SUMÁRIO

1. OBJETIVO

Estabelecer as diretrizes de segurança da informação, visando garantir os princípios básicos de integridade, confidencialidade, disponibilidade, autenticidade e legalidade das informações da Cooperativa.

2. ÂMBITO DE APLICAÇÃO

Operadora de saúde, farmácia Unimed, Rede assistencial própria da Unimed Assis e suas partes Interessadas.

3. DEFINIÇÕES

Ativos - Consiste em todo e qualquer bem tangível ou intangível pertencente, administrado, locado ou custodiado pela Unimed Assis, sejam informações, sistemas ou dispositivos fixos e móveis.

Colaborador - Empregados, estagiários, menores aprendizes, que atuam na Cooperativa. Para fins de alcance de políticas corporativas, ficam incluídos os terceiros, os médicos do corpo clínico e residentes das unidades assistenciais próprias.

Confidencialidade - Consiste na propriedade da informação que determina que esta não esteja disponível ou não seja exposta a indivíduos, entidades e/ou processos que não tenham sido previamente autorizados pelo proprietário.

Disponibilidade - Consiste na propriedade da informação que garante que esta esteja disponível, sempre que necessário, para o uso legítimo, ou seja, por aqueles usuários autorizados pelo seu proprietário visando à continuidade do negócio.

Integridade - Consiste na propriedade da informação que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo seu proprietário, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção, armazenamento e descarte).

Segurança da Informação - Consiste na preservação da confidencialidade, da integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade e confiabilidade da informação.

Prontuário do paciente - É o conjunto de documentos padronizados, ordenados e concisos, destinados ao registro de todas as informações referentes aos cuidados médicos e paramédicos prestados ao paciente.

4. DIRETRIZES

A Unimed Assis considera que suas informações são bens importantes. Seu uso deve ser dimensionado para divulgação correta e no tempo devido, objetivando estabelecer uma comunicação eficiente e esclarecedora com os diversos públicos. A segurança da informação está baseada em 3 princípios: confidencialidade, integridade e disponibilidade.

Na Unimed Assis, todos os colaboradores têm o dever de conhecer e cumprir essas diretrizes, como responsáveis pela preservação da confidencialidade, integridade e disponibilidade das informações, e somente sendo permitido a utilização das informações da Cooperativa para fins internos.

Todos devem preservar a imagem e a integridade de clientes, médicos e colaboradores, observando sempre o sigilo das informações.

A utilização de internet, e-mail e mídias sociais por qualquer profissional que se relaciona com a Unimed Assis deve ser feita de forma responsável, ética e seguir as premissas de segurança da informação.

A informação corporativa pode se apresentar em diferentes formas: estratégia, conhecimento, indicador, estatística, projeto, pesquisa, ação, receita, prática, parecer, análise, experiência, inspeção, especificação, configuração, resultado, dentre outras, e poderá existir como dados armazenados em computadores, dispositivos de armazenamento, dispositivos móveis, caixas de e-mail, escritas e/ou impressas em papel, transmitidas eletronicamente ou até em conversas.

4.1. UTILIZAÇÃO DA INFORMAÇÃO

A Unimed Assis monitora as informações corporativas, podendo estender ao recebimento, envio e armazenamento, utilização e manuseio, sem prévia notificação às áreas ou aos colaboradores, visando garantir e proteger o sigilo e a segurança das mesmas.

A utilização para outros fins e/ou divulgação de assuntos relacionados especialmente, mas não se limitando, a aspectos operacionais, comerciais, sobre pacientes, sobre cooperados, jurídicos, regulatórios, financeiros, contábeis, tecnológicos, sobre marketing, epidemiológico, assistencial ou qualquer outro que se relacione às atividades da Cooperativa obriga o colaborador a obter a autorização formal da Unimed Assis.

O conteúdo dos prontuários do paciente é amparado pelo sigilo profissional, conforme destacado na Constituição Federal e nos Conselhos de Classe dos profissionais da Saúde. O acesso às informações de pacientes é restrito aos profissionais envolvidos diretamente no atendimento ao cliente, devendo ser compartilhadas apenas com terceiros previamente autorizados e homologados, como por exemplos fornecedores de serviço de diagnósticos, serviço de transporte, serviço de guarda física de documentos, serviço de hospedagem de softwares, entre outros.

O sigilo das informações é responsabilidade de todos os colaboradores da Unimed Assis, seus cooperados e rede credenciada.

É proibida a utilização não autorizada de informações da cooperativa, de pacientes ou comentários pessoais que afetem a imagem da instituição em mecanismos de comunicação instantânea, bem como em e-mails, redes sociais ou quaisquer outros meios. Para mitigar o risco compartilhamento indevido as informações assistenciais, quando necessárias à atividade profissional, devem ser discutidas apenas pessoalmente, por telefone, por e-mail ou WhatsApp (ou instrumento de comunicação semelhante) desde que respeitadas às regras impostas pelos instrumentos normativos que tratam do sigilo e da proibição de ter pessoas alheias à medicina compondo grupos de discussão de casos onde se abordam formas de diagnosticar e da aplicação de condutas terapêuticas.

Todos os colaboradores, cooperados e rede credenciada que tenham acesso a informações da Unimed Assis ou sob a guarda da Unimed Assis – pessoais, sensíveis ou restritas – não poderão utilizá-las para fins pessoais ou divulgá-las a pessoas não autorizadas. As restrições incluem a utilização de dados em palestras, apresentações, publicações ou qualquer ato de divulgação para o público externo sem aprovação prévia da liderança responsável.

As informações devem ser classificadas como:

Públicas - São documentos sem nenhum dado pessoal e tem sua visualização permitida para qualquer tipo de público;

Restritas – Contém dados pessoais, cuja permissão de acesso é restrita apenas o público interno e/ou para pessoas especificas externas à cooperativa relacionadas a finalidade do tratamento do dado;

Confidenciais - Contém dados pessoais sensíveis, cuja permissão de acesso é restrita apenas o público interno e/ou para pessoas especificas externas à cooperativa, seguindo os critérios estabelecidos relacionadas a finalidade do tratamento do dado.

A ausência de classificação formal ocasiona a classificação automática de “Restrita”, devendo ser manuseadas e protegidas com cuidado compatível com sua classificação, não sendo deixadas expostas ou desprotegidas.

O armazenamento das informações é realizado por tempo determinado pela Cooperativa e/ou legislação vigente.

4.2. AMBIENTE FÍSICO

4.2.1. ACESSO E PERMANÊNCIA DE EMPREGADOS, PRESTADORES DE SERVIÇOS E VISITANTES

Na Unimed Assis todos colaboradores devem estar devidamente identificados, com uso do crachá em local visível quando estiverem dentro dos prédios administrativos e unidades de atendimento, retirando-o ao sair das dependências.

Os prestadores de serviços terceirizados deverão estar identificados com crachás temporários e deverão ser acompanhados por um represente da área requisitante pelo serviço.

O acesso de visitantes é de responsabilidade das áreas visitadas, cabendo zelar pela aprovação, programação e acessos aos locais, com os cuidados necessários quanto ao registro de imagens e acesso às informações por qualquer meio. Os locais onde houver informações confidenciais devem ser excluídos das rotas de visitantes e da programação de qualquer visita.

4.2.2. SEGURANÇA NO AMBIENTE DE TRABALHO

A Unimed Assis não permite a divulgação de imagens da Cooperativa, de suas instalações e de colaboradores identificados com crachás e/ou uniformizados, bem como o compartilhamento de informações restritas, pessoais ou sensíveis em sites pessoais, redes sociais, aplicativos ou qualquer

meio de comunicação sem o consentimento da Unimed Assis. Não é autorizada a exposição de imagem dos nossos clientes, a não ser que seja necessário e aprovado por escrito pela pessoa e pela Unimed Assis. Também não é permitida a divulgação de informações inverídicas de qualquer natureza em qualquer meio de comunicação.

Os colaboradores têm o dever de assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos não sejam deixados desprotegidos em locais de trabalho pessoais ou públicos quando não estão em uso, mesmo que seja por um curto período de tempo ou ao final do dia.

Além da proteção contra acesso não autorizado, as informações devem ser protegidas contra desastres tais como incêndios, terremotos, inundações ou explosões.

No acesso à informação, somente devem ser usados recursos tecnológicos devidamente homologados e autorizados.

As informações com classificação “Restrita” ou “Confidencial” deverão ser descartadas utilizando métodos que impeçam a reconstrução, tal como a utilização de fragmentadoras.

Os colaboradores devem zelar pela guarda e integridade das informações nos ambientes onde atuam, protegendo os locais onde existem armazenamento de informações, sejam físicos ou eletrônicos, por meio da guarda ou proteção por senha, além da racionalização de recursos que realizam cópia de documentos.

As informações visuais em ambientes de reuniões requerem o mesmo grau de segurança, sigilo e zelo para não visualização por pessoas não autorizadas. O colaborador deve descartar apropriadamente tais informações, de acordo com a sensibilidade da informação. A falta de cuidado com uma área de trabalho pode levar ao comprometimento de informações pessoais e organizacionais.

4.3. AMBIENTE LÓGICO

O acesso às informações pelos colaboradores, como usuários de sistemas, é restrito às necessidades inerentes ao desempenho de suas funções e atribuições. Não é permitida a manipulação ou a utilização de informações ou contas de acesso às quais a pessoa não tem necessidade ou direito de uso.

O ambiente de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos não autorizados, garantindo a integridade, disponibilidade e confiabilidade das informações.

A Unimed Assis adota medidas técnicas apropriadas para prevenir que ativos de informação possam ser acessados ilegalmente, modificados sem autorização, falsificados, destruídos ou sofram interferências que afetem a confidencialidade, integridade e/ou disponibilidade das informações que eles suportam.

Todo sistema de informação desenvolvido ou adquirido pela Unimed Assis, que se utilize ou tenha acesso à informação confidencial, deve obrigatoriamente possuir uma especificação formalizada que

tem de levar em conta a segurança dos sistemas, o controle de acesso e as devidas especificações para contingência.

Os processos de implantação de sistemas de informação devem respeitar as premissas de segregação de funções e de ambientes para serem executados. Mecanismos e soluções de continuidade são identificados, definidos, implementados e mantidos para os processos de negócios considerados críticos para a Unimed Assis.

A Cooperativa não se responsabiliza por atualização, manutenção e garantia de conectividade de dispositivos que não sejam de sua propriedade ou não tenham sido homologados. É de responsabilidade do proprietário o uso de mecanismos de proteção em seus equipamentos.

A Unimed Assis reserva para si o direito de monitorar, auditar e intervir nos acessos de dados que trafegam na internet de modo a salvaguardar os interesses corporativos de acordo com a lei 12.965 (Marco Civil da Internet) consonantes com os objetivos dessa política.

4.3.1. CONTAS E SENHAS DE ACESSO A SISTEMAS

Na Unimed Assis toda conta de acesso a sistemas terá seu proprietário ou responsável unicamente e claramente identificado. Qualquer ação executada por intermédio de uma conta será de inteira responsabilidade de seu proprietário.

A senha de acesso de cada usuário é pessoal e intransferível, sendo do colaborador ou das partes interessadas a responsabilidade por garantir seu sigilo.

A Cooperativa utiliza procedimentos e mecanismos de proteção e de gerenciamento de senhas visam a manutenção da segurança das contas de acessos e às informações.

4.3.2. PERFIS DE ACESSO A SISTEMAS

Todos os perfis de acesso ao ambiente de produção dos sistemas são concedidos respeitando-se os princípios de segregação de funções. Conflitos dessa natureza serão permitidos apenas mediante criação de controle compensatório pela área solicitante devidamente documentado e posteriormente aprovado.

A concessão dos acessos ao ambiente de infraestrutura de produção por parte de analistas e prestadores de serviço da TI deverá ser realizada de forma temporária, devidamente documentada e aprovada.

4.3.3. E-MAIL

O e-mail corporativo é uma ferramenta de trabalho, comunicação e apoio para os processos de negócios da Cooperativa, não podendo ser utilizado para fins pessoais. Com razão análoga, as informações de trabalho não podem ser trafegadas utilizando e-mails pessoais.

O e-mail corporativo é de uso exclusivo para o exercício das suas atividades, não devendo ser utilizado para cadastro em sites comerciais, redes pessoais ou qualquer plataforma que vise a interesses particulares.

Caso ocorra o envio de e-mail contendo informações restritas ou confidenciais para o destinatário errado, o colaborador se obriga a reportar a falha para o DPO.

4.3.4. INTERNET

A Internet é ferramenta de trabalho para o desenvolvimento de atividades, processos, pesquisas, tecnologias e competências. A Unimed Assis mantém regras de utilização e bloqueio de acesso a determinados sites, caixas de e-mail, conteúdos, anexos, emitentes, destinatários, assinaturas, notas, limites de tráfego e armazenamentos.

A Unimed Assis não autoriza a utilização dos meios de comunicação da Cooperativa para divulgar mensagens com conteúdo ilegal, pornográfico, com qualquer sentido discriminatório, de cunho religioso, político-partidário, ideológico ou em desacordo com os princípios éticos e morais da Unimed Assis.

Ao cadastrar no perfil das redes sociais, que é um colaborador da Unimed Assis, o profissional não deve realizar qualquer ação que impacte a marca ou contrarie os valores da Cooperativa.

4.3.5. ATIVOS DE PROCESSAMENTO DE DADOS HARDWARE

Na Cooperativa, os ativos de processamento de dados são classificados quanto a critérios de criticidade e disponibilidade para os negócios da organização.

Os locais que hospedam ativos de processamentos de dados têm níveis adequados e são controlados de segurança física.

A Unimed Assis homologa e controla os ativos de processamentos de dados, incluindo equipamentos e ativos de tecnologia.

É proibida a saída de qualquer equipamento de propriedade da empresa pelo colaborador, exceto se houver autorização por expresso neste sentido formalizada por documento escrito e assinado.

A entrada e consequente uso de equipamentos de informática pessoais tais como celulares, tablets e notebooks, deverá ser autorizada pela empresa se for necessária utilização da rede. Em hipótese alguma a empresa será responsabilizada por danos no equipamento pessoal do colaborador ou ainda em casos de furto ou roubo.

4.3.6. ATIVOS DE PROCESSAMENTO DE DADOS SOFTWARE

A Unimed Assis homologa e controla os softwares e se dá o direito de excluir e bloquear o uso de softwares não autorizados sem comunicação prévia. Os critérios padrões de utilização são: softwares licenciados ou open source (gratuitos), que não apresentam risco de vazamento de dados.

É proibido downloads de arquivos de extensões tipo: exe, .mp3, .wav, .bat, .com, .sys, .scr, .ppt, .mpeg, .avi, .rmvb, .dll, e de programas de entretenimento ou jogos, exceto os estritamente relacionados aos serviços inerentes à função do colaborador com vistas às atividades da empresa.

É proibido o uso de jogos, inclusive os da Internet (onlines).

4.4. GERENCIAMENTO DE RISCOS

Os riscos à segurança da informação são continuamente avaliados e monitorados, considerando-se as ameaças e vulnerabilidades que possam causar impactos ou danos aos processos de negócios e pessoas.

Os sistemas de proteção quanto às ameaças oriundas de ambientes externos e internos ao ambiente computacional devem ser mantidos, atualizados e monitorados.

4.5. PRAZOS DE REVISÕES

Esta política deve ser analisada anualmente e revisada caso haja necessidade.

Os acessos aos recursos tecnológicos da empresa deverão ser analisados a cada seis meses.

4.6. AUDITORIA DE SEGURANÇA DA INFORMAÇÃO

A empresa possuiu softwares e sistemas implantados que podem monitorar o uso da Internet, e-mails, chats, etc., através da rede local e das estações de trabalho da empresa.

A empresa se reserva o direto de inspecionar, sem a necessidade de aviso prévio, as estações de trabalho e qualquer arquivo armazenado, estejam no disco local da estação ou nas áreas privadas da rede, assim como monitorar o volume de tráfego na Internet e na Rede juntamente com os endereços web (http://) visitados, visando assegurar o cumprimento desta política.

4.7. PLANO DE CONTINUIDADE DE NEGÓCIOS

O objetivo deste plano é garantir a continuidade das operações críticas da cooperativa em caso de interrupções, minimizando os impactos negativos e assegurando a prestação contínua de serviços essenciais. Este plano foi desenvolvido com base na Avaliação de Impacto ao Negócio (BIA) que identificou os processos críticos mapeados no sistema de gestão da qualidade. O acompanhamento é realizado pelo indicador do Qualiex “Tempo Médio de Resposta Chamados Urgentes”.

Processo Crítico	Descrição	Impacto	Prioridade de recuperação	Estratégia

Atendimento ao Paciente no serviço de oncologia da Unimed.	Suporte via telefone, chat ou e-mail para dúvidas, reclamações e solicitações urgentes.	Interrupção de serviços. Beneficiários não conseguem resolver problemas, resultando em insatisfação e danos à imagem da operadora.	Prioridade Alta	Identificar a causa da interrupção. Acionar controles redundantes, como geradores e conexões secundárias de internet.
Atendimento aos pacientes nos hospitais da rede credenciada.	Suporte via telefone, chat ou e-mail para dúvidas, reclamações e solicitações urgentes.	Interrupção de serviços. Atrasos na realocação de beneficiários para unidades disponíveis podem comprometer o atendimento.	Prioridade Alta	Identificar a causa da interrupção. Acionar controles redundantes, como conexões secundárias de internet.
Gestão de Autorizações	Liberação de procedimentos médicos, exames, internações e tratamentos.	Beneficiários podem não acessar serviços de saúde, resultando em risco à vida e multas regulatórias.	Prioridade Alta	Implementar sistemas redundantes e criar uma equipe de contingência para processar autorizações manualmente.
Atendimento aos pacientes nos ambulatórios da Unimed	Suporte no atendimento, via telefone, chat ou e-mail para dúvidas, reclamações e solicitações urgentes.	Interrupção de serviços ou beneficiário não consegue ser atendido	Prioridade Média	Identificar a causa da interrupção. Acionar controles redundantes, como conexões secundárias de internet.
Atendimento ao paciente nos serviços da rede prestadora (consultórios, laboratórios e clínicas de diagnóstico)	Suporte no atendimento, via telefone, chat ou e-mail para dúvidas, reclamações e solicitações urgentes.	Interrupção de serviços	Prioridade Média	Identificar a causa da interrupção. Acionar controles redundantes, como conexões secundárias de internet.
Fechamento folha de pagamento	Cálculo e processamento dos salários, benefícios e encargos dos colaboradores	Atrasos podem gerar insatisfação, ações trabalhistas e multas regulatórias	Prioridade Alta	Utilizar sistemas de folha de pagamento em nuvem com backups regulares e manter processos manuais de emergência
Fechamento de produção Médica	Consolidação e validação das produções dos médicos cooperados para pagamento e repasse financeiro	Cooperados podem não receber seus valores, afetando o relacionamento e a continuidade dos atendimentos	Prioridade Média	Adotar sistemas de controle de produção médica e estabelecer rotinas manuais para envio emergencial de dados por meio de planilhas seguras
Sistemas de Comunicação internos	Fluxo de informações entre departamentos e colaboradores, incluindo atualizações	Falhas na comunicação podem gerar desorganização, atraso em decisões e falta de	Prioridade Média	Utilizar plataformas alternativas (como Teams, Bitrix ou grupos de Whatsapp dos departamentos) e criar listas de

	operacionais e de crise	alinhamento estratégico		distribuição para comunicação rápida em situações de crise
Banco de Dados	Dados pessoais internos e de beneficiários em nossos sistemas	Queda dos sistemas paralisa todas as operações críticas, incluindo autorizações e atendimento	Prioridade Alta	Utilizar data centers redundantes com failover automático e implementar planos de recuperação de desastres com RTO (Tempo de Recuperação) em até 4h
Processamento de solicitações de reembolso	Análise e pagamento de reembolsos em processos realizados no âmbito particular	Beneficiários podem enfrentar atrasos no reembolso, causando insatisfação e perda de credibilidade	Prioridade Média	Criar um fluxo para solicitações e priorizar casos urgentes manualmente com equipe responsável
Gestão de Dados Regulatórios	Coleta e envio de dados obrigatórios para a ANS, como registros de atendimentos e informações solicitadas	Penalidades da ANS por descumprimento de prazos e regulamentações	Prioridade Alta	Estabelecer um cronograma de checagem diário e manter acesso diário ao sistema

Este plano de continuidade de negócios foi estruturado para atender às especificidades da Unimed de Assis, priorizando a segurança dos beneficiários, colaboradores, cooperados e a conformidade regulatória. A implementação das estratégias descritas é essencial para minimizar os impactos de interrupções e assegurar a resiliência dos processos críticos.

O PCN é revisado sempre quando é identificado um novo risco ou uma nova alternativa para mitigação, resultando em teste antes do registro, incluindo simulações de cenários de crise, para garantir sua eficácia em situações reais.

Em linhas gerais temos as estratégias de Continuidade:

- Infraestrutura Redundante
- Utilizar servidores em nuvem com backup automático.
- Garantir redundância em sistemas de telecomunicação e energia elétrica.

Equipes de Contingência:

- Treinar colaboradores para atuar em situações de crise.
- Criar processos manuais para folha de pagamento e produção médica em caso de falha nos sistemas.

Planos de Recuperação de TI

- Implementar soluções de failover para sistemas essenciais.
- Priorizar a recuperação de sistemas relacionados a folha de pagamento e produção médica.
- Comunicação Eficiente
- Estabelecer listas de contato prioritário para emergências.
- Utilizar canais de comunicação redundantes, como aplicativos móveis e

Definições:

Tempo de Recuperação Objetivo (RTO): O RTO é o tempo máximo aceitável que um sistema, serviço ou processo pode estar indisponível após uma interrupção antes que cause um impacto significativo nas operações, ou seja, o foco é Tempo necessário para restaurar a funcionalidade.

Exemplo: Se o RTO do "Gestão de Autorização de Guia" é de 1 hora, isso significa que o sistema deve ser restaurado dentro de 1 hora após uma interrupção, pois nesta 1 hora, não acarretará danos às solicitações dos pacientes, tampouco na Auditoria médica.

Ponto de Recuperação Objetivo (RPO): O RPO é o ponto no tempo até o qual os dados devem ser recuperados após uma interrupção. Ele determina a quantidade máxima de dados que pode ser perdida, medida em tempo. O foco nesse ponto é a quantidade de dados que pode ser perdida no período de falha.

Exemplo: Se o RPO do "Gestão de Autorização de Guia" é de 24 horas, isso significa que, no caso de uma interrupção, a perda de dados não deve exceder 24 horas de transações, ou seja, em caso de falha neste processo, perder as últimas 24 horas de registros não acarretará prejuízos para cooperativa, nem à risco à vida e multas regulatórias.

Resumo das Diferenças

- RTO: Relaciona-se ao tempo de inatividade aceitável.
- RPO: Relaciona-se à quantidade de dados que pode ser perdida.

Por que são importantes?

Esses parâmetros ajudam a Unimed de Assis a:

- Priorizar recursos durante um incidente.
- Determinar a infraestrutura e as soluções de backup necessárias.
- Definir expectativas realistas de recuperação para colaboradores, cooperados e beneficiários.

Processo	(RTO)	(RPO)	Justificativa	Periodicidade de Revisão
Atendimento ao Paciente no serviço de oncologia da Unimed.	1 hora	Até 4 horas	Manter suporte imediato aos beneficiários e preservar a imagem da operadora	Anual
Atendimento aos pacientes nos hospitais da rede credenciada.	4 horas	10 horas	Manter suporte imediato aos beneficiários e preservar a imagem da operadora	Anual
Atendimento aos pacientes nos ambulatórios da Unimed	4 horas	10 horas	Manter suporte imediato aos beneficiários e preservar a imagem da operadora	Anual
Atendimento ao paciente nos demais serviços da rede prestadora (consultórios, laboratórios e clínicas de diagnóstico)	4 horas	10 horas	Manter suporte imediato aos beneficiários e preservar a imagem da operadora	Anual
Fechamento folha de pagamento	4 horas	12 horas	Garantir que colaboradores e cooperados recebam corretamente, evitando multas e ações trabalhistas.	Anual
Fechamento de produção Médica	6 horas	24 horas	Prevenir atrasos nos repasses financeiros aos cooperados.	Anual
Sistemas de Comunicação internos	2 horas	6 horas	Garantir alinhamento e fluxo de informações para evitar desorganização em situações críticas	Anual
Banco de Dados	2 horas	30 minutos	Garantir o funcionamento de sistemas críticos, como portais de beneficiários e autorizadores	Anual
Gestão de Autorizações	2 horas	15 minutos	Evitar atrasos no acesso a procedimentos médicos essenciais	Anual
Processamento de solicitações de reembolso	5 horas	10 horas	Garantir que a solicitação seja analisada e atendida em tempo hábil	Anual
Gestão de Dados Regulatórios	5 horas	24 horas	Evitar atrasos no atendimento à regulação e gerar multas	Anual

RTO e RPO mais curtos são aplicáveis a processos diretamente relacionados ao atendimento imediato aos beneficiários (ex.: autorizações e atendimento ao beneficiário).

RTO e RPO mais longos podem ser considerados para processos regulatórios ou administrativos, que não afetam imediatamente o atendimento, mas ainda são fundamentais.

5. REGRAS DE CONSEQUÊNCIA

As consequências pelo descumprimento destas diretrizes podem ser denunciadas no canal de ética e serão tratadas conforme a política do canal. Situações excepcionais serão encaminhadas ao Comitê de Proteção de Dados, à Diretoria Executiva e/ou aos demais órgãos de governança.

6. DISPOSIÇÕES FINAIS

Esta política entrou em vigor a partir de sua aprovação pela Diretoria Executiva em 16 de setembro de 2020. Foi revisada em 3 de fevereiro de 2021 e aprovada pelo Conselho de Administração em 13 de fevereiro de 2023. A última revisão e aprovação ocorreram em ata do Conselho de Administração em 9 de dezembro de 2024.