Requisitos para Certificação de Sistemas de Registro Eletrônico em Saúde

Categoria

Segurança da Informação

Versão 5.1

29/03/2021

Editor
Luiz Aparecido Virginio Junior

Autores desta edição

Cláudia de Fátima Miranda
Eduardo Pereira Marques
Luis Gustavo Gasparini Kiatake
Luiz Aparecido Virginio Junior
Marcelo Lúcio da Silva
Osmeire Aparecida Chamelette Sanzovo
Renato Duarte Rozo Fonseca

Colaboraram nas edições anteriores (Manual de Certificação de S-RES):

Adilson Eduardo Guelfi
Alex Souza Silveira
Beatriz de Faria Leão
Cláudio Giulliano Alves da Costa
Gislaine Lirian Bueno de Oliveira
John Lemos Forman
Juliana Pereira de Souza Zinader
Leopoldo Santana Luz
Luiz Renato Gonçalves Evangelisti
Marcelo Antonio de Carvalho Júnior
Matteo Nava
Osni Pereira
Ricardo Trugillo
Stanley da Costa Galvão
Tulio Toshiharu Rodrigues Takemae
Volnys Borges Bernal

Índice

1. Introdução

Este documento apresenta o conjunto de requisitos técnicos de Segurança da Informação proposto pela Sociedade Brasileira de Informática em Saúde (SBIS) para o Manual de Certificação de Sistemas de Registro Eletrônico em Saúde (S-RES) específico para **sistemas que não se enquadram nas demais categorias e modalidades publicadas pela SBIS no Manual de Certificação para S-RES em sua versão mais recente**. Outros S-RES que se enquadrem em quaisquer categorias e modalidades já publicadas **não poderão** ser certificados na categoria de Segurança da Informação isoladamente.

Vale ressaltar que, para a categoria Segurança da Informação, o conjunto de requisitos NGS2 é opcional.

A descrição do funcionamento do Processo de Certificação de S-RES SBIS, incluindo as definições das categorias, modalidades e estágios de maturidade certificáveis, está disponível no Manual de Certificação para Sistemas de Registro Eletrônico em Saúde disponível na página da SBIS na internet.

2. Estágios de Maturidade

São apresentados abaixo os principais recursos contemplados em cada estágio de maturidade para a categoria Segurança da Informação.

Quadro comparativo dos principais recursos contemplados	Estágio de Maturidade		
	1	2	3
Requisitos mínimos para aderência à legislação	✓	✓	✓
Segurança da informação	Essencial	Intermediária	Avançada
Aderência à ICP-Brasil para eliminação de papel (caso NGS2)	✓	✓	✓
Requisitos avançados para assinaturas digitais (caso NGS2)		✓	✓

3. Requisitos de Conformidade

A lista apresentada neste capítulo indica os requisitos aplicáveis a cada estágio de maturidade da categoria Segurança da Informação. Para obter o Certificado SBIS, o sistema deverá atender à **totalidade dos requisitos de NGS1 e, caso pretendido, NGS2** aplicáveis à categoria e estágio de maturidade pretendidos 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-grupo-temático.Número-do-requisito* Exemplo: NGS1.01.01
Título	Título (nome) do requisito
Requisito	Descrição do requisito, incluindo exemplos quando apropriado. Adicionalmente, pode incluir notas explicativas para melhor elucidação de seu conteúdo.
Estágio 1	Indica se o requisito se aplica (✓) ou não (célula vazia) ao Estágio 1.
Estágio 2	Indica se o requisito se aplica (✓) ou não (célula vazia) ao Estágio 2.
Estágio 3	Indica se o requisito se aplica (✓) ou não (célula vazia) ao Estágio 3.

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

A seguir, apresentam-se algumas premissas e definições:

- O termo "impressão" utilizado ao longo do documento refere-se a qualquer tipo de geração de arquivo para visualização (PDF, por exemplo) e/ou impressão em papel.

3.1. Requisitos do Nível de Garantia de Segurança 1 (NGS1)

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.01 - Controle de versão do software					
NGS1.01.01	Versão 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.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.02 - Identificação e autenticação de pessoas					
NGS1.02.01	Método de autenticação de pessoa	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.02.02	Proteção dos parâmetros de autenticação de usuário	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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 em banco de dados, de forma codificada por algoritmo de hash aberto (público) de no mínimo 160 bits. b) As codificações das senhas de acesso dos usuários devem ser protegidas contra acesso não autorizado. Apenas o usuário do banco de dados utilizado pela aplicação deve ter acesso às mesmas. 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 pela aplicação deve 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 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 utilizado pela aplicação deve ter acesso às mesmas.	✓	✓	✓
NGS1.02.03	Qualidade da senha	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.02.04	Impedimento de senhas com base em dados de identificação	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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.		✓	✓
NGS1.02.05	Parametrização da qualidade da senha	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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.			✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.02.06	Geração de senha para o usuário pelo administrador	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: Para a modalidade Consultório Individual, esse requisito é aplicável apenas para S-RES oferecido como SaaS. Condição 3: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). a) O S-RES deve permitir a geração de uma senha para um usuário pelo administrador do sistema. b) A senha pode ser definida de forma manual pelo administrador ou de forma automática pelo S-RES. c) O S-RES deve forçar que o usuário realize a troca de senha caso a mesma tenha sido definida manualmente pelo administrador. d) A troca deve ocorrer imediatamente após o usuário acessar o S-RES pela primeira vez após a geração da senha. Adicionalmente, nenhuma ação poderá ser efetuada pelo usuário no S-RES até que o mesmo efetue a troca de senha.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.02.07	Geração automática de senha para o usuário	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: Para a modalidade Consultório Individual, esse requisito é aplicável apenas para S-RES oferecido como SaaS. Condição 3: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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 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).		✓	✓
NGS1.02.08	Troca de senha pelo próprio usuário	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.02.09	Troca forçada de senha	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: Para a modalidade Consultório Individual, esse requisito é aplicável apenas para S-RES oferecido como SaaS. Condição 3: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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.		✓	✓
NGS1.02.10	Periodicidade de troca de senhas	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: Para a modalidade Consultório Individual, esse requisito é aplicável apenas para S-RES oferecido como SaaS. Condição 3: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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) Tal período máximo deve ser configurável. 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.		✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.02.11	Igualdade de senhas	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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	✓	✓	✓
NGS1.02.12	Obtenção de nova senha	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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.	✓	✓	✓
NGS1.02.13	Controle de tentativas de login	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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 configurável de tentativas consecutivas de login com autenticação inválida, que não exceda a 10 tentativas. b) Após o bloqueio da conta de um usuário, o sistema só deve permitir login deste após o seu desbloqueio pelo administrador ou por algum método definido pelo sistema que impeça o acesso por pessoas não autorizadas.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.02.14	Autenticação para operações críticas	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). a) O S-RES deve solicitar uma nova autenticação do usuário 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).			✓
NGS1.02.15	Informações na autenticação	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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).		✓	✓
NGS1.02.16	Informações em autenticação inválida	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.02.17	Revelação de credenciais na interface de autenticação	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). a) O S-RES deve 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) Toda e qualquer digitação direta de senhas deve ser feita por meio de máscara de caracteres que impeça sua visualização por outras pessoas.	✓	✓	✓
NGS1.02.18	Autenticação de dois fatores	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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: O OTP (one-time password) pode ser utilizado como segundo fator de autenticação.			✓
NGS1.02.19	Uso de SALT para a senha	Condição 1: Utilização de autenticação baseada no método de usuário e senha. Condição 2: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). a) O S-RES deve utilizar técnicas de SALT para a codificação de senhas de usuários. b) Um novo SALT deve ser gerado para cada senha		✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	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 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 bloqueado. Para que o desbloqueio de sessão seja realizado, o sistema deve requerer novo processo de autenticação do usuário bloqueado. Outro usuário deve ter a possibilidade de encerrar a sessão bloqueada anteriormente (sem reativá-la) para que só então possa prosseguir com uma nova sessão. 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.	✓	✓	✓
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.		✓	✓
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.		✓	✓
NGS1.02.23	Segurança contra roubo de sessão de usuário	a) A sessão de comunicação remota entre cliente e servidor deve possuir controles de segurança que impeçam o roubo ou reuso da sessão do usuário. b) As credenciais de acesso não devem ser transmitidas entre as partes na forma de texto claro. c) Deve haver controles que impeçam o reuso de identificadores de sessão do usuário (ataques de replay e covert-channel) e roubo da sessão. d) Não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.03 - Autorização e controle de acesso					
NGS1.03.01	Impedir acesso por pessoas não autorizadas	Todo acesso ou visualização de dados do S-RES deve ser realizado apenas por usuários previamente autorizados. Tal autorização deve ser provida por meio de permissões atribuídas a perfis de usuário.	✓	✓	✓
NGS1.03.02	Perfis mínimos de usuário	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). O S-RES deve disponibilizar minimamente três perfis de usuário: administrador do sistema, profissional administrativo (sem acesso aos dados clínicos) e profissional de saúde.	✓	✓	✓
NGS1.03.07	Atribuição de mais de um perfil para um usuário	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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.	✓	✓	✓
NGS1.03.08	Gerenciamento de usuários	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). O S-RES deve permitir o gerenciamento (cadastro, ativação/inativação e alteração de cadastro) de usuários, por meio da aplicação.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.03.09	Identidade única da pessoa e responsabilização	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). a) Identidade única: toda pessoa usuária do S-RES deverá ser identificada individualmente. b) Vinculação a número legal e único: toda pessoa usuária do S-RES deverá ser vinculada minimamente a um documento de identificação pessoal unívoco segundo a legislação brasileira vigente (por exemplo, Número de Cadastro de Pessoa Física - CPF). Qualquer alteração de cadastro nesse documento deverá exigir uma justificativa no usuário. c) Unicidade de identificação de usuários: a informação de identificação de tal documento deverá ser validada em todos os processos de inclusão ou alteração de pessoas para garantir a unicidade, ou seja, o S-RES não deve permitir a associação de um mesmo documento de identificação a dois usuários no sistema. d) Exclusão de usuários: 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) Unicidade em modalidade SaaS: caso o S-RES opere na modalidade SaaS, a unicidade do identificador da pessoa deve ser por organização.	✓	✓	✓
NGS1.03.10	Usuário mínimo ativo	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). O S-RES deve garantir que haja ao menos um usuário ativo com perfil de administrador e/ou gestor de acessos (por exemplo, por meio da criação de um usuário administrador fixo que não pode ser inativado ou ter suas permissões alteradas).	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
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 full"), 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.	✓	✓	✓
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).	✓	✓	✓
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.	✓	✓	✓
NGS1.04.05	Integridade na restauração da cópia de segurança	a) O S-RES deve possuir controle de integridade da cópia de segurança. b) A verificação da integridade deverá ocorrer durante a restauração da cópia, gerando um alerta caso ocorra alguma falha. O processo de restauração deve garantir sua completude de forma que toda informação seja restaurada. Caso haja algum erro durante a restauração, nenhuma informação deverá então ser restaurada, retornando-se, portanto, ao estado anterior (rollback).	✓	✓	✓
NGS1.04.06	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.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
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 (ex.: browser ou executável cliente) e os outros componentes do S-RES (ex.: servidor de aplicação, banco de dados, etc) 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 dos dados em trânsito (por exemplo, uso de HTTPS).	✓	✓	✓
NGS1.05.02	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.	✓	✓	✓
NGS1.05.03	Segurança da comunicação entre componentes	Condição: S-RES ser composto por componentes distribuídos. A comunicação entre componentes distribuídos (como, por exemplo, entre a aplicação e o banco de dados) deve oferecer os seguintes serviços de segurança: autenticação dos parceiros (ambas as partes), integridade dos dados e confidencialidade dos dados (criptografia). Nota: A segurança pode ser aplicada ao canal de comunicação ou às mensagens trocadas.	✓	✓	✓
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 (ex.: ActiveX, Applet, aplicações para tablet, etc) por parte do usuário. Possuir controle de integridade e possibilidade de verificação da origem/autoria (ex.: pelo uso de assinatura digital do componente) de componentes que exijam download para sua execução.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.06 - Segurança de dados					
NGS1.06.01	Utilização de SGBD	a) Todos os dados de RES em S-RES devem ser armazenados integral e exclusivamente por um Sistema de Gerenciamento de Banco de Dados (SGBD) que contemple minimamente 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, 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.	✓	✓	✓
NGS1.06.02	Segurança de componentes que manipulam dados do RES	Quaisquer arquivos que tenham sido gerados temporariamente fora do SGBD (por exemplo, para fins de interoperabilidade, visualização, assinatura, etc.) devem ser excluídos 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.			✓
NGS1.06.03	Validação de dados de entrada	Os dados inseridos pelo usuário nos campos de entrada (inputs, caixas de texto, etc) devem ser validados antes de serem processados, de forma a prevenir ataques de buffer overflow e injeção de dados.	✓	✓	✓
NGS1.06.04	Segregação dos dados por organização	Condição: S-RES ofertado na modalidade SaaS. Todos os dados do RES devem ser segregados por organização, ou seja, nenhum dado do RES de uma organização pode ser acessado ou visualizado por usuário de outra organização, salvo quando consentido pelo paciente segundo acordo de privacidade. Nota: A regra não se aplica obrigatoriamente para usuários de TI ou administrativos que sejam responsáveis pela gestão e controle centralizado (multi-organização).	✓	✓	✓
NGS1.06.05	Criptografia de documentos exportados	O S-RES deve permitir a criptografia de documentos eletrônicos exportados que contenham dados de saúde identificados (por exemplo, geração de arquivo do prontuário para visualização ou impressão) para fins de portabilidade, ou seja, armazenamento ou entrega ao paciente em mídia, dispositivo portátil ou removível (por exemplo, pen drive, CD-ROM ou notebook) ou envio (e-mail ou webservice).		✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
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.	✓	✓	✓
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.	✓	✓	✓
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 ao RES: • Criação, duplicação, consulta, inativação de registros do RES; • Importação e exportação de dados; • Impressão de registros do RES; • Solicitação de acesso de emergência a um prontuário; • Registro ou alteração de termos de consentimento; • Criação, inativação e alterações de regras de apoio à decisão clínica (por exemplo, alteração de regra de sexo x diagnóstico, por exemplo); b) Quanto às ações de usuário: • Tentativas de autenticação de usuário, com ou sem sucesso; • Troca de senha; • Realização de assinatura digital; • Validação de assinatura digital; • Falha na realização ou validação de assinatura digital; • Registro de solicitação de esquecimento. c) Quanto às ações operacionais: • Atividades de gerenciamento de usuários e perfis, incluindo inativação/bloqueio e ativação/desbloqueio de conta de usuário; • Realização e restauração de cópia de segurança.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.07.04	Eventos avançados 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 ao RES: • Validação de registros de preceptoria. b) Quanto às ações de usuário: • Encerramento e bloqueio de sessão de usuário; • Desbloqueio de sessão de usuário; • Aceitação do termo de concordância de uso. c) Quanto às ações operacionais: • Atividades de configuração do sistema (por exemplo, parâmetros de configuração de senha, limite de tentativas de login e atribuição de permissão e/ou restrição de acesso a um prontuário por um profissional de saúde); • Geração de senha para usuário; • Acesso aos registros de auditoria; • Erros relativos à execução de processos operacionais com respectiva descrição do erro (por exemplo, eventos de detecção de quebra de integridade em arquivos de cópias de segurança, conclusão de processos de exportação e importação, etc); • Indisponibilidade de comunicação que impeçam a verificação da revogação do certificado digital (aplicável apenas para sistemas certificados para NGS2).			✓
NGS1.07.05	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; • Tipo de 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 do evento (endereço IP ou MAC address, por exemplo); • Identificação do usuário gerador do evento, quando aplicável; • Identificador único e permanente do registro afetado pelo evento (por exemplo, identificador do paciente cujo prontuário foi acessado); • Informações complementares relevantes sobre o evento (ex.: motivo da falha na validação de assinatura digital, descrição do erro relativo à execução de processos operacionais, etc).	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.07.06	Privacidade do paciente na trilha de auditoria	Dados clínicos ou dados de identificação do paciente não poderão ser registrados na trilha de auditoria.	✓	✓	✓
NGS1.07.07	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 data, evento, identificador único e permanente do usuário e identificador único e permanente do registro afetado (por exemplo, identificador do paciente).	✓	✓	✓
NGS1.07.08	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).			✓

ID	Titulo	Requisito	Estágio		
			1	2	3
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); • Visão geral do S-RES, incluindo formas de operação, requisitos do ambiente computacional; • Instalação e configuração do S-RES; • Instalação e configuração dos componentes complementares e/ou distribuídos (ex: SGBD, sistema operacional, etc); • Recomendação sobre a forma de configuração segura do S-RES e componentes complementares e/ou distribuídos, e forma de operação segura do S-RES; • Instruções explicitando quaisquer limitações e restrições relacionadas à compatibilidade do S-RES e/ou seu funcionamento (por exemplo, mídias compatíveis para uso do certificado digital); • Compatibilidade com versões anteriores do S-RES. 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.	✓	✓	✓
NGS1.08.02	Referência à versão do software na documentação	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.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.08.03	Operações de backup	Condição: S-RES cuja operação de backup é realizada pelo próprio fornecedor do sistema ou pelo estabelecimento de saúde. a) O manual de instalação deve informar como realizar a configuração de um usuário com permissão de operação de backup. b) O manual de instalação deve informar como configurar o SGBD de forma que as atividades de exportação e restauração de uma cópia de segurança dos dados possa ser realizada somente pelo usuário com permissão de operação de backup. c) Os manuais pertinentes devem conter indicações de cautela caso existam outros usuários com permissão de geração ou restauração de cópia de segurança (ex.: usuário 'sa' ou equivalente). d) 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 a execução destas tarefas.	✓	✓	✓
NGS1.08.04	Restrição de acesso a entidades não autenticadas e autorizadas	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.	✓	✓	✓
NGS1.08.05	Configuração da segurança da comunicação entre componentes	Condição: S-RES ser composto por componentes distribuídos. 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.	✓	✓	✓
NGS1.08.06	Sincronização de relógio	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.	✓	✓	✓
NGS1.08.07	Guarda da cópia de segurança	O manual de operação deve informar que as cópias de segurança do RES 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.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.08.08	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.	✓	✓	✓
NGS1.08.09	Importação de dados de dispositivos externos de saúde	Condição: possibilidade de 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.	✓	✓	✓
NGS1.08.10	Idioma	Deve haver versão em Português do Brasil para todos os manuais do S-RES.	✓	✓	✓
NGS1.08.11	Recomendações sobre configurações de segurança	Os manuais devem 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.).	✓	✓	✓
NGS1.08.12	Histórico de alteração	Gerar e manter documentação contendo o histórico descritivo das alterações realizadas no S-RES ("release notes"), contendo a data, modificações e responsável, além de permitir a inclusão do impacto das alterações (módulos, funções, serviços afetados, etc) e restrições de compatibilidade, quando houver.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
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 configurável, 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.	✓	✓	✓
NGS1.09.02	Uniformidade da representação para exportação de tempo	Na exportação de dados do RES, todos os registros de tempo devem ser apresentados no formato RFC 3339.	✓	✓	✓
NGS1.09.03	Registro de tempo no banco de dados	Todo registro de tempo deve ser armazenado no banco de dados de acordo com a referência temporal configurada no servidor em uma estrutura lógica que inclua dia, mês, ano, hora, minuto, segundo (quando aplicável), milissegundo (quando aplicável) e fuso horário (UTC).	✓	✓	✓
NGS1.09.04	Uniformidade da representação para entrada de tempo	a) Toda entrada (em tela ou impressão) de data completa deve respeitar a sequência dia seguido do mês seguido do ano. b) Toda entrada (em tela ou impressão) de horário deve respeitar a sequência hora seguida dos minutos.	✓	✓	✓
NGS1.09.05	Uniformidade da representação para exibição de tempo	a) Toda exibição (em tela ou impressão) de data completa deve respeitar a sequência dia seguido do mês seguido do ano. b) Toda exibição (em tela ou impressão) de horário deve respeitar a sequência hora seguida dos minutos. Opcionalmente, pode-se exibir ainda o fuso horário (UTC), segundos e milissegundos.	✓	✓	✓
NGS1.09.06	Time zone e local da instituição de saúde	a) O S-RES deve permitir a parametrização da time zone e local onde se encontra a instituição de saúde. b) A exibição de registro de tempo, tanto em tela quanto em impressão, deve respeitar a UTC indicada na parametrização, independentemente da localização do servidor. Ou seja, caso o registro de tempo tenha sido registrado no banco de dados de acordo com a UTC da localização do servidor, o S-RES deverá converter automaticamente tal registro de acordo com a time zone da instituição.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.11 - Privacidade					
NGS1.11.01	Concordância com termos de uso	Condição: Para a modalidade de Receita Digital, esse requisito se aplica apenas aos sistemas que podem operar de forma autônoma e independente (stand-alone). 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. c) A concordância com os termos deverá ser repetida obrigatoriamente a cada alteração nas políticas de uso.	✓	✓	✓
NGS1.11.08	Contestação do paciente em relação às suas informações	a) O S-RES deve permitir o registro de queixas de pacientes em relação à integridade ou exatidão de alguma informação registrada em seu prontuário, bem como solicitações do paciente para alteração dessas informações. b) O S-RES deve permitir que, caso a organização discorde da avaliação do paciente, um profissional autorizado registre a discordância e/ou a razão para a recusa da organização em atualizar o registro.			✓
NGS1.11.11	Anonimização	O S-RES deve permitir a anonimização em bases de dados (por exemplo, anonimizar pacientes da base de dados da versão de teste ou ainda realizar uma cópia da base de dados e anonimizar dados pessoais para uso por usuários não autorizados a visualizá-los, tais como desenvolvedores e pesquisadores).		✓	✓
NGS1.11.12	Pseudonimização	O S-RES deve permitir a pseudonimização em bases de dados (por exemplo, pseudonimizar pacientes da base de dados da versão de teste ou ainda realizar uma cópia da base de dados pseudonimizando dados pessoais para uso por usuários não autorizados a visualizá-los, tais como desenvolvedores e pesquisadores).			✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.12 - Integridade					
NGS1.12.01	Regras para correção de dados já finalizados	Condição: S-RES permite a alteração de registros clínicos já finalizados. a) A correção de um dado do prontuário e/ou registro clínico só poderá ser feita pelo próprio autor. b) Qualquer correção de um dado do prontuário e/ou registro clínico já finalizado deve implicar na geração de uma nova versão para o mesmo. c) Toda correção de um dado do prontuário e/ou registro clínico deve exigir justificativa do usuário. d) A versão anterior à correção deve ser mantida no prontuário do paciente com status de inativa. e) Ao acessar a versão atual do registro, o S-RES deve indicar que o mesmo possui versões anteriores e deve permitir que tais versões sejam facilmente acessadas. Nota: Consideram-se como finalizados os registros que foram concluídos e liberados pelo profissional.	✓	✓	✓

ID	Titulo	Requisito	Estágio		
			1	2	3
NGS1.12.03	Inativação de registros clínicos já finalizados	a) O S-RES deve permitir a inativação de registros de dados clínicos e atendimentos previamente armazenados e finalizados (liberados) no sistema. Tais registros incluem, mas não se limitam a: prescrições, sinais vitais, diagnósticos, alergias e documentos clínicos (anamnese e sumário de alta, por exemplo). 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. d) Todos os dados registrados no S-RES e considerados como finalizados/definitivos/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. 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).	✓	✓	✓

3.2. Requisitos do Nível de Garantia de Segurança 2 (NGS2)

ID	Requisito	Requisito	Estágio		
			1	2	3
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.	✓	✓	✓
NGS2.01.02	Validação do CPF do usuário	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. Dessa forma, a cada processo de uso do certificado digital deverá ser verificado se o CPF do usuário executando o processo corresponde ao CPF contido no certificado digital utilizado, e o processo só será 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.	✓	✓	✓
NGS2.01.03	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.	✓	✓	✓
NGS2.01.04	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.			✓
NGS2.01.05	Compatibilidade com diferentes Autoridades Certificadoras	O S-RES deve ser capaz de produzir assinaturas geradas por certificados digitais emitidos por pelo menos duas ACs de 1º nível (empresas distintas), para cada tipo de mídia aplicável (por exemplo: cartão, token, HSM, chaves em software e PSC).	✓	✓	✓

ID	Requisito	Requisito	Estágio		
			1	2	3
NGS2.02 - Assinatura Digital					
NGS2.02.01	Formato de assinatura	O S-RES deve gerar assinaturas digitais nos formatos CAdES, XAdES ou PAdES seguindo, minimamente, a política AD-RB.	✓	✓	✓
NGS2.02.02	Verificação do propósito do certificado digital para assinatura	Antes da realização de uma assinatura digital, o S-RES deve verificar se o certificado digital a ser utilizado possui propósito de uso para assinatura digital, ou seja, se o campo key usage inclui os atributos Digital Signature e NonRepudiation e verificar se o certificado digital é compatível com o padrão ICP-Brasil de assinatura digital tipo A1, A2, A3 ou A4.	✓	✓	✓
NGS2.02.03	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.	✓	✓	✓
NGS2.02.04	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).	✓	✓	✓
NGS2.02.05	Pendência de assinatura	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), o S-RES deverá gerar uma pendência de assinatura.		✓	✓
NGS2.02.06	Aviso de registro pendente de assinatura	Condição: S-RES permite a existência de pendência de assinatura digital. a) Caso um determinado profissional deixe um registro sem assinatura digital, o S-RES deve notificá-lo no momento em que o mesmo sair da tela em que o registro está sendo apresentado, mesmo em caso de logoff ou fechamento da aplicação. b) Após o login por um profissional de saúde, o S-RES deve apresentar uma lista com todos os registros pendentes de assinatura existentes no sistema e que são de responsabilidade deste profissional, possibilitando a abertura e posterior assinatura do documento a partir da lista apresentada. O sistema deve ainda permitir o acesso à essa lista por vontade do profissional a qualquer momento.	✓	✓	✓

ID	Requisito	Requisito	Estágio		
			1	2	3
NGS2.02.08	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.			✓
NGS2.02.09	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).	✓	✓	✓
NGS2.02.10	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.			✓
NGS2.02.11	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.			✓

ID	Requisito	Requisito	Estágio 1	Estágio 2	Estágio 3
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: • Antes da inclusão do objeto digital contendo a assinatura digital no RES; • Imediatamente após a geração da assinatura digital do documento eletrônico; • Ao ser solicitada a impressão 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 (vide NGS2.02.11). 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).	✓	✓	✓
NGS2.03.02	Referência temporal para verificação de	No momento da validação de uma assinatura digital sem carimbo de tempo, a referência a ser utilizada para verificação de revogação do certificado digital deverá ser o instante presente no atributo “momento da assinatura” (signingTime ou equivalente).	✓	✓	✓

ID	Requisito	Requisito	Estágio		
			1	2	3
	revogação sem carimbo de tempo				
NGS2.03.03	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 do certificado digital deverá ser o carimbo de tempo.		✓	✓
NGS2.03.04	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 (ex: 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).	✓	✓	✓

ID	Requisito	Requisito	Estágio		
			1	2	3
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.		✓	✓
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).		✓	✓
NGS2.04.03	Parametrização de uso de Carimbo de Tempo	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.		✓	✓
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.			✓

ID	Requisito	Requisito	Estágio		
			1	2	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.			✓
NGS2.05 - Certificado de Atributo					
NGS2.05.01	Configuração das fontes de autoridade	Condição: Suporte a Certificados de Atributo a) O S-RES deve permitir a configuração das fontes de autoridade, para cada classe de privilégio (relação <privilégio, fonte_de_autoridade>, exemplo: <médico, Conselho Regional de Medicina>). b) O S-RES deve implementar controles de segurança que garantam a integridade e detecte alteração não autorizada da relação de fontes de autoridade configuradas.		✓	✓
NGS2.05.02	Tratamento de certificado de atributo	Condição: Suporte a Certificados de Atributo O S-RES deve ser capaz de tratar certificados de atributo segundo a ICP-Brasil (DOC-ICP-16), a RFC 5755 e X.509, para as seguintes atividades: • Verificação de certificado de atributo, incluindo revogação; • Geração de assinaturas com a inclusão de certificado de atributo; • Verificação de assinatura com presença de certificado de atributo.		✓	✓
NGS2.06 - Importação, Exportação e Impressão					
NGS2.06.01	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.	✓	✓	✓

ID	Requisito	Requisito	Estágio		
			1	2	3
NGS2.06.02	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).			✓
NGS2.06.03	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).	✓	✓	✓
NGS2.06.04	Exportação de documentos específicos assinados digitalmente	Para a exportação de prescrições/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 (http://sbis.org.br/documentos-e-manuais).		✓	✓
NGS2.06.05	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.	✓	✓	✓
NGS2.06.06	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 digitalmente de acordo com a ICP-Brasil, MP 2.200-2/2001, no sistema certificado SBIS nº XXX-Y, 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. Nota 1: A exibição das figuras é opcional.	✓	✓	✓

ID	Requisito	Requisito	Estágio		
			1	2	3
		Nota 2: A “MP 2.200-2/2001” deverá ser substituída na mensagem caso tenham sido utilizadas legislações mais recentes.			
NGS2.06.07	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 digitalmente de acordo com a ICP-Brasil, MP 2.200-2/2001, no sistema certificado SBIS nº XXX-Y. 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. Nota 1: A exibição das figuras é opcional. Nota 2: A “MP 2.200-2/2001” deverá ser substituída na mensagem caso tenham sido utilizadas legislações mais recentes.	✓	✓	✓

ID	Requisito	Requisito	Estágio		
			1	2	3
NGS2.07 - Autenticação de Usuário Utilizando Certificado Digital					
NGS2.07.01	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 do extensão Extended Key Usage, deve possuir ao menos o valor Client Authentication (1.3.6.1.5.5.7.3.2).	✓	✓	✓