COTAÇÃO ELETRÔNICA - AQUISIÇÃO DE BACKUP E RECUPERÇÃO DE DESASTRES EM NUVEM

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

1. OBJETO

Contratação de empresa especializada para fornecimento, implantação, operação assistida, sustentação e suporte de uma solução integrada de Backup as a Service (BaaS) e Disaster Recovery as a Service (DRaaS), em nuvem, destinada à proteção e recuperação de dados, aplicações, máquinas virtuais, servidores físicos e serviços de colaboração em nuvem da Fundação de Saúde Itaiguapy - Hospital Itamed.

A solução deverá permitir a continuidade dos serviços críticos em caso de indisponibilidade parcial ou total do ambiente principal, falha de infraestrutura, erro humano, corrupção de dados, incidente cibernético, ransomware ou desastre, mediante restauração de dados, failover para ambiente em nuvem e posterior failback controlado.

2. OBJETIVO

2.1 Objetivo Geral:

Contratar solução integrada de Backup as a Service (BaaS), Disaster Recovery as a Service (DRaaS) e sustentação especializada, destinada à proteção, retenção, recuperação e disponibilidade dos dados, sistemas, servidores, máquinas virtuais e serviços críticos da instituição, assegurando a continuidade operacional diante de falhas, indisponibilidades, incidentes cibernéticos, desastres físicos ou lógicos e demais eventos que possam comprometer o ambiente tecnológico.

A solução deverá contemplar armazenamento seguro de cópias de segurança em nuvem, incluindo recursos de imutabilidade dos dados, de forma a impedir sua alteração, exclusão ou criptografia indevida durante o período de retenção definido, inclusive em situações de comprometimento do ambiente produtivo.

2.2 Objetivo Específicos:

- Proteger os dados e sistemas críticos da instituição por meio de rotinas automatizadas de backup, com políticas de retenção, versionamento e recuperação compatíveis com a criticidade de cada serviço;
- Disponibilizar armazenamento de backups em nuvem, localizado obrigatoriamente território nacional, com criptografia dos dados em trânsito e em repouso;

- Garantir a criação e manutenção de cópias de backup imutáveis, protegidas contra alteração, exclusão, sobrescrita ou criptografia maliciosa durante o prazo de retenção estabelecido, inclusive por usuários com privilégios administrativos;
- Adotar mecanismos de proteção contra ransomware e outras ameaças cibernéticas, com monitoramento, alertas, detecção de comportamentos suspeitos e possibilidade de recuperação segura dos dados;
- Permitir a recuperação granular de arquivos, pastas, volumes, bancos de dados, aplicações, servidores físicos e máquinas virtuais, conforme necessidade operacional;
- Disponibilizar ambiente de recuperação de desastres em nuvem, com possibilidade de acionamento controlado de contingência, failover, testes sem impacto ao ambiente produtivo e retorno ao ambiente principal por meio de failback;
- Assegurar que os serviços críticos possam ser restabelecidos dentro dos parâmetros de RPO e RTO definidos pela instituição, reduzindo o impacto operacional decorrente de indisponibilidades;
- Centralizar a administração, o monitoramento, os relatórios, as auditorias e a gestão dos serviços de backup e disaster recovery em console única, com controle de acesso por perfil e autenticação multifator;
- Elaborar e manter atualizado o Plano de Recuperação de Desastres, incluindo matriz de responsabilidades, procedimentos de acionamento, dependências técnicas, plano de comunicação e cronograma de testes periódicos;
- Disponibilizar suporte técnico especializado, sustentação continuada e acompanhamento da operação do ambiente durante toda a vigência contratual.

3. ESCOPO DA CONTRATAÇÃO

O escopo da contratação compreende:

3.1. **Implantação e configuração inicial**

a) Levantamento técnico do ambiente da CONTRATANTE, incluindo servidores físicos, máquinas virtuais, sistemas operacionais, bancos de dados, aplicações críticas, volumes de dados, dependências entre serviços e requisitos de recuperação;

b) Elaboração do plano de implantação da solução, contendo cronograma, responsabilidades, premissas técnicas, etapas de configuração, validação e entrada em operação;

c) Instalação e configuração dos componentes necessários para realização dos backups, replicações e recuperação dos ambientes protegidos;

d) Configuração das políticas de backup, retenção, versionamento, criptografia, replicação, imutabilidade, alertas e monitoramento, conforme classificação de criticidade dos ativos;

e) Configuração de perfis de acesso, autenticação multifator, trilhas de auditoria e segregação de funções administrativas;

f) Realização de testes iniciais de backup e restauração, com emissão de evidências técnicas e aceite da CONTRATANTE.

3.2. **Proteção de dados e rotina de backup**

a) Proteção de servidores físicos, máquinas virtuais, sistemas operacionais, aplicações, bancos de dados, arquivos, pastas, volumes, estações de trabalho e demais ativos definidos pela CONTRATANTE;

b) Execução de backups completos, incrementais, diferenciais ou baseados em imagem, conforme a política estabelecida para cada ativo;

c) Obrigatoriamente realizar backup em ambiente local, nuvem ou modelo híbrido, sem prejuízo da proteção centralizada e do gerenciamento unificado;

d) Disponibilização de políticas de retenção configuráveis por período, quantidade de cópias, consumo de armazenamento e criticidade do ambiente;

e) Criação de cópias de backup com criptografia em trânsito e em repouso, utilizando algoritmos robustos e mecanismos seguros de gestão de chaves;

f) Disponibilização de recuperação granular de arquivos, pastas, volumes, máquinas virtuais, aplicações e bancos de dados, conforme aplicável.

3.3. **Armazenamento imutável e proteção contra ransonware**

a) Disponibilização de armazenamento de backups com recurso de imutabilidade, de forma que as cópias protegidas não possam ser alteradas, sobrescritas, excluídas ou criptografadas antes do encerramento do período de retenção definido;

b) A imutabilidade deverá ser implementada por tecnologia equivalente a WORM, Object Lock, retenção protegida ou mecanismo tecnicamente equivalente, independentemente da nomenclatura comercial adotada pelo fornecedor;

c) As cópias imutáveis deverão permanecer protegidas inclusive contra ações indevidas ou maliciosas realizadas por usuários com privilégios administrativos;

d) A solução deverá permitir a definição de período mínimo de retenção imutável, com registro auditável das políticas configuradas e das alterações realizadas;

e) A solução deverá possuir mecanismos de identificação de comportamentos suspeitos, corrupção de dados, alterações anormais, ransomware ou tentativas de exclusão de backups;

f) Em caso de incidente, deverá permitir a identificação e recuperação de ponto de restauração íntegro anterior ao evento identificado.

3.4. **Disaster Recovery em nuvem**

a) Disponibilização de ambiente de recuperação de desastres em nuvem para os sistemas e serviços classificados como críticos pela CONTRATANTE;

b) Replicação dos dados, máquinas virtuais ou imagens de servidores para ambiente de contingência, conforme o dimensionamento e os parâmetros técnicos definidos no projeto;

c) Possibilidade de acionamento de contingência por meio de failover, permitindo a execução temporária dos sistemas protegidos no ambiente em nuvem;

d) Possibilidade de retorno ao ambiente principal por meio de failback, após o restabelecimento da infraestrutura local;

e) Criação de runbooks ou planos automatizados de recuperação, contemplando sequência de inicialização, dependências entre aplicações, configurações de rede e procedimentos de validação;

f) Realização de testes de failover sem impacto ao ambiente produtivo, com emissão de relatório técnico contendo resultados, falhas identificadas e ações de melhoria;

g) Disponibilização de conectividade segura entre o ambiente da CONTRATANTE e o ambiente de contingência, mediante VPN ou tecnologia equivalente, com criptografia do tráfego.

3.5. **Sustentação, monitoramento e suporte**

a) Monitoramento contínuo das rotinas de backup, replicação, armazenamento, integridade dos dados e disponibilidade dos serviços contratados;

b) Emissão de alertas automáticos para falhas, atrasos, indisponibilidades, consumo excessivo de capacidade, tentativas de exclusão, falhas de autenticação ou eventos relacionados à segurança;

c) Disponibilização de console centralizada para gerenciamento, acompanhamento de operações, consulta a relatórios, auditoria e administração das políticas de proteção;

d) Disponibilização de relatórios periódicos contendo, no mínimo, status dos backups, falhas identificadas, capacidade utilizada, indicadores de sucesso, tentativas de restauração, eventos de segurança e aderência aos níveis de serviço;

e) Suporte técnico especializado em língua portuguesa, com canais de atendimento por portal, e-mail e telefone, conforme níveis de criticidade e SLA definidos;

f) Apoio técnico da CONTRATADA para análise de falhas, restauração de dados, acionamento de contingência, retorno ao ambiente principal e demais demandas relacionadas à operação da solução.

3.6. **Treinamento e transferência de conhecimento**

a) Realização de treinamento remoto ou presencial para a equipe técnica indicada pela CONTRATANTE, abrangendo administração da console, consulta a relatórios, abertura de chamados, acompanhamento de backup, procedimentos de restauração e acionamento do ambiente de contingência;

b) Entrega de documentação técnica do ambiente implantado, incluindo arquitetura, políticas de backup, políticas de retenção, procedimentos de recuperação, contatos de suporte e responsabilidades operacionais.

3.7. **Dimensionamento de servidores**

a) A tabela a seguir apresenta o dimensionamento dos ambientes, servidores, serviços e capacidades previstos para a contratação. A CONTRATANTE poderá reduzir os itens, quantitativos ou capacidades, conforme suas necessidades técnicas, operacionais e orçamentárias, não estando obrigada à contratação integral dos quantitativos apresentados.

Componente	Quantidade/Capacidade de referência	Observação
Servidor físico	1 servidores físicos, com referência de 6 TB podendo chegar até 15Tb.	Proteção de imagem completa, discos/volumes, arquivos e recuperação granular.
Máquinas virtuais	100 VMs, com referência de 200TB de capacidade protegida, podendo chegar até 150 VM, com referência de 300Tb.	Ambientes de produção, homologação e serviços críticos, conforme inventário da contratante.
Microsoft 365	30 identidades protegidas, podendo chegar até 150.	Proteção de Exchange Online, OneDrive, SharePoint Online e Teams, quando habilitados pela contratante.
Armazenamento de backup	Capacidade referencial de 50 TB de dados de origem, sujeita ao consumo efetivo e à política de retenção. Podendo chegar até 300Tb.	A proposta deverá discriminar claramente a unidade de cobrança.
Disaster Recovery	Até 100 cargas elegíveis para recuperação, com recursos computacionais ativados sob demanda.	O escopo final de DR deverá priorizar sistemas classificados como críticos no Plano de Recuperação de Desastres.
Endereços públicos no DR	Quantidade sob demanda, incluindo referência para publicação de serviços essenciais.	A licitante deverá apresentar valor unitário por IP público e condições de uso.

4. REQUISITOS TÉCNICOS MÍNIMOS

4.1. Arquitetura e console de gerenciamento

A solução deverá ser disponibilizada em arquitetura híbrida, baseada em nuvem, no modelo SaaS, e em com dados salvos no ambiente do CONTRATANTE, permitindo a administração integrada dos serviços de backup, recuperação de dados e armazenamento imutável por meio de uma única console de gerenciamento.

Serão aceitos componentes locais estritamente necessários à proteção dos ativos, tais como agentes, conectores, gateways, proxies ou repositórios de cache, desde que não exijam a aquisição ou manutenção de appliance proprietário dedicado como requisito obrigatório para a operação da solução.

A arquitetura deverá permitir a proteção de ambientes físicos, virtuais e em nuvem, com capacidade de expansão de recursos, inclusão ou exclusão de ativos protegidos, ajuste de políticas, aumento de capacidade de armazenamento e ampliação do ambiente de recuperação de desastres, sem necessidade de substituição integral da solução contratada.

A console de gerenciamento deverá possibilitar, em ambiente único, a visualização e administração das rotinas de backup, replicação, retenção, armazenamento em nuvem, cópias imutáveis, recuperação de dados, testes de restauração e acionamento do ambiente de Disaster Recovery.

Não será aceita solução que exija a utilização de múltiplas consoles independentes para administração das funcionalidades essenciais de backup, cópias imutáveis e recuperação de desastres, salvo quando houver integração nativa, autenticação unificada e visualização centralizada dos recursos contratados.

A console deverá permitir a criação de usuários e grupos de usuários, com definição de perfis de acesso e permissões granulares, observando o princípio do menor privilégio. Deverá possibilitar, no mínimo, a segregação entre usuários administradores, operadores de backup, auditores e usuários com permissão apenas para consulta de relatórios.

O acesso administrativo à solução deverá possuir autenticação multifator (MFA) nativa ou integrada a serviço corporativo de identidade compatível, de modo a reduzir o risco de acesso indevido às configurações, políticas, credenciais e cópias de segurança.

A solução deverá registrar trilhas de auditoria contendo, no mínimo, os acessos realizados, tentativas de autenticação, alterações em políticas de backup e retenção, inclusão ou exclusão de ativos, operações de restauração, mudanças em usuários e permissões, eventos relacionados à imutabilidade e tentativas de exclusão de cópias protegidas.

Os registros de auditoria deverão permitir consulta, filtragem, exportação e retenção pelo período definido pela CONTRATANTE, devendo conter data e hora do evento, identificação do usuário, endereço de origem quando disponível, ação executada e resultado da operação.

A console deverá disponibilizar painel centralizado para acompanhamento da operação, contendo, no mínimo, a situação das rotinas de backup, índice de sucesso e falha, ativos protegidos, consumo de armazenamento, capacidade disponível, alertas ativos, status das cópias imutáveis, pontos de recuperação disponíveis, execuções de restauração e situação dos recursos de Disaster Recovery.

A solução deverá permitir a criação, edição e aplicação centralizada de políticas de backup, retenção, criptografia, imutabilidade, replicação e recuperação, possibilitando sua associação a servidores, máquinas virtuais, grupos de ativos, aplicações ou demais recursos protegidos.

Deverá ser possível configurar alertas automáticos para eventos críticos ou relevantes, incluindo falha de backup, falha de replicação, ausência de execução programada, crescimento anormal de dados, indisponibilidade de agente, erro de autenticação, alteração de política, tentativa de exclusão de cópias protegidas e identificação de comportamento suspeito relacionado a ransomware.

Os alertas deverão poder ser encaminhados, no mínimo, por correio eletrônico, devendo a solução possuir recursos de integração por API, webhook, syslog ou mecanismo equivalente para integração com ferramentas corporativas de monitoração, centralização de logs ou gestão de eventos de segurança, quando solicitado pela CONTRATANTE.

A console deverá permitir a geração de relatórios técnicos e gerenciais, em formato visual e exportável, contendo informações sobre execução dos backups, ativos protegidos, uso de armazenamento, falhas, restaurações, cumprimento das políticas de retenção, status da imutabilidade, evolução de capacidade e indicadores de disponibilidade dos serviços.

A solução deverá possuir mecanismo de atualização e manutenção dos componentes de gerenciamento, agentes e serviços, com controle de versões, registro das alterações e comunicação prévia à CONTRATANTE quando houver impacto potencial nas rotinas de proteção ou disponibilidade do ambiente.

A arquitetura deverá assegurar comunicação criptografada entre os componentes locais e a plataforma em nuvem, utilizando protocolos seguros e versões atualizadas de criptografia, não sendo permitida a transmissão de dados administrativos ou de backup por canais não criptografados.

A CONTRATADA deverá apresentar, durante a fase de implantação, o desenho lógico da arquitetura proposta, identificando os componentes locais e em nuvem, fluxos de comunicação, portas necessárias, requisitos de conectividade, mecanismos de autenticação, local de armazenamento dos dados e controles de segurança aplicados à solução.

4.2. **Requisitos mínimos de Backup e Recuperação de dados**

A solução deverá permitir a proteção centralizada de servidores físicos, máquinas virtuais, sistemas operacionais, bancos de dados, aplicações, arquivos, pastas, volumes e serviços em nuvem definidos pela CONTRATANTE como necessários à continuidade operacional.

Deverá suportar, no mínimo, ambientes Microsoft Windows Server, Linux, VMWare e Microsoft Hyper-V, bem como bancos de dados Oracle e Microsoft SQL Server em versões compatíveis com o ambiente

tecnológico da CONTRATANTE. A solução também deverá contemplar a proteção dos serviços Microsoft 365, incluindo Exchange Online, OneDrive for Business, SharePoint Online e Microsoft Teams.

Deverá possibilitar a realização de backups completos, incrementais e por imagem, com agendamento automatizado, políticas de retenção configuráveis, controle de consumo de banda, **compactação ou** deduplicação de dados, quando aplicáveis.

Os dados deverão ser protegidos por criptografia durante a transmissão e enquanto armazenados, utilizando, no mínimo, AES de 256 bits ou tecnologia equivalente de segurança comprovada.

A solução deverá permitir a recuperação granular de arquivos e pastas, restauração de volumes, recuperação integral de servidores físicos e máquinas virtuais, restauração de aplicações e bancos de dados, bem como recuperação para o ambiente original ou alternativo definido pela CONTRATANTE.

Deverá possuir mecanismos de validação da integridade das cópias de segurança, identificação de falhas ou corrupção de dados e possibilidade de execução de testes de restauração sem impacto indevido ao ambiente produtivo.

As operações de backup, falhas, alertas e restaurações deverão ser registradas em trilha de auditoria, permitindo a identificação do ativo envolvido, data e hora da operação, usuário responsável, ponto de recuperação utilizado e resultado da execução.

A CONTRATADA deverá prestar suporte técnico especializado para análise de falhas, recuperação de dados, restauração de sistemas e validação dos backups, principalmente em situações que envolvam sistemas ou serviços críticos da CONTRATANTE.

4.3. **Requisitos mínimos de Disaster Recovery em Nuvem**

A solução deverá disponibilizar ambiente de Disaster Recovery em nuvem para os servidores, máquinas virtuais e aplicações críticas definidos pela CONTRATANTE, permitindo a recuperação dos serviços em caso de falha grave, indisponibilidade prolongada, incidente cibernético ou desastre que comprometa o ambiente principal.

Deverá possibilitar a replicação dos dados e imagens dos ambientes protegidos para a infraestrutura de contingência, bem como o acionamento controlado do ambiente por meio de failover e o retorno ao ambiente principal por meio de failback, após o restabelecimento da infraestrutura local.

A solução deverá permitir a definição de sequência de inicialização dos servidores e aplicações, considerando dependências entre serviços, rede, bancos de dados e demais componentes necessários ao correto funcionamento do ambiente recuperado.

Deverá permitir a realização de testes periódicos de contingência e failover, sem impacto indevido ao ambiente produtivo, com emissão de relatório técnico contendo os ativos testados, tempo de recuperação, resultados obtidos, falhas identificadas e ações corretivas recomendadas.

O ambiente de contingência deverá possuir conectividade segura com a infraestrutura da CONTRATANTE, por meio de VPN criptografada ou tecnologia equivalente, permitindo o acesso controlado aos sistemas recuperados durante a vigência da contingência.

A solução deverá disponibilizar recursos para publicação temporária dos serviços recuperados, incluindo endereçamento IP público ou mecanismo equivalente, quando necessário para restabelecimento do acesso externo às aplicações institucionais.

A CONTRATADA deverá elaborar, em conjunto com a CONTRATANTE, o Plano de Recuperação de Desastres, contendo os procedimentos de acionamento, responsáveis, ordem de recuperação, dependências técnicas, critérios de validação, comunicação do incidente e procedimento de retorno ao ambiente principal.

Os parâmetros de RPO (Recovery Point Objective) e RTO (Recovery Time Objective) deverão ser definidos pela CONTRATANTE de acordo com a criticidade de cada sistema, aplicação ou serviço, observando obrigatoriamente os prazos, níveis de disponibilidade e demais requisitos estabelecidos na Resolução Normativa de Política de Backup que integrará esta Especificação Técnica.

A solução deverá assegurar que os tempos de recuperação dos serviços classificados como críticos atendam integralmente aos limites máximos de RTO previstos na referida Resolução Normativa, considerando as condições de conectividade, o dimensionamento dos recursos contratados, as dependências técnicas entre aplicações e a sequência de recuperação definida no Plano de Recuperação de Desastres.

A CONTRATADA deverá prestar suporte técnico especializado em regime 24x7 para apoio ao acionamento do ambiente de contingência, recuperação dos serviços e retorno à operação normal.

5. APRESENTAÇÃO DA PROPOSTA

Deverá apresentar proposta técnica e comercial detalhada, contendo descrição da solução ofertada, arquitetura proposta, componentes incluídos, modelo de licenciamento, capacidade de armazenamento, serviços de implantação, sustentação, suporte técnico e condições de acionamento do ambiente de Disaster Recovery.

A proposta deverá informar claramente os ativos, serviços, capacidades, franquias, limitações técnicas, itens cobrados sob demanda, valores unitários adicionais e eventuais premissas necessárias para o correto funcionamento da solução.

Deverá ser apresentado cronograma de implementação contendo, no mínimo, as etapas de levantamento do ambiente, definição da arquitetura, instalação e configuração dos componentes, criação das políticas de backup e retenção, configuração da imutabilidade, execução das primeiras cópias de segurança, validação de restauração, implantação do ambiente de Disaster Recovery, elaboração do Plano de Recuperação de Desastres, treinamento da equipe técnica e aceite final da CONTRATANTE.
O cronograma deverá indicar os prazos estimados para cada etapa, os responsáveis envolvidos, os marcos de validação e as dependências atribuídas à CONTRATANTE e à CONTRATADA.

6. QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS

A CONTRATADA deverá apresentar atestado(s) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a execução satisfatória de serviços compatíveis com o objeto desta contratação, atendendo, no mínimo, aos seguintes requisitos:

1. Comprovação de implantação, operação ou suporte de ambiente de backup com capacidade igual ou superior ao ambiente atualmente utilizado pela CONTRATANTE (Itamed), ou ambiente equivalente em porte, complexidade e volumetria de dados.
2. Comprovação de implantação, operação ou suporte de solução de Disaster Recovery (DR) em ambiente de porte igual ou superior ao ambiente de DR da CONTRATANTE (Itamed), ou ambiente equivalente em complexidade operacional.
3. A CONTRATADA deverá comprovar que possui, em seu quadro próprio de colaboradores, no mínimo 04 (quatro) profissionais com capacidade técnica comprovada para execução do objeto da contratação, por meio de certificações, registros profissionais, vínculo empregatício e/ou documentação que demonstre experiência compatível com as atividades previstas neste edital.

Deverá ser indicado, no mínimo, um Gerente de Projeto responsável pelo acompanhamento da implantação, cronograma, comunicação entre as partes, gestão de riscos e entrega das etapas previstas.

Deverá ser indicado, no mínimo, um profissional técnico especializado em soluções de backup, recuperação de desastres e ambientes em nuvem, com experiência comprovada em implantação, configuração, recuperação de dados, failover, failback e testes de contingência.

Os profissionais indicados deverão possuir certificações técnicas, treinamentos oficiais, comprovação de experiência profissional ou documentação equivalente compatível com a tecnologia ofertada e com os serviços objeto desta contratação.

A CONTRATANTE poderá solicitar, durante a análise da proposta ou durante a vigência contratual, evidências das qualificações apresentadas, tais como certificados, currículo profissional, declaração de experiência ou documentação equivalente.

Qualquer substituição de profissional técnico-chave deverá ser previamente comunicada à CONTRATANTE, devendo o substituto possuir qualificação técnica equivalente ou superior à do profissional originalmente indicado.

7. LIMITES E RESPONSABILIDADE

A CONTRATADA deverá apresentar, juntamente com a proposta, uma matriz de responsabilidades contendo, de forma clara, as atribuições da CONTRATADA e da CONTRATANTE para a execução dos serviços. Não será permitida a participação de consórcios, nem a subcontratação, terceirização ou cessão, total ou parcial, de quaisquer atividades objeto deste contrato, sendo a CONTRATADA a única responsável pela execução integral dos serviços.

A CONTRATADA será responsável pela implantação, configuração, monitoramento, sustentação, suporte técnico e manutenção dos componentes contratados, incluindo as políticas de backup, retenção, imutabilidade, replicação, recuperação de dados e operação do ambiente de Disaster Recovery.

A CONTRATANTE será responsável por disponibilizar os acessos, informações técnicas, conectividade, infraestrutura local, credenciais autorizadas e demais recursos sob sua gestão necessários à implantação e operação da solução.

Eventuais limitações, premissas, dependências técnicas ou exclusões de responsabilidade deverão ser apresentadas expressamente na proposta técnica, não sendo aceitas restrições genéricas ou omissões que comprometam o entendimento do escopo contratado.

As limitações de responsabilidade não poderão afastar a obrigação da CONTRATADA quanto à confidencialidade, integridade, segurança e disponibilidade dos dados sob sua custódia, nem quanto à comunicação imediata de incidentes, falhas relevantes, indisponibilidades ou eventos que possam comprometer as cópias de segurança ou o ambiente de contingência.

A CONTRATADA deverá comunicar formalmente à CONTRATANTE qualquer condição que possa comprometer o cumprimento dos níveis de serviço, dos parâmetros de RPO e RTO, da integridade dos backups, da imutabilidade dos dados ou da capacidade de recuperação do ambiente.

Em caso de incidente, falha de backup, indisponibilidade da plataforma, identificação de ransomware, comprometimento de cópias de segurança ou necessidade de acionamento do Disaster Recovery, a CONTRATADA deverá prestar apoio técnico compatível com o nível de criticidade do evento, conforme os níveis de serviço e procedimentos definidos contratualmente.

Thiago de Lima Barbosa
Thiago de Lima Barbosa (27/07/2026 11:21:32 ADT)

Thiago de Lima Barbosa

Coordenador de Infraestrutura de T.I.

Rosangela Rubim
Rosangela Rubim (27/07/2026 12:40:20 ADT)

Rosangela Rubim

Gerente Tecnologia da Informação

2026_06_23 - ANEXO I - ESPECIFICAÇÃO TÉCNICA - SaaS Backup (2)

Relatório de auditoria final 2026-07-27

Criado em:	2026-07-27 (Horário Padrão de Brasília)
Por:	Thiago de Lima Barbosa (thiago.barbosa@itamed.com.br)
Status:	Assinado
ID da transação:	CBJCHBCAABAAyTSNG7f1vrwhmm3ULm0TPO-uSvaYBCsk

Histórico de "2026_06_23 - ANEXO I - ESPECIFICAÇÃO TÉCNICA - SaaS Backup (2)"

Documento criado por Thiago de Lima Barbosa (thiago.barbosa@itamed.com.br)
2026-07-27 - 11:20:03 ADT

Documento enviado por email para Thiago de Lima Barbosa (thiago.barbosa@itamed.com.br) para assinatura
2026-07-27 - 11:20:58 ADT

Documento assinado eletronicamente por Thiago de Lima Barbosa (thiago.barbosa@itamed.com.br)
Data da assinatura: 2026-07-27 - 11:21:32 ADT - Fonte da hora: servidor - Aparência da assinatura selecionada: TIPO

Documento enviado por email para Rosangela Rubim (rosangela.rubim@itamed.com.br) para assinatura
2026-07-27 - 11:21:33 ADT

Email visualizado por Rosangela Rubim (rosangela.rubim@itamed.com.br)
2026-07-27 - 12:39:32 ADT

Documento assinado eletronicamente por Rosangela Rubim (rosangela.rubim@itamed.com.br)
Data da assinatura: 2026-07-27 - 12:40:20 ADT - Fonte da hora: servidor - Aparência da assinatura selecionada: TIPO

Contrato finalizado.
2026-07-27 - 12:40:20 ADT