Lista de Requisitos Técnicos para Certificação de Aplicações de Inteligência Artificial em Saúde

Categoria

Aplicação de Inteligência Artificial em Saúde

Versão 1.0

02/01/2026

Editor

Luiz Virginio

Coordenador de Certificação de Sistemas – SBIS

Autores desta edição

Luiz Virginio (SBIS)

Colaboradores desta edição

Aleocidio Sette Balzanelo (SBIS)
Cláudia de Fátima Miranda (SBIS)
Grace Teresinha Marcon Dal Sasso (SBIS)
Jeancarlo Fernandes Cavalcante (CFM)
Leandro Costa Miranda (SBIS)
Luis Gustavo Gasparini Kiatake (SBIS)
Marcelo Lúcio da Silva (SBIS)
Osmeire Aparecida Chamelette Sanzovo (SBIS)
Renato Duarte Rozo Fonseca (SBIS)

Índice

1. Introdução

Este documento apresenta o conjunto de requisitos técnicos especificados pela Sociedade Brasileira de Informática em Saúde (SBIS) para a certificação na seguinte categoria:

- **Aplicação de Inteligência Artificial em Saúde:** Aplicações que utilizam funcionalidades baseadas em Inteligência Artificial (IA) com potencial impacto clínico, assistencial ou decisório direto sobre o cuidado com o paciente ou sobre a conduta de profissionais de saúde. Essas soluções podem ser oferecidas de forma autônoma (stand-alone) ou estar integradas a um sistema de informação.

Para a categoria de Aplicação de IA em Saúde, **o conjunto de requisitos NGS2 - Autenticidade e Assinatura Digital é opcional**. Entretanto, é fundamental compreender o seu papel no contexto regulatório e operacional dos sistemas de informação em saúde. A **eliminação do papel**, entendida como a substituição de documentos físicos por registros exclusivamente digitais com validade jurídica e assistencial, **somente é reconhecida quando o sistema atende integralmente aos requisitos do NGS2**. A certificação em NGS2 é, portanto, o elemento que comprova que o sistema possui os mecanismos técnicos necessários para garantir autenticidade, integridade, não repúdio, rastreabilidade e segurança dos registros eletrônicos, conforme as normas e regulamentações aplicáveis.

Sempre que a certificação do sistema **não incluir o NGS2**, essa informação será **explicitamente indicada no certificado emitido pela SBIS**, de modo a garantir transparência quanto ao escopo da certificação e às limitações de uso do sistema no que se refere à eliminação do papel.

A descrição do funcionamento do processo de certificação, incluindo suas normas, condições, processo de inscrição, processo de auditoria, etc., está disponível no Manual de Certificação para Aplicação de Inteligência Artificial em Saúde disponível na página da SBIS na internet.

2. Estágios de Maturidade

Os requisitos estão estruturados no formato de um modelo de maturidade de três estágios. Os estágios podem ser descritos como se segue:

- **Estágio 1 (Essencial):** requisitos mínimos para garantir governança em IA, gestão de riscos, transparência e explicabilidade, segurança, rastreabilidade, responsabilidade e conformidade legal.
- **Estágio 2 (Intermediário):** requisitos que aumentam a robustez, explicabilidade, qualidade técnica e governança contínua.
- **Estágio 3 (Avançado):** práticas mais complexas ou sofisticadas, desejáveis, mas que ainda não são mandatórias para uso seguro e responsável.

São apresentados abaixo os principais recursos contemplados em cada estágio de maturidade para a categoria de Aplicação de IA em Saúde.

Quadro comparativo dos principais recursos contemplados	Estágio de Maturidade		
	1	2	3
Governança e gestão de riscos	✓	✓	✓
Validação técnica e clínica dos modelos	✓	✓	✓
Monitoramento contínuo da qualidade de dados	✓	✓	✓
Transparência e explicabilidade	Essencial	Intermediário	Avançado
Qualidade em adaptações ou configurações	✓	✓	✓
Segurança, privacidade, arquitetura e infraestrutura	Essencial	Intermediário	Avançado
Aderência à ICP-Brasil para eliminação de papel (opcional)	✓	✓	✓
Gestão de Mudanças em IA		✓	✓
Avaliação dos Atributos de Qualidade da IA		✓	✓
Ativação/inativação de IA		✓	✓
Monitoramento interno e auditorias de desempenho da IA		✓	✓
Metodologia formal de ciclo de vida para desenvolvimento de IA			✓
Análise de Indicadores de impacto da solução de IA			✓
Feedback Imediato dos Usuários sobre Respostas da IA			✓

3. Requisitos de Conformidade

A lista apresentada neste capítulo indica os requisitos aplicáveis a cada estágio de maturidade da categoria Inteligência Artificial. Para obter o Certificado SBIS, o sistema deverá atender à **totalidade dos requisitos de ECF, NGS1, BPIA e, caso pretendido, NGS2** aplicáveis ao estágio de maturidade pretendido pelo Solicitante.

A lista de requisitos, apresentada a seguir, inclui as seguintes informações:

Coluna	Descrição
ID	Identificação do requisito, codificada no seguinte padrão: *<Sigla-do-conjunto>.<Número-do-domínio>.<Número-do-requisito>* Exemplo: BPIA.01.01
Título	Título (nome) do requisito
Descrição	Descrição do requisito, incluindo exemplos quando apropriado. Adicionalmente, pode incluir notas explicativas para melhor elucidação de seu conteúdo.
Aplicabilidade para Categoria de IA	Define a condição de aplicabilidade do requisito. Para a categoria de IA, alguns requisitos do grupo ECF e NGS1 são aplicáveis apenas em cenários específicos. Por exemplo, o requisito NGS1.01.01 (Exibição das informações do software) é aplicável apenas caso o sistema possua interface gráfica para interação com o usuário. Quando a condição definida for atendida pelo sistema, o requisito deverá ser avaliado; caso contrário, será considerado não aplicável.
Estágio de Maturidade	Indica o Estágio de Maturidade em que o requisito é exigido. Vale ressaltar que os estágios são cumulativos. Portanto, para atender ao estágio 2, é necessário estar aderente aos requisitos do estágio 1 e 2. Da mesma forma, para atender ao estágio 3, é necessário estar aderente aos requisitos dos estágios 1, 2 e 3.

Os requisitos iniciados com uma expressão de "**Condição**" somente são aplicáveis quando a referida condição for verdadeira, sendo desconsiderados caso contrário.

3.1. Requisitos de Boas Práticas para Inteligência Artificial em Saúde (BPIA)

ID	Título	Descrição	Estágio de Maturidade
BPIA.01 - Governança de IA			
BPIA.01.01	Estrutura de governança de IA	a) A empresa responsável pelo S-RES deve possuir e apresentar uma estrutura formal de governança de IA documentada, incluindo: • Política(s) de IA aprovada(s) pela alta direção, alinhada(s) aos objetivos estratégicos e valores da organização; • Definição clara de papéis e responsabilidades para a governança de IA (por exemplo, Comitê de IA, Chief Artificial Intelligence Officer, Data Protection Officer - DPO com atribuições de IA). As funções podem ser acumuladas por uma mesma pessoa ou área, desde que as responsabilidades estejam formalmente atribuídas e documentadas; • Processos formais de supervisão para o desenvolvimento, aquisição, implantação, monitoramento e descontinuação de sistemas/aplicações de IA, incluindo mecanismos de reporte e tomada de decisão; • Mecanismos para garantir o alinhamento das soluções de IA com requisitos legais, éticos e regulatórios. b) A empresa deve realizar a revisão anual da estrutura de governança com registros documentados de atualização.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.01.02	Atendimento aos princípios de IA responsável	a) A empresa responsável pelo S-RES deve possuir documentação técnica demonstrando que sua utilização de IA segue os princípios éticos e de governança (IA responsável), e como a conformidade é verificada e mantida, contendo minimamente: • Benefícios Pretendidos: Documentação que demonstre claramente o benefício pretendido da utilização da IA no contexto específico do sistema/aplicação, incluindo uma descrição objetiva dos impactos positivos esperados para os usuários finais e/ou pacientes, bem como indicadores de avaliação do benefício, que podem ser clínicos (por exemplo, acurácia diagnóstica, tempo de atendimento), operacionais (por exemplo, redução de etapas manuais) ou de experiência do usuário (por exemplo, satisfação). • Equidade e Mitigação de Vieses: Relatório dos testes realizados para identificar vieses relacionados a gênero, idade, etnia, situação socioeconômica ou outras características populacionais, acompanhado das ações técnicas implementadas para mitigar esses vieses. • Segurança e Privacidade: Descrição dos controles técnicos aplicados no desenvolvimento do sistema/aplicação com IA para garantir segurança e privacidade das informações dos usuários (por exemplo, anonimização de dados, criptografia, controle de acesso, logs auditáveis). • Transparência e Explicabilidade: Documentação que descreva como os usuários são informados sobre o escopo de uso de IA, incluindo limitações conhecidas, restrições de uso e riscos potenciais. Descrever como a solução de IA está aderente aos princípios de explicabilidade dos resultados da IA. • Responsabilização e Prestação de Contas: Descrição dos mecanismos para revisão humana dos resultados da IA e responsabilização pela decisão final. Descrição sobre o processo para reportar e tratar reclamações, dúvidas e incidentes associados ao uso da IA pelo software. • Excelência Científica e Técnica: Evidências de que que a solução de IA segue metodologias reconhecidas cientificamente, possui desempenho técnico/clínico validado e atende às normas técnicas, legais e regulatórias vigentes. b) A documentação deve ser revisada anualmente ou sempre que houver mudanças significativas. Nota: Documentos já produzidos para atender a outros requisitos (por exemplo, mitigação de viés, segurança, validação técnica e clínica, monitoramento pós-mercado, etc.) podem ser utilizados como evidências complementares para comprovar conformidade a este requisito, desde que estejam atualizados e claramente referenciados.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.01.03	Metodologia formal de ciclo de vida para desenvolvimento de IA	a) A empresa responsável pelo S-RES deve definir, documentar e aplicar uma metodologia formal para o ciclo de vida completo de suas soluções de IA, desde a concepção até a descontinuação. b) A metodologia deve contemplar todas as fases do ciclo de vida (concepção, desenvolvimento, validação, implantação, monitoramento e descontinuação) e estar alinhada a boas práticas internacionais, tais como o Responsible AI Guide - Coalition for Health AI (CHAI); AI Lifecycle - Food and Drug Administration (FDA); norma ISO/IEC 5338 e norma ABNT NBR IEC 62304. c) A metodologia deve formalizar artefatos esperados e critérios de aprovação para cada etapa do ciclo de vida da IA. d) A empresa deve nomear formalmente os responsáveis técnicos por cada etapa do ciclo de vida da IA. É permitido que uma mesma pessoa acumule responsabilidades por mais de uma etapa, desde que as atribuições estejam documentadas. e) Gestão do Componente de IA dentro do Ciclo de Vida: A metodologia da solução deve detalhar explicitamente como o(s) modelo(s) de IA utilizado(s) pelo S-RES são gerenciados. • Para modelos desenvolvidos e controlados pela empresa: O processo deve incluir e documentar as etapas de concepção, aquisição de dados, treinamento, teste e validação do modelo como atividades integrais do ciclo de vida da solução. • Para modelos desenvolvidos por terceiros (pré-treinados ou consumidos via API): O processo deve incluir e documentas as etapas relacionadas à seleção do modelo/fornecedor, validação contextual (testes com seus próprios dados e em seu cenário de uso específico) e monitoramento. Deve ainda haver um plano de contingência para o caso de descontinuação do serviço pelo terceiro ou encerramento do contrato.	3

ID	Título	Descrição	Estágio de Maturidade
BPIA.01.04	Processo formal de gestão de riscos para IA	a) A empresa responsável pelo S-RES deve manter um processo formal e documentado para a gestão dos riscos associados à solução de IA. b) A documentação técnica apresentada deve contemplar minimamente os seguintes elementos: • Identificação estruturada dos riscos associados à IA, incluindo riscos técnicos, operacionais, éticos e de impacto social; • Avaliação da severidade, probabilidade e detectabilidade dos riscos; • Planejamento de ações de mitigação, contingência e rastreabilidade. c) A empresa deve adotar um processo de revisão periódica dos riscos longo do tempo, garantindo que a revisão ocorra anualmente e sempre que houver mudanças significativas no modelo, nos dados ou nos requisitos regulatórios aplicáveis. Nota: A seguir, seguem alguns exemplos de referências que podem ser utilizas pela empresa responsável pelo S-RES para aplicação deste requisito: - Risk Categorization Tool - Coalition for Health AI (CHAI); - Norma ABNT NBR ISO 14971 (Dispositivos médicos — Aplicação de gerenciamento de risco a dispositivos médicos); - Artificial Intelligence Risk Management Framework do National Institute of Standards and Technology (NIST); - Metodologias específicas de análise de riscos como o Failure Mode and Effects Analysis (FMEA).	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.01.05	Gestão de Mudanças para IA	a) A empresa responsável pelo S-RES deve possuir um processo formal e documentado para gerenciar mudanças nos modelos de IA, dados de treinamento/validação ou infraestrutura associada, incluindo: • Critérios para ativação do processo, com distinção entre mudanças substanciais (por exemplo, retreinamento, fine-tuning relevante, inclusão de variáveis de entrada, mudança de arquitetura) e ajustes menores (por exemplo, alteração de limiares); • Avaliação do impacto da mudança (riscos, desempenho, segurança, ética); • Processo de validação da mudança antes da implantação em produção; • Controle de versão robusto para modelos, dados, código e system prompts; • Políticas e critérios para reprocessamento de resultados apresentados pela versão anterior do modelo (se aplicável); • Comunicação clara das mudanças para usuários. b) O processo formal de gerenciamento de mudanças deve ser obrigatoriamente acionado para quaisquer alterações que possam impactar a performance, segurança, ética ou usabilidade do modelo (por exemplo, retreinamento, fine-tuning relevante, mudança no conjunto de dados de treinamento/validação, atualização de arquitetura ou parâmetros críticos). c) O reprocessamento de resultados já apresentados pela versão anterior deve ser avaliado com base em critérios objetivos, tais como: • Potencial impacto clínico ou de segurança sobre pacientes; • Alterações que possam modificar decisões operacionais críticas ou gerar divergência em desfechos relevantes; • Requisitos regulatórios ou contratuais que determinem reprocessamento em casos específicos. Nota: Quando a mudança envolver modelo de IA fornecido por terceiros, devem ser apresentados registros do fornecedor (por exemplo, release notes) e avaliação interna de impacto.	2
BPIA.01.06	Equipe técnica qualificada para IA	A empresa responsável pelo S-RES deve possuir documentação da qualificação da equipe técnica envolvida no ciclo de vida da IA (desenvolvimento, validação, implantação, monitoramento), incluindo: • Indicação dos perfis de competências existentes na equipe (por exemplo, cientista de dados, engenheiro de machine learning, MLOps, profissional de saúde, especialista em segurança/privacidade); • Evidências de qualificação (por exemplo, currículos, certificados, portfólio/projetos, registro profissional quando aplicável); • Atribuição formal de papéis e responsabilidades, permitindo a acumulação de funções, desde que documentada a segregação mínima de responsabilidades críticas.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.02 - Qualidade dos Modelos de IA			
BPIA.02.01	Documentação sobre contexto de aplicação da IA	A empresa responsável pelo S-RES deve possuir documentação sobre o contexto exato de aplicação da IA pelo S-RES, contendo minimamente: • Descrição dos módulos, recursos e funcionalidades do S-RES que utilizam IA; • Descrição do escopo, objetivos e benefícios esperados do uso da IA pelo S-RES; • Usuários-alvo específicos da funcionalidade (por exemplo, profissionais de saúde, administradores hospitalares, gestores de operação, etc.); • Ambiente e situações específicas em que o sistema/aplicação é utilizado (por exemplo, consultórios, emergências, internação, operações administrativas, etc.); • Populações/pacientes-alvo e exclusões (por exemplo, indicações e contraindicações de uso, limites etários, condições clínicas específicas); • Descrição do que está fora do escopo ou é considerado como uso indevido da IA no S-RES (por exemplo, cenários onde o recurso de IA não deve ser utilizado); • Nível de autonomia da IA e o papel esperado do usuário na interação; • Declaração explícita de riscos conhecidos, vieses, considerações éticas e o nível de risco clínico da solução; • Condições de integração com outros sistemas, descrevendo se a aplicação funciona com interface gráfica ou se depende de integração via API para que outro sistema apresente as informações ao usuário final.	1
BPIA.02.02	Documentação técnica dos modelos de IA	A empresa responsável pelo S-RES deve possuir documentação dos algoritmos de IA utilizados, contendo minimamente: • Descrição do(s) modelo(s) de IA empregado(s), com indicação da abordagem ou técnica utilizada (por exemplo, redes neurais, deep learning, IA generativa, modelos probabilísticos, etc.); • Arquitetura técnica do(s) modelo(s) (inputs, outputs, camadas, processos internos, parâmetros, etc.); • Ferramentas, bibliotecas ou frameworks utilizados, informando o nome do fornecedor ou desenvolvedor (por exemplo, OpenAI, Google, etc.), nome do modelo ou biblioteca e Versão utilizada no momento da validação e publicação; • Em caso de IA Generativa, fontes de conhecimento (no caso de uso de Retrieval Augmented Generation - RAG, por exemplo) e processos de fine-tuning, se aplicável. Nota: Caso o S-RES utilize modelos de IA terceiros sem acesso à sua arquitetura interna, a empresa deve documentar detalhadamente entradas/saídas, limites de uso, métricas fornecidas pelo fabricante e evidências próprias de validação no contexto local.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.02.03	Avaliação dos atributos de qualidade da IA	a) A empresa responsável pelo S-RES deve possuir documentação técnica demonstrando que os seguintes atributos de qualidade da solução de IA foram definidos, avaliados e monitorados: • Precisão: grau de correção dos resultados produzidos; • Robustez: capacidade de manter desempenho em situações adversas, dados ruidosos ou incompletos; • Segurança: proteção contra ataques e manipulações externas; • Privacidade: proteção dos dados pessoais utilizados e gerados pela IA; • Interoperabilidade: capacidade de integração e comunicação segura com outros sistemas/aplicações; • Equidade: tratamento justo de diferentes grupos de usuários e populações, evitando vieses discriminatórios; • Explicabilidade: capacidade de apresentar, de forma compreensível, as razões para as decisões ou recomendações da IA; • Conformidade: aderência a requisitos regulatórios e legais aplicáveis; • Supervisão e controle humano: existência de mecanismos para que usuários possam revisar, aprovar ou intervir nas decisões da IA. b) A documentação deve demonstrar: • Como cada atributo foi interpretado e definido tecnicamente para o uso pretendido; • Quais métodos e/ou métricas (se aplicável) foram utilizados para avaliação de cada atributo; • Resultados quantitativos ou qualitativos obtidos; • Quais ações corretivas foram aplicadas, quando aplicável; • Processo adotado para revisão periódica desses atributos ao longo do tempo, garantindo que a revisão ocorra anualmente e sempre que houver mudanças significativas no modelo, nos dados ou nos requisitos regulatórios aplicáveis. c) A documentação ainda deve apresentar evidências visuais (por exemplo, prints de tela ou vídeos) que demonstrem, no próprio sistema, como os atributos estão efetivamente implementados na prática (por exemplo, mensagens de explicação apresentadas ao usuário, alertas de controle humano, telas de revisão manual, configurações de privacidade e segurança, etc.). Nota 1: Documentos já produzidos para atender a outros requisitos (por exemplo, mitigação de viés, segurança, validação clínica, etc.) podem ser utilizados como evidências complementares para comprovar conformidade a este requisito, desde que estejam claramente referenciados. Nota 2: A norma ISO/IEC 25059:2023 – Quality Model for AI Systems pode ser utilizada como referência para definição, avaliação e documentação desses atributos.	2

ID	Título	Descrição	Estágio de Maturidade
BPIA.02.04	Validação analítica e clínica dos modelos de IA	a) A empresa responsável pelo S-RES deve possuir documentação técnica contendo os resultados da validação analítica (desempenho técnico) do modelo de IA no contexto específico em que será utilizado pelo software, apresentando minimamente: • Resultados objetivos e quantitativos da validação do modelo de IA realizados no contexto de uso pelo S-RES, com indicação clara das métricas objetivas aplicadas ao uso pretendido (precisão, sensibilidade, especificidade, acurácia ou métricas equivalentes); • Comparação do desempenho da IA em relação a métodos ou processos atualmente adotados (se existentes); • Análise clara dos potenciais riscos associados à utilização da IA no contexto específico, com medidas objetivas adotadas para mitigação. b) Caso a aplicação do modelo de IA tenha finalidade clínica, a documentação deve adicionalmente apresentar validação clínica (impacto no desfecho clínico ou processo de cuidado): • Comparação do desempenho do modelo com padrões clínicos estabelecidos ou práticas clínicas aceitas como padrão-ouro ou padrão atual vigente; • Evidências sobre o impacto clínico (positivo e negativo) observado com o uso prático da IA no contexto específico. c) Para soluções que utilizam modelos de IA de base ou genéricos (por exemplo, LLMs), a documentação de validação deve ainda apresentar evidências de que: • O modelo foi adequadamente ajustado (fine-tuning) e/ou complementado (por exemplo, Retrieval Augmented Generation - RAG) com dados representativos do domínio específico (por exemplo, terminologia médica, diálogos clínicos, linguagem coloquial de pacientes brasileiros); • A validação demonstrou eficácia e segurança para as tarefas específicas do escopo (por exemplo, transcrição de consultas garante a correta interpretação de jargões técnicos e linguagem natural do paciente); • Foram avaliados e mitigados os riscos de "alucinação" (geração de informações factualmente incorretas) no contexto clínico específico. Nota 1: Caso o modelo de IA não tenha sido treinado especificamente pela empresa desenvolvedora do S-RES, a validação deverá ser obrigatoriamente realizada pela empresa em seu contexto específico de uso, usando bases representativas do cenário real de aplicação. Nota 2: Como referência para avaliação das métricas aplicáveis à solução de IA, pode-se utilizar o Testing and Evaluation (T&E) Framework da Coalition for Health AI (CHAI) de acordo com o caso de uso.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.02.05	Validação em ambiente de homologação/teste antes da entrada em produção	a) A empresa responsável pelo S-RES deve manter um ambiente de homologação ou testes controlado para validação de novos recursos com IA antes de sua ativação em ambiente real de produção. b) O processo de validação deve garantir que: • O recurso com IA seja testado com dados representativos do contexto de uso pretendido; • Participem do teste profissionais que representam o perfil de usuários finais do sistema/aplicação; • Erros, falhas ou inconsistências identificadas nesse ambiente sejam corrigidos antes da liberação para produção; • O ambiente seja segregado do ambiente de produção, com dados seguros e controlados. c) Deve haver ainda uma documentação formal com a descrição das políticas e processo de homologação e validação antes da ativação de recursos de IA no S-RES.	1
BPIA.02.06	Qualidade em adaptações ou configurações	Condição: S-RES permite ao usuário realizar adaptações ou configurações nos modelos ou recursos de IA, tais como alteração de parâmetros do modelo, mudanças em limiares de decisão, fine-tuning com dados fornecidos pelo cliente, Retrieval Augmented Generation (RAG) ou outras customizações específicas ao contexto local. a) A empresa responsável pelo S-RES deve possuir mecanismos para garantir que adaptações ou configurações realizadas pelos usuários não impliquem degradação de qualidade ou segurança em comparação aos parâmetros validados pelo fabricante. b) A empresa responsável pelo S-RES deve disponibilizar um documentação com as configurações e parâmetros padrão do modelo, definidos pelo fabricante como seguros e validados, incluindo avisos sobre limites e condições de uso. c) A empresa responsável pelo S-RES deve garantir e documentar validação técnica sempre que houver uso de RAG ou fine-tuning com dados do cliente. Essa validação deve demonstrar que a adaptação preserva a qualidade e segurança da solução antes de sua disponibilização operacional. d) Caso a solução ofereça recursos baseados em IA Generativa que permitam que usuários possam criar ou personalizar recursos da IA (por exemplo, criação de assistentes utilizando prompts), a empresa responsável pela solução de IA deve documentar e apresentar em manual as boas práticas necessárias para criação/personalização adequada.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.02.08	Qualidade e segurança na utilização de modelos de IA generativa	Condição: S-RES utiliza modelos de IA Generativa. a) O S-RES deve implementar mecanismos de mitigação de alucinações, de forma a evitar e tratar riscos de geração de respostas imprecisas, inventadas ou não fundamentadas em dados clínicos disponíveis. Isso pode incluir: • Restrição do modelo a fontes específicas de dados confiáveis, garantindo que a IA só possa utilizar informações provenientes de bases previamente validadas; • Mensagens de aviso ao usuário sobre a confiabilidade da resposta e a necessidade de validação clínica antes da tomada de decisão; • Validações automáticas de consistência, como verificações cruzadas do conteúdo gerado em relação a dados estruturados já registrados no prontuário; • Recuperação aumentada por busca (Retrieval-Augmented Generation – RAG): técnica em que o modelo acessa uma base documental validada (por exemplo, protocolos clínicos, diretrizes médicas, dados do paciente) no momento da geração, de modo a fundamentar suas respostas em informações verificáveis; • Verificação cruzada de múltiplos modelos ou algoritmos (ensemble ou cross-check), para comparar saídas e reduzir a probabilidade de respostas inconsistentes ou inventadas b) O S-RES deve implementar salvaguardas (guardrails) que limitem o comportamento da IA utilizando mecanismos técnicos e/ou de usabilidade que limitem a atuação da IA generativa, prevenindo: • Geração de conteúdo fora do escopo clínico validado; • Respostas que contenham termos impróprios, diagnósticos não validados, opiniões pessoais ou linguagem inadequada; • Interações com comandos ambíguos que possam induzir a IA a comportamentos inesperados. Nota: Além das técnicas citadas, podem ser aplicadas outras boas práticas de mercado, desde que a empresa forneça documentação técnica demonstrando como o mecanismo implementado contribui para a redução do risco de alucinações e geração de conteúdo inadequado.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.03 - Qualidade de Dados e Bases de Treinamento			
BPIA.03.01	Base de dados utilizadas pela IA	A empresa responsável pelo S-RES deve possuir documentação sobre as bases de dados de treinamento e validação utilizadas, contendo minimamente: • Descrição das bases de dados; • Origem dos dados utilizados (instituições, países, bases públicas ou privadas); • Volume total dos dados (quantidade de registros ou amostras utilizadas); • Características dos dados, incluindo descrição clara das variáveis clínicas presentes; • Representatividade populacional dos dados (faixa etária, gênero, etnia, condições clínicas específicas, etc.) e justificativa estatística para o tamanho das bases utilizadas; • Critérios e métodos detalhados utilizados para limpeza, transformação, processamento e validação interna dos dados. • Descrição do histórico de treinamento; • Indicação se as bases de dados incluem dados pessoais ou sensíveis; bem como descrição dos mecanismos utilizados para anonimização ou pseudonimização dos dados. Nota: Caso o S-RES utilize um modelo de IA pré-treinado por terceiros (por exemplo, modelos generalistas), deve haver uma documentação oficial do fornecedor do modelo de IA contendo informações gerais sobre a origem e tipos de dados utilizados para treinamento. Quando informações completas não forem disponibilizadas pelo fornecedor, a empresa deve documentar que tais limitações foram identificadas e disponibilizar essa documentação para seus clientes em manual técnico ou equivalente.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.03.02	Gestão de vieses nos dados	A empresa responsável pelo S-RES deve possuir documentação técnica contendo evidências sobre o processo de identificação, prevenção e mitigação de vieses algorítmicos em modelos de IA utilizados, incluindo minimamente: • Identificação dos tipos específicos de vieses que possam ocorrer no contexto específico de utilização da IA pelo S-RES. • Relatório de testes realizados para detecção desses vieses identificados, contendo a descrição do método utilizado para identificar vieses e os resultados quantitativos dos testes aplicados. • Descrição das ações técnicas adotadas para prevenção e mitigação dos vieses identificados, incluindo: ajustes e balanceamento das bases de treinamento e validação; implementação de técnicas específicas para correção de vieses (por exemplo, reponderação dos dados, técnicas de "fairness-aware"); revisões periódicas e contínuas da performance do modelo para identificar novos vieses emergentes. • Processo de monitoramento contínuo para detecção de vieses emergentes em produção. Nota 1: Caso o S-RES utilize um modelo de IA pré-treinado por terceiros (por exemplo, modelos generalistas), a empresa deve realizar testes independentes sobre vieses com dados representativos do contexto local. Nota 2: A título de exemplo, seguem alguns tipos de vieses: - Viés de seleção populacional: Sistema treinado apenas com dados de uma determinada população, resultando em menor eficácia em populações com características diferentes (por exemplo, treinado apenas com indivíduos adultos jovens, dificultando aplicação em idosos). - Viés relacionado ao gênero ou etnia: Modelos clínicos que funcionam adequadamente para indivíduos do sexo masculino, mas apresentam menor desempenho para mulheres. - Viés diagnóstico: IA que privilegia diagnósticos mais comuns ou frequentes em detrimento de condições clínicas raras, prejudicando diagnóstico precoce ou tratamento adequado. - Viés cultural ou linguístico: Algoritmo de IA generalista que interpreta inadequadamente contextos regionais, linguísticos ou culturais específicos, levando a decisões ou recomendações inadequadas no atendimento ao usuário.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.03.03	Qualidade dos dados em aprendizado contínuo e retreinamento	Condição: S-RES utiliza modelos de IA que utilizam aprendizado contínuo, passam por retreinamento periódico pela empresa e/ou são atualizados com base em dados obtidos de instituições usuárias do S-RES (produção). a) A empresa responsável pelo S-RES deve garantir a segurança, rastreabilidade e conformidade do processo de atualização ou evolução dos modelos de IA. b) Caso o modelo realize aprendizado contínuo automaticamente, o S-RES deve implementar mecanismos de: • Auditoria contínua de desempenho e desvio de comportamento; • Possibilidade de rollback para versões anteriores em caso de erro; • Logs detalhados das atualizações realizadas; c) Caso o modelo passe por retreinamento periódico realizado pela própria empresa: • O processo de retreinamento deve estar documentado, incluindo frequência, fontes de dados utilizadas, critérios de desempenho para aceitação do novo modelo; • O novo modelo deve passar por validação completa antes de entrar em produção; • O sistema/aplicação deve permitir controle de versão entre os modelos anteriores e atualizados; • A instituição cliente deve ser notificada sobre atualizações significativas no modelo. d) Caso o modelo passe por retreinamento utilizando dados obtidos da base de produção da instituição: • O sistema/aplicação deve garantir que os dados utilizados sejam anonimizados ou pseudonimizados antes de serem incorporados; • Deve haver declaração formal da instituição autorizando esse uso, ou previsão contratual clara; • O sistema/aplicação deve registrar data de coleta dos dados, tipo de dado utilizado e vinculação ao modelo gerado.	2

ID	Título	Descrição	Estágio de Maturidade
BPIA.03.04	Curadoria, validação e governança de bases de conhecimento	Condição: S-RES utiliza/acessa uma ou mais bases de conhecimento para apoio à decisão clínica. a) O S-RES deve utilizar bases de conhecimento clínicas validadas, garantindo curadoria formal, rastreabilidade de origem e atualização controlada de todo o conteúdo utilizado. b) Todas as bases de conhecimento acessadas pela IA devem atender aos seguintes critérios: • Origem e mantenedor identificados (por exemplo, PubMed, protocolos institucionais do cliente, etc.); • Processo formal de curadoria, revisão periódica e validação científica/documental; • Controle de versão e registro de data da última atualização; • Responsável técnico ou comitê clínico responsável pela validação e aprovação; • Critérios de exclusão de fontes não confiáveis (blogs, fóruns, textos sem revisão por pares). c) Quando a base de conhecimento utilizada for de terceiros, a empresa responsável pelo S-RES deve obter e manter documentação formal comprobatória da conformidade dessa base, incluindo: • Declaração do fornecedor confirmando a existência de processo de curadoria e revisão científica; • Descrição do processo de atualização e periodicidade de revisão dos conteúdos; • Política de versionamento e histórico de revisões; • Identificação dos responsáveis técnicos pela revisão dos conteúdos (quando aplicável); • Termo ou contrato que assegure que a base não contém informações sem validação científica, não revisadas por pares ou que contrariem diretrizes reconhecidas.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.04 - Transparência, Explicabilidade e Interação com o Usuário			
BPIA.04.01	Transparência quanto ao escopo da IA	Condição: S-RES possui uma interface gráfica para interação com o usuário ou S-RES é operado em um dispositivo físico sem interface gráfica. a) O S-RES deve disponibilizar ao profissional mensagens e/ou alertas explícitos sobre as limitações e o escopo pretendido de suas funcionalidades de IA de forma a prevenir o uso indevido. Por exemplo, um chatbot de busca de informações no prontuário exibindo uma mensagem fixa informando que ele não deve ser utilizado para fins diagnósticos. b) A mensagem/alerta deve ser apresentada em momentos críticos da interação do usuário com a funcionalidade de IA (por exemplo, mensagem fixa na tela, ao abrir a funcionalidade pela primeira vez, ao gerar um resultado sensível, etc.). Nota: Caso o S-RES seja operado em um dispositivo físico sem interface gráfica, a mensagem/alerta deve ser emitidos de forma auditiva ou equivalente.	1
BPIA.04.02	Identificação visível das informações geradas por IA	Condição: S-RES possui uma interface gráfica para interação com o usuário. O S-RES deve apresentar de forma clara e visível que a informação exibida foi gerada por IA, evitando interpretações ambíguas. Essa identificação deve: • Estar próxima ao conteúdo gerado ou em destaque visual acessível; • Ser acompanhada de um ícone, tag, texto ou outro elemento gráfico que indique: "Gerado por IA" / "Sugestão da IA" / "Resultado assistido por IA", etc..	1
BPIA.04.03	Transparência de estado e ações em tempo real	Condição: O S-RES utiliza funcionalidades de IA que operam de forma contínua ou em segundo plano, capturando dados do ambiente do usuário (por exemplo, áudio do microfone, captura de tela, monitoramento de vídeo). a) O S-RES deve garantir que o usuário seja informado de forma clara, contínua e inequívoca sobre o estado operacional da funcionalidade de IA. b) O S-RES deve exibir um indicador visual e/ou sonoro e de fácil identificação sempre que uma funcionalidade de IA estiver em um estado ativo de captura de dados. Por exemplo, um aviso textual ou aviso sonoro indicando o status de "ouvindo" (microfone) ou "vendo" (câmera/tela).	2

ID	Título	Descrição	Estágio de Maturidade
BPIA.04.04	Mecanismo de explicabilidade da decisão da IA	a) O S-RES deve disponibilizar ao profissional, de forma acessível na interface, uma explicação sobre os principais fatores que contribuíram para os dados gerados pela IA. b) A explicação deve conter, minimamente, os seguintes dados conforme o tipo de aplicação: 1) Soluções de IA que geram conclusões, recomendações, predições ou classificações (por exemplo, sugestão de diagnósticos a partir da análise de dados clínicos): • Os elementos mais relevantes (variáveis de entrada ou características do paciente) que justificam a saída apresentada; • Referências (evidências científicas, guidelines, publicações, etc.) que contribuíram para os resultados gerados pela IA (se aplicável); • Quando decorrente de protocolos ou regras determinísticas, indicação da regra disparada, do protocolo/diretriz aplicado e da respectiva versão e data. 2) Soluções de IA que geram conteúdo textual (por exemplo, sumarização de prontuário): • Indicação das fontes utilizadas para geração dos dados apresentados pela IA (por exemplo, laudos, prescrições, evolução clínica, anotações de enfermagem); • Janela temporal dos dados considerados, quando aplicável (por exemplo, “últimos 7 dias de internação”, “apenas atendimento atual”, etc.). 3) Soluções de IA que geram dados estruturados a partir de texto livre e/ou fala (por exemplo, aplicação de ambient listening que gera dados estruturados a partir da gravação de uma consulta), o S-RES deve apresentar, minimamente, os seguintes dados: • Trechos originais que deram origem aos dados estruturados; • Classificações, terminologias ou ontologias utilizadas no mapeamento, quando aplicável (por exemplo, CID10). 4) Soluções de IA que atuam como assistentes conversacionais (por exemplo, ChatBot para o profissional de saúde que busca e apresenta dados de pacientes): • Fonte de informação utilizada para as respostas, quando aplicável; • Data/hora da última atualização da fonte de informação utilizada, quando aplicável. 5) Soluções de IA que realizam análise de sinais ou imagens médicas (por exemplo, apresentação de achados suspeitos): • Destaque visual ou gráfico das regiões/sinais relevantes para a conclusão apresentada pela IA (por exemplo, heatmaps); • Principais características que levaram à conclusão;	1

ID	Título	Descrição	Estágio de Maturidade
		• Grau de confiança na classificação, quando aplicável. c) A explicação deve ser acessível na mesma tela/interface em que o usuário interage com a solução de IA. Nota 1 – Aplicações sem interface gráfica: Caso o S-RES não possua interface gráfica (por exemplo, solução integrada a um prontuário eletrônico de outro fornecedor), ele deve disponibilizar via integração (API, serviços ou conectores) os dados necessários para que o sistema que faz a exibição ao usuário final apresente a explicabilidade de forma clara, nos termos definidos neste requisito. Nota 2 - Solução de IA operada por meio de um dispositivo físico sem interface gráfica: Caso o S-RES seja operado em um dispositivo físico sem interface gráfica, a explicação deve ser disponibilizada ao profissional por meio de mecanismos alternativos adequados ao contexto do dispositivo (por exemplo, assistente de voz pergunta ao usuário se ele deseja ouvir a explicação para as decisões apresentadas pela IA). Nota 3 - Uso de Modelos de IA de Terceiros: Caso o S-RES utilize modelos de IA desenvolvidos por terceiros que não fornece explicações detalhadas sobre suas conclusões (modelo "black-box"), a empresa deve documentar que tais limitações foram identificadas e disponibilizar essa documentação para seus clientes em manual técnico ou equivalente.	

ID	Título	Descrição	Estágio de Maturidade
BPIA.04.05	Identificação correta de pacientes em interações com IA	Condição: O S-RES utiliza funcionalidades de IA para buscar e/ou acessar o prontuário ou registros de um paciente específico (por exemplo, busca via chatbot ou voz). a) A empresa responsável pelo S-RES deve implementar mecanismos de segurança para mitigar o risco de seleção ou acesso ao prontuário do paciente errado. b) Confirmação da Compreensão: Após receber um comando de busca por um paciente, o S-RES deve primeiro apresentar ao usuário qual paciente ela interpretou, solicitando confirmação antes de prosseguir. Exemplo: Comando de voz: "Abrir prontuário de João da Silva". Resposta do sistema: "Entendido: paciente 'João da Silva'. Correto?". c) Tratamento de Ambiguidade: Caso mais de um paciente corresponda aos critérios de busca, o S-RES deve obrigatoriamente apresentar uma lista de desambiguação, exigindo que o usuário selecione explicitamente o paciente correto. É vedado ao sistema selecionar automaticamente o que considera ser o resultado "mais provável". d) Dados para Identificação Inequívoca: A lista de desambiguação deve conter um conjunto mínimo de dois ou mais identificadores para permitir uma identificação inequívoca pelo profissional. Exemplos de identificadores: nome completo, data de nascimento, nome da mãe, CPF ou CNS.	1
BPIA.04.06	Garantia de uso de dados válidos	Condição: S-RES utiliza IA para gerar resultados a partir de dados existentes em um repositório de dados de pacientes (Prontuário Eletrônico do Paciente, por exemplo). a) Caso a funcionalidade de IA do S-RES gere resultados a partir de dados existentes em um repositório de dados de pacientes (por exemplo, Prontuário Eletrônico do Paciente), o sistema deverá garantir que apenas os dados válidos sejam utilizados como base para geração dos resultados. Por exemplo, ao gerar resumo de dados clínicos do prontuário, o S-RES não deve utilizar dados/documentos inativos/cancelados ou não liberados. b) Caso a solução possa ser utilizada via integração com sistemas de terceiros, a empresa responsável pelo S-RES deve fornecer uma documentação (por exemplo, manual de integração ou especificação técnica de API) que instrua explicitamente o sistema externo sobre a necessidade de enviao apenas de dados válidos.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.04.07	Validação de dados gerados por IA para incorporação ao prontuário	Condição: S-RES incorpora dados gerados por IA a um repositório de dados de pacientes (Prontuário Eletrônico do Paciente, por exemplo). a) Caso a funcionalidade de IA do S-RES gere dados para serem incorporados a um repositório de dados de pacientes (por exemplo, Prontuário Eletrônico do Paciente), o sistema deverá exigir a validação e confirmação explícita por parte do usuário antes que esses dados sejam efetivamente registrados no repositório/prontuário (human-in-the-loop). Exemplos incluem, sugestão de diagnósticos ou condutas, geração automática de documentações clínicas, geração de dados estruturados a partir de texto livre, etc. b) A efetivação da confirmação do usuário deve ser registrada no repositório/prontuário, indicando o responsável e data/hora da confirmação.	1
BPIA.04.08	Indicação de uso de IA	a) O S-RES deve identificar de forma inequívoca todo registro clínico que tenha sido gerado ou editado com o suporte de tecnologias de IA (por exemplo, textos gerados por ambient listening). b) O sistema deve gerar um indicador (metadado) associado ao registro clínico, informando se houve ou não o uso de IA em sua elaboração. Este indicador deve ser armazenado como parte integrante do registro. c) Sempre que um registro realizado com apoio de IA for visualizado na aplicação, o S-RES deve apresentar uma sinalização clara ao usuário indicando que houve uso de IA na geração daquele registro. Nota: Caso o S-RES não possua interface gráfica, a empresa responsável deve disponibilizar via integração (API, conector ou serviço) o envio deste metadado.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.04.09	Ativação/inativação de IA em nível institucional	a) O S-RES deve permitir que instituição possa ativar ou inativar recursos de IA em nível institucional (para todos os profissionais). b) A ativação/inativação deve ser de forma individualizada por funcionalidade (por exemplo, desativar a sugestão de diagnósticos e manter o ambient listening ativado com transcrição e geradação automática da documentação clínica), não sendo mandatória a desativação global da solução para inativar um recurso específico. c) Quando uma funcionalidade com IA for desativada, o S-RES deve: • Exibir mensagens/alertas informando os riscos clínicos ou operacionais da desativação; • Garantir que resultados ou recomendações geradas anteriormente por IA não permaneçam ativos de forma ambígua; • Oferecer, quando aplicável, alternativas manuais ou instruções claras de operação sem IA. d) A tela de ativação/inativação de recursos de IA deve apresentar a lista de recursos com indicação de quais estão ativas ou inativas. Deve ser possível ainda visualizar um histórico de alterações com a data/hora, usuário responsável, recurso de IA envolvido e ação realizada (ativação ou inativação). Nota 1: Caso o S-RES não possua interface gráfica, a empresa responsável deve disponibilizar via integração (API, conector ou serviço) os mecanismos de ativação/desativação, os alertas e os registros necessários, para que o sistema que estiver integrado à aplicação de IA apresente essas informações ao usuário e registre as ações da instituição. Nota 2: A inativação não se aplica a recursos onde a IA é alicerce indispensável para a conclusão do processo. Portanto, essa funcionalidade deve estar disponível apenas para recursos de IA cuja inativação não comprometa a viabilidade operacional do fluxo de trabalho principal da solução.	2

ID	Título	Descrição	Estágio de Maturidade
BPIA.04.10	Ativação/inativação de IA pelo profissional no momento do uso	a) O S-RES deve permitir que a instituição configure quais recursos de IA os profissionais terão autonomia para inativar temporariamente durante o processo (uso pontual). Por exemplo, configurar que os profissionais poderão desativar o recurso de ambient listening durante a consulta médica. b) Quando permitido pela configuração institucional, o S-RES deve oferecer ao profissional a opção de ativar ou inativar recursos de IA diretamente na aplicação (por exemplo, tela de consulta) antes do início do processo. c) Ao inativar um recurso de IA, o S-RES deve exigir uma justificativa ao usuário (por exemplo, recusa do paciente). d) O S-RES deve deixar claro para o profissional quais recursos de IA estão inativos. e) O S-RES deve permitir que a instituição visualize um histórico de ativações/inativações de recursos de IA pelos profissionais, apresentando com a data/hora, usuário responsável, recurso de IA envolvido, ação realizada (ativação ou inativação) e justificativa. Nota 1: Caso o S-RES não possua interface gráfica, a empresa responsável deve disponibilizar via integração (API, conector ou serviço) os mecanismos de ativação/desativação, os alertas e os registros necessários, para que o sistema que estiver integrado à aplicação de IA apresente essas informações ao usuário e registre as ações da instituição. Nota 2: A inativação não se aplica a recursos onde a IA é alicerce indispensável para a conclusão do processo. Portanto, essa funcionalidade deve estar disponível apenas para recursos de IA cuja inativação não comprometa a viabilidade operacional do fluxo de trabalho principal da solução.	2

ID	Título	Descrição	Estágio de Maturidade
BPIA.04.11	Feedback Imediato dos Usuários sobre Respostas da IA	a) O S-RES deve oferecer um mecanismo direto e acessível para que o usuário possa: • Relatar problemas, erros ou inadequações identificadas na resposta da IA; • Fornecer comentários ou sugestões sobre a qualidade ou utilidade do conteúdo gerado; • Classificar a resposta (por exemplo, útil / não útil, adequado / inadequado). b) Esse mecanismo de feedback deve: • Quando a aplicação possuir interface gráfica, estar disponível no ponto de uso, vinculado diretamente à resposta da IA apresentada; • Quando a aplicação não possuir interface gráfica, disponibilizar meios de integração (por exemplo, APIs, conectores) para que o sistema que exibe a resposta ao usuário final possa coletar e transmitir o feedback à aplicação de IA; • Quando a aplicação estiver embutida em um dispositivo físico sem interface gráfica, disponibilizar formas alternativas adequadas ao contexto (por exemplo, comando de voz para relatar problema). c) O mecanismo de feedback deve garantir anonimato ou identificação opcional do usuário que envia o feedback. d) O S-RES deve disponibilizar um recurso funcional (interface gráfica administrativa, relatórios, etc.) que permita à instituição de saúde visualizar os feedbacks recebidos, apresentando minimamente os seguintes dados: • Data/hora do feedback; • Qual funcionalidade estava sendo usada; • Qual foi a resposta da IA contestada; • Feedback do usuário.	3

ID	Título	Descrição	Estágio de Maturidade
BPIA.04.12	Disponibilização de documentações técnicas e de governança para clientes e usuários	a) A empresa responsável pelo S-RES deve disponibilizar aos seus clientes/usuários acesso transparente e facilitado às documentações técnicas e de governança relacionados à IA, incluindo minimamente: • Documentação sobre atendimento aos princípios de IA responsável; • Documentação sobre o processo formal de gestão de riscos para IA; • Documentação sobre contexto de aplicação da IA; • Documentação técnica dos modelos de IA; • Documentação sobre validação analítica e clínica dos modelos de IA; • Documentação sobre as base de dados utilizadas pela IA; • Documentação sobre a arquitetura de execução da IA e respectiva infraestrutura; • Plano de monitoramento pós-mercado e avaliação em ambiente real de produção. b) A disponibilização das documentações deve atender aos seguintes critérios: • Se o S-RES possuir interface gráfica, os documentos devem estar acessíveis diretamente pelo sistema/aplicação. Nesse caso, o sistema/aplicação deve apresentar as documentações pertinentes exatamente nas mesmas telas onde os recursos de IA são utilizados (por exemplo, seção “Sobre a IA”, “Documentação Técnica” ou equivalente); • Se o S-RES não possuir interface gráfica, os documentos devem estar acessíveis pelo site da empresa ou outro meio formal de comunicação; • Os documentos devem estar organizados, atualizados e em linguagem clara e acessível ao público-alvo específico de cada documento; • A documentação deve apresentar versão, data da última atualização e responsável técnico pela publicação.	2

ID	Título	Descrição	Estágio de Maturidade
BPIA.04.13	Manual de Uso Seguro e Informações Técnicas da IA	a) A empresa responsável pelo S-RES deve disponibilizar aos seus clientes/usuários do S-RES manuais relacionados aos recursos de IA, contendo minimamente: • Instruções de uso correto e seguro da IA, com exemplos de aplicação e advertências sobre limites e riscos; • Descrição dos objetivos clínicos, operacionais ou administrativos dos recursos baseados em IA; • Requisitos técnicos para funcionamento adequado (por exemplo, ambiente computacional, dependências externas, conectividade, infraestrutura mínima); • Instruções de instalação (quando aplicável); • Instruções para adaptações, configurações e atualizações da IA (quando aplicável); • Instruções para uso dos recursos de IA no contexto de uso do S-RES da IA (quando aplicável); • Recomendações para supervisão humana e validação dos resultados; • Canal de contato técnico para dúvidas ou incidentes. b) A disponibilização dos manuais deve atender aos seguintes critérios: • Se o S-RES possuir interface gráfica, os documentos devem estar acessíveis diretamente pelo sistema/aplicação. Nesse caso, o sistema/aplicação deve apresentar as documentações pertinentes exatamente nas mesmas telas onde os recursos de IA são utilizados (por exemplo, seção “Sobre a IA”, “Documentação Técnica” ou equivalente); • Se o S-RES não possuir interface gráfica, os documentos devem estar acessíveis pelo site da empresa ou outro meio formal de comunicação; • Os documentos devem estar organizados, atualizados e em linguagem clara e acessível ao público técnico-clínico ou institucional que utiliza o sistema/aplicação; • A documentação deve apresentar versão, data da última atualização e responsável técnico pela publicação.	1

ID	Título	Descrição	Estágio de Maturidade
BPIA.05 - Monitoramento e Avaliação Contínua			
BPIA.05.01	Monitoramento interno e auditorias de desempenho da IA	a) A empresa responsável pelo S-RES deve manter um plano formal de auditoria e monitoramento interno dos modelos de IA utilizados, com o objetivo de garantir a revisão periódica da performance, confiabilidade e segurança da IA. Esse plano deve incluir, minimamente: • Plano de auditorias internas periódicas para avaliação da IA, com definição de escopo, frequência e responsáveis; • Indicadores internos que serão utilizados para análise da performance da IA, segurança, qualidade, impacto clínico ou operacional (conforme o contexto de uso); • Metodologia que será utilizada para detectar e documentar degradações de desempenho, desvios em relação aos padrões estabelecidos ou riscos residuais emergentes; • Metodologia que será utilizada para registro e execução das ações corretivas adotadas com base nos achados das auditorias. b) Deve haver ainda documentações que apresentem as auditorias internas já realizadas, incluindo datas, escopo avaliado, resultados, medidas corretivas, logs ou históricos de revisão dos modelos e das decisões técnicas associadas.	2

ID	Título	Descrição	Estágio de Maturidade
BPIA.05.02	Monitoramento pós-mercado e avaliação em ambiente real de produção	a) A empresa responsável pelo S-RES deve manter um plano de monitoramento contínuo da IA em ambiente real de produção, voltado à identificação de problemas, manutenção da performance e coleta estruturada de feedback dos usuários. O plano deve conter, minimamente: • Descrição dos mecanismos técnicos implantados no S-RES para monitorar a performance da IA em produção, como coleta de métricas de desempenho, logs de decisão, alertas de inconsistência, etc.; • Estratégia para coleta ativa e passiva de feedback de usuários, incluindo canais de comunicação integrados ou não ao S-RES (por exemplo, botão de “reportar problema”, formulários de avaliação de resultado, etc.); • Processo para notificação, registro e resposta a eventos adversos, falhas ou erros percebidos pelos usuários; • Procedimento para incorporar os achados do uso em produção à melhoria contínua do modelo de IA. b) Caso o S-RES e respectivos recursos de IA já estejam em uso em ambiente real, a empresa ainda deve manter relatórios gerados a partir do uso real, incluindo minimamente: • Feedbacks coletados; • Eventos registrados; • Métricas de desempenho da IA coletadas; • Registro das ações realizadas com base no monitoramento em produção (por exemplo, ajustes, retreinamento, bloqueios, mudanças de interface).	1
BPIA.05.05	Análise de Indicadores de impacto da solução de IA	a) A empresa responsável pelo S-RES deve estabelecer, documentar e monitorar indicadores de impacto/desfecho relacionados ao uso de sua solução de IA, abrangendo dimensões de acordo com o escopo da solução de IA, tais como: • Clínicos: impacto em diagnósticos, desfechos de pacientes, segurança clínica. • Operacionais: tempo de atendimento, tempo de espera, tempo para execução de tarefas. • Financeiros: redução de custos, otimização de recursos, retorno sobre investimento. • Experiência do usuário: satisfação de pacientes e profissionais. b) O plano de monitoramento de desfechos deve incluir: • Definição formal dos indicadores a serem acompanhados (com critérios de medição e periodicidade); • Mecanismos para coleta estruturada desses indicadores junto às instituições clientes (por exemplo, dashboards, formulários padronizados, integração de dados anonimizados ou relatórios periódicos compartilhados); • Processo de retroalimentação, onde os indicadores coletados alimentam o ciclo de melhoria contínua do modelo e do sistema.	3

3.2. Requisitos de Estrutura, Conteúdo e Funcionalidade (ECF)

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
ECF.02 - Identificação de Profissionais da Organização				
ECF.02.01	Identificação dos profissionais da organização	a) O S-RES deve permitir o cadastro de profissionais da organização permitindo registrar minimamente os seguintes campos: • nome; • nome social/apelido; • sexo (designação biológica); • gênero (identidade de gênero do profissional); • data de nascimento; • nacionalidade; • idioma falado pelo profissional; • município de nascimento e UF; • data de naturalização (para estrangeiros); • país de nascimento (para estrangeiros); • número do passaporte, país emissor, data de emissão e data de validade (para estrangeiros); • e-mail principal; • tipo de telefone, DDD e número de telefone; • endereço completo: tipo de logradouro, nome do logradouro, número, complemento, bairro/distrito, município, Unidade Federativa, país e CEP; • número do CPF; • número de identidade – complemento, UF, órgão e data de emissão; • conselho profissional e respectivo número de registro e Unidade Federativa; • código e descrição CBO. Nota: Os campos apresentados acima devem estar presentes no formulário, mas não necessariamente de preenchimento obrigatório.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e ser utilizada por profissionais de saúde.	1
ECF.02.02	Duplicidade de cadastros de profissionais	O S-RES deve possuir um mecanismo de validação que emita uma mensagem de aviso ao usuário e impeça a continuidade do registro em caso de duplicidade de cadastro de profissional. A validação deve ser realizada pelo menos para o número do CPF e conselho profissional.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
			ser utilizada por profissionais de saúde.	
ECF.03 - Identificação de Pacientes				
ECF.03.01	Dados demográficos do paciente	a) O S-RES deve identificar o sujeito da atenção de forma unívoca e estar aderente à plenitude das regras vigentes estabelecidas pelo Ministério da Saúde para o Cartão Nacional de Saúde (CNS). O cadastro do sujeito deve conter minimamente os seguintes campos: • nome; • nome social/apelido; • nome da mãe, permitindo indicação de mãe desconhecida de forma estruturada; • sexo (designação biológica); • gênero (identidade de gênero do paciente); • data de nascimento; • raça/cor (branca, preta, parda, amarela, indígena e "sem informação"); • nacionalidade; • idioma falado pelo paciente; • município de nascimento e UF; • data de naturalização (para estrangeiros); • país de nascimento (para estrangeiros); • número do passaporte, país emissor, data de emissão e data de validade (para estrangeiros); • e-mail principal; • tipo de telefone, DDD e número de telefone; • endereço completo: tipo de logradouro, nome do logradouro, número, complemento, bairro/distrito, município, Unidade Federativa, país e CEP; • número do CPF; • número de identidade – complemento, UF, órgão e data de emissão; • número do Cartão Nacional de Saúde (CNS); • guardião ou representante legal (nome, grau de relacionamento ou parentesco com o paciente e CPF). Nota: Os campos apresentados acima devem estar presentes no formulário, mas não necessariamente de preenchimento obrigatório.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir um repositório de dados de pacientes.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
ECF.03.02	Número de identificação do paciente no sistema	a) Para todo paciente cadastrado, o S-RES deve gerar automaticamente um número de identificação no sistema (ID do paciente/prontuário). b) Esse número deve ser passível de visualização na aplicação.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir um repositório de dados de pacientes.	
ECF.03.07	Verificação de duplicidade de cadastros de pacientes	O S-RES deve possuir um mecanismo de validação que emita uma mensagem de aviso ao usuário e impeça a continuidade do registro em casos de duplicação de cadastro de paciente. A validação deve ser realizada pelo menos para o número do CPF.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir um repositório de dados de pacientes.	1
ECF.16 - Integridade e Ciclo de Vida de Registros Clínicos				
ECF.16.04	Inativação de registros clínicos já finalizados	a) O S-RES deve permitir a inativação (cancelamento) de registros de dados clínicos e atendimentos previamente armazenados e finalizados no sistema (prescrições, sinais vitais, diagnósticos, alergias, documentos clínicos, etc.). b) Toda inativação de registros de dados clínicos ou atendimentos deve exigir uma justificativa ao usuário. A inativação só poderá ser concluída após indicação da justificativa. c) A inativação de um registro deve alterar seu respectivo status para inativo (ou outro termo de mesmo significado) e registrar a data/hora e usuário responsável pela inativação/cancelamento. d) Todos os dados registrados no S-RES e considerados como finalizados (registros definitivos e liberados) devem ser mantidos permanentemente. Dessa forma, registros inativos devem continuar vinculados ao prontuário do respectivo paciente e ser passíveis de visualização tanto em tela quanto exportação, incluindo data/hora, profissional responsável e justificativa da inativação.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução permitir o registro e armazenamento de dados clínicos diretamente no sistema.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
		e) Qualquer registro que tenha sido inativado deve ter seu status de inativo apresentado de forma clara e destacada tanto em tela quanto exportação, de forma a deixar evidente o conteúdo que está inativo (tachando o texto, por exemplo). Nota 1: Consideram-se como finalizados os registros que foram concluídos e liberados pelo profissional, não considerando registros salvos em caráter provisório (salvo como rascunho). Nota 2: O conceito de inativação/cancelamento utilizado neste requisito não deve ser confundido com o estado de resolução de um determinado problema do paciente (diagnóstico, alergia, intolerância, etc.). A inativação ou cancelamento de um diagnóstico indica que o respectivo registro foi realizado de forma incorreta e, portanto, deve ser desconsiderado no prontuário. Já a alteração do estado de um diagnóstico para “resolvido” indica que o problema existiu, foi corretamente registrado e que o paciente não apresenta mais a condição no momento atual.		
ECF.16.05	Regras para correção de dados já finalizados	Condição: S-RES permite a alteração de registros clínicos já finalizados/liberados pelo profissional. a) A correção de qualquer dado do prontuário e/ou registro clínico somente poderá ser realizada pelo profissional que realizou o registro original. b) Qualquer correção aplicada a um dado do prontuário e/ou registro clínico já finalizado/liberado deverá implicar na geração de uma nova versão do registro, devendo a versão anterior ser mantida no prontuário do paciente com status explicitamente identificado como inativa/cancelada. c) Toda correção de um dado do prontuário e/ou registro clínico deverá exigir o registro de uma justificativa, informada pelo usuário no momento da alteração. d) Ao acessar a versão atual de um registro no sistema, o S-RES deverá indicar de forma clara a existência de versões anteriores, bem como permitir o acesso fácil a essas versões, garantindo sua visualização integral juntamente com a indicação da data/hora da inativação/cancelamento, usuário responsável e justificativa. e) Nos casos de exportação, impressão ou geração de documentos externos (por exemplo, em formato PDF), o S-RES também deverá permitir a visualização das	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução permitir o registro e armazenamento de dados clínicos diretamente no sistema.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
		versões anteriores do registro, deixando explícito que correspondem a registros inativos/cancelados (tachando o texto, por exemplo) e apresentando a data/hora da inativação/cancelamento, usuário responsável e justificativa. Opcionalmente, o S-RES pode ocultar registros inativos/cancelados por padrão, mas deve haver uma opção/filtro para que a exportação também possa ocorrer com a inclusão desses registros caso desejado pelo usuário. Nota: Consideram-se como finalizados/liberados os registros que foram concluídos e liberados pelo profissional, não considerando registros salvos em caráter provisório (salvo como rascunho).		
ECF.17 - Estrutura, Metadados, Consistência e Cronologia				
ECF.17.01	Identificação do profissional responsável pelo registro	Todo registro realizado no S-RES deve identificar e apresentar, tanto em tela quanto impressão, a identificação do profissional usuário pelo registro.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução permitir o registro e armazenamento de dados clínicos diretamente no sistema.	1
ECF.17.02	Registro de tempo do armazenamento do evento no S-RES	O S-RES deve registrar automaticamente e apresentar, tanto em tela quanto impressão, a data/hora do registro de qualquer dado no sistema.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução permitir o registro e armazenamento de dados clínicos diretamente no sistema.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
ECF.17.04	Cronologia de eventos	O S-RES deve assegurar a correta cronologia dos eventos e informações clínicas, de modo que os registros sejam apresentados, tanto em tela quanto em documentos exportados ou impressos, ordenados cronologicamente com base na data e hora de ocorrência do evento clínico.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário e realizar armazenamento persistente de dados.	1
ECF.17.07	Corretude funcional	Durante a auditoria do S-RES, deve ser possível executar todos os testes referentes às funcionalidades delimitadas pelo escopo da certificação sem a ocorrência de defeitos, erros ou falhas.		1
ECF.21 - Usabilidade e Interação com o Usuário				
ECF.21.01	Idioma do S-RES	Todos os dados e informações exibidas e controladas pelo S-RES (por exemplo, rótulos, mensagens controladas pelo S-RES, títulos de tela, descritivos, menus, etc), tanto em tela quanto em impressões, deverão obrigatoriamente estar no idioma português do Brasil.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário.	1
ECF.21.02	Mensagens do sistema	Todas as mensagens sob controle do S-RES devem ser apresentadas em linguagem não técnica ao usuário, em português do Brasil. Mensagens técnicas (sistemas operacionais, banco de dados, componentes de segurança, etc) ou em outros idiomas e que possam ser tratadas pelo S-RES não devem ser apresentadas em seu conteúdo original.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
ECF.21.04	Testes e avaliação de usabilidade para o S-RES	a) A empresa responsável pelo S-RES deve realizar e documentar testes formais de usabilidade com usuários representativos do público-alvo para validar o design da interface. Os testes devem gerar uma documentação incluindo minimamente: • Plano de teste; • Funcionalidades/telas avaliadas no teste; • Métricas utilizadas na avaliação, utilizando minimamente as métricas de número de cliques e tempo médio para conclusão de processos/tarefas; • Relatório de resultados apresentando as métricas obtidas e nível de satisfação dos usuários participantes; • Análise de risco de usabilidade que identifique potenciais erros de uso; • Plano de ação para mitigação de riscos de usabilidade; • Plano de ação para melhoria do design do sistema com base nos resultados obtidos. b) A validação de usabilidade deve ser repetida periodicamente sempre que houver mudanças significativas na interface. c) A empresa responsável pelo S-RES deve possuir um processo documentado de coleta e análise sistemática de feedbacks de clientes em ambiente de produção, visando à melhoria contínua da usabilidade e da experiência do usuário. Esse processo deve contemplar, minimamente: • Canais formais de coleta de feedback; • Registro e categorização de feedbacks relacionados à usabilidade e interface com o usuário; • Plano de ação para melhoria do design do sistema com base nos feedbacks coletados. Nota: Seguem alguns exemplos de referências que podem ser utilizas pela empresa responsável pelo S-RES para aplicação deste requisito: - ISO 9241-210:2019 - Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems; - ISO 25065:2019 - Systems and software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for Usability: User requirements specification; - ISO 25062:2025 - Systems and software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for reporting usability evaluations.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário.	2

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
ECF.21.05	Práticas de Design Centrado no Ser Humano	a) O S-RES/aplicação deve estar aderente aos princípios do Design Centrado no Ser Humano (Human-Centred Design - HCD), garantindo que a interface seja clara, consistente, eficiente e minimize a carga cognitiva e o risco de erro de uso. b) O S-RES deve apresentar, minimamente, as seguintes características: • Itens/botões que envolvem ações utilizadas com frequência na operação (imprimir, visualizar, assinar, etc.) posicionados em destaque, dentro do campo de visão principal e com acesso ágil (com apenas um clique); • Itens/botões que envolvem ações que encaminham o usuário para a próxima etapa do processo posicionados em destaque, dentro do campo de visão principal, com acesso ágil (com apenas um clique) e próximos ao item/botão associado à ação anterior (por exemplo, botão de "liberar" um documento clínico ao lado do botão de "salvar" o documento, ou preferencialmente um botão único para “salvar e liberar”); • Visualização completa e otimizada de todo o conteúdo necessário para completar uma tarefa (por exemplo, completar uma prescrição sem a necessidade de alternar entre múltiplas telas); • Minimização de redundâncias evitando reentrada de dados já informados em etapas anteriores e ações duplicadas que possam ser automatizadas (por exemplo, preenchimento automático de dados de identificação do paciente em formulários); • Ordenação de itens (itens/menu do prontuário, ações de botão direito, colunas em tabelas, abas, etc.) de acordo com as etapas do fluxo de trabalho e/ou frequência de uso; • Uso de atalhos de teclado para funcionalidades utilizadas com frequência na operação; • Campos obrigatórios destacados visualmente; • Feedback visual claro e imediato sobre o estado do sistema (por exemplo, mensagem de "processando" ao executar tarefas mais demoradas); • Consistência e padrões para apresentação de dados (por exemplo, padronização para labels de campos, cabeçalho padrão para apresentação de tabelas com os mesmos tipos de dados, etc.). • Consistência e padrões de design por meio de elementos visuais e comportamentais padronizados (por exemplo, uso consistente de cores, tipografia, iconografia e componentes de interface para ações equivalentes em diferentes telas).	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário.	2

3.3. Requisitos NGS1 - Segurança da Informação, Privacidade e Infraestrutura (NGS1)

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.01 - Controle de versão do software				
NGS1.01.01	Exibição das informações do software	a) O S-RES (conjunto de componentes principais) deve apresentar as informações de identificação do software desenvolvido pelo fornecedor, contendo minimamente o nome do software, nome do fornecedor, identificação completa da versão e/ou release e/ou build. Essas informações deverão corresponder à da versão certificada do produto, e será utilizada como referência em todos os documentos, selo, e outros documentos relacionados à certificação. b) Essas informações deverão estar disponíveis minimamente: • Na tela inicial do S-RES; • Nas telas de cada módulo (por exemplo, cabeçalho, rodapé ou ainda em um item de um menu), de modo que quando o sistema esteja em uso essas informações estejam sempre acessíveis; • Impressões geradas oriundas do S-RES. Neste caso, tais informações deverão ser exibidas minimamente na última página do documento impresso (em um cabeçalho ou rodapé, por exemplo). • Arquivo de exportação da trilha de auditoria, se aplicável.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.02 - Identificação e autenticação de pessoas				
NGS1.02.01	Método de autenticação de pessoa	a) Todo usuário do S-RES deve ser identificado e autenticado antes de qualquer acesso a dados ou funcionalidades do S-RES. b) Utilizar, em todos os processos autenticação de pessoa, no mínimo um dos seguintes métodos de autenticação de pessoa: • Digitação de um nome de usuário e senha secreta de acesso; • Certificado digital e PIN (Personal Identifier Number); • Validação biométrica associada ao PIN (Personal Identifier Number); c) As credenciais para autenticação no S-RES devem ser validadas após a submissão das mesmas ao serviço de autenticação do sistema no lado do servidor, evitando que a validação ocorra somente no lado do cliente. d) Em caso de aplicação móvel, a autenticação pode ser realizada no lado do cliente, caso haja uso do aplicativo de forma off-line. No momento da sincronização dos dados, deve haver a autenticação no lado servidor antes do registro dos dados no sistema. Nota: Quaisquer outras técnicas diferentes das exigidas acima, tais como OTP (one-time password) e Captcha, são considerados complementares, podendo ser utilizados apenas em conjunto com um dos métodos supracitados.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.02.02	Proteção dos parâmetros de autenticação de usuário	O S-RES deve armazenar de forma protegida todos os dados ou parâmetros utilizados no processo de autenticação de usuário. Método: Nome de usuário e senha a) A senha deve ser armazenada após uso de uma função de derivação de chaves resistente a ataques (KDF) apropriada para senhas (por exemplo, Argon2id, scrypt, etc.). b) O comprimento efetivo do resultado da derivação (dklen) deve ser maior ou igual a 256 bits. c) Deve-se utilizar salt aleatório e exclusivo por credencial, com comprimento maior ou igual a 128 bits. É vedado reutilizar o mesmo salt entre credenciais. d) As codificações das senhas de acesso dos usuários devem ser protegidas contra acesso não autorizado. Apenas o usuário do banco de dados ou o componente de autenticação devem ter acesso às mesmas.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
		Método: Biometria (condição: somente para pessoas) c) Os templates biométricos das pessoas devem ser protegidos contra acesso não autorizado. Apenas o usuário do banco de dados utilizado ou o componente de autenticação devem ter acesso aos mesmos. d) As amostras biométricas coletadas e transmitidas durante o processo de autenticação devem ser protegidas contra acesso não autorizado. e) Em caso de aplicação móvel, deve ser utilizada a biometria nativa do sistema operacional. Método: One-time password (OTP) f) As sementes de geração dos valores numéricos devem ser protegidas contra acesso não autorizado. Apenas o usuário do banco de dados ou o componente de autenticação devem ter acesso às mesmas. Método: Credencial Federada g) Em caso de autenticação realizada por provedor de credenciais externo (Credencial Federada), o S-RES deve armazenar apenas o identificador único do usuário (e não a senha original), e este identificador deve ser protegido contra acesso não autorizado. Nota: Caso a autenticação seja realizada por ferramenta/serviço externo, a empresa responsável pelo S-RES deve apresentar evidências de que a tecnologia atende a este requisito (por exemplo: documentação oficial e amostra anonimizada do formato armazenado com algoritmo e parâmetros) e que o S-RES não armazena senha em texto claro.		

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.02.03	Unicidade de Sessão e Integridade de Identidade	a) O S-RES deve restringir o acesso a apenas uma sessão ativa por instância do navegador ou da aplicação desktop. b) Em caso de aplicação web, caso ocorra um novo login no mesmo navegador (em aba ou janela distinta), a sessão anterior deve ser imediatamente encerrada. Em caso de aplicação desktop, o sistema deve impedir a execução de múltiplas instâncias simultâneas do software no mesmo sistema operacional. c) O sistema deve bloquear qualquer tentativa de salvar dados ou realizar assinaturas digitais a partir de uma tela que pertença a uma sessão expirada ou substituída.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.02.04	Qualidade da senha	Condição: Utilização de autenticação baseada no método de usuário e senha. a) O S-RES deve exigir que toda senha de usuário seja definida seguindo minimamente os seguintes critérios: • Pelo menos 8 caracteres • Pelo menos um caractere alfabético • Pelo menos um caractere numérico b) Esses critérios devem ser obedecidos em qualquer processo de geração de senha para usuários, inclusive ao cadastrar o usuário ou geração automática de senhas.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.02.05	Impedimento de senhas com base em dados de identificação	Condição: Utilização de autenticação baseada no método de usuário e senha. O S-RES deve impedir que o usuário gere senhas fracas com base em seus dados de identificação, tais como o próprio nome ou data de nascimento.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	2

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.02.06	Parametrização da política de força de senha	Condição: Utilização de autenticação baseada no método de usuário e senha. O S-RES deve permitir a parametrização da qualidade da senha, permitindo indicar minimamente: • Quantidade mínimas de caracteres; • Se a senha deve incluir ao menos um caractere alfabético; • Se a senha deve incluir ao menos um caractere numérico; • Se a senha deve incluir ao menos um caractere especial; • Se a senha deve incluir ao menos uma letra minúscula; • Se a senha deve incluir ao menos uma letra maiúscula.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	3
NGS1.02.07	Troca obrigatória de senha inicial	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: A senha do usuário pode ser gerada de forma padrão e/ou por um administrador com conhecimento da senha. Caso a senha de um determinado usuário tenha sido gerada de forma padrão ou por um administrador com visibilidade dessa senha, o S-RES deve forçar a troca de senha imediatamente no primeiro acesso do usuário após a geração. Até a conclusão da troca, nenhuma outra ação no S-RES poderá ser executada pelo usuário.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.02.08	Geração automática de senha para o usuário	Condição: Utilização de autenticação baseada no método de usuário e senha. a) Toda geração de senha para um usuário deve ocorrer de forma automática pelo sistema, de forma que a senha não seja de conhecimento do administrador ou de terceiros em nenhum momento. b) A senha deve ser gerada de forma aleatória, de forma que não seja possível a geração de senha padrão. c) O envio da senha ou do link/token de reset para o usuário deve ser realizado de forma automática por meio de algum canal de comunicação cuja identificação esteja constante no cadastro do usuário (por exemplo, envio da senha para o e-mail especificado no cadastro do usuário).	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	2

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.02.09	Troca de senha pelo próprio usuário	Condição: Utilização de autenticação baseada no método de usuário e senha. O S-RES deve permitir que um usuário efetue a troca de sua senha no sistema, sendo que a mesma deve seguir as regras de parametrização da qualidade da senha.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.02.10	Troca forçada de senha	Condição: Utilização de autenticação baseada no método de usuário e senha. a) O S-RES deve permitir que um usuário autorizado (um administrador ou gestor de acessos, por exemplo) possa configurar a troca de senha forçada de um determinado usuário no próximo login (por exemplo, caso de comprometimento da segurança do banco de dados e/ou aplicação). b) Ao tentar efetuar login, nenhuma ação poderá ser efetuada pelo usuário no S-RES até que o mesmo efetue a troca de senha.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	2
NGS1.02.11	Periodicidade de troca de senhas	Condição: Utilização de autenticação baseada no método de usuário e senha. a) O S-RES deve permitir a parametrização de um período máximo para expiração de senhas de forma a tornar obrigatória a troca de senhas pelos usuários. b) O período para expiração de senhas deve ser configurável na aplicação e armazenado no banco de dados. c) O controle de tempo para periodicidade de senha deve ser realizado pelo servidor. d) O tempo de expiração deverá ser contado a partir da data da última troca de senha do usuário.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	2
NGS1.02.12	Igualdade de senhas	Condição: Utilização de autenticação baseada no método de usuário e senha. Em todos os processos de troca de senha, o S-RES deve exigir que a nova senha do usuário seja diferente da atual e da imediatamente anterior	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
			possuir interface gráfica para interação com o usuário.	
NGS1.02.13	Obtenção de nova senha	Condição: Utilização de autenticação baseada no método de usuário e senha. a) O S-RES deve permitir que, na tela inicial de login no sistema, o usuário possa obter uma nova senha (opção “esqueci a senha”). b) No momento em que o usuário solicitar a recuperação de senha, o S-RES deve realizar uma das seguintes opções: • Gerar uma nova senha automaticamente e enviá-la ao usuário, ou • Encaminhar ao usuário instruções para que o mesmo possa definir uma nova senha. c) A geração e envio da senha ou encaminhamento das instruções deve ser realizado por meio de um canal (SMS ou e-mail, por exemplo) cuja identificação tenha sido registrada previamente no cadastro do usuário.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.02.14	Controle de tentativas de login	a) O S-RES deve possuir, em todos os processos de autenticação de usuário, independentemente do método utilizado, mecanismos para bloquear seu acesso após um número máximo de tentativas consecutivas de login com autenticação inválida. b) O número de tentativas de login deve ser configurável na aplicação, armazenado no banco de dados e não deve ultrapassar o limite de 10 tentativas. c) Após o bloqueio da conta de um usuário, o login só deve ser permitido novamente por um dos seguintes meios: • Desbloqueio da conta do usuário por um administrador, ou • Auto desbloqueio com verificação forte: o sistema permite que o próprio usuário desbloqueie a conta após comprovar a identidade por um fator forte previamente cadastrado (por exemplo, link/código de uso único e expiração curta enviado para e-mail/telefone cadastrado para redefinição de senha). Nota: Caso a autenticação seja realizada por ferramenta/serviço externo, o S-RES deve garantir o atendimento a todas as exigências deste requisito, admitindo-se as seguintes flexibilizações: • A configuração do número máximo de tentativas de login pode ser realizada diretamente na ferramenta/serviço externo, e não na aplicação do S-RES; • O armazenamento do valor do número máximo de tentativas de login pode ser realizado pela ferramenta/serviço externo, fora do banco de dados do S-RES; • Caso a ferramenta/serviço externo permita configurar um limite de tentativas superior a 10, a empresa responsável pelo S-RES deve manter documentação informando que a recomendação de segurança é não configurar um limite superior a 10. Quando a própria empresa for responsável por definir esse limite no provedor, deve haver documento interno formalizando que a política da empresa respeita o limite de 10 tentativas.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.02.15	Autenticação para operações críticas	a) O S-RES deve solicitar uma nova autenticação do usuário, ou exigir a confirmação de um segundo fator (OTP, por exemplo), para a realização de operações críticas ou sensíveis, configuráveis no sistema. b) Esta prática deve ser realizada minimamente para as seguintes operações: • Troca de senha; • Vínculo de usuários com o certificado digital (quando aplicável); • Gestão de perfis e usuários (quando aplicável).	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	2

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.02.16	Informações na autenticação	Assim que completada uma autenticação com sucesso, o sistema deve permitir a visualização pelo usuário das seguintes informações: • Data e hora da última autenticação com sucesso de seu usuário; • Data e hora das tentativas de autenticação sem sucesso depois da última autenticação com sucesso. Nota 1: Considera-se como “última autenticação” a autenticação imediatamente anterior à que está ocorrendo. Nota 2: Essas informações podem ser exibidas por meio de um alerta (pop up) na tela ou ainda estar disponíveis para acesso sempre que desejado pelo usuário (em um item de menu, por exemplo).	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	2
NGS1.02.17	Informações em autenticação inválida	Em caso de autenticação inválida em tentativa de acesso, a mensagem de erro emitida pelo sistema para o usuário não deve informar qual o motivo da falha da autenticação. Por exemplo, pode-se emitir uma mensagem informando que os dados de autenticação estão incorretos, sem especificar que o usuário não existe ou que a senha está incorreta.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.02.18	Memorização e visualização de credenciais na interface de autenticação	Condição: Utilização de autenticação baseada no método de usuário e senha. a) O S-RES deve, por padrão, impedir que a interface de usuário utilizada para digitação de credenciais de acesso (nome de usuário e senha, por exemplo) permita a memorização ou visualização de dados anteriores (lista de logins já digitados, lembrança automática de senhas associadas a um login, etc.). b) De forma opcional, o S-RES pode permitir a memorização de credenciais de acesso, desde que essa funcionalidade seja configurável pela instituição. c) Toda e qualquer digitação direta de senhas deve ser feita por meio de máscara de caracteres que impeça sua visualização por outras pessoas.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.02.19	Autenticação de dois fatores	a) O S-RES deve oferecer pelo menos dois métodos de autenticação (login/senha e biometria, por exemplo). b) O S-RES deve permitir parametrizar qual método deverá ser utilizado, permitindo ainda o uso dos dois métodos simultaneamente (autenticação de dois fatores). Nota: Técnicas como OTP (one-time password), Push Notification, Autenticador (App) ou Token Físico podem ser utilizados como segundo fator de autenticação.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	3
NGS1.02.20	Bloqueio ou encerramento por inatividade	a) A sessão de usuário deve ser automaticamente bloqueada ou encerrada forçadamente pelo sistema após um período de inatividade. b) O período máximo de inatividade deve ser configurável na aplicação e armazenado no banco de dados. c) Caso o S-RES possibilite ao usuário o desbloqueio de sessão, essa operação deve ser permitida apenas quando o desbloqueio for realizado pelo mesmo usuário. Para que o desbloqueio de sessão seja realizado, o sistema deve requerer novo processo de autenticação do usuário. Dever ser possível ainda encerrar a sessão de forma a permitir que outros usuários possam efetuar um novo login. d) Após o bloqueio ou encerramento da sessão de usuário, as informações em tela não deverão mais estar visíveis, sendo necessária uma nova autenticação para a retomada da atividade. e) Não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles. Nota: Caso o controle de bloqueio/encerramento de sessão por inatividade seja realizado por ferramenta/serviço externo, o S-RES deve garantir o atendimento a todas as exigências deste requisito, admitindo-se as seguintes flexibilizações: • A configuração do período máximo de inatividade pode ser realizada diretamente na ferramenta/serviço externo, e não na aplicação do S-RES. • O armazenamento desse valor pode residir na ferramenta/serviço externo, fora do banco de dados do S-RES. • Quando a ferramenta/serviço externo encerrar ou bloquear a sessão por inatividade, o	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
		S-RES deve reconhecer imediatamente o estado (por exemplo: token inválido/expirado, sessão revogada) e exigir nova autenticação.		
NGS1.02.21	Bloqueio por inatividade	A sessão de usuário deve ser automaticamente bloqueada forçadamente pelo sistema após um período de inatividade, sem que a sessão seja encerrada. Dessa forma, ao efetuar o login novamente, o usuário deverá ser direcionado para a mesma tela em que estava no momento do bloqueio, sem que haja quaisquer perdas de dados digitados e não salvos. Nota: Caso o controle de bloqueio/encerramento de sessão por inatividade seja realizado por ferramenta/serviço externo, o S-RES deve garantir o atendimento a todas as exigências deste requisito, admitindo-se as seguintes flexibilizações: • A configuração do período máximo de inatividade pode ser realizada diretamente na ferramenta/serviço externo, e não na aplicação do S-RES. • O armazenamento desse valor pode residir na ferramenta/serviço externo, fora do banco de dados do S-RES. • Quando a ferramenta/serviço externo encerrar ou bloquear a sessão por inatividade, o S-RES deve reconhecer imediatamente o estado (por exemplo: token inválido/expirado, sessão revogada) e exigir nova autenticação.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	2
NGS1.02.22	Aviso de bloqueio ou encerramento de sessão	a) Anteriormente ao encerramento ou bloqueio da sessão por inatividade, o S-RES deve informar ao usuário que o encerramento/bloqueio irá acontecer em um determinado período de tempo. b) O período de tempo em que o aviso será ser emitido deve ser configurável.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	2
NGS1.02.23	Configuração de parâmetros de segurança por cliente	Condição: S-RES ofertado como SaaS. O S-RES deve permitir que os seguintes parâmetros de segurança sejam configuráveis por cliente não apenas de forma global: • Limite de tentativas consecutivas de login inválidas; • Política de força de senha; • Expiração de senha; • Encerramento/bloqueio da sessão por inatividade.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	2

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.03 - Autorização e controle de acesso				
NGS1.03.01	Impedir acesso por pessoas não autorizadas	a) Todo acesso, visualização de dados ou execução de funcionalidade do S-RES deve ser realizado apenas por usuários previamente autenticados e autorizados. b) O S-RES deve garantir que, mesmo com um token de sessão válido, o usuário só consiga acessar dados ou executar funcionalidades para os quais seu perfil de acesso tenha permissão explícita. c) O S-RES deve invalidar o acesso caso a sessão não seja legítima (por exemplo, URL copiada para outro navegador ou sessão expirada), redirecionando o usuário para a tela de login. d) Quaisquer arquivos, documentos ou dados gerados ou importados no sistema (por exemplo, PDFs, imagens, etc.) não devem ser acessíveis diretamente pela URL do servidor (ou via caminhos de rede no caso de aplicações desktop) sem que haja uma autenticação e autorização prévia do usuário pelo S-RES. Se o acesso ao arquivo for por URL temporária, essa URL deve possuir mecanismos de segurança que impeçam o acesso por um usuário não autorizado (por exemplo, vincular o token de acesso da URL ao ID da sessão do usuário logado, de modo que a URL só funcione enquanto essa sessão específica estiver ativa).		1
NGS1.03.02	Perfis mínimos de usuário	O S-RES deve disponibilizar minimamente dois perfis de usuário: administrador do sistema (sem acesso a dados clínicos) e profissional de saúde (com acesso a dados clínicos).	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.03.07	Atribuição de mais de um perfil para um usuário	a) O S-RES deve permitir que mais de um perfil possa ser atribuído a um usuário (por exemplo, profissional de saúde e administrador). b) Tal atribuição deverá implicar na necessidade de escolha de um perfil pelo usuário no momento do login ou no acúmulo de permissões para o usuário de acordo com os perfis a ele atribuídos.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.03.08	Gerenciamento de usuários	a) O S-RES deve permitir o gerenciamento (cadastro, ativação/inativação e alteração de cadastro) de usuários, por meio da aplicação. b) Todo usuário deve possuir um número de identificação unívoca gerado automaticamente pelo S-RES (ID do usuário). Esse número deve ser passível de visualização na aplicação.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.03.09	Identidade única da pessoa e responsabilização	a) Todo usuário do S-RES deve estar vinculado à uma pessoa com registro obrigatório de ao menos um documento de identificação pessoal unívoco segundo a legislação brasileira vigente (por exemplo, CPF ou passaporte). b) O S-RES não deve permitir a associação de um mesmo documento de identificação a dois ou mais usuários no sistema. c) Qualquer alteração de cadastro nesse documento deverá exigir uma justificativa no usuário e registrar em um histórico de alterações acessível na aplicação. d) Para fins de responsabilização, não deve ser possível remover o cadastro ou o vínculo de um usuário a um profissional, caso alguma operação tenha sido realizada pelo mesmo. e) Caso o S-RES seja ofertado como SaaS, a unicidade do identificador da pessoa deve ser por organização.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.03.10	Usuário mínimo ativo	O S-RES deve garantir que haja ao menos um usuário ativo com perfil de administrador. Dessa forma, o sistema não deve permitir a inativação ou a alteração de perfil do último usuário administrador ativo, garantindo que sempre haja ao menos uma conta com plenos poderes de gestão de acesso.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução puder operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.04 - Disponibilidade do RES				
NGS1.04.01	Geração de cópia de segurança	a) O S-RES deve permitir a geração de cópia de segurança (backup), pela aplicação ou SGBD, contendo informações suficientes para restauração. b) A geração de cópia de segurança deve exportar os atributos de segurança e metadados em conjunto com os dados. Nota: Considera-se como atributos de segurança todos os parâmetros e configurações existentes.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução realizar armazenamento persistente de dados.	1
NGS1.04.03	Sigilo da cópia de segurança	O S-RES (aplicação ou SGBD) deve garantir o sigilo de suas cópias de segurança (por exemplo, realizando encriptação automática).	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução realizar armazenamento persistente de dados.	1
NGS1.04.04	Restauração de cópia de segurança	a) O S-RES deve permitir a restauração da cópia de segurança, pela aplicação ou SGBD. b) Na restauração de uma cópia de segurança os atributos de segurança e metadados devem ser automaticamente recuperados, sem a intervenção do administrador.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução realizar armazenamento persistente de dados.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.04.05	Integridade na restauração da cópia de segurança	a) O S-RES deve garantir a integridade da cópia de segurança por meio de mecanismos de verificação (por exemplo, checksum ou hash), assegurando que o arquivo não sofreu alterações desde sua criação. b) O processo de restauração deve realizar obrigatoriamente a validação da integridade antes da persistência dos dados. Caso o arquivo esteja corrompido ou adulterado, o sistema deve interromper a operação, emitir um alerta e garantir o estado anterior do banco de dados (atomicidade/rollback).	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução realizar armazenamento persistente de dados.	1
NGS1.04.06	Cópia de segurança e restauração para SaaS	Condição: S-RES ofertado como SaaS e gerenciamento do banco de dados realizado pela própria empresa ou terceiro. a) A empresa fornecedora deve comprovar que o serviço de nuvem e suas políticas internas garantem a realização automática e periódica do backup. Essas políticas devem estar documentadas e disponibilizadas ao cliente. b) Caso uma mesma base de dados seja utilizada para armazenar dados de diferentes organizações/clientes (multi-tenant), a empresa fornecedora deve oferecer um serviço e possuir ferramentas ou processos documentados que permitam a extração isolada dos dados de um cliente específico e sua respectiva reintegração/restauração, sem impactar a integridade ou a disponibilidade dos dados dos demais clientes.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução realizar armazenamento persistente de dados.	2
NGS1.04.07	Alerta de limiar de ocupação	Condição: S-RES não dispõe de infraestrutura com espaço de armazenamento dinâmico. a) S-RES deve permitir o gerenciamento do espaço de armazenamento de registros por meio da configuração de um limiar de ocupação. b) O S-RES deve ainda permitir a configuração de um ou mais usuários com perfil de administrador do sistema que deverão receber uma notificação do S-RES no caso desse limite de ocupação ser atingido.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução realizar armazenamento persistente de dados.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.04.08	Infraestrutura de alta disponibilidade para execução do S-RES	Condição: S-RES é totalmente ou parcialmente executado em uma infraestrutura sob controle da empresa fornecedora ou terceiro. a) O S-RES deve ser executado em ambiente de infraestrutura que possua redundância ativa para seus componentes, assegurando a continuidade do serviço mesmo em caso de falha pontual de hardware ou conectividade. b) A empresa deve manter e disponibilizar: • Evidência de Auditoria de Infraestrutura: Certificações do Datacenter (por exemplo, Tier III, ISO 27001) ou laudo técnico de vulnerabilidades. • Métrica de SLA: A empresa deve garantir e documentar um Acordo de Nível de Serviço (SLA) de disponibilidade mensal não inferior a 99,5% para o acesso ao S-RES e seus componentes críticos. • Evidência Histórica: Relatório de monitoramento dos últimos 6 meses, demonstrando o cumprimento do SLA acordado e detalhando eventuais interrupções e as ações corretivas aplicadas. • Plano de Continuidade de Negócios: Protocolo documentado que defina os tempos máximos de recuperação e o fluxo de comunicação de incidentes críticos aos clientes.		1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.04.12	Prevenção de perda de dados durante interação com o usuário	a) O S-RES deve incorporar mecanismos técnicos para garantir a persistência dos dados gerados ou inseridos pelo usuário durante a interação com o sistema, protegendo-os contra perdas decorrentes de falhas na aplicação, interrupções de conexão ou fechamento inesperado. b) O S-RES deve possuir uma lógica de salvamento automático baseada em eventos (por exemplo, mudança de campo, pausa na digitação, etc.) ou intervalos curtos de tempo. c) Caso seja utilizado armazenamento local temporário ou em cache, os dados devem ser criptografados e descartados imediatamente após a sincronização bem-sucedida. d) Ao reiniciar a funcionalidade, o sistema deve detectar ativamente a existência de dados da sessão anterior e oferecer ao usuário de forma clara e explícita a opção de restaurar seu trabalho. e) Esses recursos devem estar disponíveis em todas as aplicações que fazem parte do S-RES nativamente (por exemplo, aplicações de IA, sistema de receita digital integrado, etc.). Por exemplo, em uma ferramenta de ambient listening integrada nativamente ao S-RES, a transcrição da consulta deve ser salva localmente de forma contínua de forma que, se a conexão com a internet falhar, a transcrição daquele período não é perdida e pode ser sincronizada posteriormente.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas a aplicações que demandam interações com o usuário e que permitem a geração de resultados parciais, tais como ferramentas de Ambient Listening (transcrição contínua). O requisito não se aplica a aplicações ou recursos que necessitam realizar processamentos de forma atômica (completos em uma única requisição), como a análise de dados clínicos para sugestão de diagnósticos.	3

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.05 - Comunicação entre componentes do S-RES				
NGS1.05.01	Segurança da comunicação com componente de interação com o usuário	a) A sessão de comunicação entre o componente de interação com o usuário (browser, aplicativo móvel ou executável cliente) e os outros componentes do S-RES deve oferecer os seguintes serviços de segurança: autenticação do servidor, integridade dos dados e confidencialidade dos dados. b) O serviço de segurança empregado deve implementar criptografia de dados em trânsito utilizando obrigatoriamente o protocolo TLS na versão 1.2 ou superior (por exemplo, HTTPS). c) Para aplicações Web, o S-RES deve forçar o uso de HTTPS em todas as comunicações, com redirecionamento automático de qualquer tentativa de acesso por protocolo HTTP. d) Para aplicações Desktop ou Mobile, a tentativa de comunicação por canal não criptografado deve ser obrigatoriamente rejeitada na origem. Mesmo que o servidor de backend seja temporariamente configurado para aceitar apenas tráfego HTTP, o S-RES deve detectar a ausência de um canal seguro e interromper o fluxo de execução, impedindo o acesso à tela de login ou a qualquer funcionalidade que envolva tráfego de dados.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.05.02	Segurança da comunicação entre componentes	Condição: S-RES ser composto por componentes distribuídos. a) A comunicação entre componentes distribuídos (como, por exemplo, entre o servidor de aplicação e o banco de dados, ou no acesso a serviços externos) deve oferecer os seguintes serviços de segurança: • Autenticação dos parceiros (ambas as partes) • Integridade dos dados e confidencialidade dos dados (criptografia). b) Deve-se utilizar o protocolo TLS 1.2 ou superior. Nota 1: A segurança pode ser aplicada ao canal de comunicação (TLS, VPN) ou às mensagens trocadas (assinatura e criptografia da mensagem). Nota 2: Exemplos de componentes distribuídos que exigem essa segurança: • Servidor de banco de dados; • Serviços de assinatura digital; • Bases de conhecimento clínico; • Serviços ou modelos de IA.		1
NGS1.05.03	Processamento de dados no lado servidor	Condição: S-RES em arquitetura Web. a) Todo processamento (modificação) de dados de RES deve ocorrer no lado do servidor. Todos os dados apresentados no lado cliente devem ter sido gerados e processados no lado servidor. b) Todos os processos de validação de dados devem ser realizados no lado do servidor. Nota: Opcionalmente, por questões de performance, poderá haver validação de dados inicialmente no lado cliente desde que seguida de validação no lado do servidor.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário.	1
NGS1.05.04	Integridade e origem de componentes dinâmicos	Condição: S-RES utilizar componentes que exijam download (descarregamento do servidor para o cliente) para sua execução (por exemplo: ActiveX, Applet, aplicações para tablet, etc) por parte do usuário. Possuir controle de integridade e possibilidade de verificação da origem/autoria (por exemplo: pelo uso de assinatura digital do componente) de componentes que exijam download para sua execução.		1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.06 - Segurança de dados				
NGS1.06.01	Utilização de SGBD	a) Todos os dados registrados no S-RES devem ser armazenados integral e exclusivamente por um Sistema de Gerenciamento de Banco de Dados (SGBD) que contemple o sigilo dos dados. b) Arquivos e documentos anexados ou gerados pelo S-RES (por exemplo, laudos em PDF, áudios, vídeos, etc.) podem, opcionalmente, ser armazenados em estrutura de diretórios ou soluções de armazenamento em nuvem (por exemplo, S3), desde que o S-RES garanta o sigilo desses documentos de forma que os mesmos somente possam ser visualizados por meio de seu acesso pelo S-RES. Adicionalmente, o nome dos arquivos e diretórios não podem conter qualquer informação que permita a identificação de seu conteúdo.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução realizar armazenamento persistente de dados.	1
NGS1.06.02	Segurança de arquivos temporários	Condição: S-RES gera arquivos temporários fora do SGBD (por exemplo, para fins visualização, assinatura digital, etc.) Quaisquer arquivos que tenham sido gerados temporariamente fora do SGBD devem ser excluídos ou ter seu acesso revogado após o término da operação. Por exemplo, cache de arquivos PDF após a sua a visualização e resquícios de arquivos XML ou DICOM após o seu processamento.		2
NGS1.06.03	Segregação dos dados por organização	Condição: S-RES ofertado como SaaS. a) O S-RES deve implementar isolamento lógico em nível de aplicação e banco de dados, garantindo que os dados (clínicos, administrativos e metadados) de uma organização sejam totalmente inacessíveis a usuários de outras organizações. b) O mecanismo de controle de acesso deve validar o ID da Organização em cada requisição (API ou consulta ao banco), impedindo que a alteração manual de identificadores em URLs ou parâmetros de busca permita o acesso a dados de terceiros.		1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.06.05	Criptografia de Dados em Repouso	a) O S-RES deve garantir que todos os dados armazenados em mídias permanentes sejam protegidos por meio de criptografia em repouso. b) O S-RES deve ser compatível com recursos de criptografia nativos do SGBD ou da infraestrutura de armazenamento subjacente. c) As chaves de criptografia utilizadas devem ser geridas e protegidas de forma segregada e segura (por exemplo, uso de um Key Management Service - KMS ou Hardware Security Module - HSM). d) O S-RES deve incluir em seu manual de administração e instalação as instruções para que o cliente possa configurar a criptografia em repouso no ambiente do SGBD. Nota: Em modelos SaaS, a responsabilidade pela implementação, gestão de chaves e operação da criptografia é integralmente do fornecedor. Em modelos on-premise, a responsabilidade operacional é do cliente, devendo o fornecedor garantir a compatibilidade técnica e prover a documentação de configuração.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução realizar armazenamento persistente de dados.	2
NGS1.06.06	Proteção contra ataques de injeção	O S-RES deve implementar controles técnicos para prevenir, detectar e mitigar ataques de injeção (SQL injection, Code Injection, OS Command Injection) por meio de mecanismos como: • Validar dados inseridos pelo usuário antes de serem processados; • Utilizar consultas parametrizadas (Prepared Statements) ou Mapeamento Objeto-Relacional (ORMs), evitando a concatenação direta de entrada do usuário em comandos do banco de dados (SQL) ou do sistema operacional. Nota 1: A conformidade com os mecanismos de prevenção a ataques pode ser demonstrada apresentando a documentação oficial (incluindo guias de desenvolvedor ou artigos técnicos) de frameworks e bibliotecas de segurança, além de evidências de que o S-RES utiliza e configura corretamente essas ferramentas. Nota 2: Ataques de Injeção ocorrem quando dados não confiáveis são enviados para um interpretador (como um banco de dados) como parte de um comando ou consulta, alterando o comando original e permitindo que um atacante execute código malicioso ou acesse dados indevidamente.	Para a categoria de Inteligência Artificial, este requisito se aplica apenas se a solução receber dados de entrada e realizar armazenamento persistente de dados.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.06.07	Proteção contra ataques roubo ou reuso da sessão do usuário	O S-RES deve implementar controles técnicos para prevenir, detectar e mitigar roubo ou reuso da sessão do usuário por meio de mecanismos como: • Utilizar tokens de sessão seguros com validade limitada e mecanismo de renovação segura (refresh token). • Assegurar que os cookies de sessão utilizem os atributos de segurança Secure e HttpOnly. • Invalidação da sessão (tokens) de forma explícita após o logout do usuário. • Implementar um controle de segurança na comunicação remota entre cliente e servidor que impeça o roubo ou reuso da sessão do usuário. Nota 1: A conformidade com os mecanismos de prevenção a ataques pode ser demonstrada apresentando a documentação oficial (incluindo guias de desenvolvedor ou artigos técnicos) de frameworks e bibliotecas de segurança, além de evidências de que o S-RES utiliza e configura corretamente essas ferramentas. Nota 2: Roubo ou reuso da sessão do usuário abrangem o roubo/reuso de identificadores de sessão válidos, permitindo que um atacante se faça passar por um usuário legítimo após a autenticação.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.06.08	Proteção contra ataques de XSS	Condição: S-RES em arquitetura Web. O S-RES deve implementar controles técnicos para prevenir, detectar e mitigar ataques de Cross-Site Scripting (XSS) por meio de mecanismos como: • Aplicar codificação de saída (Output Encoding) nos dados de entrada do usuário sempre que forem renderizados na interface gráfica, impedindo a execução de códigos maliciosos no browser do usuário. • Utilizar Política de Segurança de Conteúdo - Content Security Policy (CSP) - como uma camada de defesa para restringir as fontes de conteúdo que o browser pode carregar (como scripts e estilos). Nota 1: A conformidade com os mecanismos de prevenção a ataques pode ser demonstrada apresentando a documentação oficial (incluindo guias de desenvolvedor ou artigos técnicos) de frameworks e bibliotecas de segurança, além de evidências de que o S-RES utiliza e configura corretamente essas ferramentas. Nota 2: XSS é um tipo de injeção que permite a um atacante inserir código (normalmente	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
		JavaScript) no conteúdo que será visualizado por outro usuário, podendo roubar dados da sessão ou realizar ações em nome da vítima.		
NGS1.06.09	Proteção contra ataques de CSRF	Condição: S-RES em arquitetura Web. O S-RES deve implementar controles técnicos para prevenir, detectar e mitigar ataques de Cross-Site Request Forgery (CSRF) por meio de mecanismos como: • Implementar mecanismos de sincronização de tokens ou outros métodos de verificação de origem em requisições que alteram o estado do sistema (operações críticas). O CSRF ocorre quando um atacante força o browser da vítima a enviar uma requisição indesejada para o S-RES onde ela está autenticada. Nota 1: A conformidade com os mecanismos de prevenção a ataques pode ser demonstrada apresentando a documentação oficial (incluindo guias de desenvolvedor ou artigos técnicos) de frameworks e bibliotecas de segurança, além de evidências de que o S-RES utiliza e configura corretamente essas ferramentas. Nota 2: CSRF é um ataque que engana o browser de um usuário autenticado a enviar uma requisição HTTP indesejada para o S-RES, forçando o sistema a executar ações não autorizadas pelo usuário.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário.	1
NGS1.07 - Auditoria				
NGS1.07.01	Auditoria contínua	O S-RES deve gerar registros de auditoria de forma contínua e permanente, não sendo permitida a sua desativação ou interrupção, ainda que temporária.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.07.02	Proteção dos registros de auditoria	a) Os registros de auditoria devem ser protegidos contra acesso não autorizado e contra qualquer tipo de alteração. b) Apenas usuários com perfil de auditor ou, na ausência deste, o administrador do sistema, podem ter acesso (consulta) a esses dados.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.07.03	Eventos registrados na trilha de auditoria	O S-RES deverá registrar em trilha de auditoria minimamente os seguintes tipos de eventos, quando contemplados pelo sistema: a) Quanto aos dados clínicos: • Criação, duplicação, consulta, inativação de registros clínicos; • Importação e exportação de dados (aplicável apenas caso o S-RES realize importação e/ou exportação de dados para outros sistemas); • Impressão de registros clínicos, incluindo a geração de arquivos em PDF; • Bloqueio de acesso a um prontuário • Solicitação de acesso de emergência a um prontuário; • Registro ou revogação de termos de consentimento para acesso a dados pessoais; • Criação, inativação e alterações de regras de apoio à decisão clínica, tais como regras de interação medicamentosa (aplicável apenas caso as regras de apoio à decisão clínica sejam controladas pelo próprio S-RES e não por uma solução de terceiro integrada); b) Quanto às ações de usuário: • Tentativas de autenticação de usuário, com ou sem sucesso; • Troca de senha; • Encerramento e bloqueio de sessão de usuário; • Desbloqueio de sessão de usuário; • Aceitação do termo de concordância de uso; • Realização de assinatura digital (aplicável apenas para NGS2); • Validação de assinatura digital (aplicável apenas para NGS2); • Falha na realização ou validação de assinatura digital (aplicável apenas para NGS2). • Ativação/desativação de recursos de IA no momento do uso (aplicável apenas para categoria de IA)	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
		c) Quanto às ações de administração do sistema: • Atividades de gerenciamento de usuários e perfis, incluindo alterações de cadastro, inativação/bloqueio e ativação/desbloqueio de conta de usuário; • Realização e restauração de cópia de segurança (aplicável apenas caso as operações de backup sejam realizadas na aplicação); • Atividades de configuração do sistema (por exemplo, parâmetros de configuração de senha, limite de tentativas de login, etc.); • Geração de senha para usuário; • Acesso à trilha de auditoria; • Ativação/desativação de recursos de IA em nível institucional (aplicável apenas para categoria de IA) Nota: A exigência de alguns eventos em trilha de auditoria pode variar de acordo com a categoria/modalidade e estágio de maturidade sendo avaliadas. Por exemplo, para certificação em clínica/ambulatório estágio 1, o evento "solicitação de acesso de emergência a um prontuário" não será exigido, uma vez que este recurso é requirido apenas no estágio 2.		

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.07.04	Informações do registro de auditoria	O S-RES deve registrar, para cada registro de auditoria, minimamente as seguintes informações: • Número de identificação unívoca do registro da trilha; • Data e hora do evento com fuso horário; • Tipo de ação/evento (por exemplo: criação de atendimento, acesso ao prontuário, acesso a documento de sumário de alta, impressão de documento, troca de senha, etc.); • Identificação do componente gerador da ação/evento (endereço IP ou MAC address, por exemplo); • Identificação do usuário que executou a ação/evento, quando aplicável; • Identificador da entidade afetada pela ação/evento (por exemplo, ID do paciente cujo prontuário foi acessado ou ainda ID do usuário que teve sua conta inativada); • Identificador da instituição de saúde em que a ação/evento ocorreu (ID da instituição no sistema ou CNES); • Informações complementares relevantes sobre a ação/evento, quando aplicável (por exemplo: motivo da falha na validação de assinatura digital, descrição do erro relativo à execução de processos operacionais, etc). Nota 1: O "identificador da entidade afetada pela ação/evento" visa permitir a identificação não apenas do usuário que executou a ação, mas também da entidade (paciente, usuário, profissional, etc) que recebeu a ação. Por exemplo, usuário A (executor) acessou o prontuário do paciente B (entidade afetada), ou ainda o usuário A (executor) inativou a conta do usuário C (entidade afetada). Nota 2: Opcionalmente, a trilha de auditoria também pode indicar o ID do dado/registro específico afetado por uma determinada ação (por exemplo, ID da evolução registrada por um usuário, ID do documento impresso, etc.). Neste caso, o identificador da entidade afetada (paciente, usuário, profissional, etc.) deve ser apresentado separadamente.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.07.05	Privacidade do paciente na trilha de auditoria	Dados clínicos ou dados de identificação do paciente não devem ser registrados na trilha de auditoria. O registro deve se limitar ao identificador da entidade afetada (por exemplo, ID do paciente), permitindo a rastreabilidade sem expor o dado sensível na trilha de auditoria.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.07.06	Visualização dos registros da trilha de auditoria	a) O S-RES deve possuir uma interface na aplicação para visualização dos registros de auditoria em ordem cronológica. b) Todos os registros da trilha de auditoria devem ser passíveis de visualização por meio dessa interface. c) Tal interface deve permitir a filtragem de registros minimamente por: • Período de tempo data (data de início e fim) • Tipo de evento; • Identificação do usuário que executou a ação/evento; • Identificador do registro afetado pela ação/evento (por exemplo, ID do paciente cujo prontuário foi acessado ou ainda ID do usuário que teve sua conta inativada); • Identificador da instituição de saúde em que a ação/evento ocorreu. Nota: O filtro pelo "identificador da entidade afetada pela ação/evento" visa permitir a busca por ações/eventos que afetaram uma determinada entidade no sistema. Por exemplo, busca por todas as ações/eventos que envolveram o paciente X (entidade afetada).	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.07.07	Exportação dos registros da trilha de auditoria	a) Possuir uma interface na aplicação para exportação dos registros da trilha de auditoria em formato aberto (por exemplo, CSV, XML, HTML e ODX), de tal forma que possam ser visualizados e processados em aplicativo externo. b) A interface de exportação também deverá ter a funcionalidade de filtragem. c) O arquivo exportado deve ainda incluir as informações de identificação do software (nome do software, nome do fornecedor, identificação completa da versão e/ou release e/ou build) e instituição (nome, CNES e CNPJ). d) Todos os registros de tempo no arquivo exportado devem ser apresentados no formato ISO 8601, incluindo o offset do fuso horário em relação ao UTC.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	3

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.07.08	Acesso à trilha de auditoria em ambientes SaaS	Condição 1: S-RES ofertado na modalidade SaaS. Condição 2: S-RES pode ser utilizado por mais de um usuário na instituição de saúde. a) A empresa responsável pelo S-RES deve fornecer à instituição de saúde (cliente) acesso integral à sua trilha de auditoria por meio de interface na aplicação. b) Caso a base de dados do S-RES seja única para todos os clientes (multi-tenant), deve haver um controle lógico que garanta a segregação dos registros por organização, impedindo que a trilha de auditoria de uma instituição contenha informações de outra instituição.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.08 - Documentação				
NGS1.08.01	Tópicos dos manuais	a) O S-RES deve possuir manuais que apresentem minimamente as seguintes informações: • Instruções de uso do S-RES para os usuários contemplando todos os perfis/papéis existentes (por exemplo: administrador, operador, operador de backup, etc); • Instalação e configuração do S-RES; • Instalação e configuração dos componentes complementares e/ou distribuídos (por exemplo, SGBD, sistema operacional, etc); • Recomendações sobre a forma de configuração segura do S-RES e componentes complementares e/ou distribuídos; • Instruções explicitando quaisquer exigências de ambiente computacional, limitações e restrições relacionadas à compatibilidade do S-RES e/ou seu funcionamento (por exemplo, navegadores compatíveis, mídias compatíveis para uso do certificado digital, etc.); • Os requisitos técnicos mínimos de infraestrutura, incluindo especificações de CPU, GPU (se aplicável), memória, rede, sistema/aplicação operacional e segurança; • Recomendações para plano de contingência para situações de falha ou indisponibilidade; • Instruções e procedimentos para operações de cópia de segurança e restauração; • Compatibilidade com versões anteriores do S-RES, quando aplicável. b) Os manuais poderão ser apresentados em documentos separados ou em um mesmo documento dividido em diferentes capítulos, em suporte em papel e/ou eletrônico. Essa separação deve incluir minimamente os temas: instalação, operação, administração e recomendações de segurança. Nota 1: Os manuais podem ser disponibilizados em quaisquer formatos abertos e inteligíveis, tais como texto (impresso ou eletrônico), audiovisual, etc. Nota 2: No caso de SaaS, os manuais dirigidos à instalação e configuração do S-RES e de seus componentes podem ficar restritos ao fornecedor (administrador da plataforma), sendo dispensada a sua disponibilização aos usuários finais.		1
NGS1.08.02	Referência à versão do S-RES	Todos os manuais devem indicar, no início do documento, seu versionamento documental, bem como a identificação da versão do S-RES a que se referem.		1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.08.03	Idioma dos manuais	Todos os manuais do S-RES devem possuir uma versão em português do Brasil.		1
NGS1.08.04	Operações de backup	a) O manual sobre operações de cópia de segurança e restauração deve incluir minimamente as seguintes informações: • Instruções de configuração de usuários/perfis com permissões exclusivas para backup; • Instruções para restringir operações de exportação/restauração apenas a contas autorizadas no SGBD; • Alertas de segurança sobre o uso de contas administrativas genéricas (como 'sa') para estas tarefas; • Procedimentos passo a passo de Backup e Restauração; • Instruções para ativação de encriptação nas mídias de backup; • Instruções para validação da integridade das cópias geradas (verificação de sucesso); • Aviso de que as cópias de segurança devem ser guardadas em local físico ou lógico seguro, em ambiente físico distinto afastado do local original, em repositório provido de controle de acesso e com garantia de sigilo. b) Caso o S-RES não possua a funcionalidade de exportação e restauração em sua interface diretamente, deve referenciar em seu manual procedimento ou link do fabricante do SGBD contendo informações pertinentes para execução destas tarefas. c) Para S-RES ofertado no modelo SaaS, o fornecedor deve possuir uma documentação interna contento todas as instruções relacionadas à cópia de segurança. Adicionalmente, o fornecedor deve disponibilizar ao cliente uma documentação informando minimamente: • Declaração de Responsabilidade: Termo explícito informando que a gestão, integridade e execução das cópias de segurança são de responsabilidade integral do fornecedor; • Periodicidade e Janelas: Informação sobre a frequência das cópias automáticas (por exemplo, a cada 4 horas); • Política de Retenção: Prazo de guarda das versões (por exemplo, retenção por 10 dias); • Protocolo de Solicitação: Instruções detalhadas sobre como o cliente pode solicitar a restauração de dados ou uma cópia integral.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução realizar armazenamento persistente de dados.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.08.05	Restrição de acesso a entidades não autenticadas e autorizadas	a) O manual de instalação deve informar como configurar o SGBD e todos os demais componentes complementares e/ou distribuídos do S-RES de forma a impedir o acesso de entidades (usuários ou outros sistemas) não autenticadas ou não autorizadas pelo controle de acesso. b) Para S-RES ofertado no modelo SaaS, o fornecedor deve documentar internamente os procedimentos de configuração do SGBD e demais componentes complementares quanto ao controle de acesso, e o manual do cliente deve informar que esses procedimentos são de responsabilidade do fornecedor e que garantem a segurança de acesso ao SGBD.		1
NGS1.08.06	Sincronização de relógio	a) O manual de administração e operação deve informar ao administrador que os componentes complementares e/ou distribuídos do S-RES devem estar com seus relógios sincronizados e referenciados ao UTC (Coordinated Universal Time). O manual deve também informar de que forma esta sincronização pode ser configurada no ambiente computacional. b) Para S-RES ofertado no modelo SaaS, o fornecedor deve documentar internamente os procedimentos de configuração de sincronização de relógio, e o manual do cliente deve informar que esses procedimentos são de responsabilidade do fornecedor e que garantem a sincronização adequadamente.		1
NGS1.08.07	Segregação dos componentes	Condição: S-RES composto por componentes distribuídos. a) O manual de instalação deve informar claramente se o S-RES possui uma segregação lógica e física, se for o caso, dos diferentes componentes do sistema, tais como servidor de banco de dados, servidor de aplicação, servidor de autenticação, servidor de backup, servidor de validação de certificados digitais, etc. b) O manual deve exemplificar uma ou mais arquiteturas de configuração, propiciando o atendimento do cenário de componentes distribuídos. c) O manual deve conter um diagrama que represente a comunicação entre componentes e seus respectivos métodos de comunicação segura. d) Para S-RES ofertado no modelo SaaS, o fornecedor deve documentar internamente a arquitetura do S-RES mostrando os seus componentes, e o manual do cliente deve apresentar essa arquitetura.		1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.08.08	Configuração da segurança da comunicação entre componentes	Condição: S-RES ser composto por componentes distribuídos. a) O manual de instalação deve informar que a comunicação entre os componentes distribuídos do S-RES deve implementar os serviços de segurança de autenticação de parceiro, integridade e sigilo dos dados, e dar orientações para tal configuração. b) Para S-RES ofertado no modelo SaaS, o fornecedor deve documentar internamente os procedimentos de configuração para garantia de canal seguro de comunicação entre os componentes, e o manual do cliente deve informar que esses procedimentos são de responsabilidade do fornecedor e que garantem a comunicação segura.		1
NGS1.08.09	Recomendações sobre configurações de segurança	O manual do S-RES deve conter informações, alertas e/ou recomendações sobre configurações relacionadas à segurança do S-RES (por exemplo, tempo máximo para periodicidade de troca de senha, tempo máximo para expiração de sessão, etc.).	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1
NGS1.08.10	Histórico de alterações entre versões do S-RES	A empresa responsável pelo S-RES deve manter e disponibilizar documentações contendo o histórico descritivo das alterações realizadas entre diferentes versões do S-RES ("release notes"), contendo a data e modificações, além de permitir a inclusão do impacto das alterações (módulos, funções, serviços afetados, etc.) e restrições de compatibilidade, quando houver.		1
NGS1.08.11	Importação de dados de dispositivos externos de saúde	Condição: S-RES possui recursos para importação automática de dados de dispositivos externos de saúde. a) O manual deve indicar os procedimentos necessários para importação, incluindo parametrização quando aplicável. b) O manual deve conter um aviso de que, em caso de importação de dados de dispositivos externos de saúde, é necessário que exista um termo de responsabilidade referente à aferição e calibração periódica desses dispositivos, ou que haja um profissional de saúde que valide essas informações antes de sua aceitação pelo S-RES.		1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.09 - Tempo				
NGS1.09.01	Fonte temporal	a) Todo registro de tempo do S-RES deverá ser baseado em uma fonte de referência temporal confiável, ou seja, utilizar a referência de tempo do servidor e não da estação do usuário, exceto no caso de aplicação “desktop” (onde o sistema está em um único computador, sem servidor separado). b) O registro de tempo deve ser contínuo, utilizando o protocolo de sincronismo de tempo NTP.		1
NGS1.09.02	Registro de tempo no banco de dados	a) Todo registro de tempo (data/hora) deve ser armazenado no banco de dados incluindo obrigatoriamente o offset do fuso horário em relação ao UTC (por exemplo, -03:00), independentemente de o dado ser armazenado no formato UTC ou em outro fuso horário configurado. b) A estrutura lógica deve incluir, minimamente: dia, mês, ano, hora, minuto e segundo e offset do fuso horário em relação ao UTC (por exemplo, 2025-10-19T13:30:15-03:00). c) Quando um usuário realizar um registro na aplicação, o S-RES deve capturar o fuso horário configurado para a instituição e aplicar a conversão para o fuso do banco de dados antes de persistir o dado. Essa conversão deve garantir que a cronologia dos eventos seja preservada, independentemente de diferenças entre o fuso da instituição e o fuso do servidor de banco de dados.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução realizar armazenamento persistente de dados.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.09.03	Conversão de fuso horário de acordo com a instituição	a) O S-RES deve permitir a configuração do fuso horário onde se encontra a instituição de saúde. A configuração pode ser implementada em qualquer camada da solução (aplicação, banco de dados ou infraestrutura em nuvem), desde que garanta a correta exibição dos registros de tempo de acordo com o fuso horário da instituição. b) Ao exibir um registro de tempo (data/hora), tanto em tela quanto em documentos gerados pelo S-RES (PDF, impressão, etc.), o sistema deve garantir que esse registro seja exibido de acordo com o fuso horário indicado na configuração. Por exemplo, caso os registros de data/hora sejam armazenados no banco de dados no fuso horário UTC-3 e a instituição se encontra no UTC-4, esses registros deverão ser convertidos para o fuso horário da instituição ao serem exibidos na aplicação. c) As instruções para realização da configuração deverão estar disponíveis em manual. d) Para S-RES ofertado como SaaS com uma arquitetura em que diferentes clientes compartilham uma mesma base de dados (multi-tenant), essa configuração deve ser por cliente e não como um parâmetro geral.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário e realizar armazenamento persistente de dados.	1
NGS1.09.04	Uniformidade da representação para exibição de tempo	a) Toda exibição de data em telas e documentos gerados pelos S-RES (PDF, impressão, etc.) deve respeitar a sequência dia seguido do mês seguido do ano. b) Toda exibição de horário em telas e documentos gerados pelos S-RES (PDF, impressão, etc.) deve respeitar a sequência hora seguida dos minutos e, opcionalmente, segundos. c) Em documentos gerados pelo S-RES (PDF, impressão, etc.), incluindo o prontuário impresso, a exibição de horários deve ainda incluir o fuso horário de referência após conversão de acordo com o fuso horário da instituição (por exemplo, UTC-3).	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário.	1
NGS1.09.05	Uniformidade da representação para entrada de tempo	a) Toda entrada de data completa deve respeitar a sequência dia seguido do mês seguido do ano. b) Toda entrada de horário deve respeitar a sequência hora seguida dos minutos.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.09.06	Uniformidade da representação para exportação de tempo	Condição: S-RES realiza exportação de dados em formatos abertos (por exemplo, XML, JSON, etc.) para integração com outros sistemas/dispositivos. Na exportação de dados do RES, todos os registros de tempo devem ser apresentados no formato ISO 8601, incluindo o offset do fuso horário em relação ao UTC.		1
NGS1.10 - Notificação de ocorrências				
NGS1.10.01	Gerenciamento de incidentes e vulnerabilidades	a) A empresa responsável pelo S-RES deve possuir um processo formal e documentado para gerenciamento de incidentes e vulnerabilidades de segurança da informação, privacidade e segurança do paciente, incluindo: • Canal de Reporte: A empresa fornecedora deve disponibilizar um canal de comunicação para que o cliente possa reportar incidentes de segurança, problemas e/ou vulnerabilidades encontradas. • Tratamento e Classificação Interna: A empresa fornecedora deve possuir procedimentos internos documentados que definam como as ocorrências reportadas serão classificadas, escaladas, resolvidas e registradas. • Comunicação ao Cliente: Em casos de descoberta e correção de vulnerabilidades críticas no S-RES, a empresa fornecedora deve notificar os clientes afetados, informando sobre a vulnerabilidade e disponibilização das correções. b) Caso o sistema seja ofertado como SaaS com infraestrutura gerenciada pela própria empresa responsável pelo S-RES, deve ainda haver um processo formal para notificar clientes e realizar ações corretivas em caso de ocorrência de incidentes de segurança da informação e privacidade (vazamento de dados, por exemplo).		2
NGS1.11 - Privacidade				
NGS1.11.01	Concordância com termos de uso	a) O S-RES deve exibir imediatamente após o primeiro acesso do usuário no sistema, um termo de concordância sobre o uso do sistema e as políticas de privacidade sobre o tratamento apropriado das informações pessoais e de saúde, alertando para o devido cuidado visando a confidencialidade dos dados e as consequências do uso inadequado dos mesmos. b) O usuário só deve poder prosseguir após aceitar explicitamente as condições ali dispostas.	Para a categoria de Inteligência Artificial, esse requisito se aplica apenas se a solução operar no modelo stand-alone e possuir interface gráfica para interação com o usuário.	1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
		c) A concordância com os termos deverá ser repetida obrigatoriamente a cada alteração nas políticas de uso.		
NGS1.11.11	Tratamento e proteção de dados de pacientes em infraestrutura própria	Condição: o S-RES armazena ou processa dados de pacientes em infraestrutura sob controle da própria empresa responsável pelo S-RES (por exemplo, SaaS). a) A empresa responsável pelo S-RES deve possuir e disponibilizar aos seus clientes um documento formal que descreva quais tratamentos de dados pessoais e de saúde são realizados pela empresa quando os dados são armazenados ou processados em sua infraestrutura. b) O documento deve identificar e descrever todas as finalidades para as quais os dados dos pacientes podem ser acessados, copiados, processados ou utilizados pela empresa, incluindo finalidades técnicas (por exemplo: hospedagem, backup, pesquisa, treinamento de modelos de IA, analytics, etc.). c) O documento deve especificar se há compartilhamento com terceiros ou transferência internacional de dados. d) Qualquer mudança nas finalidades de tratamento ou nas condições de uso dos dados pela empresa deve ser formalmente comunicada e autorizada pelo cliente antes da implementação, indicando o tipo de alteração (por exemplo: nova finalidade, novo subprocessador, etc.) e data prevista de início. e) A empresa deve manter registro histórico das versões anteriores do documento, com data de vigência de cada uma, para permitir rastreabilidade das comunicações e auditoria. Nota: Este requisito se estende também aos subprocessadores, ou seja, a quaisquer empresas ou serviços terceirizados contratados pela empresa responsável pelo S-RES que tratem, armazenem, transmitam ou tenham acesso aos dados pessoais ou de saúde em nome da empresa ou de seus clientes. Dessa forma, a empresa responsável pelo S-RES deve garantir que os subprocessadores adotem as mesmas práticas de transparência descritas neste requisito.		1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.12 - Segurança da Informação, Privacidade e Infraestrutura para IA				
NGS1.12.01	Mecanismos de proteção da privacidade de dados submetidos pelos usuários	Condição: S-RES recebe dados de usuários diretamente (via interface, por exemplo) ou indiretamente (via integração com outros sistemas, por exemplo). a) O S-RES deve assegurar que dados pessoais e sensíveis enviados para processamento por modelos de IA não sejam utilizados para treinamento, melhoria ou reaproveitamento dos modelos, nem armazenados de forma persistente fora dos repositórios do próprio sistema, salvo quando houver consentimento explícito e finalidade claramente definida. b) Os modelos de IA devem estar configurados para não reter ou utilizar dados de entrada para treinamento de modelos de terceiros (por exemplo, modo Zero Data Retention). Nota 1: Este requisito refere-se exclusivamente aos dados enviados para processamento por modelos de IA (por exemplo, prompts, textos para sumarização, áudios transcritos, etc.), não se aplicando aos dados clínicos e cadastrais que precisam ser armazenados pelo sistema. Nota 2: O modo Zero Data Retention (ZDR) — em português, Retenção Zero de Dados — é uma configuração de segurança e privacidade em plataformas de IA que garante que nenhum dos dados enviados pelo usuário (prompts/perguntas) ou gerados pela IA (respostas) seja armazenado nos servidores do fornecedor após o processamento.		1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.12.02	Proteção contra ataques de Injeção de Prompt	Condição: S-RES utiliza IA generativa que recebam prompts de entrada de usuários diretamente (via interface, por exemplo) ou indiretamente (via integração com outros sistemas, por exemplo). a) A empresa responsável pelo S-RES deve implementar e documentar controles técnicos e processuais para proteger os modelos de IA contra ataques de Injeção de Prompt (Prompt Injection) que consiste em inserir instruções maliciosas dentro do input do usuário (prompt) para fazer com que um modelo de linguagem (LLM) ignore suas instruções originais e execute uma ação não intencional ou maliciosa. b) Pode-se utilizar técnicas como: • Input Sanitization e Filtering: Filtrar e limpar os prompts de entrada para remover ou neutralizar possíveis instruções, código ou sequências de caracteres de controle. • Separar Instruções de Dados: Estruturar a interação com o modelo de forma que as instruções do sistema e os dados do usuário sejam tratados como entidades distintas, evitando que o modelo confunda dados com novas ordens. • Monitoramento de Saídas: Analisar as saídas do modelo para detectar desvios, anomalias ou respostas que não condizem com o prompt original, bloqueando-as antes de serem apresentadas ao usuário. c) Deve haver uma documentação que descreva a descrição da análise de risco para esses ataques e dos mecanismos adotados para mitigação e monitoramento de sua efetividade. Nota: Caso o S-RES utilize modelos de IA desenvolvidos por terceiros, a empresa deve demonstrar que implementa filtros de entrada e mecanismos de validação de saída antes da apresentação ao usuário, evidenciando que prompts maliciosos são bloqueados e que as respostas fornecidas pela API externa foram checadas quanto a comportamentos inesperados ou riscos de segurança.		2

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.12.03	Proteção contra ataques de Envenenamento de Dados	Condição: S-RES realiza treinamento ou retreinamento de modelos, incluindo fine-tuning ou uso de dados locais do cliente. a) A empresa responsável pelo S-RES deve implementar e documentar controles técnicos e processuais para proteger os modelos de IA contra ataques de Envenenamento de Dados (Data Poisoning) que consiste na manipulação maliciosa dos dados de treinamento para inserir vulnerabilidades, "backdoors" ou vieses no modelo. b) Pode-se utilizar técnicas como: • Controle de Acesso e Proveniência de Dados: Implementar controles rigorosos sobre quem pode adicionar ou modificar dados de treinamento e manter um registro auditável da origem e linhagem de todos os dados. • Validação e Limpeza de Dados: Utilizar técnicas para detectar anomalias, outliers e inconsistências nos dados de treinamento antes do uso. • Treinamento Robusto: Usar métodos como Differential Privacy, que adiciona ruído estatístico ao processo de treinamento para diminuir o impacto de pontos de dados individuais, tornando o envenenamento mais difícil. c) Deve haver uma documentação que descreva a descrição da análise de risco para esses ataques e dos mecanismos adotados para mitigação e monitoramento de sua efetividade. Nota: Caso o S-RES utilize modelos de IA desenvolvidos por terceiros, a empresa deve apresentar documentação do fornecedor sobre medidas de proteção contra envenenamento de dados. Quando informações completas não forem disponibilizadas pelo fornecedor, a empresa deve documentar que tais limitações foram identificadas e disponibilizar essa documentação para seus clientes em manual técnico ou equivalente.		3

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.12.04	Proteção contra ataques de Inferência de Membresia	Condição: S-RES realiza treinamento ou retreinamento de modelos, incluindo fine-tuning ou uso de dados locais do cliente. a) A empresa responsável pelo S-RES deve implementar e documentar controles técnicos e processuais para proteger os modelos de IA contra ataques de Inferência de Membresia (Membership Inference) que visam determinar se os dados de um indivíduo específico foram utilizados no conjunto de treinamento do modelo, podendo revelar informações sensíveis. b) Pode-se utilizar técnicas como: • Privacidade Diferencial: Adicionar ruído durante o treinamento para que a saída do modelo não seja excessivamente dependente de nenhum registro de treinamento individual. • Redução de Overfitting: Utilizar técnicas de regularização (por exemplo, dropout) para que o modelo generalize em vez de "memorizar" os dados de treinamento, tornando a inferência de membresia mais difícil. c) Deve haver uma documentação que descreva a descrição da análise de risco para esses ataques e dos mecanismos adotados para mitigação e monitoramento de sua efetividade. Nota: Caso o S-RES utilize modelos de IA desenvolvidos por terceiros, a empresa deve apresentar documentação do fornecedor sobre técnicas utilizadas para proteção contra inferência de membresia. Quando informações completas não forem disponibilizadas pelo fornecedor, a empresa deve documentar que tais limitações foram identificadas e disponibilizar essa documentação para seus clientes em manual técnico ou equivalente.		3

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.12.05	Proteção contra ataques de Extração de Modelo	Condição: S-RES permite acesso direto aos modelos por meio de APIs, serviços online ou outras interfaces técnicas que possibilitem múltiplas consultas externas para obtenção de pares de entrada e saída. Se o modelo de IA não puder ser acessado diretamente (por exemplo: modelo rodando apenas embarcado em um S-RES), o requisito não se aplica. a) A empresa responsável pelo S-RES deve implementar e documentar controles técnicos e processuais para proteger os modelos de IA contra ataques de Extração de Modelo (Model Extraction) que Consiste em "roubar" a propriedade intelectual do modelo. O atacante interage repetidamente com a IA (geralmente via API) para coletar um grande número de pares de entrada-saída, que são então usados para treinar um modelo "clone" com funcionalidade semelhante. b) Pode-se utilizar técnicas como: • Limitação de Taxa de API (API Rate Limiting): Restringir o número de requisições que um único usuário ou IP pode fazer em um determinado período, dificultando a coleta de dados em larga escala. • Retornar Saídas com Menor Precisão: Em vez de retornar probabilidades detalhadas (por exemplo, 0.9785), retornar apenas a classe de maior probabilidade ou valores arredondados. Isso dificulta o treinamento de um modelo clone preciso. • Marca d'água no Modelo (Model Watermarking): Incorporar "gatilhos" específicos nos dados de treinamento que fazem o modelo gerar saídas únicas e identificáveis, provando que o modelo foi copiado se o clone exibir o mesmo comportamento. c) Deve haver uma documentação que descreva a descrição da análise de risco para esses ataques e dos mecanismos adotados para mitigação e monitoramento de sua efetividade. Nota: Caso o S-RES utilize modelos de IA desenvolvidos por terceiros, a empresa deve apresentar documentação do fornecedor que comprove a adoção de mecanismos adicionais de proteção contra extração de modelo. Quando informações completas não forem disponibilizadas pelo fornecedor, a empresa deve documentar que tais limitações foram identificadas e disponibilizar essa documentação para seus clientes em manual técnico ou equivalente.		3

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.12.06	Herança e aplicação do controle de acesso por funcionalidades de IA	Condição: S-RES incorpora recursos de IA (por exemplo, comando de voz, chatbot, etc.) para buscar, selecionar ou acessar prontuários e dados de pacientes dentro do próprio sistema. a) O S-RES deve garantir que a funcionalidade de IA respeite integralmente as permissões de acesso já definidas no sistema. b) Todas as solicitações de dados iniciadas pela funcionalidade de IA devem ser processadas pela camada de autorização e controle de acesso central do S-RES. A IA deve atuar como um "agente" do usuário logado, herdando todas as suas permissões e restrições. Nota: Exemplo de um cenário: Um enfermeiro autenticado no setor de emergência, onde sua permissão só permite visualizar pacientes admitidos naquele setor, utiliza um comando de voz ou interação com chatbot para buscar e acessar o prontuário de um paciente internado na UTI. O sistema deve identificar e impedir o acesso ao prontuário solicitado.		1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.12.07	Autenticação de usuário em dispositivos de IA autônomos ou embarcados	Condição: Solução de IA que acessa dados de paciente e é operada por meio de um dispositivo físico que não possui uma sessão de usuário atrelada a um login tradicional em tela (por exemplo, assistente de voz em ambiente compartilhado, totem interativo, dispositivo de ambient listening, etc.). a) O S-RES deve implementar um mecanismo robusto para identificar e autenticar o usuário antes de permitir o processamento de qualquer comando que envolva o acesso a dados de pacientes. b) A operação do dispositivo deve incluir, minimamente, um dos seguintes métodos de autenticação ou um método de segurança equivalente: • Biometria: Utilização de características biométricas para identificar o usuário autorizado (por exemplo, reconhecimento de voz, biometria facial). • Pareamento com Dispositivo Pessoal: Exigência de que o profissional inicie uma sessão no dispositivo de IA através do pareamento seguro com um dispositivo pessoal previamente autenticado (por exemplo, aproximar um crachá com tecnologia NFC, autenticação via aplicativo em um smartphone pareado por Bluetooth). • Sessão por Proximidade ou Token: Início de uma sessão em um terminal de computador seguro próximo, que habilita o dispositivo de IA para o usuário autenticado por um período de tempo limitado ou enquanto o usuário permanecer em proximidade. c) O S-RES deve implementar um mecanismo para logoff explícito. Deve existir um comando simples e inequívoco para que o usuário encerre sua sessão ativamente. Exemplo: Um comando de voz claro como "Encerrar sessão" ou "Sair do sistema". d) O S-RES deve implementar um mecanismo para timeout por inatividade. A sessão do usuário deve ser encerrada automaticamente após um período predefinido de inatividade. O tempo de expiração da sessão deve ser configurável.		1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.12.08	Proteção da confidencialidade no compartilhamento de interações	Condição: S-RES oferece funcionalidades para compartilhar interações ou resultados gerados pela IA (por exemplo, compartilhar um chat ou um resumo de consulta). O S-RES deve possuir controles técnicos e processuais para impedir a exposição pública inadvertida ou não autorizada de dados pessoais ou sensíveis. A empresa deve documentar e evidenciar, no mínimo: • Mecanismos para impedir a indexação por mecanismos de busca públicos, como o uso de tags "no-index, no-follow" em páginas de compartilhamento. • Alertas de consentimento explícito, que informem o usuário de forma clara e inequívoca sobre as consequências de privacidade do compartilhamento antes de confirmar a ação. • A disponibilidade de mecanismos de compartilhamento restrito, como controle de acesso por senha, links com tempo de expiração definido ou compartilhamento limitado a usuários autenticados		1
NGS1.12.09	Gestão de Versões e Configurações de IA	a) A empresa responsável pelo S-RES deve manter controle de versão documentado e auditável de todos os componentes que influenciam o resultado de uma funcionalidade baseada em IA. Isso inclui a identificação do modelo base, refinamentos (por exemplo, fine-tuning), bases de conhecimento (por exemplo, RAG), parâmetros técnicos, e instruções de sistema (prompts). Qualquer alteração nestes componentes deve gerar uma nova versão identificável, registrando-se o usuário responsável e a data/hora da modificação. b) O controle de versão deve permitir identificar mudanças em camadas específicas, mesmo que o modelo principal permaneça o mesmo. Por exemplo, em um recurso de ambient listening para documentação clínica, o sistema pode manter a mesma versão do modelo de IA, mas atualizar o prompt para melhorar a estruturação do texto final. Nesse cenário, o controle de versão deve indicar que a versão do system prompt foi alterada de 1.0 para 1.1, com registro de data/hora e responsável. c) Caso o S-RES ofereça recursos que permitam à própria instituição cliente criar, configurar ou customizar agentes de IA ou seus comportamentos (por exemplo, por meio da definição de system prompts, regras ou fluxos), essas configurações também devem estar sujeitas aos mesmos mecanismos de controle de versão, garantindo rastreabilidade, histórico de alterações e possibilidade de identificação da versão em uso em cada execução da funcionalidade.		1

ID	Título	Descrição	Aplicabilidade para Categoria de IA	Estágio de Maturidade
NGS1.12.10	Rastreabilidade das interações com os recursos de IA	a) O S-RES deve manter registros completos e auditáveis das interações e decisões apoiadas por IA, garantindo a rastreabilidade de cada uso da IA (trilha de auditoria). b) A trilha de auditoria deve incluir, minimamente: • Identificação do evento realizado conforme escopo/funcionalidade da IA (por exemplo, sumarização do prontuário, gravação e transcrição de consulta, predição de risco de reinternação, etc.); • Dados de entrada relevantes ou referência aos conteúdos clínicos utilizados pela IA para geração do resultado (por exemplo, identificadores de registros, transcrição consolidada ou resumo dos dados analisados); • Resultado gerado pela IA; • Versão dos componentes utilizados: identificação clara da versão do modelo de IA e, quando aplicável, das versões vigentes do prompt, fine-tuning ou base de conhecimento que influenciaram o resultado; • Identificação do usuário que acessou ou utilizou o recurso de IA; • Indicação de aceite, recusa ou edição das sugestões da IA pelo usuário, quando aplicável, nos casos em que o sistema permita interação direta do profissional com as recomendações apresentadas (por exemplo, diagnósticos sugeridos pela IA e diagnósticos aceitos e não aceitos pelo profissional). • Data e hora da interação. c) Para funcionalidades de interação contínua ou conversacional (por exemplo, chatbots e transcrição de consultas), o registro na trilha de auditoria pode ocorrer no desfecho da interação ou na entrega de recomendações específicas, sendo dispensável o registro de mensagens intermediárias não relevantes (por exemplo, saudações em interações com chatbot). Devem ser registrados os dados consolidados de entrada (por exemplo, sintomas relatados ou transcrição da consulta) e o resultado final entregue (por exemplo, lista de diagnósticos sugeridos ou documentação da consulta). Caso a interface permita ao profissional interagir com a sugestão (por exemplo, botões de aceitar e recusar), a ação realizada também deve ser registrada. d) O S-RES deve disponibilizar o acesso à trilha de auditoria: • Diretamente em sua interface gráfica, quando existente; ou • Por meio de integração (por exemplo, APIs, exportação de relatórios ou conectores), de forma que os sistemas consumidores (por exemplo, prontuário eletrônico) possam apresentar a trilha aos administradores/auditores da instituição.		1

3.4. Requisitos NGS2 - Autenticidade e Assinatura Digital (NGS2)

ID	Título	Descrição	Estágio de Maturidade
NGS2.01 - Certificado Digital			
NGS2.01.01	Certificado digital ICP-Brasil	O S-RES deve permitir que certificados digitais ICP-Brasil possam ser utilizados por profissionais de saúde para o processo de assinatura digital de documentos do prontuário do paciente, atendendo às normas de uso definidas pela ICP-Brasil na utilização desses certificados.	1
NGS2.01.02	Configuração para ativação ou desativação da assinatura digital	a) O S-RES deve permitir configurar se a assinatura digital será ou não utilizada nos registros clínicos. b) O S-RES deve permitir que o prontuário eletrônico opere integralmente sem exigência de assinatura digital quando a instituição optar por não utilizá-la, não devendo impedir finalização de registros clínicos.	1
NGS2.01.04	Validação do CPF do usuário	a) O S-RES deverá permitir o uso de um certificado digital (assinatura digital e autenticação no S-RES) por um usuário apenas se o CPF informado no cadastro deste usuário for idêntico ao identificado no certificado digital utilizado. b) Deve ser utilizada a extensão Nome Alternativo do Titular (Subject Alternative Name) do certificado digital na validação, seja PF ou PJ, utilizar o campo correspondente ao CFP. c) A cada processo de uso do certificado digital, o S-RES deverá validar se o CPF do usuário executando o processo corresponde ao CPF contido no certificado digital utilizado, e o processo só deverá ser finalizado com sucesso em caso de igualdade dos CPFs. Nota: Opcionalmente, o S-RES poderá exigir que no momento do cadastro do usuário faça-se uma restrição a um ou mais certificados digitais específicos, por exemplo fornecendo o número serial dos mesmos.	1

ID	Título	Descrição	Estágio de Maturidade
NGS2.01.05	Validação do certificado digital antes do uso	a) O S-RES deve validar o certificado digital e sua cadeia de certificação antes de sua utilização ou imediatamente após sua utilização. A validação do certificado digital envolve a validação criptográfica, verificação de validade e revogação, inclusive dos certificados da sua cadeia de certificação. b) A validação deve ocorrer no lado do servidor utilizando-se os certificados raiz de confiança configurados no servidor. Dessa forma, apenas certificados raiz existentes no repositório gerenciado podem ser utilizados para atividades de autenticação e/ou assinatura. Nota: Em caso de S-RES local, não existe segregação entre servidor e cliente.	1
NGS2.01.06	Configuração de certificados raiz do S-RES	a) O S-RES deve permitir a configuração (inclusão e exclusão) dos certificados raiz de confiança do S-RES. b) Esta funcionalidade deve ser restrita, com atuação obrigatória de mecanismos de controle de acesso.	3
NGS2.01.07	Compatibilidade com diferentes AC, tipos de certificados e mídias de armazenamento	a) O S-RES deve suportar nativamente a realização de assinaturas digitais utilizando certificados emitidos por, no mínimo, duas Autoridades Certificadoras (ACs 1) distintas credenciadas à ICP-Brasil, conforme estrutura.iti.gov.br, garantindo que o sistema não possua dependência exclusiva de um único fornecedor de tecnologia. b) O S-RES não deve restringir o uso de certificados por tipo de mídia, garantindo compatibilidade obrigatória com certificados A3 em nuvem, além de permitir o uso de certificados em mídias físicas (Tokens/Smartcards) e arquivos (A1).	1
NGS2.02 - Assinatura Digital			
NGS2.02.01	Assinatura digital para todos os documentos clínicos	O S-RES deve permitir que quaisquer registros clínicos possam ser objeto de assinatura digital (prescrições, evoluções, laudos, procedimentos, administração de medicamentos, etc.), incluindo documentos criados pela própria instituição (formulários dinâmicos) e documentos digitalizados e anexados ao prontuário eletrônico.	1
NGS2.02.02	Visualização das informações a serem assinadas	a) O S-RES deve permitir a visualização das informações a serem assinadas antes da sua assinatura. b) O sistema deverá exibir apenas as informações que realmente serão assinadas, excluindo-se quaisquer informações de outras telas adjacentes ou aspectos relacionados à interface (como botões ou menus).	1

ID	Título	Descrição	Estágio de Maturidade
NGS2.02.03	Informações sobre assinatura	a) O S-RES deve exibir uma indicação de que um determinado documento foi assinado digitalmente (por exemplo, exibindo um status de “assinado”). b) O S-RES deve ainda permitir que o usuário possa visualizar por meio da aplicação as informações sobre a assinatura (minimamente quais profissionais assinaram e registro de tempo).	1
NGS2.02.04	Pendência de assinatura	a) No momento de uma assinatura digital, caso o profissional de saúde não assine o documento no ato do registro (por exemplo, esquecimento do cartão/token ou indisponibilidade do serviço de assinatura), o S-RES deverá gerar uma pendência de assinatura. b) Caso um profissional tente sair da tela de um registro clínico sem efetuar a assinatura digital, o sistema deverá notificá-lo imediatamente, inclusive em casos de logoff ou encerramento da aplicação. O alerta deve permitir que o usuário permaneça na tela para concluir a assinatura. c) O S-RES deve permitir que o profissional acesse de forma ágil no sistema uma lista de seus registros pendentes de assinatura. Quando o usuário selecionar um item da lista, o sistema deve exibir o documento para conferência e permitir sua assinatura. Uma vez assinado, o registro deve ter seu status atualizado e ser removido automaticamente da lista de pendências.	1
NGS2.02.05	Assinatura em lote de registros clínicos pendentes	a) O S-RES deve permitir que o profissional resolva múltiplas pendências de assinatura de forma eficiente, por meio de assinatura em lote. b) O usuário deve poder selecionar um ou mais registros da lista de documentos pendentes de assinatura para assiná-los simultaneamente, utilizando uma única ação de assinatura. c) O S-RES deve permitir, sem exigir, que o usuário visualize o conteúdo de cada registro individual caso assim desejado pelo profissional.	2

ID	Título	Descrição	Estágio de Maturidade
NGS2.02.06	Consistência de documentos assinados após inativação ou alteração	a) O S-RES deve garantir a consistência entre registros clínicos assinados digitalmente e o estado atual dos registros de origem, quando estes forem inativados ou alterados. b) Quando um registro clínico for inativado/cancelado, o documento assinado associado deve ser igualmente marcado como inativo, permanecendo no prontuário apenas como evidência histórica. Essa informação deve ser exibida claramente na aplicação. c) Quando um registro clínico for alterado e uma nova versão for gerada, o documento assinado associado deve ser inativado e a aplicação deve permitir a assinatura da nova versão do documento. Essa informação deve ser exibida claramente na aplicação.	1
NGS2.02.07	Formato de assinatura	O S-RES deve gerar assinaturas digitais nos formatos CAdES, XAdES ou PAdES seguindo, minimamente, a política AD-RB.	1
NGS2.02.08	Instante da assinatura	O S-RES deve incluir em toda assinatura realizada: • no caso do formato CMS/CAdES, o atributo id-signingTime; • no caso do formato XMLDSIG/XAdES, a propriedade SigningTime; • no caso do formato PAdES, a entrada no dicionário de assinatura chamada de “M”. Este atributo representa o instante de assinatura (signingTime ou “M”) adotado pelo signatário.	1

ID	Título	Descrição	Estágio de Maturidade
NGS2.02.09	Portal de assinatura	Condição: a geração da assinatura ser realizada em portal integrado de assinatura a) O portal de assinatura deve atender aos seguintes requisitos de comunicação entre componentes: • Autenticação dos parceiros (ambas as partes) • Integridade dos dados e confidencialidade dos dados (criptografia). • Uso do protocolo TLS 1.2 ou superior. b) O armazenamento de documentos e metadados no portal externo deve seguir as seguintes diretrizes: • Para portais de assinatura de propósito geral, o armazenamento deve ser estritamente temporário, limitado ao tempo necessário para a coleta das assinaturas. • O período exato de retenção e a política de descarte definitivo dos dados devem estar documentados de forma clara no Manual do Usuário. • Portais especificamente projetados para a custódia de dados de saúde (que atendam aos requisitos de conformidade para prontuário eletrônico) podem manter o armazenamento permanente, desde que respeitados os prazos legais de guarda de documentos clínicos.	1
NGS2.02.10	Autenticação para sessões de assinatura digital	a) O S-RES deve implementar mecanismo seguro de autenticação para realização de assinaturas digitais, evitando a necessidade de inserção de PIN ou código OTP a cada assinatura individual. a) O S-RES deve permitir o estabelecimento de uma sessão de assinatura após autenticação forte inicial (por exemplo, PIN do certificado, autenticação multifator ou biometria), possibilitando a assinatura de múltiplos registros durante a vigência dessa sessão. b) O S-RES deve permitir a configuração da duração máxima da sessão de assinatura, devendo expirar automaticamente quando atingido o tempo limite. c) A sessão deve ser exclusivamente vinculada ao profissional autenticado, devendo o S-RES impedir seu reaproveitamento por outro usuário. d) Após a expiração da sessão de assinatura, deve ser obrigatória nova autenticação para renovação do sessão de assinatura.	2

ID	Título	Descrição	Estágio de Maturidade
NGS2.02.11	Assinatura automática de registros clínicos	a) O S-RES deve permitir que a assinatura digital de registros clínicos seja realizada de forma automática no momento da finalização do documento, sem necessidade de ação explícita do usuário (por exemplo, assinar o documento automaticamente após sua liberação no prontuário, sem que haja a necessidade de clicar em um botão de “assinar”). b) O uso de assinatura automática deve ser configurável no sistema, permitindo que a instituição de saúde defina se a assinatura automática será ou não utilizada. c) A assinatura automática deve estar vinculada única e exclusivamente ao profissional autenticado no momento da liberação do documento. d) A assinatura automática somente pode ocorrer quando existir sessão de assinatura válida, estabelecida previamente por autenticação forte. Caso a sessão de assinatura expire ou seja invalidada, o sistema deve impedir novas assinaturas automáticas até que o profissional realize nova autenticação forte para uso do certificado digital. e) O S-RES deve impedir a assinatura automática em registros que não estejam finalizados/liberados no prontuário do paciente. f) Caso o usuário autenticado não possua um certificado digital, o S-RES deverá gerar uma pendência de assinatura sem impedir que o documento seja liberado.	2
NGS2.02.13	Indisponibilidade de acesso a serviços externos	No momento da assinatura, caso não haja disponibilidade de serviços externos (tais como, a OCSP, LCR ou carimbo de tempo), o S-RES deverá adotar um dos seguintes métodos: • Não dar continuidade ao processo de assinatura, tornando-a pendente; ou • Registrar que a assinatura está pendente de atualização e validação, emitindo um aviso da pendência para o usuário que está assinando e para o administrador do S-RES ou diretor técnico da organização de saúde. A assinatura deverá ser atualizada com os dados que estavam indisponíveis tão logo o serviço externo esteja disponível.	3
NGS2.02.14	Encadeamento de registros assinados digitalmente	O S-RES deve garantir a ordem temporal de assinatura e presença de todos os registros assinados para cada paciente. Por exemplo, para não repúdio, uma função hash pode ser aplicada sucessivamente a partes adicionais dos dados para registrar a cronologia da existência dos mesmos.	3
NGS2.02.15	Verificação do encadeamento de registros	O S-RES deve possuir funcionalidade para que o usuário, a qualquer momento, consiga validar o encadeamento dos registros assinados digitalmente.	3

ID	Título	Descrição	Estágio de Maturidade
NGS2.03 - Validação da Assinatura Digital			
NGS2.03.01	Validação da assinatura digital	a) O S-RES deverá realizar a validação da assinatura minimamente nas seguintes situações: • Imediatamente após a geração da assinatura digital do documento eletrônico; • Ao ser solicitada a impressão ou exportação de múltiplos registros (como por exemplo: em uma exportação de completa do PEP) de documentos previamente assinados digitalmente; • Na importação de registro eletrônico assinado digitalmente: a assinatura deve ser validada antes de iniciar sua inclusão no RES; • Na exportação de registro eletrônico assinado digitalmente: a assinatura deve ser validada antes de iniciar sua exportação no RES; • Por vontade e ação do usuário, ao ter acesso a todo e qualquer documento assinado, durante pesquisa ou consulta. b) A validação de um documento eletrônico assinado deve exibir o status (resultado) da validação da assinatura ao usuário e permitir sua revalidação a qualquer tempo. c) Em caso de mais de uma assinatura no documento eletrônico (co-assinaturas), todas estas deverão ser validadas. d) A validação de uma assinatura deve incluir: • A validação do carimbo de tempo, quando presente: verificação da assinatura do carimbo de tempo, do certificado da autoridade de carimbo de tempo e dos certificados da cadeia de certificação, conforme requisitos da ICP-Brasil e da RFC 3161; • A verificação do certificado do signatário e dos certificados da cadeia de certificação; • A verificação do estado de revogação do certificado do signatário e dos certificados da cadeia de certificação, utilizando como referência temporal o instante presente no carimbo de tempo, e utilizando LCR (Lista de Certificados Revogados) [RFC 5280] ou Resposta OCSP (Online Certificate Status Protocol) [RFC 2560]. Caso o objeto de revogação (LCR ou resposta OCSP) não esteja presente, obtê-lo e incluí-lo na assinatura no momento da validação. Nota: Na validação da assinatura de documentos/registros antigos do S-RES sem a presença de carimbo de tempo, a referência temporal a ser utilizada para verificação de revogação é o instante presente no atributo “momento de assinatura” (signingTime).	1

ID	Título	Descrição	Estágio de Maturidade
NGS2.03.02	Homologação do Serviço de Validação de Assinaturas	O processamento das validações de assinaturas digitais deve ser realizado exclusivamente em ambiente controlado, observando os seguintes critérios: • A validação deve ocorrer nativamente no S-RES ou por meio de serviço de terceiros integrado via API, desde que este seja formalmente vinculado à solução. • É vedado o uso de validadores públicos (ex: portais web de uso comum), ferramentas de código aberto sem suporte corporativo ou qualquer plataforma que não permita auditoria e controle de logs pelo S-RES. • Todo serviço de validação externo deve estar amparado por um Acordo de Nível de Serviço (SLA) e um contrato de suporte técnico com uma entidade jurídica responsável, garantindo a disponibilidade e a continuidade operacional necessária para o fluxo clínico.	1
NGS2.03.03	Referência temporal para verificação de revogação sem carimbo de tempo	No momento da validação de uma assinatura digital sem carimbo de tempo, a referência a ser utilizada para verificação de revogação ou vigência do certificado digital deverá ser o instante presente no atributo “momento da assinatura” (signingTime ou equivalente).	1
NGS2.03.04	Referência temporal para verificação de revogação com carimbo de tempo	No momento da validação de uma assinatura digital com carimbo de tempo, a referência a ser utilizada para verificação de revogação ou vigência do certificado digital deverá ser o carimbo de tempo.	2
NGS2.03.05	Resultado da validação da assinatura digital	a) O S-RES deve, a qualquer tempo, prover meios para validação e exibição do estado de validade de uma assinatura digital. b) O resultado da validação de uma assinatura digital deve retornar um dos seguintes estados: • Válida: assinatura válida; • Inválida: assinatura inválida; • Indeterminada: quando não é possível determinar se a assinatura está válida ou inválida, geralmente devido à falta de objetos críticos (por exemplo: certificado, objeto de revogação, carimbo de tempo, certificado da cadeia, atributos obrigatórios, etc.). c) Exceto para o estado válido, a causa deverá ser indicada. d) Na impressão de um documento assinado, deverá constar o estado da assinatura (resultado da validação).	1

ID	Título	Descrição	Estágio de Maturidade
NGS2.04 - Carimbo de Tempo			
NGS2.04.01	Política AD-RT para assinaturas digitais	As assinaturas digitais geradas pelo S-RES devem seguir, ao menos, a política AD-RT (Assinatura Digital com Referências de Tempo), com a inclusão de todos os objetos necessários à validação (certificados dos signatários, cadeias de certificação, objetos de revogação, carimbo de tempo, etc.). Nota 1: Opcionalmente, tais objetos podem não ser incluídos, desde que: • Os objetos necessários à validação referenciados (certificados digitais, objetos de revogação, etc.) estejam armazenados localmente ao S-RES; • Seja garantida a disponibilidade do armazenamento e a recuperação futura de todos os objetos necessários para realizar a validação; • O S-RES seja capaz de incluir na assinatura AD-RT todos os objetos necessários para realizar a validação (necessário, por exemplo, quando um registro assinado for exportado). Nota 2: Opcionalmente, ao utilizar PAdES, pode ocorrer o encapsulamento de LTV (Long Term Validation), SDO (Signed Data Object) e/ou carimbo de tempo.	2
NGS2.04.02	Suporte ao Carimbo de Tempo homologado ICP-Brasil	a) O S-RES deve ser capaz de requisitar e incluir o carimbo de tempo após a realização da assinatura digital. O carimbo de tempo deve ser incluído tão logo seja possível. b) A assinatura deve ser revalidada no momento da inclusão do carimbo de tempo. c) O provedor do serviço de carimbo de tempo deverá ser homologado ICP-Brasil (Autoridade de Carimbo de Tempo ICP-Brasil).	2
NGS2.04.03	Parametrização de uso de Carimbo de Tempo	Condição: S-RES possui suporte para incluir o carimbo de tempo após a realização da assinatura digital. a) O S-RES deve permitir parametrizar por meio da aplicação se as assinaturas digitais realizadas no sistema terão ou não um carimbo de tempo associado. Dessa forma, o S-RES não deverá impor o uso obrigatório de carimbo de tempo homologado ICP-Brasil. b) O S-RES deve exibir na aplicação se um determinado registro teve ou não a inclusão de carimbo de tempo.	1

ID	Título	Descrição	Estágio de Maturidade
NGS2.04.04	Parametrização de uso de Carimbo de Tempo por tipo de documento	O S-RES deve permitir parametrizar os tipos de documentos clínicos que serão assinados digitalmente com carimbo de tempo. Nesse caso, apenas os tipos de documentos indicados deverão ser assinados com carimbo de tempo. Deve ser possível indicar o uso de carimbo de tempo minimamente para os seguintes tipos de documentos: • Prescrição de medicamentos e receitas; • Atestado médico.	3
NGS2.04.05	Verificação do carimbo de tempo	A verificação de um carimbo de tempo deve incluir a verificação do certificado de assinatura do carimbo de tempo.	3
NGS2.05 - Importação, Exportação e Impressão			
NGS2.05.01	Validação da assinatura de documentos importados	Condição: S-RES ser capaz de importar registros externos assinados digitalmente. No momento da importação de um registro externo assinado digitalmente, o S-RES deve validar as assinatura(s) digital(is): • Em caso de impossibilidade de validação, o S-RES deverá gerar uma pendência para validação do registro. • Caso o resultado aponte que a assinatura digital é “inválida” ou “indeterminada”, o S-RES deverá registrar este resultado, informando ao usuário em consultas futuras. • O S-RES deve ser capaz de validar assinaturas geradas por certificados digitais emitidos por qualquer AC da cadeia ICP-Brasil.	1
NGS2.05.02	Adequação da assinatura de documentos importados	Condição: S-RES ser capaz de importar registros externos assinados digitalmente. No momento da importação de um registro externo assinado digitalmente, o S-RES deve alertar sobre as não conformidades quanto aos formatos AD-RB, AD-RT, AD-RV ou AD-RC (presença de objetos estado de revogação, presença de carimbo de tempo, etc).	3
NGS2.05.03	Exportação de registros assinados digitalmente	O S-RES deve ter a possibilidade de exportar os registros eletrônicos assinados, de forma que seja possível efetuar a validação da assinatura digital externamente ao S-RES (por exemplo, utilizando o verificador do ITI).	1
NGS2.05.04	Exportação de documentos específicos assinados digitalmente	Para a exportação de receitas, solicitações de exames, atestados médicos e laudos, o S-RES deve estar aderente às especificações apresentadas no documento "Especificações Técnicas para Exportação de Documentos Assinados Digitalmente" em sua versão mais recente, disponível no website da SBIS (https://sbis.org.br/certificacoes/certificacao-software/manuais-e-listas-de-requisitos/).	2

ID	Título	Descrição	Estágio de Maturidade
NGS2.05.05	Impressão de registros assinados digitalmente	O S-RES deve permitir a impressão de registros assinados digitalmente utilizando ao menos uma das seguintes opções: • Mensagem de rodapé: impressa em cada registro assinado digitalmente; e/ou • Relatório de assinaturas: impresso para um conjunto de registros assinados digitalmente.	1
NGS2.05.06	Impressão de mensagem de rodapé	Condição: impressão de mensagem de rodapé. a) Em caso de impressão de mensagem de rodapé (em cada registro assinado digitalmente), as assinaturas dos registros devem ser validadas no momento da impressão e deve ser adicionada a seguinte mensagem na parte inferior de cada página. “Documento assinado eletronicamente no sistema certificado SBIS, por <nome do signatário>, às <HH:MM±UTC de DIA/MÊS/ANO>. Estado da assinatura: <estado>”. b) Os dados variáveis (nome, data e hora) deverão ser extraídos da assinatura. As informações de hora e a data devem ser obtidas a partir do atributo signingTime, ou entrada no dicionário de assinatura, chamada de “M”. c) Caso haja mais de uma assinatura, os mesmos dados devem ser apresentados para os outros signatários na sequência.	1

ID	Título	Descrição	Estágio de Maturidade
NGS2.05.07	Impressão de relatório de assinaturas	Condição: impressão de relatório de assinaturas. a) Em caso de impressão de relatório de assinaturas (para um conjunto de registros assinados digitalmente), todos os registros assinados devem ser validados no momento da geração do relatório e da impressão dos registros, e a seguinte mensagem deve ser impressa: “Os documentos a seguir foram assinados eletronicamente no sistema certificado SBIS. A lista abaixo indica o número do documento e seus signatários.” b) Em seguida, deverá vir a lista dos documentos assinados digitalmente, numerados e paginados sequencialmente, e para cada registro, indicar: • Seu número sequencial; • As páginas a que se referem; • Assinado por: <nome do signatário>, às <HH:MM+-UTC de DIA/MÊS/ANO>. Estado da assinatura: <estado>. c) Caso haja mais de uma assinatura, os mesmos dados devem ser apresentados para os outros signatários na sequência.	1
NGS2.06 - Autenticação de Usuário Utilizando Certificado Digital			
NGS2.06.01	Certificado digital para autenticação	Condição: Utilizar certificado digital como método de autenticação. Para o processo de autenticação por meio do uso de certificado digital, o S-RES deve validar: • Instante atual dentro da vigência do certificado digital; • Confiança da cadeia de certificação; • Revogação; • Correspondência dos valores CPF do usuário e do certificado; • Emissão com propósito de autenticação, por meio da extensão Extended Key Usage, deve possuir ao menos o valor Client Authentication (1.3.6.1.5.5.7.3.2).	1