SAÚDE BRB	**POLÍTICA** Segurança da Informação	Revisão:	02
		Página:	1/18
		C.I.	#10

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

Revisões[1]		
Revisão	**Data**	**Registros de Deliberação**
00	27/12/2019	Aprovada pelo Órgão Executivo, na 72ª reunião ordinária, revogadas as disposições em contrário.
01	31/05/2021	Aprovada em 1ª instância pelo Órgão Executivo, na 89ª reunião ordinária, revogadas as disposições em contrário.
	05/07/2021	Aprovada em 2ª instância pelo Conselho Deliberativo, na 58ª reunião ordinária, revogadas as disposições em contrário.
02	15/10/2025	Aprovada em 1ª instância pelo Órgão Executivo, na 142ª reunião ordinária, revogadas as disposições em contrário.
	04/12/2025	Aprovada em 2ª instância pelo Conselho Deliberativo, na 76ª reunião, revogadas disposições em contrário.

[1] Registros alterados – consultar Anexo 4

SUMÁRIO

1. INTRODUÇÃO

Esta Política tem como objetivo estabelecer princípios, diretrizes e responsabilidades em relação à segurança da informação.

É importante destacar que a Saúde BRB tem como missão cuidar da saúde e do bem-estar dos seus beneficiários, fornecendo serviços de excelência. Diante disso, é fundamental uma estrutura de segurança da informação adequada que forneça, não apenas amparo na execução das atividades, mas também segurança a e confiança aos beneficiários, parceiros, prestadores e patrocinadores.

2. OBJETIVOS

2.1. Promover a conformidade dos processos e atividades internas com a legislação e as melhores práticas relativas à segurança da informação.

2.2. Estabelecer as diretrizes e os princípios associados à segurança da informação.

2.3. Fortalecer a cultura de riscos, controle internos e conformidade pertinentes à segurança da informação, 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.

3. APLICAÇÃO

Saúde BRB – Caixa de Assistência e Clínica Saúde BRB.

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

4. PÚBLICO ALVO

As diretrizes e regras deste normativo destinam-se aos colaboradores permanentes ou temporários, membros dos órgãos estatutários, prestadores de serviços, parceiros e/ou quaisquer outros terceiros que mantenham relacionamento com a Saúde BRB e que, no âmbito dessa relação, possam vir a ter acesso às áreas, equipamentos, informações, arquivos, redes e dados de titularidade da Caixa de Assistência.

5. REFERÊNCIAS

- Lei 12.527/2011 - regula o acesso a informações[2] previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal [Lei de Acesso à Informação]

[2] Inclusive informações de saúde de beneficiários/dependentes

- Lei 12.414/2011 - disciplina a formação e consulta a bancos de dados e contém informações sobre adimplemento de pessoas naturais ou de pessoas jurídicas a vista de estabelecer um histórico de crédito [Lei do cadastro positivo].

- Lei Federal nº 12.965/2014 - estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil [Marco Civil da Internet].

- Decreto n. 8.771/2016 - regulamenta a Lei nº 12.965/2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

- Lei Federal nº 13.709/2018 – define as normas e procedimentos para o tratamento de dados pessoais [Lei Geral de Proteção de Dados Pessoais – LGPD].

- Decreto nº 11.856/2023 - institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.

- Resolução Normativa ANS 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.

- Resolução CD/ANPD nº 15/2024 - aprova o Regulamento de Comunicação de Incidente de Segurança.

- 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.

- ISO 27002 - Tecnologia da informação. Técnicas de segurança. Código de prática para a gestão da segurança da informação, incluindo sua versão original e posteriores atualizações.

- Estatuto.

- Código de Ética e Conduta Corporativa.

- Regulamento Organizacional.

- Regulamento de Pessoal.

6. DEFINIÇÕES

- Acordo de Confidencialidade - documento formal, juridicamente respaldado, que contém a descrição de uso permitido da informação, tempo de duração, responsabilidades e consequências por violação do acordo.

- Ameaça - causa potencial de um incidente, que possa vir a comprometer ou prejudicar uma organização.

- Aplicativos de Mensagens - WhatsApp, Telegram, Face Time, Skype, Facebook, Messenger, Instagram, Twitter e outros que tenham finalidade igual ou similar.

- Ativos de Informação - conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a organização. Trata-se de patrimônio intangível, constituído por informações de qualquer natureza, incluindo aquelas de caráter estratégico, técnico, administrativo, mercadológico, financeiro, de recursos humanos ou legais, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, compra, licenciamento, ou confiadas à organização por colaboradores, parceiros, clientes, fornecedores, terceiros, em formato escrito, verbal, físico, digitalizado, que seja armazenado, transitado ou trafegado pelas estruturas da organização , além de documentos em suporte físico ou mídia eletrônica que transitarem interna ou externamente.

- Autenticidade - propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa, equipamento, sistema, órgão ou entidade;

- 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.

- Confidencialidade - propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizadas;

- Controle - medida de segurança adotada para tratamento de um risco específico.

- Dados pessoais - Dados específicos relativos a um indivíduo, definidos por meio da LGPD.

- Disponibilidade - propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa ou determinado sistema, órgão ou entidade devidamente autorizados.

- Incidente de Segurança - toda a ação que viole as políticas e demais normativos internos, tais como - quaisquer ações ou situações que possam expor uma organização a perdas financeiras ou de imagem, direta ou indiretamente, potenciais ou reais, uso indevido de dados corporativos ou institucionais, divulgação não autorizada de informações ou de

segredos comerciais e industriais sem a autorização expressa dos proprietários ou da área competente, uso de dados, informações, equipamentos, softwares, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, a não comunicação imediata de quaisquer violações ou atitudes

- Informação - dados [eletrônicos ou físicos] ou registros de um sistema devidamente processados.

- Informações da organização - ativos de Informação que se relacionem diretamente à organização, suas atividades, dados de clientes, fornecedores, funcionários, estagiários, visitantes ou terceiros, e qualquer tipo de dado ou informação gerada ou alterada por membros da organização, no exercício de suas funções.

- Integridade - propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

- Primariedade - qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

- Risco de Segurança da Informação - efeito da incerteza sobre os objetivos da segurança da informação de uma organização.

- 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.

- Sistemas de Informação - sistemas computacionais utilizados pela organização para suportar suas operações. Pode haver exceções em que, mesmo não sendo sistemas informáticos, suportem operações da organização.

- Usuário de ativos de informação - colaboradores permanentes ou temporários, membros dos órgãos estatutários, prestadores de serviços, parceiros e/ou quaisquer outros terceiros que mantenham relacionamento com a Saúde BRB e que, no âmbito dessa relação, possam vir a ter acesso às áreas, equipamentos, informações, arquivos, redes e dados de sua titularidade.

7. SIGLAS

- ANS – Agência Nacional de Saúde Suplementar.

- GT - PTDI - Grupo de Trabalho de Privacidade, Transformação Digital, e Inovação.

8. ÁREAS ENVOLVIDAS

- Conselho Deliberativo [CONDE]

- 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 segurança da informação:

9.1. Confidencialidade: garante que o acesso às informações seja efetuado somente pelas pessoas autorizadas, durante o período necessário;

9.2. Integridade: garante que a Informação esteja íntegra e completa durante todo o seu ciclo de vida;

9.3. Disponibilidade: garante que a Informação esteja disponível para as pessoas autorizadas, sempre que se fizer necessária;

9.4. Autenticidade: garante a veracidade da autoria da informação;

9.5. Legalidade: o uso da informação deve estar de acordo com as leis, regulamentos, licenças e contratos em vigência.

10. DIRETRIZES

As seguintes diretrizes norteiam a governança da segurança da informação na Saúde BRB:

10.1. Adotar procedimentos padronizados e medidas para preservar a integridade, confidencialidade, disponibilidade, autenticidade e legalidade no tratamento das informações, possuídas ou custodiadas, que possam promover impactos na continuidade de suas atividades.

10.2. Utilizar medidas de proteção das informações contra acesso, modificação, destruição ou divulgação não autorizada.

10.3. Buscar garantir a segurança dos ativos que custodiam informações e utilizar mecanismos de controle para verificação dos fatores de risco de suas atividades, custo e valor agregado em relação à tecnologia.

10.4. Formalizar acordos de confidencialidade e de não divulgação de informações confidenciais, ou sigilosas, que visam a proteção das informações e comunicam aos signatários as suas responsabilidades.

10.5. Aplicar requisitos e controles de segurança quando da necessidade de acesso aos recursos de processamento da informação, ou a informação propriamente dita por partes externas, prestadores ou beneficiários.

10.6. Treinar os usuários dos ativos de informação quanto sistemas, ambientes de trabalho, equipamentos, documentos, informações, bens e materiais, de forma a certificá-los sobre as ameaças e riscos relacionados à segurança da informação, bem como orientar quanto ao uso correto desses ativos.

10.7. Dispor de sistema de segurança física para proteção dos acessos aos ambientes, do transporte de equipamentos e de documentação, com perímetro estabelecido de acordo com a criticidade dos locais, atividades e informações , bem como manter em segurança e protegidos por barreiras, eletrônicas ou não, todos os recursos e instalações de processamento de informações críticas ou sensíveis às atividades, inclusive equipamentos para contingência e mídia de backup, de acordo com a avaliação dos riscos e procedimentos claramente definidos.

10.8. Promover a segregação de funções e unidades organizacionais para reduzir os riscos de segurança da informação, como também dos ambientes de recursos de desenvolvimento, teste e produção, para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais.

10.9. Buscar a utilização de procedimentos de backups que permitam, em quaisquer situações, a recuperação de softwares, sistemas, dados e documentação, armazenados em meio físico ou lógico, e que devem ser verificados e testados regularmente, para garantir sua efetividade.

10.10. Realizar análises críticas periódicas dos riscos de segurança e dos controles implementados bem como quando houver mudanças nos requisitos das atividades e de suas prioridades, nas novas ameaças e vulnerabilidades.

10.11. Dispor — para os casos de terceirização do desenvolvimento de softwares — de acordos de licença e de evolução do sistema e de cobrança dos requisitos contratuais com respeito à qualidade do código e à existência de garantias.

10.12. Gerenciar efetivamente os incidentes para a garantia de resposta rápida, efetiva e ordenada, por meio da adoção de controles adequados e tempestivos.

10.13. Implementar mecanismo que permita registrar os incidentes de segurança, tão logo sejam detectados.

11. CLASSIFICAÇÃO DAS INFORMAÇÕES

Na Saúde BRB, as informações corporativas são assim classificadas:

11.1. Ostensivas:

São dados ou informações cujo acesso é irrestrito e não há precauções adicionais a serem tomadas quanto ao seu manuseio. Subdividem-se em:

a. Públicas: informação que não expõe a Saúde BRB a riscos e que, por imposição legal ou quando autorizada por seu gestor, pode ser divulgada sem restrição ao público em geral e distribuição externa. Ex.: informações voltadas ao público externo [clientes, mercado, imprensa etc.], documentos e contratos públicos etc.;

b. Internas: informação com base em interesse negocial e de acordo com as normas internas, que pode ser divulgada sem restrição, apenas, ao público interno e partes externas interessadas, com anuência do gestor da informação ou por imposição legal. Todos os documentos não classificados serão considerados com essa classificação. Ex.: Manuais e outros normativos da Instituição.

11.2. Sigilosas:

São dados ou informações cujo conhecimento irrestrito ou divulgação pode acarretar qualquer risco à segurança da organização, do Estado e da sociedade, como os necessários ao resguardo da inviolabilidade da intimidade, da honra e da imagem das pessoas.

Quando estritamente necessária a divulgação, o acesso deverá ser autorizado por seu gestor e monitorado. Caso a matéria seja encaminhada para fora da Caixa de Assistência, padrões de segurança adicionais devem ser estabelecidos. Subdividem-se em:

a. Reservadas: informação que exige cuidados especiais quanto à preservação das suas propriedades e cuja divulgação indevida expõe a Saúde BRB a riscos significativos. Ex.: Votos, Atas de Reuniões da Diretoria, etc.;

b. Secretas: informação cuja preservação das suas propriedades é fundamental para a continuidade dos negócios da Saúde BRB e de seus objetivos e que a divulgação indevida sujeita a Instituição a riscos elevados. Ex.: documentos ou informações de cunho estratégico.

12. RESPONSABILIDADES

12.1. Órgão Executivo - [OEX]

I. Assegurar que a Política de Segurança da Informação seja aderente aos objetivos e estratégias corporativas.

II. Assegurar que esta Política de Segurança da Informação e normas correlatas sejam efetivamente cumpridas.

III. Ter comprometimento com as diretrizes de segurança da informação 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 Segurança da Informação.

V. Implementar controles internos - normativos e reportes sistematizados periódicos - que documentem processos e procedimentos e evidenciem a gestão adequada das atividades relacionadas à segurança da informação.

12.2. Diretor-Superintendente, Gerentes, Coordenadores e Supervisores

I. 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.

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

III. 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.

IV. Comunicar à [ASTEC - Segurança e Privacidade] e ao [SETIN] os casos de descumprimento de políticas, normas ou procedimentos, e os casos de falhas na execução de atividades operacionais.

V. Nos casos de remanejamento interno de usuários, providenciar tempestivamente a adequação dos acessos físicos permitidos e acionar o [SETIN] para que sejam adotadas alterações relativas aos acessos lógicos.

VI. Nos processos de demissão, providenciar tempestivamente o cancelamento dos acessos físicos permitidos ao usuário desligado.

VII. Obter a ciência do colaborador no termo de compromisso e responsabilidade sobre a Política de Segurança da Informação, no processo de admissão e sempre que houver atualização de seus dispositivos.

VIII. Orientar suas equipes sobre o uso adequado das informações e recursos de informações disponibilizados pela Saúde BRB.

IX. Prover informações necessárias para a identificação e tratamento de riscos e incidentes de segurança da informação.

X. 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.

XI. Sempre que necessário, documentar orientações específicas e regulamentar os níveis de confidencialidade das informações que geram e processam, bem como os direitos de acesso a essas informações.

12.3. 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.

12.4. 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.

12.5. Público Interno:

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

II. Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela Saúde BRB.

III. Fazer uso adequado e assegurar que os recursos tecnológicos, informações e sistemas à sua disposição 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 qualquer descumprimento ou violação desta Política e de normas correlatas, ou qualquer evento que possa trazer impactos na segurança dos ativos de informação ou recursos de processamento.

13. 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.

14. MONITORAMENTO E AUDITORIA

14.1. Todas as informações produzidas, acessadas, armazenadas ou distribuídas pelos recursos disponibilizados pela Saúde BRB poderão ser monitoradas e controladas.

14.2. O acesso e uso das informações corporativas e pessoais para o desempenho de atividades de monitoramento e auditoria na Saúde BRB são de uso restrito da [ASTEC] e [SETIN].

14.3. O processo de monitoramento e auditoria é autorizado exclusivamente para atender o objetivo de averiguar o cumprimento das diretrizes corporativas, identificar conteúdo e/ou acessos indevidos, detectar fraudes ou coletar evidências para dar suporte à Saúde BRB em processos judiciais ou em atendimento às auditorias externas, órgãos reguladores e fiscalizadores.

14.4. Os acessos às informações com finalidade diversa das acima citadas serão interpretados como uso impróprio.

14.5. A Saúde BRB se reserva o direito de registrar e examinar todos os eventos relacionados aos acessos à Internet dos usuários de ativos de informação, a fim de garantir que os recursos não sejam utilizados de forma indevida, ou, para fins não autorizados.

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 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.

16. DOCUMENTOS COMPLEMENTARES

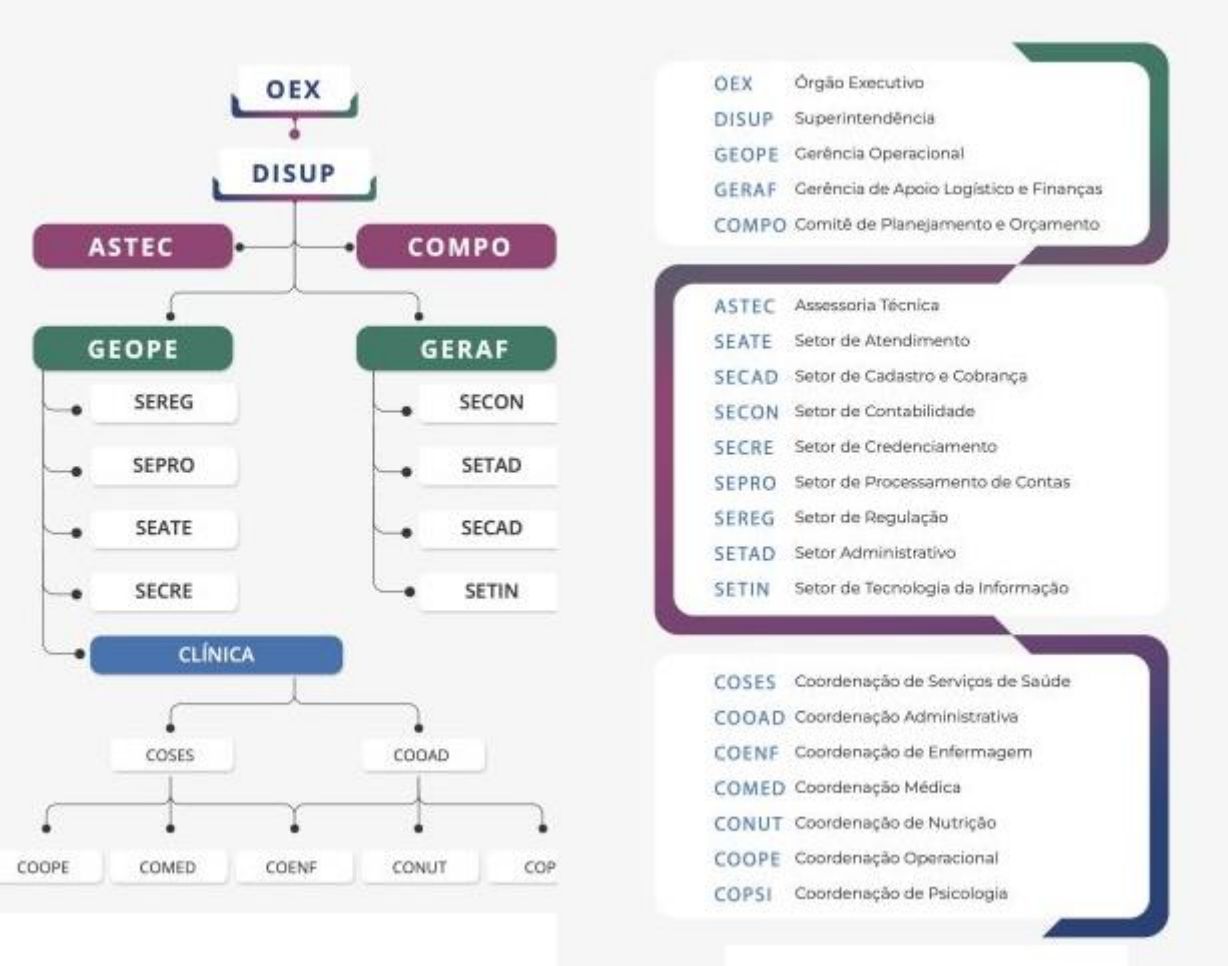
Anexo 1 – Organograma

Anexo 2 – Cadeia de Valor

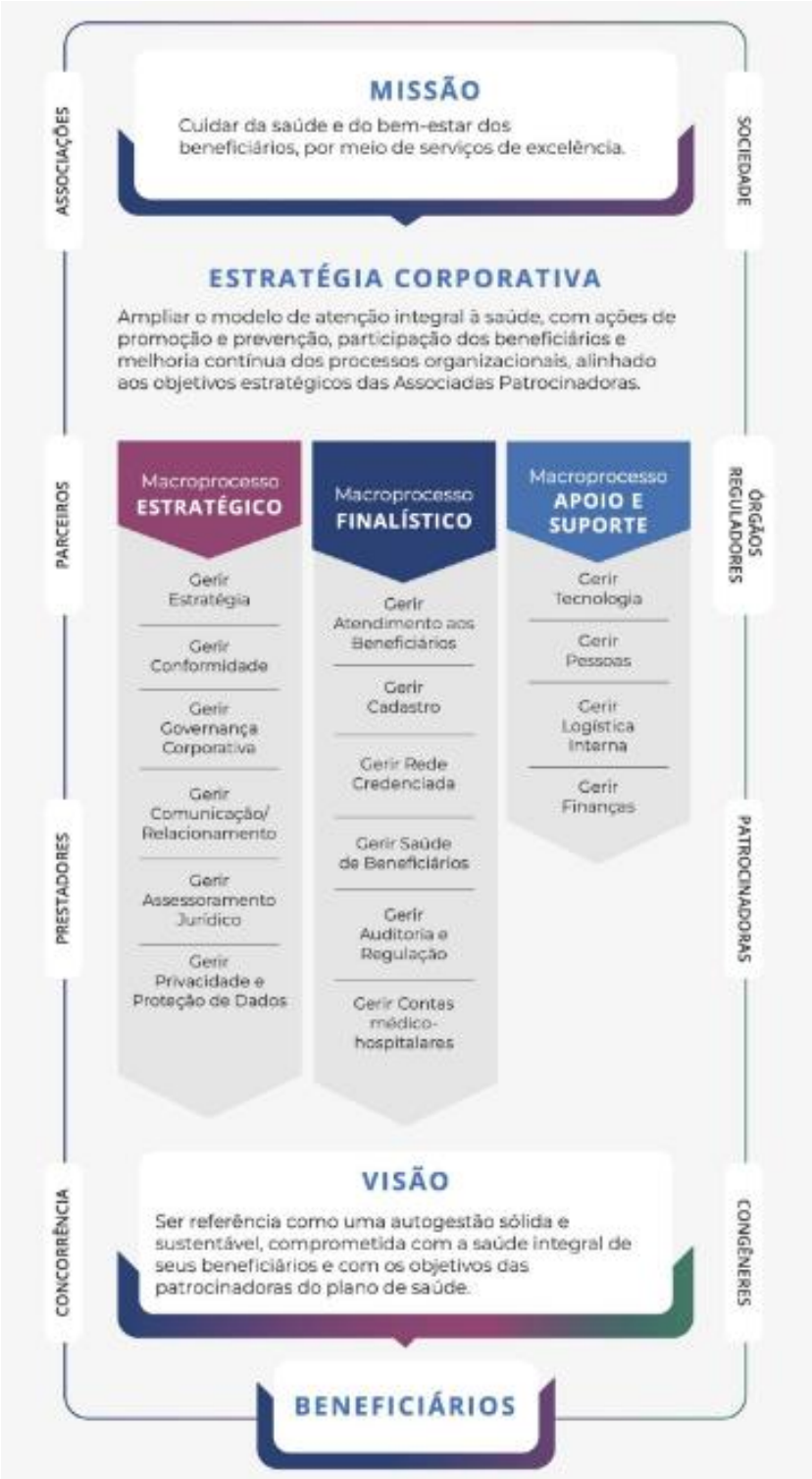
Anexo 3 – Termo de Ciência

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.