interesse como base legal, a Brphonia:

- realizará teste de balanceamento para cada operação, ou grupo de operações de mesma natureza, considerando finalidade, necessidade, expectativa do titular, impacto e salvaguardas;
- documentará o resultado desse teste em registro próprio de **Legitimate Interest Assessment (LIA)**, vinculado ao ROPA correspondente;
- revisará periodicamente o teste, especialmente em tratamentos que envolvam monitoramento extensivo, perfilhamento ou marketing;
- evitará utilizar legítimo interesse para:
 - tratamento em larga escala de dados pessoais sensíveis;
 - tratamento de dados de crianças e adolescentes em contextos de risco elevado, privilegiando bases mais protetivas.

As LIAs:

- utilizarão modelo padronizado com, no mínimo, descrição da operação, interesse legítimo, avaliação de necessidade, expectativa do titular, riscos e salvaguardas;
- serão aprovadas pelo gestor do processo e pelo DPO;
- serão revistas, no mínimo, a cada 2 (dois) anos ou quando houver mudanças relevantes nas operações.

9.2 Consentimento e Revogação

Quando o tratamento tiver como fundamento exclusivamente o consentimento:

- a revogação implicará, sempre que possível, a eliminação ou anonimização dos dados relativos às finalidades consentidas;
- permanecerão retidos apenas os dados necessários ao cumprimento de obrigações legais ou regulatórias, ao exercício regular de direitos ou a outras bases legais supervenientes, que deverão ser informadas ao titular.

Quando os dados forem também necessários para outras finalidades baseadas em hipóteses legais distintas do consentimento, a revogação:

- não acarretará a eliminação automática de todos os dados;
- implicará avaliação caso a caso, preservando-se apenas os dados indispensáveis às demais finalidades, com transparência ao titular.

A Brphonia manterá um **sistema centralizado de gestão de consentimento e preferências**, que registrará, no mínimo:

- data e hora da manifestação;
- canal e contexto de coleta;
- versão do Aviso/Nota de Privacidade e, quando aplicável, da Política de Cookies;
- finalidades específicas às quais o consentimento se refere;
- registro de revogações e alterações de preferências.

Esses registros serão preservados como evidência para auditorias e eventuais solicitações da ANPD.

10. CICLO DE VIDA DOS DADOS PESSOAIS

10.1 Coleta

A coleta de dados pessoais pela Brphonia deverá:

- ser limitada ao mínimo necessário para as finalidades informadas;
- ocorrer por meios lícitos;
- observar, quando exigido, a obtenção de consentimento prévio, específico e destacado;

- ser acompanhada de informações claras ao titular, por meio de Avisos/Notas de Privacidade, sobre finalidade, forma e duração do tratamento, identidade do controlador, compartilhamentos relevantes e direitos.

10.2 Uso, Acesso e Compartilhamento Interno

Durante o uso e acesso interno:

- os dados deverão ser utilizados apenas para finalidades legítimas e compatíveis com as informadas ao titular;
- o acesso será concedido com base em perfis de função, necessidade de conhecimento e princípio do privilégio mínimo;
- haverá revisão periódica de perfis e revogação tempestiva de credenciais de usuários desligados ou transferidos;
- serão aplicados controles de IAM e arquitetura Zero Trust, conforme PSI;
- serão gerados e monitorados logs de acesso a dados pessoais de maior risco, em conformidade com a legislação e a regulamentação aplicáveis.

10.3 Compartilhamento com Terceiros

O compartilhamento de dados pessoais com terceiros:

- ocorrerá somente quando necessário, legítimo e amparado por base legal apropriada;
- será formalizado por contratos ou instrumentos equivalentes contendo cláusulas específicas de proteção de dados, segurança, confidencialidade, subcontratação, cooperação em incidentes e suporte ao exercício de direitos de titulares;
- será precedido de due diligence de privacidade e segurança para operadores que tratem dados de maior risco, podendo envolver questionários, relatórios de conformidade, certificações e outras evidências;
- será periodicamente reavaliado por meio de monitoramento, relatórios, auditorias ou revisões contratuais, conforme o risco.

Operadores somente poderão **subcontratar suboperadores** para tratamento de dados pessoais da Brphonia mediante autorização prévia e por escrito, devendo garantir que:

- o suboperador observe, no mínimo, o mesmo nível de proteção exigido ao operador principal;

- seja mantida lista atualizada dos suboperadores, disponível à Brphonia.

10.4 Retenção, Anonimização e Eliminação

- Os dados pessoais serão mantidos pelo tempo necessário ao cumprimento das finalidades do tratamento e das obrigações legais e regulatórias aplicáveis.
- A Brphonia manterá Tabela de Retenção de Dados Pessoais, na qual constarão:
 - categorias de dados e de titulares;
 - finalidades associadas;
 - prazos de retenção ou critérios para sua definição;
 - fundamentos legais dos prazos (normas legais, regulatórias ou contratuais, quando existentes).
- A Tabela de Retenção será controlada como documento vinculado a esta PPDP, com histórico de versões e revisão periódica.

Ao término do tratamento, aplicam-se, conforme o caso:

- eliminação segura dos dados;
- anonimização, para uso em estudos, estatísticas ou melhoria de serviços, após avaliação da irreversibilidade razoável e dos riscos de reidentificação;
- bloqueio ou arquivamento em ambiente de acesso restrito, quando exigido por lei ou para exercício de direitos.

Sempre que possível, serão priorizados o uso de dados anonimizados ou pseudonimizados para fins de análise, teste e desenvolvimento. A Brphonia realizará, quando necessário, análises de reversibilidade das técnicas de anonimização aplicadas em dados de alto risco e atualizará as medidas técnicas e organizacionais de proteção.

10.5 Uso de Canais de Comunicação e Mensageria Digital

O tratamento de dados pessoais e de dados pessoais sensíveis de clientes, colaboradores, terceiros e fornecedores deverá ocorrer exclusivamente por meio de canais e ferramentas corporativas ou expressamente autorizadas, em conformidade com esta PPDP, com a PSI e com a legislação aplicável.

É vedado o tratamento de dados pessoais por meio de contas ou aplicações de mensageria particular, ainda que acessadas ou instaladas em dispositivos corporativos, incluindo, entre

outras, WhatsApp pessoal, Telegram pessoal, Signal, Discord, Facebook Messenger, Instagram Direct e SMS/MMS pessoais.

Nos canais de mensageria particular é proibida qualquer forma de tratamento de dados, incluindo:

- coleta, envio, recebimento, troca, compartilhamento, encaminhamento, armazenamento ou exclusão de dados;
- gravação de áudio, envio de documentos ou compartilhamento de links que exponham dados pessoais;
- envio de fotografias, capturas de tela ou quaisquer registros que contenham dados pessoais relacionados às atividades da Brphonia.

As áreas de Tecnologia da Informação, Segurança da Informação e o Encarregado definirão e divulgarão, em alinhamento com a PSI, a lista de canais e ferramentas oficialmente autorizados para comunicação e tratamento de dados, bem como os controles aplicáveis. Alterações nessa lista serão formalmente registradas e comunicadas às áreas impactadas.

Exceções somente poderão ocorrer mediante processo formal de gestão de exceções e aceite de risco, com aprovação das instâncias competentes e definição de controles compensatórios.

O descumprimento das regras deste item constitui violação desta PPDP e da PSI, sujeitando o infrator às medidas disciplinares internas e às responsabilizações cabíveis.

11. DADOS SENSÍVEIS E DE CRIANÇAS/ADOLESCENTES

O tratamento de dados pessoais sensíveis será realizado apenas nas hipóteses previstas no art. 11 da LGPD, com aplicação de controles adicionais de segurança, tais como:

- acessos estritamente limitados e segregados;
- logs de acesso e monitoramento proporcional ao risco;
- pseudonimização e criptografia, sempre que tecnicamente viável;
- avaliações de risco e, quando cabível, RIPD.

A Brphonia **não realiza, em hipótese alguma, o tratamento de dados pessoais de crianças e adolescentes** no escopo da prestação de seus serviços a clientes ou ao público em geral. A única exceção para o tratamento de dados de menores de idade restringe-se aos filhos e dependentes de colaboradores, exclusivamente quando estritamente

necessário para a concessão de benefícios (tais como auxílio-creche, auxílio educacional e plano de saúde).

Nestes casos específicos de dependentes, o tratamento observará sempre o melhor interesse do menor, a transparência e, quando exigido, o consentimento específico de pelo menos um dos pais ou responsável legal, com esforços razoáveis de verificação da legitimidade.

12. COOKIES E TECNOLOGIAS DE RASTREAMENTO

A Brphonia poderá utilizar cookies e tecnologias similares (pixels, tags, SDKs) em seus sites, portais e aplicações para:

- autenticação e segurança;
- medição de audiência e estatísticas;
- melhoria da experiência do usuário;
- ações de marketing e personalização, quando cabível.

A Brphonia mantém Política de Cookies específica, documento público que:

- descreve os tipos de cookies utilizados, suas finalidades e prazos de retenção;
- indica as bases legais aplicáveis;
- fornece orientações para gestão de preferências de cookies pelos titulares.

O mecanismo de consentimento de cookies deverá:

- exibir banner em dois níveis, permitindo aceitar ou rejeitar cookies não estritamente necessários e gerenciar preferências;
- evitar “dark patterns” que dificultem a rejeição ou alteração de preferências;
- garantir que cookies não estritamente necessários somente sejam ativados após ação positiva do titular;
- registrar logs e evidências das escolhas dos titulares.

Os registros de preferências de cookies e de consentimento/revogação integrarão o sistema centralizado de gestão de consentimentos e poderão ser correlacionados, quando necessário, com outras manifestações do titular para fins de auditoria e atendimento de direitos.

Quando houver alteração relevante na Política de Cookies, nas categorias de cookies utilizados ou em suas finalidades, a Brphonia:

- reapresentará o banner de consentimento, permitindo revisão e renovação das preferências;
- registrará as alterações realizadas e os novos consentimentos obtidos, quando aplicável.

13. TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

Em transferências internacionais de dados pessoais, a Brphonia observará:

- as hipóteses dos arts. 33 a 36 da LGPD;
- o uso de mecanismos adequados, tais como:
 - decisões de adequação;
 - cláusulas contratuais específicas ou padrão compatíveis com a LGPD;
 - normas corporativas globais (BCRs), quando aplicáveis;
 - certificações, selos ou códigos de conduta reconhecidos;
 - consentimento específico e em destaque, quando cabível;
- o registro dessas transferências no ROPA, com indicação:
 - dos países ou organismos internacionais de destino;
 - do mecanismo jurídico utilizado;
 - das salvaguardas técnicas e organizacionais aplicáveis.

Os titulares poderão obter informações sobre transferências internacionais de seus dados por meio dos canais indicados nesta PPDP e nos Avisos de Privacidade, incluindo referência à lista atualizada de países ou organizações internacionais de destino, quando aplicável.

Antes de realizar transferências internacionais, a Brphonia:

- realizará due diligence de privacidade e segurança em relação ao importador de dados;
 - avaliará a legislação de proteção de dados do país de destino, quando for o caso;
 - manterá evidências dos instrumentos contratuais utilizados e das avaliações realizadas.
-

14. SISTEMAS AUTOMATIZADOS, PERFILHAMENTO E INTELIGÊNCIA ARTIFICIAL

A Brphonia poderá utilizar sistemas automatizados e técnicas de IA em atividades como:

- atendimento e suporte a clientes;
- análise de risco e prevenção a fraudes;
- monitoramento de redes e desempenho de serviços;
- classificação e priorização de chamados.

Quando houver decisões exclusivamente automatizadas que afetem interesses dos titulares de forma relevante, a Brphonia:

- avaliará previamente riscos, elaborando RIPD específico, quando cabível;
- prestará informações claras sobre a existência de decisões automatizadas, respeitados segredos comercial e industrial;
- possibilitará, nos casos previstos em lei, a revisão da decisão por pessoa natural;
- disponibilizará canal para contestação da decisão.

Serão adotadas medidas para identificar e mitigar eventuais vieses discriminatórios, em conformidade com os princípios da LGPD.

A Brphonia manterá metodologia documentada de **Avaliação de Impacto à Privacidade para sistemas de IA e decisões automatizadas**, contemplando:

- descrição do sistema, dos dados utilizados, das finalidades e do contexto de uso;
- análise de riscos específicos de discriminação e vieses algorítmicos;

- avaliação de impactos sobre direitos e liberdades dos titulares;
- definição de salvaguardas (por exemplo, revisões humanas, explicabilidade, limitação de uso);
- critérios de aceitação de riscos.

Sistemas que realizem decisões exclusivamente automatizadas que produzam efeitos relevantes sobre os titulares deverão:

- manter trilhas de auditoria (logs) suficientes para reconstruir decisões e principais entradas de dados;
- garantir prazos razoáveis para revisão humana de decisões contestadas;
- ser periodicamente reavaliados quanto a riscos, vieses e eficácia dos controles implementados.

15. DIREITOS DOS TITULARES E CANAIS DE ATENDIMENTO

Os titulares de dados pessoais podem exercer, nos termos da LGPD, os seguintes direitos:

- confirmação da existência de tratamento;
- acesso aos dados;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade;
- portabilidade de dados a outro fornecedor de serviço ou produto, observados segredos comercial e industrial e a regulamentação da ANPD;
- eliminação de dados pessoais tratados com base no consentimento, quando aplicável;
- informação sobre as entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

- revogação do consentimento;
- oposição a tratamento realizado com fundamento em hipóteses de dispensa de consentimento, em caso de descumprimento da LGPD;
- peticionamento em relação aos seus dados perante a ANPD, contra o controlador ou o operador;
- revisão de decisões automatizadas, nos casos previstos em lei.

15.1 Canais de Atendimento

A Brphonia disponibiliza canais específicos para o exercício dos direitos dos titulares, tais como:

- formulários eletrônicos ou seção própria em seu site institucional;
- endereço de e-mail institucional do Encarregado (DPO);
- outros canais indicados nos Avisos/Notas de Privacidade.

Existem, como documentos públicos vinculados a esta PPDP:

- Aviso de Privacidade para Clientes;
- Aviso de Privacidade para Colaboradores e Candidatos;
- outros Avisos específicos, conforme o contexto de tratamento.

Nos casos envolvendo dados de crianças e adolescentes, os direitos serão exercidos pelos pais ou responsáveis legais, com validação adequada de identidade e legitimidade.

Caso o titular não esteja satisfeito com a resposta inicial recebida, poderá registrar **reclamação interna** pelos mesmos canais, indicando o protocolo e os motivos de sua insatisfação. Haverá processo de escalonamento interno, com revisão por instância superior (por exemplo, Comitê de Privacidade ou Diretoria, conforme a gravidade), e resposta final ao titular em prazo razoável.

Nada nesta PPDP impede o titular de peticionar diretamente à ANPD em qualquer momento.

15.2 Prazos, Portabilidade e Evidências

A Brphonia se compromete a:

- fornecer **confirmação da existência de tratamento e acesso aos dados pessoais** em prazo máximo de 15 (quinze) dias, contados do recebimento da solicitação, em conformidade com a LGPD;
- responder às demais solicitações dos titulares em prazo razoável, buscando observar o mesmo prazo de 15 (quinze) dias, ressalvadas situações justificadas de maior complexidade, que serão comunicadas ao titular;
- analisar pedidos de portabilidade considerando a viabilidade técnica, a proteção de segredos comercial e industrial e as orientações da ANPD.

Enquanto a ANPD não publicar regulamento específico sobre portabilidade de dados pessoais, a Brphonia aplicará os entendimentos disponíveis em guias, notas técnicas e demais orientações oficiais, comprometendo-se a:

- revisar esta PPDP, as normas e os POPs de atendimento a titulares em prazo razoável após a publicação de regulamentação específica;
- adequar procedimentos, prazos e formatos de resposta às exigências então vigentes.

Todas as solicitações de titulares, bem como as decisões e respostas correspondentes, serão registradas em sistema ou ferramenta apropriada, constituindo evidências para auditorias e prestações de contas perante a ANPD e demais órgãos competentes.

16. GESTÃO DE TERCEIROS, OPERADORES E CO-CONTROLADORES

Terceiros que tratem dados pessoais em nome da Brphonia (operadores) deverão:

- ser submetidos a due diligence prévia de privacidade e segurança, proporcional ao risco do tratamento;
- celebrar contratos ou instrumentos equivalentes com cláusulas específicas de proteção de dados, segurança da informação, confidencialidade, subcontratação, cooperação em incidentes e suporte a direitos de titulares e à ANPD;
- adotar medidas de segurança compatíveis com os riscos das operações sob sua responsabilidade;
- cooperar com a Brphonia em auditorias, incidentes, elaboração de RIPD (quando aplicável) e atendimento a solicitações de titulares.

A Brphonia manterá modelos padronizados de cláusulas contratuais para operadores, a serem utilizados como referência nas contratações.

Nos casos de co-controladoria, as responsabilidades das partes serão formalizadas por escrito, incluindo:

- finalidades e bases legais do tratamento;
- delimitação de responsabilidades por atendimento a titulares;
- responsabilidades perante a ANPD;
- responsabilidades pela comunicação e gestão de incidentes e pela guarda de evidências.

A Brphonia manterá modelo padronizado de instrumento para situações de co-controladoria, que deverá ser utilizado como referência na construção de acordos específicos, reduzindo riscos jurídicos e operacionais.

Serão realizadas, de forma periódica, avaliações de conformidade de operadores e co-controladores, por meio de relatórios, evidências, auditorias ou outros mecanismos adequados ao risco. A periodicidade e profundidade dessas avaliações serão definidas a partir de critérios de risco estabelecidos pelo Comitê de Privacidade e revisados anualmente.

17. SEGURANÇA DA INFORMAÇÃO APLICADA À PROTEÇÃO DE DADOS

A Brphonia integra a proteção de dados pessoais à sua Política de Segurança da Informação e Cibersegurança (PSI) e ao seu Sistema de Gestão de Segurança da Informação (SGSI), adotando medidas proporcionais ao risco, tais como:

- gestão de identidades e acessos (IAM), com concessão baseada em papéis, necessidade de conhecimento e revisão periódica de privilégios;
- autenticação forte, quando apropriado;
- criptografia de dados em trânsito e em repouso, quando aplicável;
- segmentação de redes, controle de perímetro e filtragem de tráfego;
- proteção reforçada de ativos core de rede e sistemas críticos;
- geração, retenção e monitoramento de logs de acesso a dados pessoais e registros de conexão, em conformidade com o Marco Civil da Internet, a regulamentação da Anatel e a LGPD;
- backups periódicos, testes de restauração e planos de continuidade de negócios;

- gestão de vulnerabilidades, aplicação de correções e realização de testes de segurança;
- descarte seguro de mídias, equipamentos e documentos.

Sempre que tecnicamente viável e proporcional ao risco, a Brphonia adotará:

- criptografia forte para dados em repouso (por exemplo, AES-256 ou equivalente) em bases e repositórios que armazenam dados pessoais de alto risco;
- protocolos seguros para dados em trânsito (por exemplo, TLS 1.2 ou superior, com configurações atualizadas de segurança);
- práticas adequadas de gestão de chaves criptográficas, alinhadas à PSI.

Sempre que possível, serão priorizados o uso de dados anonimizados ou pseudonimizados para fins de análise, teste e desenvolvimento.

18. GESTÃO DE INCIDENTES E VAZAMENTOS

Qualquer suspeita ou ocorrência de incidente de segurança envolvendo dados pessoais deverá ser comunicada imediatamente por meio dos canais internos definidos. Recomenda-se que esta comunicação ocorra, preferencialmente, em até 24 (vinte e quatro) horas após a ciência do fato pelo colaborador ou terceiro.

A Brphonia manterá normas e POPs específicos para gestão de incidentes envolvendo dados pessoais, prevendo:

- identificação, classificação e registro dos incidentes;
- ações de contenção, erradicação e recuperação;
- avaliação de risco e impacto aos titulares e à organização;
- definição e implementação de ações corretivas e preventivas;
- critérios para comunicação à ANPD e aos titulares, nos termos do art. 48 da LGPD e do RCIS;
- documentação e guarda de evidências.

Quando o incidente preencher os critérios do Regulamento de Comunicação de Incidentes de Segurança (RCIS), a Brphonia:

- realizará comunicação preliminar à ANPD em até 3 (três) dias úteis contados do conhecimento do incidente;
- apresentará informações complementares em até 20 (vinte) dias úteis, ou outro prazo definido pela ANPD, contendo os dados exigidos pelo RCIS;
- avaliará a necessidade de comunicação individualizada aos titulares afetados, em linguagem clara e acessível, indicando riscos decorrentes e medidas de mitigação recomendadas.

Todas as decisões relativas à classificação do incidente, à necessidade de comunicação e às medidas adotadas deverão ser devidamente registradas.

19. TREINAMENTO, CONSCIENTIZAÇÃO E CULTURA DE PRIVACIDADE

A Brphonia promoverá:

- treinamentos periódicos em proteção de dados pessoais, LGPD, segurança da informação e uso adequado de tecnologias, inclusive IA, direcionados aos diferentes públicos internos;
 - ações de conscientização, como campanhas, comunicados, cartilhas e materiais educativos;
 - treinamentos específicos para colaboradores que atuem em operações de tratamento de maior risco;
 - registro da participação em treinamentos, para fins de evidência junto a auditorias e órgãos reguladores.
-

20. CONFORMIDADE, AUDITORIA E MELHORIA CONTÍNUA

O cumprimento desta PPDP poderá ser verificado por meio de:

- auditorias internas e, quando aplicável, externas;
- revisões integradas com o SGSI e eventuais processos de certificação;
- monitoramento de indicadores de desempenho e risco (KPIs/KRIs), como:
 - número e gravidade de incidentes com dados pessoais;

- prazos médios de resposta às solicitações de titulares;
- percentual de colaboradores treinados em privacidade e segurança;
- atualização do ROPA e dos RIPDs;
- implementação de planos de ação em privacidade.

Além disso, a Brphonia manterá metodologia para avaliar a **eficácia dos controles de privacidade**, incluindo:

- definição de metas e critérios de sucesso para os controles implementados;
- realização de testes de amostragem sobre processos-chave (como atendimento a titulares, gestão de consentimentos, execução de LIAs e RIPDs, due diligence de terceiros);
- registro estruturado dos resultados, das não conformidades identificadas e dos planos de ação;
- apresentação de relatórios periódicos à Diretoria Executiva, ao DPO e ao Comitê de Privacidade.

Os resultados dessas avaliações subsidiarão ações de melhoria contínua desta PPDP, da PSI e dos processos correlatos.

21. EXCEÇÕES À POLÍTICA

21.1 Processo Formal de Exceções

Exceções à PPDP, às normas e aos POPs associados devem:

- ser solicitadas formalmente, com descrição do escopo, justificativa e análise de risco;
- indicar prazos de vigência pretendidos e controles compensatórios;
- ser avaliadas pelo DPO, pelo gestor responsável e, quando aplicável, pela Diretoria Executiva.

21.2 Aprovação e Registro

Exceções aprovadas:

- serão registradas em repositório apropriado, com identificação do solicitante, aprovadores, prazo de validade e controles associados;
- serão comunicadas às áreas impactadas, com orientações claras sobre sua aplicação.

21.3 Revisão Periódica das Exceções

As exceções serão revisadas periodicamente, em conjunto com o processo de gestão de riscos da PSI, podendo ser:

- renovadas, com nova avaliação de risco;
 - ajustadas, com alteração de escopo ou controles;
 - revogadas, reintegrando os processos à plena conformidade.
-

22. REVISÃO, ATUALIZAÇÃO E VIGÊNCIA DA POLÍTICA

22.1 Periodicidade de Revisão

Esta PPDP será revisada:

- ordinariamente, em periodicidade não superior a 24 (vinte e quatro) meses contados da última aprovação;
- extraordinariamente, sempre que houver alterações relevantes na legislação, na regulamentação, nas orientações da ANPD, na estrutura organizacional, nos processos ou nas tecnologias que impactem o tratamento de dados pessoais;
- após incidentes relevantes ou auditorias que evidenciem a necessidade de ajustes;
- sempre que avaliações de eficácia dos controles de privacidade indicarem a necessidade de revisão.

22.2 Controle de Versões

O controle de versões desta PPDP será mantido no início do documento, registrando:

- data da aprovação;

- número da versão;
- descrição das principais alterações realizadas;
- responsável pela atualização.

22.3 Vigência

Esta versão da Política de Proteção de Dados Pessoais entra em vigor a partir de sua aprovação pela Diretoria Executiva da Brphonia e revoga integralmente as versões anteriores.