SAÚDE BRB	**POLÍTICA** Privacidade e Proteção de Dados	Revisão:	02
		Página:	1/21
		C.I.	#10

Alçadas	
Elaboração	Assessoria Técnica [ASTEC - Segurança e Privacidade]
Validação	Superintendência [DISUP]
Aprovação	Órgão Executivo [OEX] e Conselho Deliberativo [CONDE]

Revisão	**Aprovação**	**Revisões[1]**
00	27/11/2020	Aprovada em 1ª instância pelo Órgão Executivo, em sua 83ª reunião ordinária, revogadas disposições em contrário.
	16/12/2020	Aprovada em 2ª instância pelo Conselho Deliberativo, em sua 82ª reunião extraordinária, revogadas disposições em contrário.
01	31/05/2021	Aprovada em 1ª instância pelo Órgão Executivo, em sua 89ª reunião ordinária, revogadas disposições em contrário.
	05/07/2021	Aprovada em 2ª instância pelo Conselho Deliberativo, em sua 58ª reunião ordinária, revogadas disposições em contrário.
02	15/10/2025	Aprovada em 1ª instância pelo Órgão Executivo, em sua 142ª reunião ordinária, revogadas disposições em contrário.
	04/12/2025	Aprovada em 2ª instância pelo Conselho Deliberativo, em sua 76ª reunião ordinária, revogadas disposições em contrário.

[1] Registros alterados – consultar Anexo 1

SAÚDE BRB	**POLÍTICA** Privacidade e Proteção de Dados	Revisão:	02
		Página:	2/21
		C.I.	#10

SUMÁRIO

1. INTRODUÇÃO

Esta Política tem como objetivo estabelecer princípios, diretrizes e responsabilidades em relação à proteção de dados pessoais e foi formulada tendo como referência a Missão, a Visão e os Valores Corporativos da Saúde BRB – Caixa de Assistência.

2. OBJETIVOS

2.1. Estabelecer as diretrizes e os princípios associados à privacidade e proteção de dados pessoais, observando leis, boas práticas de gestão e regulamentações aplicáveis.

2.2. Fortalecer a cultura de riscos, controle internos e conformidade pertinentes à privacidade e proteção de dados pessoais, com vistas a ratificar a geração de valor, a sustentabilidade do negócio, a perenidade da Caixa de Assistência e o cumprimento de sua missão institucional.

2.3. Esta Política foi formulada tendo como referência a Missão, a Visão e os Valores Corporativos da Saúde BRB e tem também como objetivo promover a conformidade dos processos e atividades internas com a legislação e as melhores práticas relativas à proteção de dados pessoais.

3. APLICAÇÃO

Esta Política se aplica à Saúde BRB e à Clínica Saúde BRB, em consonância com as melhores práticas de governança corporativa, devendo ser cumprida, no limite de suas atribuições, pelos colaboradores[2],, fornecedores, prestadores de serviços, parceiros, beneficiários, demais partes relacionadas, pessoas que tenham acesso a quaisquer dados pessoais sob a responsabilidade da Saúde BRB, em seu nome ou de terceiros, com especial atenção por aqueles profissionais alocados em áreas que possuem relacionamento com beneficiários, fornecedores e prestadores de serviço.

Nota 1 - Consultar [Anexo 2 – Cadeia de Valor]

4. PÚBLICO ALVO

As diretrizes e regras deste normativo destinam-se aos colaboradores[2], independentemente de cargo ou função exercidos, bem como aos administradores da Caixa de Assistência, compreendidos aqui os membros do Conselho Deliberativo [CONDE], Conselho Fiscal [CONFI] e o Órgão Executivo [OEX].

Esta Política estabelece as orientações gerais para a proteção de dados pessoais e sensíveis no ambiente corporativo, de beneficiários, fornecedores e parceiros no Brasil e no exterior, uma vez que na execução de suas operações coleta, manuseio e armazenamento de informações que podem estar relacionadas a pessoas naturais identificadas e/ou identificáveis, com vistas a:

[2] Consultar item 5. Definições

4.1. Estar em conformidade com as leis e regulamentações aplicáveis de proteção de dados pessoais, e seguir as melhores práticas;

4.2. Proteger os direitos dos empregados da Instituição, beneficiários, fornecedores e parceiros contra os riscos de violações de dados pessoais;

4.3. Ser transparente em relação aos procedimentos da Saúde BRB no Tratamento de dados pessoais; e

4.4. Promover a conscientização do público interno sobre a proteção de dados pessoais e questões de privacidade.

Em particular, esta política exige que a equipe garanta que o DPO [Data Protection Officer] ou Encarregado de Proteção de Dados seja consultado antes que qualquer nova atividade significativa de processamento de dados seja iniciada para garantir que as etapas de conformidade relevantes sejam tratadas.

5. REFERÊNCIAS

- Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais, que define as normas e procedimentos para o tratamento de dados pessoais [LGPD].
- Resolução CD/ANPD nº 1/2021 - aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador.
- Resolução CD/ANPD nº 4/2023 - aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas.
- Resolução CD/ANPD nº 15/2024 - aprova o Regulamento de Comunicação de Incidente de Segurança [RCIS], que define os procedimentos para a comunicação de incidentes de segurança de dados pessoais.
- Resolução CD/ANPD nº 18/2024 - aprova o regulamento sobre as diretrizes para atuação do Encarregado pelo Tratamento de Dados Pessoais [DPO] no Brasil.
- Resolução CD/ANPD Nº 19/2024 - aprova o regulamento que estabelece os procedimentos e as regras para a transferência internacional de dados pessoais no Brasil.
- Resolução Normativa ANS - RN nº 518/2022 - dispõe sobre adoção de práticas mínimas de governança corporativa, com ênfase em controles internos e gestão de riscos, para fins de solvência das operadoras de planos de assistência à saúde.
- ISO 27001 - Sistema de Gestão de Segurança da Informação – norma para implementação de um sistema de gestão com foco em segurança da informação.
- ISO 27701 – Sistema de Gestão de Segurança Privada – extensão da ISO 27001, tem como objetivo adicionar novos controles no sistema de gestão para garantir a total privacidade especificamente dos dados pessoais.
- Estatuto.

- Código de Ética e Conduta Corporativa.
- Política de Integridade.
- Política de Segurança da Informação.
- Regulamento Organizacional.

6. DEFINIÇÕES

- Agentes de tratamento - o controlador e o operador.
- 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.
- Avaliação de Impacto à Privacidade [AIP] ou Privacy Impact Assessment [PIA] - análise dos riscos de privacidade associados ao tratamento de informações pessoais em relação ao projeto, produto ou serviço. Sugere ou fornece ações de remediação ou mitigações necessárias para evitar ou reduzir/minimizar esses riscos.
- Banco de dados - conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- Bloqueio - suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.
- Cibersegurança - prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra-ataques maliciosos. Também é chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas.
- Colaborador - pessoa natural, que tenha vínculo empregatício com a organização [empregado efetivo ou temporário, ocupantes de cargos ou funções de confiança], pessoas contratadas em regime temporário, estagiários, aprendizes, prestador de serviços, mediante contrato firmado com empresa interposta [serviços terceirizados] e consultor.
- Consentimento - manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
- Controlador - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- Dado anonimizado - dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- Dado pessoal - informação relacionada à pessoa natural identificada ou identificável.
- Dado pessoal de criança e de adolescente - o Estatuto da Criança e do Adolescente [ECA] considera criança a pessoa até 12 anos de idade incompletos e adolescente aquela entre 12 e 18 anos de idade. Em especial, a LGPD determina que as informações sobre o tratamento de dados pessoais de crianças e de adolescentes deverão ser fornecidas de maneira simples, clara e acessível de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

- Dado pessoal sensível - dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- Eliminação - exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
- Encarregado de Dados - agente [PF ou PJ] indicado pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados [ANPD].
- Garantia da segurança da informação - capacidade de sistemas e organizações assegurarem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.
- Garantia da segurança de dados - ver garantia da segurança da informação
- Interoperabilidade - capacidade de sistemas e organizações operarem entre si. A ANPD poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, além dos padrões de interoperabilidade do governo eletrônico [ePING].
- Operador - pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador
- Privacidade desde a concepção [Privacy by Design] – aplicação pelo agente de tratamento, de medidas técnicas e organizacionais adequadas, como a pseudonimização, tanto no momento de definição dos meios de tratamento, como no momento do próprio tratamento.
- Privacidade por padrão [Privacy by Default] - utilização de medidas técnicas e organizacionais para assegurar que, por padrão, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento.
- Relatório de impacto à proteção de dados pessoais - documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
- Relatório de Impacto de Proteção de Dados [RIPD] ou Data Protection Impact Assessment [DPIA] – relatório elaborado antes de determinado tratamento em determinadas operações de risco elevado como, por exemplo, situações que envolvem dados sensíveis e que deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.
- Segregação de funções - consiste na separação entre as funções de autorização, aprovação de operações, execução, controle e contabilização, de maneira que nenhum colaborador, visitante, estagiário ou prestador de serviços, detenha poderes e atribuições em desacordo com este princípio, ou conflitantes entre si.
- Titular - pessoa natural a quem se referem os dados pessoais que são objeto de tratamento Transferência internacional de dados.

- Transferência internacional de dados - transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.
- Tratamento - toda operação realizada com dados pessoais, tais como:
  - Acesso - possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo etc.; visando receber, fornecer, ou eliminar dados;
  - Armazenamento - ação ou resultado de manter ou conservar em repositório um dado;
  - Arquivamento - ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotada a sua vigência;
  - Avaliação - ato ou efeito de calcular valor sobre um ou mais dados;
  - Classificação - maneira de ordenar os dados conforme algum critério estabelecido;
  - Coleta - recolhimento de dados com finalidade específica;
  - Comunicação - transmitir informações pertinentes a políticas de ação sobre os dados;
  - Controle - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
  - Difusão - ato ou efeito de divulgação, propagação, multiplicação dos dados;
  - Distribuição - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
  - Eliminação - ato ou efeito de excluir ou destruir dado do repositório;
  - Extração - ato de copiar ou retirar dados do repositório em que se encontrava
  - Modificação - ato ou efeito de alteração do dado;
  - Processamento - ato ou efeito de processar dados;
  - Produção - criação de bens e de serviços a partir do tratamento de dados;
  - Recepção - ato de receber os dados ao final da transmissão;
  - Reprodução - cópia de dado preexistente obtido por meio de qualquer processo;
  - Transferência - mudança de dados de uma área de armazenamento para outra, ou para terceiro;
  - Transmissão - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.;
  - Utilização - ato ou efeito do aproveitamento dos dados.
- Uso compartilhado de dados - comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

7. SIGLAS

- ANPD – Agência Nacional de Proteção de Dados.
- ANS – Agência Nacional de Saúde Suplementar.
- GT-PTDI - Grupo de Trabalho de Privacidade, Transformação Digital, e Inovação.

8. ÁREAS ENVOLVIDAS

- Conselho Deliberativo [CONDE]
- Conselho Fiscal [CONFI]
- Órgão Executivo [OEX]
- Assessoria Técnica [ASTEC]
- Setor de Tecnologia da Informação [SETIN]
- Unidades Organizacionais

Nota 2 - Consultar [Anexo 1 – Organograma]

9. PRINCÍPIOS

A Saúde BRB resguarda os seguintes princípios de privacidade de dados pessoais:

- Adequação – os dados coletados pela organização devem ser usados de forma condizente com o que foi informado e permitido pelo titular;
- Finalidade: a Saúde BRB deverá comunicar, de forma clara e tempestiva, as destinações dos dados pessoais coletados.
- Livre acesso: o proprietário dos dados deve ter pleno acesso a informações sobre a forma como as suas informações estão sendo tratadas;
- Não-discriminação: nunca, em qualquer hipótese que seja, haverá discriminação ou abuso contra o titular com base no tratamento de seus dados;
- Necessidade – os dados pessoais do titular coletados pelo controlador devem ser específicos e suficientes para a finalidade, sendo impositivo que esta esteja claramente definida;
- Prevenção: a Instituição deve estar apta para resolver quaisquer problemas com os dados de forma antecipada, no intuito de evitar ônus a si e ao titular;
- Qualidade: diz respeito à clareza, exatidão, relevância e atualização dos dados utilizados pela Saúde BRB;
- Responsabilização e prestação de contas: a Caixa de Assistência é responsável pela adoção de medidas que comprovem boa-fé e diligência relacionadas à proteção de dados;
- Segurança: consiste na garantia de confidencialidade prestada pela Organização sobre os dados dos proprietários;

- Transparência - a organização deve prestar informações claras e precisas obre as atividades relativas aos dados pessoais, bem como estar acessível para esclarecimentos e atendimento de demandas do titular;

10. DIRETRIZES

As seguintes diretrizes norteiam a governança e privacidade de dados pessoais na Saúde BRB:

10.1. Garantir ao titular a escolha de permitir ou não o tratamento de seus dados pessoais, excetuando-se casos em que a lei aplicável permitir especificamente o processamento de dados pessoais sem o consentimento do titular;

10.2. Garantir que o objetivo do tratamento de dados pessoais esteja em conformidade com a legislação vigente e de acordo com uma base legal permitida;

10.3. Comunicar, de forma clara e adequadamente adaptada às circunstâncias, o tratamento de dados pessoais ao titular, antes do momento em que eles sejam coletados ou usados pela primeira vez para um novo propósito;

10.4. Fornecer ao titular, sempre que necessário, explicações suficientes sobre o tratamento de seus dados pessoais, conforme previsto na legislação vigente;

10.5. Aplicar a privacidade por padrão [Privacy by Default], limitando a coleta de dados pessoais estritamente ao que é permitido pela legislação vigente e em conformidade com o consentimento do titular, minimizando, quando possível;

10.6. Limitar o uso, retenção, divulgação e transferência de dados pessoais ao necessário para cumprir com objetivos específicos, explícitos e legítimos;

10.7. Reter dados pessoais apenas pelo tempo necessário ao cumprimento dos propósitos declarados e, posteriormente, destruí-los, bloqueá-los ou anonimizá-los com segurança;

10.8. Bloquear o acesso a dados pessoais, e não realizar qualquer tratamento quando os propósitos declarados expirarem, mas reter os dados pessoais quando for exigido pela legislação vigente;

10.9. Garantir a precisão e qualidade dos dados pessoais tratados, excetuando-se casos em que exista base legal para manter dados desatualizados;

10.10. Fornecer, aos titulares dos dados pessoais tratados, informações claras e facilmente acessíveis sobre as políticas, procedimentos e práticas com relação ao tratamento de dados pessoais realizado pela Organização, incluindo os dados que são efetivamente tratados, a finalidade desse tratamento e informações sobre como entrar em contato para obter informações adicionais;

10.11. Notificar titulares, quando ocorrerem alterações significativas no tratamento dos seus dados pessoais;

10.12. Garantir que titulares tenham a possibilidade de acessar e revisar seus dados pessoais, desde que sua identidade seja autenticada com nível apropriado de garantia e que não haja qualquer restrição legal a esse acesso ou a revisão dos seus dados pessoais;

10.13. Garantir a rastreabilidade e prestação de contas durante o tratamento de dados pessoais, inclusive quando esses forem compartilhados com terceiros;

10.14. Tratar integralmente de violações de dados, garantindo que sejam adequadamente registradas, classificadas, investigadas, corrigidas e documentadas;

10.15. Garantir que, na ocorrência de violação de dados, as partes interessadas sejam notificadas, conforme requisitos e prazos previstos na legislação vigente;

10.16. Documentar e comunicar, conforme apropriado, as políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados;

10.17. Definir responsável por documentar, implementar e comunicar políticas, procedimentos e práticas relacionadas à privacidade e proteção de dados;

10.18. Adotar controles de segurança da informação, tanto técnicos quanto administrativos, suficientes para garantir níveis de proteção adequados para dados pessoais;

10.19. Disponibilizar políticas, normas e procedimentos sobre proteção de dados pessoais às partes interessadas e autorizadas, tais como: empregados, terceiros contratados, e, onde pertinente, de parceiros e beneficiários;

10.20. Garantir a educação continuada e a conscientização de empregados e, onde pertinente, de parceiros, beneficiários e terceiros contratados sobre as práticas de proteção de dados pessoais adotadas pela Saúde BRB;

10.21. Aprimorar, de forma contínua, a gestão de proteção de dados pessoais, por meio da definição e revisão sistemática dos objetivos de privacidade e de proteção de dados pessoais em todos os níveis da Instituição;

10.22. Garantir a não discriminação no tratamento de dados pessoais, impossibilitando que sejam usados para fins discriminatórios, ilícitos ou abusivos;

10.23. Garantir a conformidade integral com leis e regulamentações de proteção de dados pessoais;

10.24. Tratar os dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, assim como o livre desenvolvimento da personalidade da pessoa natural;

10.25. Adotar a privacidade desde a concepção [Privacy by Design] o que importa na aplicação de medidas para garantir que as regras de privacidade e proteção de dados sejam cumpridas ao implementar processos, procedimentos ou sistemas que envolvam tratamento de dados pessoais, desde a fase de concepção até o lançamento/implantação de cada projeto.

11. DIREITOS DOS TITULARES DE DADOS PESSOAIS

A Saúde BRB está comprometida com os direitos dos titulares de dados pessoais, quais sejam:

11.1. Ser informado de como serão tratados os seus dados pessoais coletados e sob a guarda da Saúde BRB;

11.2. Possibilitar o acesso aos seus dados pessoais sob a guarda da Saúde BRB;

11.3. Corrigir os seus dados pessoais se estiverem imprecisos, incorretos ou incompletos;

11.4. Excluir, bloquear e/ou anonimizar seus dados pessoais em determinadas circunstâncias ["direito de ser esquecido"]. Isso pode incluir, mas não se limita às circunstâncias em que não é mais necessário que a Saúde BRB retenha seus dados pessoais para os propósitos para os quais foram coletados;

11.5. Restringir o tratamento de seus dados pessoais em determinadas circunstâncias;

11.6. Opor-se ao tratamento dos seus dados pessoais, caso seja baseado em legítimo interesse;

11.7. Revogar o consentimento a qualquer momento;

11.8. Possibilitar a portabilidade dos seus dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa;

11.9. Revisar as decisões tomadas unicamente com base em tratamento automatizado de dados pessoais; e

11.10. Apresentar queixa à Saúde BRB ou à Agência Nacional de Proteção de Dados, caso suspeite que qualquer um de seus direitos de proteção de dados pessoais tenha sido violado.

12. RESPONSABILIDADES

13.1. Órgão Executivo - [OEX]

I. Assegurar que a Política de Privacidade Corporativa seja aderente aos objetivos estratégicos da Saúde BRB.

II. Assegurar que esta Política de Privacidade Corporativa e normas correlatas sejam efetivamente cumpridas.

III. Ter comprometimento com as diretrizes de privacidade e atuar como agente mobilizador para o cumprimento dos dispositivos desta Política.

IV. Prover os recursos necessários para o cumprimento das diretrizes desta Política de Privacidade Corporativa.

V. Implementar controles internos - normativos e reportes sistematizados periódicos ao [OEX] que documentem processos e procedimentos e evidenciem a gestão adequada das atividades relacionadas à proteção de dados pessoais.

13.2. Diretor-Superintendente, Gerentes, Coordenadores e Supervisores

I. Assegurar que os subordinados estejam conscientizados da importância das boas práticas de privacidade de dados em suas rotinas de trabalho e demandar ao [SETAD] as capacitações adequadas às responsabilidades inerentes aos cargos que ocupam, incluindo aspectos relevantes da legislação, regulamentos e contratos, dentre outros.

II. Segregar as funções de aprovação de operações, execução e controle na equipe subordinada, de modo que nenhuma pessoa possa ter completa autoridade sobre uma parcela significativa de qualquer processo.

III. Assegurar que as permissões de acesso aos sistemas dos seus colaboradores estejam registradas, controladas e aderentes às atribuições dos cargos que ocupam.

IV. Acompanhar o cumprimento dessa Política e das normas internas correlatas, bem como assegurar que os riscos corporativos, em suas unidades organizacionais, estejam avaliados e controlados adequadamente.

V. Orientar suas equipes sobre o uso adequado de dados pessoais manuseados na Saúde BRB.

VI. Comunicar à [ASTEC - Segurança e Privacidade] e ao [SETIN] os casos de descumprimento de Políticas, Normas ou Procedimentos internos, e os casos de falhas na execução de atividades operacionais.

VII. Prover informações necessárias para a identificação e tratamento de riscos relacionados à privacidade de dados.

13.3. Assessoria Técnica - [ASTEC - Segurança e Privacidade]

I. Avaliar, sob o aspecto jurídico e regulatório, os riscos relacionados à privacidade de dados e a suficiência dos controles identificados nos incidentes de segurança da informação e reportar às instâncias competentes, provendo suporte nas eventuais ações preventivas e/ou corretivas.

II. Assessorar, sob o aspecto jurídico e regulatório, quanto à identificação, planejamento e coordenação de programas para melhoria das atividades relacionadas à proteção de dados pessoais, implementando e aprimorando os processos e controles.

III. Prover consultoria e suporte às unidades organizacionais para quaisquer requerimentos de privacidade, propor controles apropriados e verificar a implementação, manutenção e operação destes controles.

IV. Orientar novos colaboradores, sobre suas responsabilidades e as diretrizes e regras definidas nesta Política e normas internas correlatas.

V. Desenvolver e implementar, em conjunto com o [SETIN], programas periódicos de capacitação e conscientização para os colaboradores sobre privacidade e proteção de dados

VI. Monitorar, em conjunto com o [SETIN], o cumprimento desta Política de Privacidade Corporativa e normas correlatas.

VII. Assegurar que nos contratos celebrados pela Saúde BRB estejam presentes cláusulas de sigilo e confidencialidade que reflitam os princípios e normatizações aqui dispostas, quando cabível.

VIII. Revisar periodicamente as regras de privacidade corporativa estabelecidas e propor alterações.

13.4. Setor de Tecnologia da Informação - [SETIN]

I. Propor soluções para monitoração da utilização dos recursos tecnológicos disponibilizados aos usuários, para que o tratamento dos dados seja realizado adequadamente.

II. Definir e configurar equipamentos e aplicativos para correta utilização dos recursos tecnológicos, atentando, inclusive, para que os requisitos de segurança e privacidade sejam aplicados e os respectivos controles estejam adequadamente implementados, operados e mantidos de acordo com esses padrões.

III. Monitorar, em conjunto com a [ASTEC - Segurança e Privacidade], o cumprimento desta Política de Privacidade Corporativa e normas correlatas.

IV. Propor ações para melhoria da cibersegurança com vistas à otimização dos recursos alocados em ativos de informação, projetos, processos de negócio e proteção dos dados.

V. Homologar os recursos tecnológicos, de forma a garantir segurança da informação, considerando a privacidade por padrão, atentando sempre os princípios e diretrizes estabelecidos nesta Política.

VI. Monitorar impactos na segurança e de privacidade do ambiente tecnológico quando da alteração ou inclusão de recursos, ou decorrentes da aquisição de serviços e ativos da informação, emitindo parecer sobre as necessidades de adequação dos mesmos antes de iniciarem suas operações.

VII. Manter registros e documentação relativos à cibersegurança em nível corporativo, incluindo um banco de dados de riscos e assuntos de segurança tecnológica e privacidade.

VIII. Detectar, identificar e registrar violações, ou tentativas de acessos relevantes e significativas não autorizadas, para tomada de providências corretivas, legais e de auditoria.

IX. Monitorar os acessos visando verificar: vazamento de informações, acessos ou tentativas de acessos a sites com conteúdo inadequado, repasse de conteúdo inadequado, tentativa de quebra de controles de segurança da informação e privacidade dos dados e armazenamento de arquivos multimídia.

X. Restringir e controlar os acessos e os privilégios de usuários dos ativos de informação, incluindo os aqueles com privilégios de acesso remoto e externo, para que o tratamento dos dados seja realizado apenas por quem de direito.

XI. Registrar formalmente todos os incidentes de segurança da informação identificados e/ou reportados, facilitando a identificação e tratamento dos incidentes envolvendo dados pessoais.

XII. Encaminhar, para ciência da [ASTEC - Segurança e Privacidade], os incidentes de segurança da informação identificados e/ou reportados, facilitando a identificação e tratamento dos incidentes envolvendo dados pessoais.

XIII. A qualquer tempo, efetivar a restrição, bloqueio, suspensão e/ou cancelamento de acessos e/ou tecnologias [hardware e/ou software] que estejam infringindo as políticas de segurança, como também nos casos em que sejam verificados incidentes de segurança ou que haja identificação de vulnerabilidades.

XIV. Manter registros atualizados de solicitações, permissões, alterações e cancelamentos de acessos de usuários de ativos de informação.

XV. Nos casos de remanejamento interno de usuários, providenciar tempestivamente a adequação dos acessos a dados pessoais permitidos e, nos processos de demissão, providenciar tempestivamente o cancelamento dos acessos a dados pessoais permitidos ao usuário desligado.

13.5. Público Interno:

I. Ler, compreender e cumprir fielmente a Política de Privacidade Corporativa e as normas correlatas, como também quaisquer outras leis ou normas aplicáveis.

II. Proteger os dados pessoais contra acessos, modificação, destruição ou divulgação não autorizada pela Saúde BRB.

III. Fazer uso adequado dos dados pessoais manuseados no exercício de suas atribuições, de forma que sejam utilizados exclusivamente para as finalidades definidas pela Saúde BRB.

IV. Em lugares públicos, áreas expostas, blogs, sites e redes sociais, observar o sigilo profissional sobre as informações a que tem acesso na Caixa de Assistência, em especial aquelas que possam ensejar riscos relacionados à privacidade de indivíduos e à reputação da Instituição.

V. Comunicar, por meio do e-mail lgpd@saudebrb.com.br qualquer descumprimento ou violação desta Política e de normas correlatas, ou qualquer evento que possa trazer impactos na proteção de dados pessoais.

13. ENCARREGADO DE DADOS

O [OEX] designará o agente responsável para atuar como canal de comunicação entre a Caixa de Assistência, os titulares dos dados e a ANPD.

São atribuições do Encarregado de Dados:

I. Acolher reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.

II. Receber comunicações da ANPD e adotar providências.

III. Orientar os empregados e os contratados da Instituição a respeito das práticas e serem tomadas em relação à proteção de dados pessoais.

IV. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

V. Conduzir, em conjunto com o Grupo de Trabalho de Privacidade, Transformação Digital e Inovação, o Programa de Governança em Privacidade da Saúde BRB, zelando pela sua fiscalização;

VI. Monitorar o cumprimento das legislações de proteção de dados pessoais aplicáveis, de acordo com as políticas da Saúde BRB;

VII. Orientar os destinatários desta Política quanto ao regime de privacidade e proteção de dados pessoais da Saúde BRB;

VIII. Assegurar que as regras e orientações relativas à proteção de dados sejam informadas e incorporadas nas rotinas e práticas da Saúde BRB;

IX. Organizar treinamentos sobre proteção de dados pessoais na Saúde BRB;

X. Prestar esclarecimentos, oferecer informações e apresentar relatórios sobre as operações de tratamento de dados pessoais e seus impactos para as autoridades públicas competentes;

XI. Responder às solicitações e reclamações de titulares de dados pessoais cujos dados tenham sido objeto de tratamento por uma unidade da Saúde BRB.

XII. Auxiliar em auditorias ou qualquer outra medida de avaliação e monitoramento envolvendo proteção de dados.

XIII. Elaborar os relatórios de impacto à privacidade e proteção de dados, pareceres técnicos e revisão de documentos no que se refere à proteção de dados.

XIV. Outras atribuições a serem definidas no Termo de Nomeação do Encarregado.

O encarregado de dados será contatado por meio do canal exclusivo instituído para acolher manifestações dos titulares dos dados pessoais, no Portal na Internet ou por mensagem eletrônica para lgpd@saudebrb.com.br.

14. REGRAS DE CONSEQUÊNCIAS

O descumprimento ou infrações que configurem os ilícitos previstos na presente Política, darão ensejo a procedimento disciplinar, observando a gravidade da infração de acordo com o Código de Ética e Conduta Corporativa e o Regimento Interno do Comitê de Ética e Conduta Corporativa.

15. GESTÃO DA POLÍTICA

15.1. Nos termos do Manual de Normas vigente, este normativo interno será tempestivamente atualizado sempre que houver alteração nas atividades documentadas, seja por efeito de norma emanada de órgão regulador, alteração em sistemas informatizados que suportam a operação, ajustes organizacionais e administrativos decorrentes de avaliação de indicadores e riscos, dentre outros.

15.2. O [GT-PTDI] é responsável por manter atualizados os dispositivos e as regras consolidadas nesta Política.

15.3. Casos omissos, situações específicas e esclarecimentos adicionais decorrentes da implementação das regras desta Política, ou de normativos internos que a complementem, serão apreciados pelo [OEX], mediante análise técnica e manifestação do [GT-PTDI].

15.4. Os dispositivos desta Política não constituem rol enumerativo, sendo obrigação dos administradores e gestores adotar, sempre que possível, medidas adicionais cabíveis, além das previstas em normativos internos, com o objetivo de garantir a conformidade legal e regulatória da Caixa de Assistência.

15.5. Os colaboradores[3] deverão assinar termo de ciência das regras estabelecidas nesta Política.

Nota 4 – Consultar [Anexo 3 – Termo de Ciência]

Esta Política entrará em vigor quando aprovada pelo Conselho Deliberativo.

[3] Empregado efetivo ou temporário, estagiário, aprendiz, prestador de serviços e consultor.

16. DOCUMENTOS COMPLEMENTARES

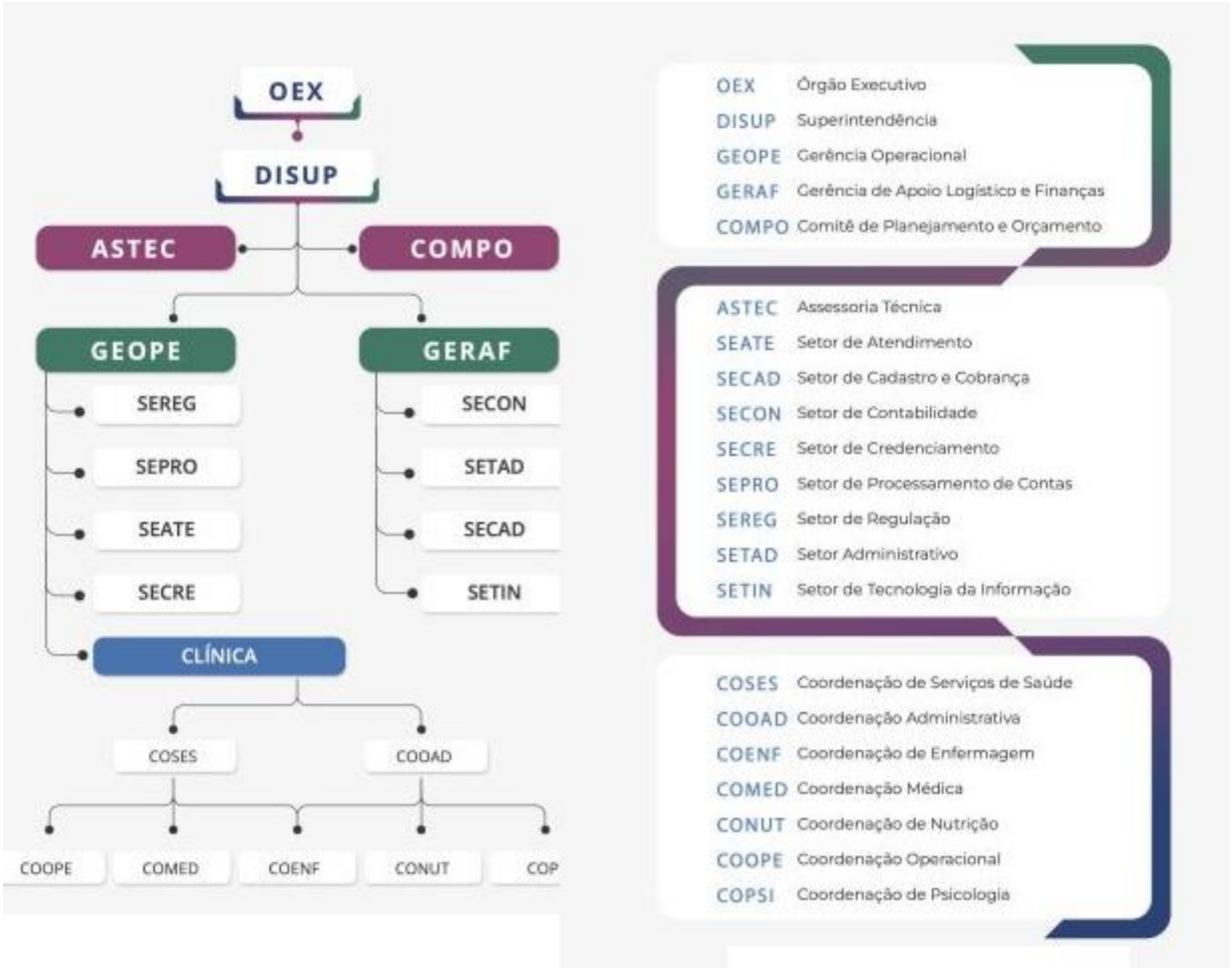
Anexo 1 – Organograma

Anexo 2 – Cadeia de Valor

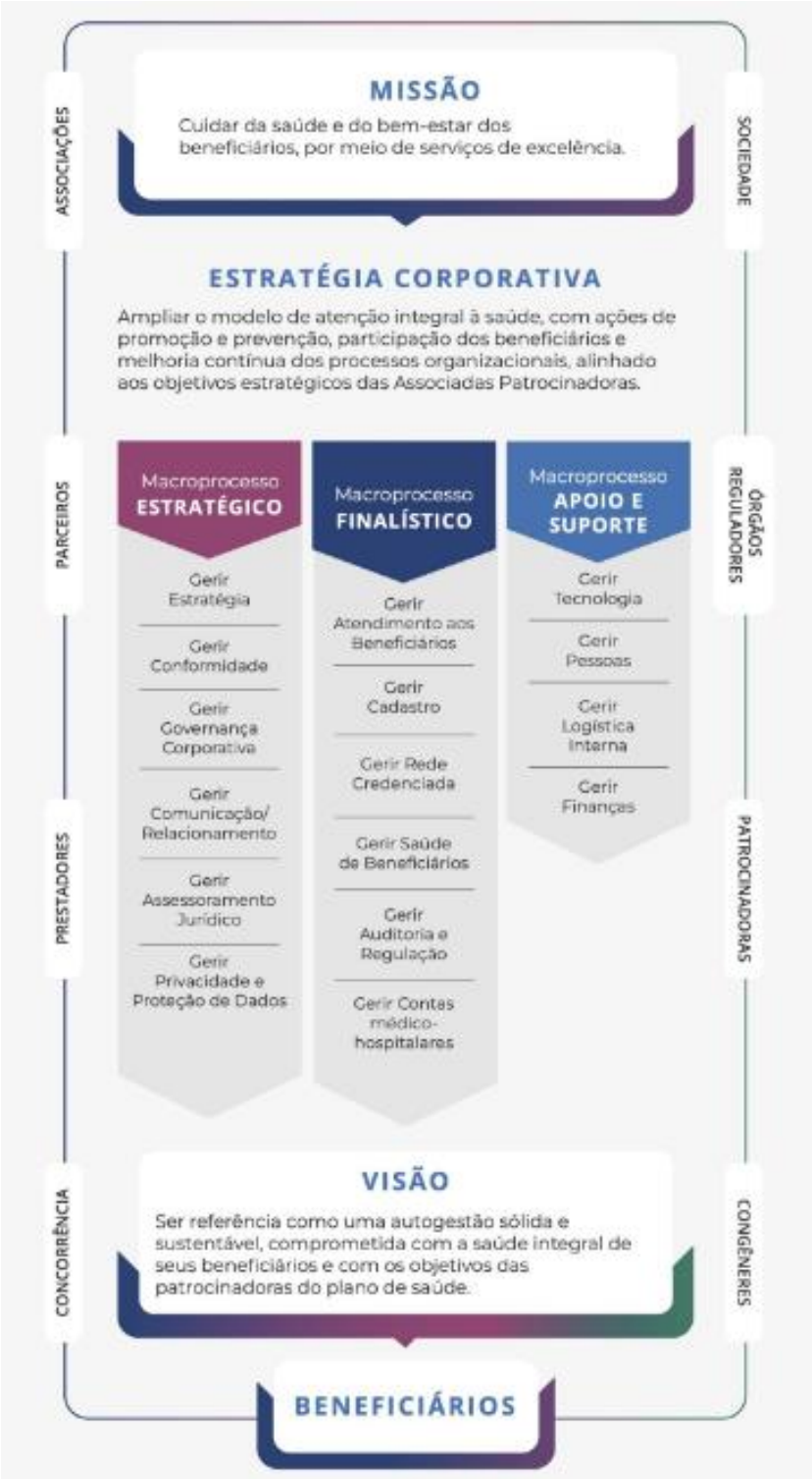
Anexo 3 – Termo de Ciência

Anexo 4 – Registros Alterados – Revisões do Normativo

Anexo 1 – Organograma



Anexo 2 – Cadeia de Valor



Anexo 3 – Termo de Ciência

Eu, _____[nome], CPF nº _____, _____ [cargo/função], matrícula nº _____, **DECLARO** que tomei ciência e compreendi as disposições contidas na Política _____ da **SAÚDE BRB – CAIXA DE ASSISTÊNCIA**, e me comprometo a acompanhar as atualizações dos normativos internos pertinentes.

Anexo 4 – Registros Alterados – Revisões do Normativo

Revisão	Item	Detalhamento
00	N/A	Edição inicial
01	N/A	Atualização integral do normativo.
02	N/A	Não informados.