sbis
sociedade brasileira
de informática em saúde

CFM
CONSELHO FEDERAL DE MEDICINA

Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES)

Versão 3.3

CERTIFICAÇÃO 2009

Editores:

Beatriz de Faria Leão
Cláudio Giulliano Alves da Costa
Marcelo Lúcio da Silva
Stanley da Costa Galvão

Maio de 2009

Conselho Federal de Medicina

Diretoria

Gestão de 13/10/2004 à 12/10/2009

Presidente:	Edson de Oliveira Andrade
1º Vice-Presidente:	Roberto Luiz D'Avila
2º Vice-Presidente:	Rafael Dias Marques Nogueira
3º Vice-Presidente:	Gerson Zafalon Martins
Secretário-geral:	Livia Barros Garcao
1º Secretário:	Henrique Batista e Silva
2º Secretário:	Clóvis Francisco Constantino
Tesoureiro:	José Hiran da Silva Gallo
2º Tesoureiro:	Ricardo José Baptista
Corregedor:	Pedro Pablo Magalhães Chacel
Vice-Corregedor:	Jose Fernando Maia Vinagre

Câmara Técnica de Informática em Saúde

Roberto Luiz D'Avila (Coordenador)
Gerson Zafalon Martins
Beatriz de Faria Leão
Cláudio Giulliano Alves da Costa
Ricardo de Oliveira Bessa
Cristianne da Silva Gonçalves
Jussara Pinho Macedo
Goethe Ramos de Oliveira
José Mário Morais Mateus
Luciano Maurício Sampaio Barreto

Sociedade Brasileira de Informática em Saúde

Diretoria

Gestão 2009-2010

Presidente:	Cláudio Giulliano Alves da Costa
Vice-Presidente:	Marco Antônio Gutierrez
Secretária:	Claudia Moro
Tesoureiro:	Ivan Torres Pisa
Gerente de Certificação:	Marcelo Lúcio da Silva

Membros do Grupo de Interesse (GI) em Certificação de Software e Padrões que participaram da elaboração desta edição do manual

Alex Souza Silveira
Beatriz de Faria Leão
Cláudio Giulliano Alves da Costa (Coordenador)
Eduardo Pereira Marques
Luis Gustavo Gasparini Kiatake
Luiz Renato Evangelisti
Marcelo Lúcio da Silva (Secretário)
Stanley da Costa Galvão (Vice-Coordenador)
Tulio Toshiharu Rodrigues Takemae

Consultoria e Revisão Jurídica

Leopoldo Santana Luz

Índice

Histórico das Revisões **6**

Glossário **7**

Definição de Termos Utilizados **8**

1. Introdução **9**

2. Referencial Teórico **11**

2.1. Padrões Utilizados 11
2.2. Definições 15
2.3. Princípios da Certificação 16

3. Escopo de Certificação **19**

3.1. Categorias e Enquadramento dos Sistemas 20

4. Conceitos, Normas e Condições da Certificação **23**

4.1. Componentes de um S-RES 23
4.2. Configurações de S-RES 24
4.3. Versões de S-RES 24
4.4. Validade da Certificação 26
4.5. Extensão da Certificação para Outras Configurações ou Versões 26
4.6. Instrumentos Formais 28
4.7. Taxas e Preços 28

5. Processo de Certificação **30**

5.1. Processo Padrão 30
5.2. Processo para Extensão da Certificação 39
5.3. Apelações, Reclamações e Disputas 40
5.4. Auditorias Internas do Processo de Certificação 40

6. Estrutura do Centro de Certificação da SBIS **41**

6.1. Comitê de Certificação 41
6.2. Gerente do Centro de Certificação 41
6.3. Auditores 42
6.4. Secretaria 42
6.5. Diretoria da SBIS 43

7. Uso da Informação Relacionada com a Certificação **44**

7.1. Referências ao Estado de S-RES Certificado 45

7.2. Uso do Selo de Certificação SBIS/CFM 46
7.3. Referências ao Processo de Certificação 46
7.4. Reclamações de Solicitantes e Clientes Certificados 47

8. Requisitos de Conformidade 48

8.1. Introdução aos Requisitos 49
8.2. Requisitos do Nível de Garantia de Segurança 1 (NGS1) 52
8.3. Requisitos do Nível de Garantia de Segurança 2 (NGS2) 62
8.4. Requisitos de Estrutura e Conteúdo para S-RES Assistencial 66
8.5. Requisitos de Funcionalidades para S-RES Assistencial 73
8.6. Requisitos para GED 81
8.7. Requisitos para TISS 82

9. Referências 91

Histórico das Revisões

Data	Versão	Descrição	Autores	Distribuição
25/08/2003	1.0	Especificação Inicial	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	GT Certificação SBIS
30/11/2003	1.1	Primeira Revisão	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	GT Certificação SBIS / Diretoria SBIS / Câmara Técnica Informática em Saúde do CFM
02/12/2003	1.2	Segunda Revisão	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	GT Certificação SBIS / Diretoria SBIS / Câmara Técnica Informática em Saúde do CFM
03/12/2003	1.3	Terceira Revisão	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	GT Certificação SBIS / Diretoria SBIS / Câmara Técnica Informática em Saúde do CFM
15/12/2003	1.4	Quarta Revisão	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	GT Certificação SBIS / Diretoria SBIS / Câmara Técnica Informática em Saúde do CFM
12/02/2004	2.0	Quinta Revisão	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	GT Certificação SBIS / Diretoria SBIS / Câmara Técnica Informática em Saúde do CFM
19/02/2004	2.1	Sexta Revisão	GT Certificação SBIS - CT Informática em Saúde e Telemedicina CFM	Público
12/09/2007	2.2	Inicio Revisão Fase 2	Consultores SBIS	Diretoria SBIS e Coordenação GI Certificação
01/10/2007	2.3	Fase 2 – 2ª Revisão	Consultores SBIS	Diretoria SBIS e Coordenação GI Certificação
04/10/2007	2.4	Fase 2 – 3ª Revisão	Consultores SBIS	Diretoria SBIS e Coordenação GI Certificação
16/10/2007	2.5	Fase 2 – 4ª Revisão	Consultores SBIS	Diretoria SBIS e Coordenação GI Certificação
16/10/2007	2.6	Revisão pré-consulta pública	Consultores SBIS	Diretoria SBIS e Coordenação GI Certificação
19/10/2007	2.7	Revisão Final p/ consulta pública	Consultores SBIS	Consulta Pública
08/11/2007	3.0	Revisão Final p/ publicação	Consultores SBIS	Público
10/03/2008	3.1	Adequação ao MEA 1.0	Consultores SBIS	Consulta Pública
01/08/2008	3.2	Revisão final (pós-consulta pública) para publicação	Consultores SBIS	Público
20/05/2009	3.3	Publicação da Edição 2009	Consultores SBIS	Público

Glossário

ABNT	Associação Brasileira de Normas Técnicas
ABRAHUE	Associação Brasileira de Hospitais Universitários e de Ensino
AC	Autoridade Certificadora
AMB	Associação Médica Brasileira
ANS	Agência Nacional de Saúde Suplementar
ANSI	American National Standards Institute
ANVISA	Agência Nacional de Vigilância Sanitária
AR	Autoridade Registradora
ASSESPRO	Associação das Empresas Brasileiras de Tecnologia da Informação, Software e Internet
CC	Centro de Certificação SBIS
CCHIT	Certification Commission for Healthcare Information Technology
CFM	Conselho Federal de Medicina
CNES	Cadastro Nacional de Estabelecimentos e Profissionais de Saúde do SUS
CNU	Cadastro Nacional de Usuários do SUS
CONARQ	Conselho Nacional de Arquivos
CRO	Conselho Regional de Odontologia
HL7	Health Level Seven
ICP	Infraestrutura de Chaves Públicas
IEC	International Eletrotechnical Commission
ISO	International Organization for Standardization
ITI	Instituto Nacional de Tecnologia da Informação
MS	Ministério da Saúde
ONA	Organização Nacional de Acreditação
PEP	Prontuário Eletrônico do Paciente
RES	Registro Eletrônico em Saúde
SBIS	Sociedade Brasileira de Informática em Saúde
SGBD	Sistema de Gerenciamento de Banco de Dados
S-RES	Sistema de Registro Eletrônico em Saúde
TISS	Troca de Informação em Saúde Suplementar
UTC	Coordinated Universal Time

Definição de Termos Utilizados

Cliente certificado	Organização cujo S-RES foi certificado
Empresa de conectividade	Empresa que provê ou executa a troca eletrônica de dados entre a Operadora e o Prestador
Imparcialidade	Presença real e perceptível de objetividade
Operadora (de plano de saúde)	Empresa do setor de saúde suplementar que oferece aos consumidores os planos de assistência à saúde.
Prestador (de serviço de saúde)	Empresa ou profissional autorizado a executar ações e/ou serviços de saúde, que prestam serviços às operadoras de plano de saúde
Solicitante	Organização ou pessoa solicitante (contratante) da certificação
Representante legal	Pessoa com poderes para representar juridicamente a organização, conforme designação em seu estatuto ou contrato social ou em procuração
Responsável técnico pelo S-RES	Profissional designado pela organização desenvolvedora ou detentora dos direitos do S-RES, como responsável pelas questões técnicas relativas ao sistema

1. Introdução

O Conselho Federal de Medicina (CFM) tem recebido nos últimos anos uma série de solicitações de pareceres a respeito da legalidade da utilização de sistemas informatizados para capturar, armazenar, manusear e transmitir dados do atendimento em saúde. Uma das indagações mais frequentes é a substituição do papel pelo formato eletrônico. Ciente da complexidade do assunto e da necessidade de aprofundar os aspectos técnicos sobre esta questão, o CFM, através da Câmara Técnica de Informática em Saúde e Telemedicina, estabeleceu convênio de cooperação técnica com a Sociedade Brasileira de Informática em Saúde para desenvolver o processo de certificação de sistemas informatizados em saúde.

O primeiro produto da parceria SBIS/CFM foi a elaboração da resolução n.º 1639/2002 que aprovou as "Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico", dispondo sobre o tempo de guarda dos prontuários, estabelecendo critérios para certificação dos sistemas de informação e dando outras providências. Posteriormente, esta foi revogada e substituída pela resolução n.º 1821/2007, que aprovou as “Normas Técnicas Concernentes à Digitalização e Uso dos Sistemas Informatizados para a Guarda e Manuseio dos Documentos dos Prontuários dos Pacientes, Autorizando a Eliminação do Papel e a Troca de Informação Identificada em Saúde”, a qual faz referência, em seu artigo 1º, a este Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES).

O segundo produto foi a elaboração do Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES). Com base nesse manual, publicado em 2004 nos sítios da SBIS e do CFM, teve início a Fase 1 do Processo de Certificação SBIS/CFM, que, até a presente data, conta com mais de 70 sistemas declarados pelos representantes legais das organizações detentoras, como estando aderentes ao conjunto de requisitos da versão 2.1 do manual (auto-declaração). A Fase 1 teve objetivo de preparar o mercado para o processo de certificação, o que foi plenamente atingido.

A atualização desse manual reflete o início da Fase 2 do Processo de Certificação SBIS/CFM, com a auditoria efetiva dos Sistemas de Registro Eletrônico em Saúde (S-RES). A atualização foi bastante abrangente, procurando refletir as experiências internacionais desenvolvidas desde 2004. Naquela ocasião, não havia ainda no mundo um processo de certificação de S-RES em operação. Os EUA foram os primeiros a certificar S-RES, começando seu processo em 2006. Outros países ainda estão em fase de estudos e definições, sem sequer terem iniciado uma etapa de auto-declaração com requisitos já definidos.

A publicação da versão 3.2 do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) em 01/08/2008 encerrou as possibilidades de auto-declaração (Fase 1). A lista das organizações que haviam declarado seus S-RES conformes com a versão 2.1 do manual permaneceu disponível para consulta no sítio da SBIS na internet pelo período de 06 (seis) meses, sendo, portanto, retirada em 01/02/2009.

A lista das organizações cujos S-RES forem auditados e vierem a receber o Selo de Certificação SBIS/CFM poderá ser consultada no sítio da SBIS na internet.

A versão atual (3.3) apresenta, em relação à versão anterior, uma revisão editorial do texto para facilitar o entendimento a respeito dos requisitos. Adicionalmente, foram incluídas algumas definições das normas ABNT da Comissão de Estudo Especial em Informática em Saúde no referencial teórico, com o intuito de melhorar a compreensão dos temas presentes nos requisitos.

Esta versão (3.3) do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) revoga e substitui todas as suas versões anteriores.

2. Referencial Teórico

A Certificação SBIS/CFM se baseia em conceitos e padrões nacionais e internacionais da área de Informática em Saúde. Este capítulo apresenta um breve resumo dos principais padrões e iniciativas utilizados como referências na definição do Processo de Certificação SBIS/CFM.

2.1. Padrões Utilizados

Segundo a Organização Internacional de Padronização (*International Organization for Standardization* - ISO), *padrão* é um documento estabelecido por consenso e aprovado por um grupo reconhecido, que estabelece para uso geral e repetido um conjunto de regras, protocolos ou características de processos com o objetivo de ordenar e organizar atividades em contextos específicos para o benefício de todos.

2.1.1. Resolução CFM N.º 1638/2002

A Resolução CFM nº 1638/2002[1] define prontuário médico e atribui as responsabilidades por seu preenchimento, guarda e manuseio. Essa resolução torna obrigatória a existência de comissões de revisão de prontuários médicos nos estabelecimentos de saúde onde se presta assistência médica, estabelecendo as informações de caráter obrigatório que devem constar no prontuário médico, seja ele eletrônico ou em papel.

2.1.2. Resolução CFM N.º 1639/2002

A Resolução CFM nº 1639/2002[2] aprova as "Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico", dispõe sobre tempo de guarda dos prontuários médicos e estabelece critérios para certificação dos sistemas de informação. Esta resolução estabelece a guarda permanente para os prontuários médicos arquivados eletronicamente, em meio óptico ou magnético e microfilmados, bem como o prazo mínimo de 20 (vinte) anos para a preservação dos prontuários médicos em suporte de papel. Essa resolução foi o primeiro produto do Convênio SBIS/CFM para o estabelecimento da Certificação de S-RES, sendo, posteriormente, revogada e substituída pela Resolução CFM nº 1821/2007.

2.1.3. Resolução CFM N.º 1821/2007

A Resolução CFM nº 1821/2007[3] aprova as "Normas Técnicas Concernentes à Digitalização e Uso dos Sistemas Informatizados para a Guarda e Manuseio dos Documentos dos Prontuários dos Pacientes, Autorizando a Eliminação do Papel e a Troca de Informação Identificada em Saúde". Essa resolução aprova o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, versão 3.0 e/ou outra versão aprovada pelo Conselho Federal de Medicina, autoriza a digitalização de prontuários médicos conforme normas específicas e estabelece a guarda permanente para prontuários médicos arquivados eletronicamente, em meio óptico ou magnético e microfilmados, bem como o prazo mínimo de vinte anos para a preservação dos prontuários médicos em suporte de papel.

2.1.4. A Infraestrutura de Chaves Públicas ICP-Brasil

A Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil foi criada através da Medida Provisória 2.200-2 de 24 de agosto de 2001[4], transformando o Instituto Nacional de Tecnologia da Informação – ITI em autarquia ligada à Casa Civil da Presidência da República. Por meio dessa MP e das resoluções publicadas pela ICP-Brasil, são estabelecidos os critérios para o estabelecimento e funcionamento do sistema, servindo de base para os serviços de assinatura, não-repúdio, identificação e sigilo. Como resultados, têm-se o aumento de segurança das transações eletrônicas e aplicações que façam uso de certificados digitais, assim como a possibilidade da migração total de processos em papel para meios eletrônicos, sem prejuízo do reconhecimento legal destes documentos. Mais informações podem ser obtidas em http://www.icpbrasil.gov.br.

2.1.5. Os Cadastros Nacionais em Saúde

Os principais cadastros nacionais são o Cadastro Nacional de Usuários do SUS[5] e o Cadastro Nacional de Estabelecimentos e Profissionais de Saúde - CNES[6].

O Cadastro Nacional de Usuários estabelece o conjunto de informações necessárias para que uma pessoa seja identificada no Sistema de Saúde Brasileiro. Hoje, existem no País 165 milhões de pessoas cadastradas na base federal.

O CNES estabelece a identificação de todos os estabelecimentos de saúde públicos e privados no País. O número CNES é de uso obrigatório na área pública e privada. O conjunto de dados de ambos os cadastros foi utilizado como padrão de identificação nos requisitos deste manual.

2.1.6. O Padrão TISS

O padrão TISS - Troca de Informação em Saúde Suplementar[7] é o padrão definido pela Agência Nacional de Saúde Suplementar – ANS (www.ans.gov.br) para registro e intercâmbio de dados entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde. O objetivo do padrão TISS é atingir a compatibilidade e interoperabilidade funcional e semântica entre os diversos sistemas independentes para fins de avaliação da assistência à saúde (caráter clínico, epidemiológico ou administrativo) e seus resultados, orientando o planejamento do setor.

O padrão TISS se divide em 4 categorias: conteúdo e estrutura, representação de conceitos em saúde, comunicação, e segurança e privacidade, conforme descrevem as Resoluções Normativas publicadas no sítio da ANS na internet, na seguinte URL:

- http://www.ans.gov.br/portal/site/_hotsite_tiss/f_materia_21227.htm

A ANS determinou que as normas técnicas estabelecidas na Resolução CFM N.º 1639/2002 supracitada, e os requisitos do Nível de Garantia de Segurança 1 (NGS1) deste manual (ver item 8.2.) devem obrigatoriamente ser observados no padrão TISS. Para as entidades que utilizam *web services* como padrão de comunicação é recomendada a utilização do Nível de Garantia de Segurança 2 (NGS2), também descrito neste manual (ver item 8.3.). Ressalta-se que a eliminação do papel só é possível quando cumprido o NGS2.

Como descrito no capítulo 3, o escopo da certificação SBIS/CFM estabelece uma categoria específica que engloba todo e qualquer sistema que apresente entre as suas funcionalidades a capacidade de ser uma das pontas em um canal de comunicação entre operadoras de planos de saúde e prestadores de serviços de saúde. Deste modo, qualquer S-RES poderá se submeter ao processo de certificação visando apenas a validar sua aderência ao padrão TISS.

2.1.7. Normas ISO TC-215

A norma ISO/TR 20.514:2005[8] é um documento de referência técnica ("TR - *Technical Report*") que estabelece as definições de RES e de Sistemas de RES. Esse relatório descreve as principais categorias de sistemas, define cenários de utilização, e a necessidade de interoperabilidade semântica entre os diferentes S-RES. Adicionalmente esse relatório introduz o conceito de Registro Pessoal de Saúde – RPS. O documento 20.514:2005 é um marco referencial na área de RES e S-RES e representa vários anos de trabalho na área de padrões para S-RES.

A norma ISO/TS 18.308:2004[9] é um documento formal de especificação técnica ("TS – *Technical Specification*") que define os requisitos para um S-RES. A especificação apresenta os requisitos categorizados em estrutura, processo, comunicação, privacidade e segurança, médico-legal, ético, consumidor/cultural e também os requisitos relacionados à evolução de sistemas de RES.

Estas duas normas encontram-se traduzidas (ABNT ISO/TR 20.514 – Informática em saúde - Registro eletrônico de saúde - Definição, escopo e contexto[10] e ABNT ISO/TS 18.308 - Informática em saúde - Requisitos para uma arquitetura do registro eletrônico[11]) e disponíveis no sitio da ABNT na internet.

O projeto de norma ISO/DIS 27.799 "*Health informatics -- Information security management in health using ISO/IEC 17.799*", que está em fase final para publicação, detalha e destaca a importância do emprego dos controles de segurança descritos na ISO/IEC 27.002[12] com foco na área de saúde.

2.1.8. Comissão Especial de Informática em Saúde da ABNT

A ABNT – Associação Brasileira de Normas Técnicas (www.abnt.org.br) é a representante oficial do Brasil junto à ISO. Em outubro de 2006, a ABNT criou a Comissão Especial de Estudos em Informática em Saúde, inspirada no Comitê de Informática em Saúde da ISO, também conhecido como TC-215. A criação desta comissão é um marco importante para o desenvolvimento da área de padrões em saúde no Brasil, estando estruturada nos mesmos moldes do TC-215, com os seguintes Grupos de Trabalho – GT:

GT 1 – Modelos – concentra-se no estudo dos modelos e padrões de conteúdo para representar a informação em saúde.

GT 2 - Interoperabilidade – concentra-se nos padrões para estabelecer a comunicação efetiva entre sistemas e equipamentos na área da saúde. É um dos grupos mais ativos no

Comitê ISO, contando já com vários padrões aprovados. No Brasil, este grupo tem-se dedicado às questões específicas da área de Telemedicina.

GT 3 – Conceitos – concentra-se nas terminologias em saúde. O trabalho é extenso e no Brasil o grupo já traduziu dois documentos de referência sobre o tema de terminologias e indicadores em saúde.

GT 4 – Segurança – concentra-se nos padrões de segurança da informação em saúde. A questão da assinatura digital e privacidade é um dos temas em discussão. No Brasil, esse grupo tem trabalhado e colaborado com a ISO 27.799, norma internacional de segurança da informação em saúde.

Os padrões em discussão pela Comissão Especial de Estudos em Informática em Saúde da ABNT são os documentos de referência para o Processo de Certificação SBIS/CFM.

2.1.9. Normas ISO/IEC JTC1/SC27

O *Joint Technical Committee* 1 (JTC1) é o comitê técnico da ISO responsável pela elaboração de normas sobre tecnologia da informação. Seu sub-comitê 27 (SC27) é responsável pelas normas que tratam das técnicas de segurança em tecnologia da informação. Desta forma, várias de suas normas são de interesse também para a área de saúde, destacando-se as apresentadas a seguir.

O código de prática ISO/IEC 27.002:2005 "*Information technology - Security techniques - Code of practice for information security management*"[12], comumente conhecido por sua antiga numeração ISO/IEC 17.799, é o guia mais difundido mundialmente no assunto segurança e apresenta os principais controles de segurança a serem empregados por qualquer instituição com o objetivo de proteger suas informações. Esse código de prática possui sua versão brasileira NBR ISO/IEC 27.002:2005 – "Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação" [13].

A norma ISO/IEC 15.408:2005 "*Information technology -- Security techniques - Evaluation criteria for IT security*" em suas três partes: "*Part 1: Introduction and general model*"[14], *"Part 2: Security functional requirements*"[15] e "Part 3: *Security assurance requirements*"[16], descreve um processo e requisitos específicos para certificação de segurança de sistemas.

2.1.10. ANSI HL7 Functional Model (EHR-S FM)

O HL7 é o padrão mais utilizado para intercâmbio de dados na área da saúde no cenário internacional, há mais de 15 anos. Hoje, na versão 3.0, o padrão incorpora um modelo de referência RIM – *Reference Information Model* com conceitos dos domínios clínico e administrativo[17].

Em 2001, o HL7 estabeleceu um grupo de trabalho em Registros Eletrônicos em Saúde (EHR-SIG). Este grupo de trabalho definiu um conjunto de requisitos funcionais para S-RES: o EHR *Functional Model*[18]. O trabalho realizado por este comitê é extenso e cobre diferentes perfis de sistema, com um enfoque prático e proposta de *scripts* para validação dos requisitos.

No Brasil, em fevereiro de 2007, foi criado o Instituto HL7 Brasil a fim de dar respaldo jurídico e administrativo às atividades da representação do HL7 no Brasil (www.hl7brazil.org), com o intuito de "*promover e prover padrões relacionados com a troca, integração, compartilhamento e recuperação de informação eletrônica, para apoio da prática médica e administrativa, permitindo um maior controle dos serviços de saúde*". Os grupos de trabalho estão em fase de organização, dentre eles, o Grupo de Registro Eletrônico de Saúde e Registro Pessoal em Saúde, que discute os requisitos funcionais de S-RES.

2.1.11. Processo de Certificação CCHIT

A *Certification Commission for Healthcare Information Technology* – CCHIT desenvolveu o processo de certificação de S-RES[19] adotado no mercado americano. Sua origem é posterior à Certificação SBIS/CFM, uma vez que foi criado em 2005, com um aporte inicial da ordem de 7.5 milhões de dólares, e é administrado pelas seguintes organizações:

- *American Health Information Management Association* (AHIMA);
- *Healthcare Information and Management Systems Society* (HIMSS); e
- *National Alliance for Healthcare Information Technology (the Alliance)*.

O processo americano é voluntário e baseado em conjuntos de *scripts* para diferentes categorias de S-RES. Inicialmente apenas sistemas ambulatoriais podiam ser certificados, mas a CCHIT está expandindo as categorias de sistemas que podem se submeter ao processo de certificação. Os critérios são bastante detalhados e analisam a funcionalidade, conteúdo, estrutura, segurança e aspectos de interoperabilidade dos S-RES. Os S-RES são avaliados por três auditores, à distância, a partir de ambiente cooperativo especializado para esta finalidade. O processo do ponto de vista técnico é semelhante ao da SBIS/CFM.

2.2. Definições

As normas ABNT ISO/TR 20514[10] e ISO/TS18308[11] apresentam definições utilizadas na elaboração deste manual, em especial nos requisitos de conteúdo, estrutura e funcionalidades. As seguintes definições, extraídas destas normas, são relevantes para o entendimento deste manual:

- **Registro Eletrônico em Saúde (RES)**: Um repositório de informação a respeito da saúde de indivíduos, numa forma processável eletronicamente.

- **Sistema de Registro Eletrônico em Saúde (S-RES)**: Sistema para registro, recuperação e manipulação das informações de um Registro Eletrônico em Saúde.

- **Arquitetura**: Conjunto de artefatos de projeto ou representações descritivas que são relevantes para descrever um objeto de modo que ele possa ser produzido com base em requisitos (qualidade), como também mantido durante o período de sua vida útil (alteração).

- **Arquitetura do Registro Eletrônico em Saúde (ARES)**: Componentes estruturais genéricos a partir dos quais todos os RES são construídos, definidos em termos de um modelo de informação.

- **Informação processável em computador**: Informação que pode ser programaticamente criada, armazenada, manipulada e recuperada de um computador eletrônico.

- **Interoperabilidade Funcional**: A habilidade de dois ou mais sistemas trocarem informações.

- **Interoperabilidade semântica**: A habilidade da informação compartilhada entre sistemas ser entendida em nível dos conceitos de domínio formalmente definidos.

- **Modelo lógico de informação**: Modelo de informação que especifica as estruturas e relações entre as informações, mas é independente de qualquer tecnologia particular ou ambiente de implementação.

O conceito de modelo de informação em saúde, explicitado na arquitetura do S-RES, é considerado como essencial para existência de um RES. Os requisitos descritos neste manual buscam, em última análise, comprovar a existência deste modelo de informação representado através da arquitetura de software.

O S-RES é um sistema complexo que exige métodos robustos de engenharia de software na sua construção para garantir que a informação em saúde possa ser capturada, armazenada, exibida e compartilhada de forma segura, íntegra e completa. A perspectiva de ambientes sem-papel só aumenta a necessidade de robustez e escalabilidade dos S-RES.

Além dos componentes que implementam as funcionalidades de um S-RES (componente principal), em geral desenvolvidos pelo Solicitante da Certificação SBIS/RES, podem existir componentes acessórios (ainda que indispensáveis), dos quais dependerá a implementação de diversas funcionalidades do S-RES. Exemplos típicos são o sistema de gerenciamento de base de dados (SGBD), um componente dinâmico WEB (Applet ou ActiveX), ou ainda um sistema de diretórios (AD, LDAP, etc.) utilizado para armazenar parâmetros dos usuários, papeis e grupos. Um S-RES é o conjunto de todos estes componentes que são necessários para atender aos requisitos especificados neste manual. Não faz parte do escopo da certificação, entretanto, certificar isoladamente cada um desses componentes, como por exemplo, o SGDB ou o sistema operacional.

2.3. Princípios da Certificação

2.3.1. Imparcialidade

Para que a SBIS possa oferecer uma certificação que proporcione confiança, é necessário que todo o processo seja imparcial e percebido como tal. Todas as atividades e decisões do Processo de Certificação SBIS/CFM serão baseadas em evidências objetivas de conformidade e que as decisões não serão influenciadas por interesses espúrios.

As principais fontes de ameaça à imparcialidade são:

- Ameaças de interesse próprio, que surgem de alguém que atua em seu próprio interesse.
- Ameaças de auto-avaliação, que surgem de alguém que avalia seu próprio trabalho.
- Ameaças de familiaridade, que surgem de alguém que, por ser muito familiar ou confiante em algo ou em alguém, não procura evidências objetivas.
- Ameaças de intimidação, que surgem de alguém que está sendo coagido, abertamente ou veladamente, a tomar ou deixar de tomar alguma decisão.

A SBIS manterá procedimentos para detectar, avaliar, documentar e combater todas as ameaças à imparcialidade da Certificação SBIS/CFM, em todos os níveis da organização, preventiva e corretivamente, inclusive com aplicação de sanções, quando necessário.

2.3.2. Competência

Para que a certificação ofereça confiança, é necessário que o Processo de Certificação SBIS/CFM utilize apenas recursos humanos competentes, entendendo-se por competência a capacidade demonstrada de aplicar conhecimentos e habilidades.

A SBIS utilizará no Processo de Certificação SBIS/CFM somente recursos humanos comprovadamente competentes e autorizados, e manterá registros de formação, experiência, habilidade e treinamento dos mesmos.

2.3.3. Responsabilidade

Para que a certificação ofereça confiança, é necessário que o Cliente Certificado entenda e assuma que é ele, e não a SBIS, quem possui a responsabilidade pela conformidade com os requisitos da certificação. Por exemplo, diante de uma reclamação de um cliente usuário do S-RES, a certificação jamais poderá ser invocada como evidência objetiva de que o S-RES não apresente a deficiência apontada pelo cliente. Pelo contrário, a certificação reforça o compromisso do Cliente Certificado em promover todas as investigações e subsequentes correções ou esclarecimentos para sanar as reclamações de seus clientes.

A SBIS é responsável por avaliar evidências objetivas suficientes nas quais possa basear sua decisão de certificação, conforme requisitos expressos neste manual. A certificação SBIS-CFM será concedida se houver evidência suficiente de conformidade aos requisitos do manual, com base nos resultados das auditorias.

O processo de auditoria baseia-se em amostragem. Não existe, portanto, garantia de 100% de conformidade com os requisitos; há sempre um risco associado ao processo que deve ser entendido e assumido por todas as partes envolvidas.

2.3.4. Transparência

Transparência é um princípio de acesso ou divulgação de informações. Para obter e manter confiança na certificação, a SBIS oferecerá acesso público sobre seu processo de

certificação, exceto informações de natureza confidencial, tais como as informações privadas dos Solicitantes e Clientes Certificados.

2.3.5. Confidencialidade

A confidencialidade é um princípio que favorece à SBIS obter confiança do Solicitante de que não terá sua imagem ou seus interesses, de alguma forma, prejudicados por submeter seus S-RES ao processo de certificação.

Para que possa obter acesso privilegiado às informações necessárias para avaliar adequadamente a conformidade dos S-RES com os requisitos da certificação, a SBIS compromete-se a manter a confidencialidade de todas as informações privadas dos Solicitantes e Clientes Certificados, à exceção dos dados cadastrais essenciais da organização e do S-RES e da situação da certificação (concessão, extensão, renovação, suspensão, ou cancelamento), que serão publicados no sítio da SBIS na internet e em outros meios, a critério da SBIS/CFM.

2.3.6. Capacidade de Respostas a Reclamações

Para que a certificação adquira confiança das partes interessadas, é necessário que tanto a SBIS quanto o Cliente Certificado sejam capazes de prontamente registrar e tratar adequadamente as reclamações a que tiverem acesso. A efetiva capacidade para respostas a reclamações é uma salvaguarda fundamental para a proteção da Certificação SBIS/CFM, seus clientes e outras partes interessadas contra erros, omissões ou comportamentos impróprios.

A SBIS manterá procedimentos sistemáticos para registrar e tratar reclamações e exigirá, mediante contrato, que os Solicitantes e Clientes Certificados mantenham sistemas para registro e tratamento formalizados de reclamações. Os registros de reclamações que digam respeito a Clientes Certificados serão considerados informações privadas desses clientes e, portanto, não serão divulgados a terceiros pela SBIS, à exceção do próprio Cliente Certificado e do reclamante.

3. Escopo de Certificação

O Processo de Certificação SBIS/CFM destina-se, genericamente, a Sistemas de Registro Eletrônico de Saúde (S-RES). Como já visto no item 2.2. , a definição do que é um S-RES é bastante ampla e abrangente. Engloba todos os subsistemas e componentes (SGBDs, servidores, bibliotecas, etc.). Será avaliado o conjunto completo de subsistemas e componentes que compõem o S-RES, devidamente configurados de forma a atender os requisitos especificados neste manual.

De acordo com a definição das normas ABNT ISO/TR 20514 e ISO/TS18308, qualquer sistema que capture, armazene, apresente, transmita ou imprima informação identificada em saúde pode ser considerado como sendo um S-RES. Tendo em vista a existência de um grande número de S-RES no mercado brasileiro, englobando uma ampla faixa de sistemas focados em diferentes nichos do mercado de saúde, não seria possível, num primeiro momento, certificar todos e quaisquer S-RES existentes.

Inicialmente, o processo de Certificação SBIS/CFM estará disponível apenas para algumas categorias mais genéricas de S-RES. No futuro próximo, e considerando a demanda futura, as categorias poderão ser ampliadas, e em alguns casos, especializadas.

É importante ressaltar que é dever do desenvolvedor do S-RES indicar para seus usuários e clientes todas as interdependências entre os subsistemas e componentes necessários para que o S-RES esteja configurado e funcione corretamente, especialmente quando os subsistemas ou componentes não são fornecidos juntamente com o S-RES, cabendo ao usuário/cliente contratar o licenciamento destes à parte.

É imprescindível que a documentação do S-RES indique o nome e versão de cada um de seus subsistemas ou componentes, bem como o local onde os mesmos podem ser obtidos (seja um fornecedor comercial ou o repositório de um projeto de software livre). Além disso, devem ser informadas todas as instruções sobre a configuração necessária para o correto funcionamento destes subsistemas/componentes em conjunto. Todas estas informações devem ter como referência o nome e versão do sistema operacional sobre o qual irão funcionar.

3.1. Categorias e Enquadramento dos Sistemas

Para fins da Certificação SBIS/CFM, atualmente poderão ser submetidos ao processo de certificação apenas os S-RES enquadrados em ao menos uma das categorias abaixo:

a) **Assistencial Ambulatorial** – S-RES voltados para a assistência ambulatorial, tais como: sistemas de automação de consultórios clínicos, de informação ambulatorial, de unidades básicas de atendimento à saúde, etc., assim como a parte ambulatorial de sistemas hospitalares ou de sistemas integrados de informação em saúde.
Atenção: Sistemas ou funcionalidades voltadas a outros tipos de atendimento assistencial, como internação hospitalar, vigilância epidemiológica, medicina ocupacional, etc., serão gradualmente agregados a esta categoria nas próximas versões deste manual.

b) **GED** – Sistemas de gerenciamento eletrônico de documentos, utilizados para o armazenamento e visualização de documentos relacionados à informação de saúde.

c) **TISS** – Categoria dirigida ao atendimento do padrão TISS da ANS. Inúmeros S-RES, especialmente aqueles em uso por operadoras de planos de saúde e prestadores de serviços de saúde, são obrigados a trocar informações usando o TISS. Atende também aos aplicativos de comunicação ("empresas de conectividade") que realizam a troca de informações entre Operadoras e Prestadores.

Ao inscrever-se no processo de certificação (ver capítulo 5), o Solicitante deverá indicar uma ou mais categorias onde o seu sistema se enquadra.

Como poderá ser visto adiante no item 8.1. , a Certificação SBIS/CFM prevê ainda níveis diferenciados nos requisitos de segurança. O S-RES poderá ser enquadrado em dois níveis distintos de garantia de segurança: um primeiro nível mais amplo e um segundo nível que, além de contemplar todos os requisitos do primeiro nível, exige também que o S-RES incorpore as funcionalidades necessárias para trabalhar com certificados digitais padrão ICP-Brasil. Adicionalmente, o S-RES deverá ser identificado como sendo um S-RES local ou um S-RES remoto, refletindo se o mesmo funciona isoladamente ou se pode ser acessado simultaneamente por diferentes usuários a partir de estações de trabalho conectadas ao computador onde o S-RES está instalado.

Para ser aprovado, um S-RES precisará necessariamente se enquadrar em pelo menos uma das categorias de S-RES descritas acima, atendendo a todos os requisitos obrigatórios estabelecidos para aquela categoria, além de atender também a todos os requisitos obrigatórios previstos pelo menos no Nível de Garantia de Segurança 1 - NGS1 (ver item 8.1.).

A categoria TISS apresenta algumas variações nos requisitos, de acordo com os agrupamentos adotados pela ANS no cronograma de implantação do TISS, conforme a Tabela 1 a seguir.

Tabela 1: Categorias de Prestadores e Operadoras para a Implantação do TISS

	Prestadores	**Operadoras**
Grupo 1	Hospitais gerais Hospitais especializados Hospitais/dia–isolado Pronto socorro especializado Pronto socorro geral Clínica especializada / ambulatório de especialidade Unidade de apoio à diagnose e terapia (SADT isolado) Unidade móvel de nível pré-hospitalar - urgência/emergência Unidade móvel fluvial Unidade móvel terrestre	Operadoras de planos de assistência médica
Grupo 2	Consultório isolado Profissionais de saúde ou pessoa jurídica que presta serviço em consultório médico	
Grupo 3	Clínica radiológica em odontologia Consultório odontológico isolado Odontologista ou pessoa jurídica da área odontológica que presta serviço em consultório	Operadoras de planos odontológicos

Além das divisões acima, a categoria TISS apresenta o recurso da "Comunicação", responsável pelo envio e recebimento dos dados transitados entre o Prestador e a Operadora. Cada uma destas partes ("lados" da comunicação) pode apresentar este recurso como uma funcionalidade agregada ao seu aplicativo (S-RES) ou utilizar um aplicativo específico para tal finalidade, sendo que esse último pode estar em seus domínios ou ser terceirizado através das chamadas "empresas de conectividade". Este recurso, quando incluído pelo Solicitante no enquadramento para certificação, requer, obrigatoriamente, a adoção do NGS2.

Caberá ao Solicitante indicar as categorias de sistema e o nível de garantia de segurança do seu S-RES, para que estas informações sejam consideradas no processo de certificação.

O enquadramento de um S-RES se faz, portanto, pelas seguintes opções:

a) Nível de Garantia de Segurança: **NGS1 (Local** ou **Remoto)** ou **NGS2**
+
b) Categoria: **Assistencial (Ambulatorial)** e/ou **GED** e/ou **TISS**

Caso o S-RES apresente a categoria TISS, haverá, ainda, as seguintes opções:

c) Tipo TISS: **Prestador** e/ou **Comunicação** e/ou **Operadora**
+
d) Grupo TISS: **Grupo 1** e/ou **Grupo 2** e/ou **Grupo 3**

Assim, obtém-se o enquadramento de um S-RES através da escolha de uma opção do item “a” acima, mais a escolha de uma ou mais opções do item “b”. Caso haja a escolha, no item “b”, da opção TISS, deve-se acrescentar a escolha de uma ou mais opções do item “c”, mais a escolha de uma ou mais opções do item “d”. Deve-se observar que a escolha da opção Comunicação no item “c” requer, obrigatoriamente, a adoção do NGS2.

Caso seja solicitada a certificação no nível de garantia de segurança NGS2 e a auditoria apontar não-conformidade aos requisitos deste nível, mas apontar conformidade aos requisitos do NGS1, e não sendo obrigatória a adoção do NGS2, conforme condições descritas anteriormente, será possível, a critério do Solicitante, a obtenção da certificação no nível NGS1, desde que atingida a conformidade em no mínimo uma das categorias inscritas.

Caso seja solicitada a certificação em mais de uma categoria e a auditoria não apontar conformidade a todas, mas apontar conformidade a no mínimo uma das categorias inscritas, será possível, a critério do Solicitante, a obtenção da certificação nas categorias que atingirem a conformidade.

4. Conceitos, Normas e Condições da Certificação

4.1. Componentes de um S-RES

Para submeter um S-RES a uma auditoria de certificação, o Solicitante deve identificá-lo e descrever cada um de seus componentes. A descrição deve incluir a infraestrutura necessária para o S-RES funcionar corretamente, incluindo todos os componentes de hardware e software que serão utilizados no processo de certificação, além dos respectivos parâmetros que devam ser eventualmente ajustados. A seguir apresenta-se uma lista, não exaustiva, de itens que devem ser considerados ao elaborar a descrição do S-RES:

- Sistema Operacional
- SGBD (Banco de Dados) e conectores
- Arquitetura do S-RES (cliente/servidor, ASP, *Mainframe*, etc.)
- Componentes do tipo *web* dinâmicos (*Applet, ActiveX, etc.*)
- Sistema de diretórios (AD, LDAP, etc.)

A SBIS fará a auditoria com base no S-RES identificado e descrito pelo Solicitante, considerando ainda as categorias para as quais a certificação está sendo solicitada. É importante lembrar que a descrição fornecida pelo Solicitante deverá ser fiel à versão do S-RES que será efetivamente submetida ao processo de auditoria.

4.1.1. Componentes alternativos

Além dos componentes descritos na auditoria, o Solicitante poderá informar uma lista contendo os Sistemas Operacionais e SGBDs para os quais o S-RES também funciona e e produzem exatamente os mesmos efeitos no que tange à conformidade aos requisitos deste manual.

Sendo o S-RES aprovado na auditoria, a SBIS publicará sua descrição no Certificado SBIS/CFM emitido em papel e na lista de sistemas certificados disponível em seu sítio na internet. Desta descrição constarão, de forma distinta, os componentes utilizados na configuração auditada e a lista dos componentes alternativos habilitados declarada pelo Solicitante. Esta última será acompanhada de informação explícita de que tais componentes alternativos não sofreram verificação durante o processo de auditoria, ficando sob responsabilidade exclusiva do Solicitante a veracidade da declaração de manutenção da conformidade do S-RES quando da utilização dos referidos componentes.

Considera-se grave violação contratual o Solicitante declarar em sua lista de componentes alternativos habilitados qualquer componente que, quando utilizado, não mantenha as mesmas conformidades obtidas com a utilização do respectivo componente auditado. Nesse caso, o Solicitante estará sujeito às penalidades previstas no Contrato de Certificação (ver item 4.6.), as quais poderão incluir o cancelamento do Certificado e a proibição de submeter qualquer S-RES ao processo de certificação pelo período de um ano, contado da data em que a Diretoria da SBIS anunciar sua decisão em relação ao ocorrido.

4.2. Configurações de S-RES

Cada certificado está relacionado a uma configuração específica do S-RES, testada no processo de auditoria com um conjunto de componentes e em total conformidade com os requisitos estabelecidos, além de uma lista de componentes alternativos habilitados (ver item 4.1.1) declarada pelo Cliente Certificado. Por outras configurações entende-se o mesmo S-RES funcionando com um conjunto de componentes diferente do utilizado na configuração auditada, como por exemplo, outros sistemas operacionais, outros SGBDs, etc.

4.3. Versões de S-RES

Cada certificado está relacionado a uma versão específica do S-RES, testada no processo de auditoria e totalmente de acordo com os requisitos estabelecidos. Assim, a descrição de um S-RES deverá incluir também a identificação da sua versão e a data em que ela foi produzida, liberada para o mercado ou utilizada pela primeira vez.

Para efeito da Certificação SBIS/CFM, uma nova versão de um S-RES corresponde a uma evolução do mesmo, seja pela adição, ampliação ou aperfeiçoamento de funcionalidades, ou pela correção de problemas ou inconsistências verificados. Uma nova versão necessariamente trará consigo ajustes em relação às versões anteriores, sendo que estes podem ser classificados como “pequenos ajustes” ou “ajustes relevantes”.

É possível solicitar que a certificação concedida a uma determinada configuração/versão de um S-RES seja estendida para outras configurações ou versões (ver item 4.5.), considerando-se a classificação dos ajustes conforme exposto adiante.

4.3.1. Pequenos Ajustes

Entende-se por “pequenos ajustes” as modificações e atualizações que não afetam a conformidade do S-RES aos requisitos da certificação. Como exemplos de pequenos ajustes, lembrando que eles não podem afetar, modificar ou remover uma ou mais funcionalidades ou características necessárias para a certificação, podem ser citados:

- Modificações no nome do produto;
- Correções de *bugs* com o único objetivo de sanar uma falha de funcionamento do S-RES;
- Pequenas modificações na interface com o usuário (esquemas de cores, fontes, estilos de botões, etc.);
- Adição de novas funcionalidades ou módulos (por exemplo, incluir uma consulta aos médicos usuários do sistema) fora do escopo da certificação;
- Substituição de componentes internos do S-RES que possuam interfaces ou características padronizadas (por exemplo, substituição de SGBD, desde que o S-RES anteriormente certificado só dependesse de funcionalidades amplamente disponíveis naquele ou em qualquer outro SGBD).

4.3.2. Ajustes Relevantes

Entende-se por "ajustes relevantes" as modificações que impliquem em risco significativo de afetar a conformidade do S-RES aos requisitos da certificação. Como exemplos de ajustes relevantes, e que necessariamente irão impactar em uma ou mais funcionalidades ou características do S-RES consideradas no processo de certificação, podem ser citadas:

- Remoção de qualquer funcionalidade ou módulo essencial para a obtenção da certificação (por exemplo, retirada da função de registro de *log*);
- Substituição de bibliotecas ou componentes de software (por exemplo, substituindo um editor de textos desenvolvido internamente e utilizado na edição do prontuário do paciente por um componente de editor de textos desenvolvido por terceiros, ou vice-versa);
- Remodelagem significativa da interface com o usuário, por exemplo, mudando a estrutura dos menus, nomenclatura de telas, ou ainda migrando o sistema para uma nova interface (por exemplo, via *web-browser*);
- Substituição de componentes internos do S-RES que, mesmo possuindo interfaces ou características padronizadas, oferecem características específicas utilizadas pelo S-RES para obter a certificação (por exemplo, substituição de SGBD cujo módulo de criptografia de dados era utilizado para garantir aspectos de segurança da informação avaliados na certificação);
- Mudança de modelo de informação. Por exemplo, se o sistema adotava o modelo HL7 V3 e passa a adotar o modelo Open-EHR baseado em arquétipos.

4.3.3. Declaração de manutenção da conformidade

O Cliente Certificado poderá, opcionalmente, declarar que uma nova versão de um S-RES certificado mantém total conformidade aos requisitos estabelecidos, sem qualquer prejuízo em relação à versão originalmente certificada. Não há, neste caso, a necessidade de execução do processo de Extensão da Certificação (ver item 4.5.), cabendo integral e exclusivamente ao Solicitante a responsabilidade pela veracidade da declaração de manutenção da conformidade da nova versão do S-RES. Deverá, contudo, atender obrigatoriamente ao requisito de segurança NGS1.01.03 (ver item 8.2.), mantendo os respectivos históricos de alterações em seu poder pelo prazo mínimo de 05 (cinco) anos, obrigando-se, durante este prazo, a disponibilizá-los à SBIS para consulta sempre que solicitados.

À SBIS reserva-se o direito de convocar o Cliente Certificado para uma verificação e/ou auditoria sobre o S-RES sempre que houver qualquer indício ou denúncia de falsidade acerca de uma declaração de manutenção de conformidade.

Considera-se grave violação contratual o Cliente Certificado declarar a manutenção da conformidade de uma nova versão de um S-RES certificado quando esta nova versão não atender integralmente as mesmas conformidades da versão originalmente certificada. Nesse caso, o Cliente Certificado estará sujeito às penalidades previstas no Contrato de Certificação (ver item 4.6.), as quais poderão incluir o cancelamento do Certificado e a proibição de submeter qualquer S-RES ao processo de certificação pelo período de um

ano, contado da data em que a Diretoria da SBIS anunciar sua decisão em relação ao ocorrido.

4.4. Validade da Certificação

O Certificado SBIS/CFM será válido por um período calculado da seguinte forma: dois anos a partir da emissão, ou um ano a partir da publicação pela SBIS de versão do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) posterior à que serviu de base para o certificado, sendo considerado o evento que ocorrer na data mais avançada.

Portanto, o Cliente Certificado terá a segurança de que o Certificado SBIS/CFM não terá duração inferior a dois anos e que, se for publicada uma nova versão do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES), ele terá prazo não inferior a um ano para adequar seu S-RES à nova versão do manual, antes que expire a validade do seu Certificado.

A data de emissão do certificado nunca será anterior à data em que a Diretoria da SBIS decidir pela certificação do S-RES (passo [S-11] do processo de certificação).

Quando da publicação de uma nova versão do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES), durante um período de 90 dias, poderão ser emitidos Certificados SBIS/CFM com base na versão anterior do manual, a pedido do Solicitante, tanto para processos de certificação que se iniciaram antes da data da publicação, quanto para processos novos. Nesse caso, a validade do certificado expirará na data em que a publicação da nova versão do manual completar um ano.

4.5. Extensão da Certificação para Outras Configurações ou Versões

O Certificado SBIS/CFM é específico para a configuração e para a versão do S-RES nele discriminadas.

A SBIS poderá estender a certificação para outras configurações ou versões de um S-RES já certificado, desde que tal extensão seja obtida durante o período de validade da certificação do S-RES original. Para tanto, o Solicitante deverá preencher a Ficha de Inscrição para Extensão de Certificação (ver item 4.6.) e submetê-la ao processo descrito no capítulo 5 deste manual.

No caso de extensão para outras configurações, a solicitação deverá conter a descrição das configurações alternativas para as quais se solicita a extensão. O Responsável Técnico pelo S-RES deverá declarar que estas configurações alternativas são idênticas em funcionalidades à configuração certificada, e que atendem integralmente aos requisitos para a certificação. A Ficha de Inscrição deverá ser assinada por este Responsável Técnico e pelo Representante Legal do Solicitante.

Já no caso de solicitações de extensão da certificação do S-RES para novas versões, o Solicitante deverá primeiramente avaliar os ajustes realizados na nova versão. A solicitação deverá conter a descrição de todos os ajustes realizados na nova versão, desde que estes ajustes se enquadrem, todos, na definição de “pequenos ajustes” (ver

item 4.3.1). Se a nova versão contiver qualquer "ajuste relevante" (ver item 4.3.2), isto será motivo suficiente para que a nova versão do S-RES seja submetida a uma nova auditoria.

Considera-se grave violação contratual o Cliente Certificado deixar de comunicar à SBIS a existência de ajustes em seu S-RES que afetam sua conformidade aos requisitos para a Certificação SBIS/CFM. Nesse caso, o Cliente Certificado estará sujeito às penalidades previstas no Contrato de Certificação (ver item 4.6.), as quais poderão incluir o cancelamento do Certificado e a proibição de submeter qualquer S-RES ao processo de certificação pelo período de um ano, contado da data em que a Diretoria da SBIS anunciar sua decisão em relação ao ocorrido.

No caso de nova versão de um S-RES já certificado que contenha ajustes relevantes, uma das seguintes alternativas deverá ser observada:

- Caso a versão do Manual de Certificação vigente à época da solicitação de extensão for a mesma da certificação da versão anterior do S-RES, o Solicitante deverá pagar uma Taxa de Extensão de Certificação. A critério da SBIS, o escopo desta nova auditoria poderá ser reduzido, considerando-se as informações prestadas pelo Solicitante sobre os pequenos ajustes e os ajustes relevantes contidos na nova versão do S-RES. No caso da nova versão ser aprovada nesta nova auditoria, o prazo de validade da certificação passará a ser contado a partir desta última auditoria.

- Caso a versão do Manual de Certificação vigente à época da solicitação de extensão for diferente daquela na qual se baseou a certificação da versão anterior do S-RES, o Solicitante deverá submeter o S-RES a uma nova certificação completa, não podendo ser efetuado o processo de extensão de certificação.

Mesmo nos casos onde é possível estender a certificação de um S-RES sem a necessidade de uma nova auditoria, é imperativo aguardar o pronunciamento formal da SBIS sobre o assunto. O Solicitante não poderá fazer qualquer alusão ao fato de que uma nova configuração ou versão de um S-RES previamente certificado é também certificada, sem antes obter formalmente tal extensão da SBIS. Ao conceder tal extensão, a SBIS irá incluir a nova configuração ou versão na lista de configurações/versões certificadas daquele específico S-RES, disponível para consulta no sítio da SBIS na internet. Apenas então o Solicitante poderá se referir a esta nova configuração ou versão como sendo igualmente certificada pela SBIS.

As configurações e versões do S-RES anteriormente certificadas continuarão constando da lista de S-RES certificados disponível no sítio da SBIS na internet até o final dos respectivos prazos de validade de cada certificação, exceto nos casos onde o Cliente Certificado solicitar explicitamente sua exclusão de tal lista.

4.6. Instrumentos Formais

A certificação será formalizada e regulamentada pelos seguintes instrumentos:

- **Ficha de Inscrição para Certificação**: formulário eletrônico (ou, excepcionalmente, em papel) a ser preenchido e enviado pelo Solicitante à SBIS para indicar a intenção de submeter um produto (S-RES) ao processo de certificação. Contém, em seu corpo, a descrição das condições que regulamentam tal inscrição.

- **Ficha de Inscrição para Extensão de Certificação**: formulário eletrônico (ou, excepcionalmente, em papel) a ser preenchido e enviado pelo Solicitante à SBIS para indicar a intenção de submeter um produto (S-RES) ao processo de extensão de certificação. Contém, em seu corpo, a descrição das condições que regulamentam tal inscrição.

- **Contrato de Certificação**: contrato firmado entre o Solicitante e a SBIS antes do início da auditoria do S-RES, o qual regulamenta tanto a execução do processo de certificação quanto as normas a serem cumpridas pelas partes após tal processo, seja o produto certificado ou não. Estabelece, entre outras coisas, as regras do processo, os preços avençados, as obrigações das partes (incluindo os termos de confidencialidade de informações) e seus direitos (incluindo as regras de uso do Selo SBIS/CFM, Certificado e informações correlatas), e os devidos termos jurídicos referentes ao contexto pactuado.

- **Termo de Extensão de Certificação:** termo aditivo firmado entre a SBIS e o Cliente Certificado com o objetivo de estender os direitos atribuídos a um determinado S-RES, tornando-os aplicáveis às demais configurações e/ou versões discriminadas em tal termo.

- **Certificado (Diploma de Certificação)**: documento probatório da certificação de um determinado S-RES pela SBIS/CFM.

- **Selo de Certificação SBIS/CFM**: elemento gráfico de concepção artística indicador da obtenção do Certificado a um determinado S-RES. As normas de uso do selo encontram-se dispostas no item 7.2. deste manual.

4.7. Taxas e Preços

Serão cobradas do Solicitante as seguintes taxas, cujos valores encontram-se disponíveis para consulta no sítio da SBIS na internet.

- **Taxa de Inscrição**: valor a ser pago pelo Solicitante à SBIS imediatamente após o envio da Ficha de Inscrição para Certificação ou da Ficha de Inscrição para Extensão de Certificação, e que proporciona ao mesmo unicamente o direito à análise e avaliação de tal ficha pela SBIS e à elaboração do Contrato de Certificação ou do Termo de Extensão de Certificação.

- **Taxa de Certificação:** valor a ser pago pelo Solicitante à SBIS no momento da assinatura do Contrato de Certificação, e que proporciona ao mesmo o direito a

todo o processo de auditoria do S-RES objeto do contrato e, caso seja aprovado (certificado), à emissão do Certificado e do Selo de Certificação. Confere ainda ao Solicitante o direito de uso do referido selo e da divulgação da condição de S-RES Certificado no sítio da SBIS na internet durante todo o prazo de validade da certificação (ver item 4.4.).

- **Taxa de Extensão de Certificação:** valor a ser pago pelo Solicitante à SBIS no momento da assinatura do Termo de Extensão de Certificação, e que proporciona ao mesmo o direito a todo o processo de avaliação e/ou auditoria do S-RES objeto do termo e, caso seja aprovado (obtenha a extensão do certificado), à emissão do Certificado e do Selo de Certificação. Confere ainda ao Solicitante o direito de uso do referido selo e da divulgação da condição de S-RES Certificado no sítio da SBIS na internet durante todo o prazo de validade da certificação (ver item 4.4.).

- **Taxa de Realização de 2º Ciclo de Auditoria:** valor a ser pago pelo Solicitante à SBIS para a realização, quando necessário, de um 2º ciclo de auditoria dentro de um processo de certificação (ver item 5.1. , passo A.01), e que proporciona ao mesmo apenas o direito à execução desta parte do processo.

- **Taxa de Reagendamento de Auditoria:** valor a ser pago pelo Solicitante à SBIS quando houver, a pedido do Solicitante, a necessidade de reagendamento de uma auditoria cujo cronograma tenha sido previamente aprovado entre as partes. Caso o Solicitante comunique a necessidade de reagendamento com mais de 05 (cinco) dias úteis de antecedência (fora o próprio dia) do início previsto para o primeiro dia da auditoria, o valor a ser pago será de 30% (trinta por cento) desta taxa.

4.7.1. Devolução de Taxas

Não haverá devolução de taxas pagas à SBIS, independentemente do resultado obtido pelo Solicitante no respectivo processo, exceto nos casos onde a SBIS recusar-se, por qualquer motivo, a executar a atividade pela qual recebeu a referida taxa. Assim, a não aprovação de uma determinada ficha de inscrição ou a não obtenção da certificação ou extensão por um determinado produto (S-RES) após o devido processo de auditoria ou avaliação, não constituirão motivo para a devolução, por parte da SBIS, de qualquer taxa paga pelo Solicitante.

Caberá única e exclusivamente à Diretoria da SBIS a decisão a respeito de situações excepcionais.

5. Processo de Certificação

Assim como nos processos de acreditação hospitalar e/ou certificações ISO, a Certificação SBIS/CFM estabelece que a auditoria seja realizada por equipe especializada, a qual verificará se, realmente, os requisitos obrigatórios para a categoria selecionada são atendidos pelo S-RES.

A auditoria constitui-se na realização de uma bateria de testes sobre o sistema alvo da certificação. Os testes são realizados e analisados por um grupo de auditores devidamente treinados, credenciados e selecionados pela SBIS, todos membros titulares da Sociedade.

Em linhas gerais, a empresa ou pessoa interessada em certificar o seu S-RES deve proceder às seguintes etapas:

a) Analisar a documentação sobre o processo de certificação disponível no sítio da SBIS na internet;
b) Verificar se o S-RES a ser certificado atende a todos os requisitos obrigatórios para as categorias desejadas (lembrando que os requisitos de segurança são obrigatórios para qualquer categoria);
c) Realizar a bateria de testes internamente em sua instituição, conforme descrito no Manual Operacional de Ensaios e Análises;
d) Cumpridas as etapas anteriores, estando a empresa ou pessoa interessada segura de que seu S-RES está em condições de ser aprovado na auditoria, deverá iniciar formalmente o processo para obtenção do Selo de Certificação SBIS/CFM conforme descrito a seguir.

Existem dois fluxos possíveis no processo de certificação, a saber:

a) Processo Padrão: representa o fluxo básico a ser seguido para a obtenção da certificação, para um S-RES ainda não certificado ou que esteja com a sua validade expirada, ou para uma nova versão que contenha ajustes relevantes (ver item 4.3.2) em relação à versão anteriormente certificada.
b) Processo para Extensão de Certificação: representa o fluxo a ser seguido para a extensão da certificação para outras configurações ou versões de um S-RES já certificado, conforme descrito no item 4.5.

5.1. Processo Padrão

Este é o processo básico a ser seguido para a obtenção da certificação, para um S-RES ainda não certificado ou que esteja com a sua validade expirada, ou para uma nova versão que contenha ajustes relevantes (ver item 4.3.2) em relação à versão anteriormente certificada. É composto por uma série de atividades a serem executadas pelo Solicitante e pela SBIS, conforme demonstrado no fluxo da Figura 1 abaixo.

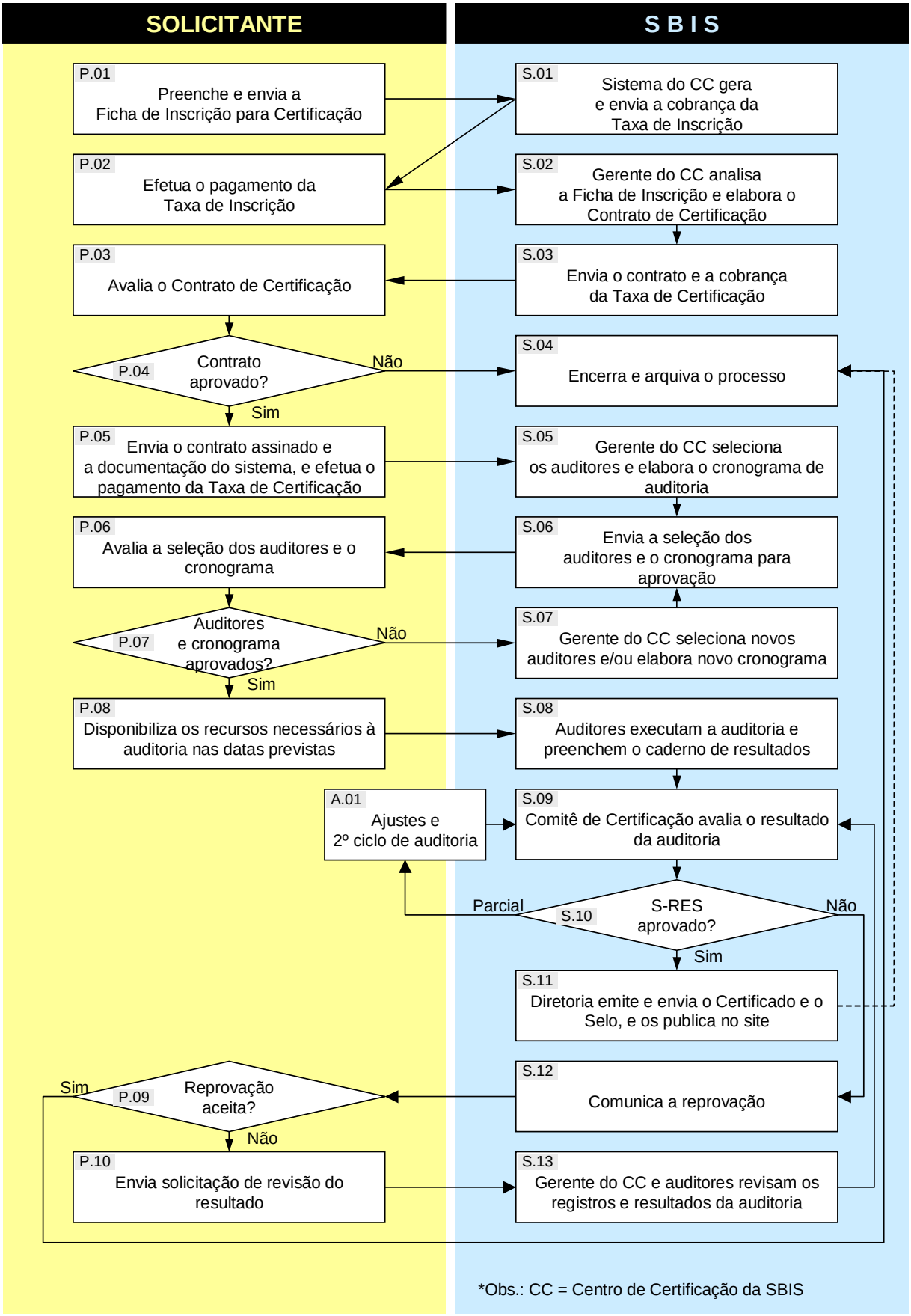

Figura 1 : Fluxo do processo de certificação

Atenção: o fluxo acima apresenta apenas as descrições resumidas de cada passo, de forma a facilitar a visualização e entendimento de todo o processo. As descrições completas dos passos encontram-se detalhadas a seguir.

5.1.1. Atividades do Solicitante no Processo

O Solicitante deverá executar as atividades apresentadas na coluna esquerda do fluxo do processo de certificação (ver Figura 1), descritas a seguir:

[P.01] Preenche e envia a Ficha de Inscrição para Certificação

O Solicitante deverá preencher a Ficha de Inscrição para Certificação (ver item 4.6.), disponível no sítio da Certificação SBIS/CFM na internet. Uma vez preenchida, tal ficha deverá ser enviada (submetida) eletronicamente através do próprio sítio eletrônico. Após o envio, uma mensagem de confirmação de recebimento será enviada pela SBIS ao endereço de e-mail do Solicitante.

[P.02] Efetua o pagamento da Taxa de Inscrição

A SBIS enviará por e-mail ao Solicitante, no prazo máximo de 02 (dois) dias úteis após o recebimento da Ficha de Inscrição, um boleto bancário referente à Taxa de Inscrição no processo de certificação (ver item 4.7.). A SBIS dará andamento às atividades subsequentes do processo somente após o recebimento desta taxa, a qual deverá ser paga pelo Solicitante na rede bancária dentro do prazo de vencimento disposto no boleto.

[P.03] Avalia o Contrato de Certificação

Caso a análise da Ficha de Inscrição pela SBIS não aponte nenhuma restrição à participação do Solicitante e do S-RES inscrito no processo de certificação, o Solicitante receberá da SBIS, no prazo máximo de 10 (dez) dias úteis após o pagamento da Taxa de Inscrição, o Contrato de Certificação (ver item 4.6.), ainda não assinado. O Solicitante deverá analisar cuidadosamente o contrato, questionando a SBIS sobre qualquer dúvida que porventura seja suscitada.

Caso haja alguma restrição à participação do Solicitante ou do S-RES inscrito no processo de certificação, o Solicitante receberá da SBIS, no prazo máximo de 10 (dez) dias úteis após o pagamento da Taxa de Inscrição, um comunicado da impossibilidade de execução do processo de certificação, onde serão expostos os motivos para tal rejeição.

[P.04] Contrato aprovado?

Caso o Solicitante concorde com todos os termos do contrato, deverá devolvê-lo assinado à SBIS (passo P.05 adiante). Caso contrário, solicita-se que tal decisão seja comunicada por e-mail à SBIS, para que o processo seja arquivado.

Na ausência de pronunciamento formal positivo (caracterizado pelo passo P.05 adiante) ou negativo no prazo de 30 (trinta) dias úteis após o recebimento da documentação (passo P.03 acima), o processo será considerado encerrado e, então, arquivado pela SBIS.

Processos encerrados e arquivados pela SBIS não poderão ser reativados, devendo o Solicitante, quando necessário, iniciar um novo processo, submetendo nova Ficha de Inscrição (passo P.01).

[P.05] Envia o contrato assinado e a documentação do sistema, e efetua o pagamento da Taxa de Certificação

Caso o Solicitante concorde com todos os termos do Contrato de Certificação, seu representante legal deverá assinar as 02 (duas) vias do mesmo e enviá-las de volta à SBIS, juntamente com toda a documentação técnica do sistema necessária ao processo de certificação, tais como manuais de instalação e de operação.

Juntamente com o Contrato de Certificação, o Solicitante receberá da SBIS (no passo P.03 acima) um boleto bancário referente à Taxa de Certificação (ver item 4.7.). A SBIS dará andamento às atividades subsequentes do processo somente após o recebimento desta taxa.

O prazo para a execução deste passo (envio do contrato assinado e da documentação, e pagamento da taxa) é de 30 (trinta) dias úteis após o recebimento da respectiva documentação (passo P.03 acima). Caso tais tarefas não sejam executadas neste prazo, o processo será considerado encerrado e, então, arquivado pela SBIS.

[P.06] Avalia a seleção dos auditores e o cronograma

No prazo máximo de 10 (dez) dias úteis após a efetivação do Contrato de Certificação (passo P.05 acima), o Solicitante receberá da SBIS, por e-mail, uma proposta de cronograma para a auditoria e a relação dos auditores selecionados. O Solicitante deverá, então, avaliar tais elementos, verificando a viabilidade do cronograma proposto e a eventual existência de restrições à participação de qualquer dos auditores indicados.

Caso o Solicitante tenha rejeitado uma proposta anterior de cronograma e auditores (passo P.07 adiante), receberá, no prazo máximo de 10 (dez) dias úteis após ter comunicado tal rejeição, uma nova proposta de cronograma e relação dos auditores selecionados, devendo efetuar nova avaliação.

[P.07] Auditores e cronograma aprovados?

O Solicitante deverá comunicar formalmente à SBIS, por e-mail e no prazo máximo de 05 (cinco) dias úteis após o recebimento das informações (passo P.06 acima), seu parecer quanto ao cronograma proposto e relação dos auditores selecionados.

Caso o Solicitante concorde com a proposta apresentada, bastará comunicar tal aprovação à SBIS.

Caso o Solicitante discorde da proposta apresentada, seja do cronograma ou de algum dos auditores selecionados, deverá comunicar tal rejeição à SBIS, justificando explicitamente os motivos. Caso haja, dentre os motivos, a indisponibilidade do Solicitante face ao cronograma sugerido pela SBIS, o mesmo poderá, visando agilizar esta definição, adicionar à justificativa uma ou mais propostas de datas, desde que posteriores às datas originalmente sugeridas pela SBIS.

Atenção: na ausência de comunicação formal do Solicitante no prazo citado de 05 (cinco) dias úteis, o cronograma proposto e a seleção dos auditores serão automaticamente considerados aprovados.

O Solicitante poderá rejeitar no máximo 03 (três) propostas efetuadas pela SBIS, independentemente dos motivos alegados, sendo a quarta proposta, quando houver, impassível de rejeição e automaticamente considerada aprovada.

[P.08] Disponibiliza os recursos necessários à auditoria nas datas previstas

Após a aprovação do cronograma de auditoria e da relação de auditores, o Solicitante deverá disponibilizar, nas datas previstas, o produto (S-RES) objeto da certificação e todos os aplicativos e produtos necessários à sua execução. A auditoria ocorrerá na sede da SBIS, em São Paulo/SP. O Solicitante poderá disponibilizar o S-RES para auditoria através de qualquer um dos seguintes meios:

- Instalação em um microcomputador (desktop) da SBIS, necessariamente sob o sistema operacional *Windows* ou *Linux*;
- Instalação em um microcomputador (desktop ou notebook) do próprio Solicitante;
- Acesso direto ao sistema através da internet;
- Acesso indireto ao sistema através da internet, utilizando algum aplicativo de controle remoto (ex.: *VNC*, *PC Anywhere* etc.);
- Outro meio equivalente que atenda a este objetivo, desde que previamente acordado com a SBIS.

O Solicitante deverá, também, disponibilizar de 01 (um) a 03 (três) profissionais para operarem o sistema na sede da SBIS, em São Paulo/SP, durante todo o período da auditoria. Tais profissionais deverão, conjuntamente, estar aptos a operar todos os módulos e funcionalidades do S-RES pertinentes às categorias sob certificação, e deverão atender às orientações e solicitações efetuadas pelos auditores durante toda a auditoria.

Caso haja a necessidade de algum outro recurso ou material adicional, a SBIS poderá requisitá-lo ao Solicitante, o qual deverá providenciá-lo.

Todos os custos e despesas decorrentes da disponibilização dos recursos aqui citados serão de total responsabilidade do Solicitante, e não serão passíveis de qualquer tipo de remuneração, auxílio financeiro ou reembolso por parte da SBIS.

[P.09] Reprovação aceita?

Ao receber da SBIS o comunicado de reprovação da certificação de seu S-RES, o Solicitante deverá analisar e avaliar os resultados obtidos na auditoria. Caso não concorde com tal reprovação, deverá solicitar à SBIS a revisão do resultado (passo P.10 adiante). Caso contrário, deverá comunicar por e-mail à SBIS, para que o processo seja arquivado.

Caso o Solicitante não se pronuncie formalmente a respeito do resultado no prazo de 15 (quinze) dias úteis após o recebimento do comunicado, o processo será encerrado e arquivado pela SBIS.

Apenas o resultado da auditoria original é passível de revisão, não cabendo tal solicitação sobre um resultado já revisado.

[P.10] Envia solicitação de revisão do resultado

Caso não concorde com a reprovação da certificação de seu S-RES, o Solicitante deverá enviar formalmente à SBIS, no prazo máximo de 15 (quinze) dias úteis após o recebimento do comunicado, uma solicitação de revisão do resultado, a qual deverá, necessariamente, conter as justificativas e embasamento para a discordância.

As solicitações de revisão de resultado serão analisadas e respondidas pela SBIS no prazo de 15 (quinze) dias úteis após o seu recebimento.

5.1.2. Atividades da SBIS no Processo

A SBIS executará as atividades apresentadas na coluna direita do fluxo do processo de certificação (ver Figura 1 :), descritas a seguir:

[S.01] Sistema do CC gera e envia a cobrança da Taxa de Inscrição

Ao receber o cadastramento da Ficha de Inscrição para Certificação, o sistema do CC (Centro de Certificação) da SBIS enviará uma mensagem de confirmação de recebimento ao e-mail do Solicitante. No prazo máximo de 02 (dois) dias úteis após o recebimento de tal ficha, o CC emitirá um boleto bancário para a cobrança da Taxa de Inscrição (ver item 4.7.) e o enviará por e-mail ao Solicitante.

[S.02] Gerente do CC analisa a Ficha de Inscrição e elabora o Contrato de Certificação

Ao detectar o recebimento da Taxa de Inscrição, o Gerente do CC analisará a Ficha de Inscrição, verificando se o Solicitante e o produto (S-RES) inscrito atendem às condições necessárias à participação no processo de certificação.

Caso as condições estejam atendidas, o Gerente do CC, com base no enquadramento do S-RES (ver item 3.1.) e na tabela de preços em vigor (ver item 4.7.), elaborará o Contrato de Certificação (ver item 4.6.), o qual explicitará, entre outras coisas, a parte contratante (Solicitante), o produto (S-RES) a ser certificado e o valor a ser pago pelo Solicitante a título de Taxa de Certificação.

Caso as condições à participação não estejam atendidas, o Gerente do CC enviará um comunicado ao Solicitante sobre tal impossibilidade, descrevendo os motivos para tal rejeição.

[S.03] Envia o contrato e a cobrança da Taxa de Certificação

No prazo máximo de 10 (dez) dias úteis após o pagamento da Taxa de Inscrição, o CC enviará ao Solicitante o Contrato de Certificação em 02 (duas) vias não assinadas e um boleto bancário para a cobrança da Taxa de Certificação, no valor definido no contrato.

Caso a participação no processo tenha sido rejeitada, o CC enviará ao Solicitante somente o comunicado elaborado no passo anterior (S.02) e arquivará o processo (passo S.04 adiante).

[S.04] Encerra e arquiva o processo

Quando configurado, em qualquer momento e por qualquer causa, o encerramento do processo, esteja o mesmo concluído ou não, a SBIS efetuará o seu arquivamento, armazenando toda a documentação e material relativos ao mesmo, tanto em meio eletrônico quanto em papel, pelo período mínimo de 05 (cinco) anos.

[S.05] Gerente do CC seleciona os auditores e elabora o cronograma de auditoria

Ao receber as 02 (duas) vias do Contrato de Certificação assinadas, a documentação do sistema e confirmar o recebimento da Taxa de Certificação, o representante legal da SBIS assinará as 02 (duas) vias do contrato e, no prazo máximo de 10 (dez) dias úteis, reenviará uma das vias ao Solicitante.

O Gerente do CC analisará o processo e elaborará uma proposta de cronograma para a auditoria. As datas propostas seguirão, obrigatoriamente, a ordem cronológica de recebimento dos contratos assinados pelos Solicitantes (fila no método 'FIFO'), com exceção dos casos de reagendamento (citado no passo S.08) ou de 2º ciclo (passo A.01) de auditoria, os quais terão prioridade na obtenção das datas mais próximas disponíveis. Não há prazo máximo pré-determinado para a data de início da auditoria, já que tal prazo dependerá da quantidade de contratos celebrados e ainda não auditados ("fila de espera") e da duração de cada auditoria, o que poderá variar conforme o enquadramento de cada S-RES.

O Gerente do CC efetuará, também, a seleção dos auditores dentro do quadro de auditores credenciados pela SBIS. Esta atividade será executada de acordo com as normas internas do CC, considerando, entre outros fatores, a rotatividade entre os auditores, a disponibilidade dos mesmos e eventuais impedimentos por questões éticas ou profissionais. Cada auditoria será executada obrigatoriamente por 03 (três) auditores *seniores*, e poderá ser acompanhada por um ou mais auditores *trainees*, cujos papéis encontram-se descritos no passo S.08 adiante e no capítulo 6.

[S.06] Envia a seleção dos auditores e o cronograma para aprovação

No prazo máximo de 10 (dez) dias úteis, o Gerente do CC encaminhará, por e-mail, a proposta de cronograma para a auditoria e a relação dos auditores selecionados ao Solicitante, para sua aprovação.

[S.07] Gerente do CC seleciona novos auditores e/ou elabora novo cronograma

Na eventualidade da rejeição, pelo Solicitante, da proposta de cronograma ou da relação de auditores, o Gerente do CC elaborará um novo cronograma e/ou selecionará outros auditores, seguindo os mesmos procedimentos adotados no passo S.05 acima.

[S.08] Auditores executam a auditoria e preenchem o caderno de resultados

Nas datas previstas no cronograma e utilizando os recursos apontados no passo P.08, a equipe de auditores realizará a auditoria do S-RES objeto da certificação.

Todas as sessões de auditoria serão gravadas, registrando-se, durante todo o tempo, os sons do ambiente e as imagens da tela (navegação e operação) do S-RES auditado.

Cada auditoria será executada obrigatoriamente por 03 (três) auditores *seniores* (ver capítulo 6), que solicitarão aos profissionais disponibilizados pelo Solicitante operarem o sistema. Serão executados todos os procedimentos (*scripts*) definidos no Manual Operacional de Ensaios e Análises para todos os requisitos obrigatórios das categorias nas quais o S-RES auditado se enquadra, verificando-se a obtenção ou não dos resultados esperados. Após a execução de cada *script*, cada auditor registrará o seu parecer em seu Caderno de Resultados, os quais serão consolidados pelo Gerente do CC ao final da auditoria. Caso haja divergência entre os resultados observados por cada auditor na avaliação de um determinado requisito, prevalecerá o resultado apontado pela maioria, ou seja, por 02 (dois) auditores, o qual passará a ser considerado como resultado final para tal requisito.

A auditoria poderá, ainda, ser acompanhada por um ou mais auditores *trainees* (ver capítulo 6), os quais participarão apenas com a finalidade de capacitação e progressão no processo de credenciamento, não sendo seus registros considerados no resultado da auditoria.

Caso a auditoria não seja realizada nas datas previstas devido a qualquer impossibilidade por parte do Solicitante, fundamentalmente por não disponibilizar algum recurso previsto no passo P.08, será elaborado um novo cronograma, mediante o pagamento, pelo Solicitante, da Taxa de Reagendamento de Auditoria. Caso o Solicitante comunique tal impossibilidade e solicite o reagendamento com mais de 05 (cinco) dias úteis de antecedência (fora o próprio dia) do início previsto para o primeiro dia da auditoria, o valor a ser pago será de 30% (trinta por cento) da referida taxa.

Caso a auditoria não seja realizada nas datas previstas devido a qualquer impossibilidade por parte da SBIS, será elaborado um novo cronograma, isento de qualquer taxa adicional.

A elaboração de um novo cronograma, independentemente do motivo, compreende a execução do passos S.05, S.06, S.07, P.06, P.07 e P.08. Deve-se observar que qualquer alteração no cronograma poderá provocar uma consequente alteração da seleção dos auditores, caso haja conflitos nas agendas dos auditores previamente selecionados.

[S.09] Comitê de Certificação avalia o resultado da auditoria

Todos os meses, uma vez por mês, conforme cronograma definido oportunamente, o Comitê de Certificação (ver capítulo 6) se reunirá para a discussão e avaliação das auditorias realizadas no período (desde a reunião antecedente), emitindo um parecer unificado para cada auditoria. Este parecer poderá indicar a aprovação ou reprovação do S-RES na auditoria realizada. Após a auditoria inicial (primeiro ciclo), o Comitê poderá recomendar ao Solicitante a realização de ajustes no S-RES para a execução de um

segundo ciclo de auditoria, ainda dentro do mesmo processo original, cujo parecer indicará, finalmente, a aprovação ou reprovação do S-RES.

Conforme já exposto anteriormente, para a obtenção da certificação, o S-RES deverá demonstrar, em sua auditoria, conformidade a todos os requisitos obrigatórios das categorias nas quais se enquadra.

Dentre os membros do Comitê que avaliarem um específico S-RES e respectivas auditorias, não poderão estar auditores que participaram das auditorias daquele S-RES.

[S.10] S-RES aprovado?

O Comitê de Certificação fará o encaminhamento do processo com o resultado de seu parecer à Diretoria da SBIS para que esta proceda à emissão e envio do Certificado e Selo ao Solicitante (passo S.11 adiante) ou à comunicação da reprovação ao Solicitante (passo S.12 adiante).

Conforme já mencionado anteriormente, o Comitê poderá recomendar ao Solicitante a realização de ajustes no S-RES para a execução de um segundo ciclo de auditoria (passo A.01).

[S.11] Diretoria emite e envia o Certificado e o Selo, e os publica no site

No prazo máximo de 05 (cinco) dias úteis após a aprovação pelo Comitê de Certificação, a Diretoria da SBIS emitirá e enviará ao Solicitante o Certificado e o Selo de Certificação SBIS/CFM (ver item 4.6.) em arquivos eletrônicos e em papel, e os publicará no sítio da Certificação na internet. Em seguida, encerrará e arquivará o processo (passo S.04).

Dentre os membros da Diretoria que decidirem sobre a certificação de um específico S-RES, não poderão estar auditores nem membros do Comitê de Certificação que participaram da avaliação daquele S-RES.

[S.12] Comunica a reprovação

No prazo máximo de 05 (cinco) dias úteis após a reprovação pelo Comitê de Certificação, a Diretoria da SBIS comunicará tal fato por escrito ao Solicitante, justificando os motivos e apontando explicitamente os resultados negativos que determinaram tal reprovação.

[S.13] Gerente do CC e auditores revisam os registros e resultados da auditoria

Ao receber uma solicitação de revisão de resultado de auditoria, o Gerente do CC se reunirá com os auditores que executaram a auditoria contestada. A partir dos argumentos expostos pelo Solicitante na solicitação e com o apoio das imagens e sons gravados durante as sessões de auditoria, o grupo reavaliará os resultados apontados e emitirá um documento que poderá ratificar ou retificar os resultados originais.

5.1.3. Sub-Processos Alternativos

Os processos aqui descritos representam subconjuntos de atividades integrantes do processo padrão, e são compostos de atividades executadas tanto pela SBIS quanto pelo Solicitante.

[A.01] Ajustes e 2º ciclo de auditoria

Ao concluir a auditoria de um S-RES, a SBIS poderá, exclusivamente a seu critério, considerando a quantidade e abrangência das não-conformidades identificadas, proporcionar ao Solicitante oportunidade para que este realize no S-RES os ajustes necessários à solução das não-conformidades apontadas na auditoria, Em seguida, será executado um segundo ciclo de auditoria, ainda dentro do mesmo processo. Caso o Solicitante aceite tal oportunidade, deverá efetuar o pagamento da Taxa de Realização de 2º Ciclo de Auditoria (ver item 4.7.).

O prazo máximo para a realização dos ajustes será de 90 (noventa) dias corridos a partir da comunicação da SBIS ao Solicitante, devendo a nova auditoria (2º ciclo) ser realizada na data mais próxima disponível após este período. A nova auditoria será realizada obrigatoriamente sobre o mesmo S-RES e na mesma configuração originalmente auditadas, atualizando-se apenas a versão constante no processo para a nova versão resultante dos ajustes efetuados pelo Solicitante, a qual deverá conter apenas as alterações necessárias à solução das não-conformidades apontadas.

Este passo compreende a execução, por parte da SBIS, do passos S.05, S.06, S.07 e S.08, e por parte do Solicitante dos passos P.06, P.07 e P.08, todos descritos anteriormente neste manual. Deve-se atentar para que a somatória dos prazos estipulados para cada passo não ultrapasse o prazo máximo definido para o presente processo.

Este passo poderá ser realizado uma única vez dentro de um processo de certificação, não sendo passível de repetição. Caso este segundo ciclo de auditoria ainda aponte para não-conformidades, independentemente da quantidade ou abrangência das mesmas, o S-RES terá sua certificação rejeitada.

5.2. Processo para Extensão da Certificação

Este é o processo a ser seguido para a obtenção de extensões da certificação para outras configurações ou versões de um S-RES já certificado, conforme descrito no item 4.5.

Este processo segue o mesmo fluxo de atividades descrito para o processo padrão (ver item 5.1. , Figura 1), exceto nos pontos destacados a seguir:

a) Toda referência à Ficha de Inscrição para Certificação deve ser substituída pela Ficha de Inscrição para Extensão de Certificação (ver item 4.6.);

b) Onde há referência à assinatura e envio do Contrato de Certificação, deve-se considerar a assinatura e envio do Termo de Extensão de Certificação (ver item 4.6.), o qual se constitui de um aditivo a um contrato previamente firmado entre a SBIS e o Solicitante;

c) Toda referência à Taxa de Certificação deve ser substituída pela Taxa de Extensão de Certificação (ver item 4.7.);

d) Dependendo do tipo (outra configuração ou nova versão) e abrangência da extensão solicitada, a SBIS poderá, exclusivamente a seu critério, dispensar a necessidade de realização de auditoria do S-RES inscrito, não sendo executadas, neste caso, as atividades pertinentes ao cronograma de auditoria e seleção de auditores existentes no passo S.05, e nem executados os passos S.06, S.07, S.08, P.06, P.07, P.08 e A.01, os quais deverão ser desconsiderados. Também deverão ser desconsideradas as referências à auditoria nos passos S.09, S.10, S.13 e P.09, considerando-se, no seu lugar, a decisão quanto à concessão ou não da extensão pretendida.

5.3. Apelações, Reclamações e Disputas

Todas as apelações, reclamações e disputas apresentadas à SBIS pelos Solicitantes, outros fornecedores, clientes ou outras partes interessadas, serão registradas pela Secretaria da SBIS e encaminhadas ao Gerente do Centro de Certificação e à Diretoria da SBIS para solução.

Toda a apelações, reclamações e disputas serão devidamente analisadas e realizadas as ações apropriadas para sanar as deficiências apontadas e confirmadas. Se o reclamante se identificar, deverá ser fornecida resposta formal.

Caso a reclamação refira-se a um Cliente Certificado, este será comunicado formalmente e será intimado a apresentar resposta formal, sob pena de aplicação de sanção, que irá desde a advertência até a eventual suspensão do certificado, a critério da Diretoria da SBIS.

5.4. Auditorias Internas do Processo de Certificação

A SBIS realizará auditorias internas periódicas, de maneira planejada e sistemática, abrangendo todos os procedimentos, para verificar se os processos se desenvolvem de maneira regular, de acordo com as disposições planejadas. Os resultados das auditorias internas serão documentados e levados ao conhecimento da Diretoria da SBIS, que determinará a realização de ações para corrigir as desconformidades detectadas e suas causas, no devido tempo e de maneira apropriada.

As auditorias internas serão realizadas por pessoal indicado pela Diretoria da SBIS e independente das atividades auditadas.

6. Estrutura do Centro de Certificação da SBIS

O Centro de Certificação (CC) é o departamento interno da SBIS responsável pela operacionalização do processo de Certificação SBIS/CFM. Localizado na sede da SBIS e subordinado à sua Diretoria, é composto por colaboradores com dedicação não-exclusiva, os quais serão contratados conforme a demanda observada ao longo da implantação desta Fase 2 da Certificação.

São apresentados, a seguir, os papéis desempenhados pelo Centro de Certificação:

6.1. Comitê de Certificação

Trata-se de comitê formado por 03 (três) pessoas, com a seguinte composição:

- 01 (um) integrante da Coordenação do GICSP (Coordenador, Vice-Coordenador ou Secretário);
- 01 (um) membro representante do CFM;
- 01 (um) membro indicado pela Diretoria da SBIS.

Compete ao Comitê:

- Auxiliar no desenvolvimento das políticas relativas à imparcialidade das atividades de certificação;
- Impedir qualquer tendência por parte da SBIS em permitir que interesses comerciais ou outros impeçam a provisão regular e objetiva de atividades de certificação;
- Aconselhar sobre questões que afetem a confiança na certificação, incluindo transparência e imagem pública;
- Realizar uma análise crítica, pelo menos uma vez por ano, da imparcialidade dos processos de auditoria, certificação e tomada de decisão da SBIS;
- Avaliar as auditorias realizadas e os atos do Gerente do Centro de Certificação e emitir pareceres indicativos de aprovação ou reprovação dos procedimentos do Centro de Certificação.

O Comitê de Certificação terá acesso a todas as informações necessárias para possibilitar o cumprimento de suas funções.

6.2. Gerente do Centro de Certificação

O Centro de Certificação, unidade funcional da SBIS na qual são desenvolvidas as principais atividades do Processo de Certificação SBIS/CFM, é gerenciado em todas suas ações, tanto no âmbito interno quanto no relacionamento com os Solicitantes, Clientes Certificados e demais interessados na certificação por um profissional contratado pela Diretoria da SBIS e nomeado como Gerente do Centro de Certificação.

Compete ao Gerente do Centro de Certificação:

- Analisar as solicitações de certificação;
- Elaborar e gerir os contratos com os Solicitantes;
- Elaborar contratos com os profissionais envolvidos;

- Elaborar cronogramas;
- Convocar os auditores;
- Responder as dúvidas e questionamentos sobre o processo de certificação e
- Interagir com a Diretoria da SBIS nas questões pertinentes à certificação.

6.3. Auditores

O Centro de Certificação conta com um quadro de auditores credenciados para a execução das auditorias dos S-RES submetidos à certificação.

Compete aos auditores:

- Realizar as auditorias conforme as regras estabelecidas pela SBIS;
- Documentar todos os resultados obtidos, de forma objetiva e sem influência de valores ou opiniões pessoais;
- Declarar-se impedido quando houver algum conflito de interesse que impeça a realização do trabalho com objetividade e imparcialidade;
- Manter em sigilo, permanentemente, todas as informações sobre o Solicitante, o S-RES e a certificação a que tenha acesso em razão de sua participação no processo de certificação;
- Não estar envolvido, diretamente ou indiretamente, com a organização cujo S-RES está sendo avaliado, com seus fornecedores, clientes, concorrentes ou outra qualquer parte interessada, de maneira tal que sua imparcialidade possa ser comprometida.

Para se tornar um auditor do Centro de Certificação, o profissional deve obrigatoriamente atender aos seguintes requisitos:

- Ser Membro Titular da SBIS e estar em dia com suas obrigações perante a mesma;
- Ter realizado e sido aprovado no Curso para Auditores do Centro de Certificação da SBIS;
- Para se tornar um auditor *senior*, o auditor deve ter participado de, no mínimo, duas auditorias na condição de *trainee*.

O processo de credenciamento de auditores, incluindo as regras detalhadas e a programação das turmas do respectivo curso, estará, em breve, disponível no sítio da SBIS na internet.

6.4. Secretaria

A Secretaria do Centro de Certificação é responsável pelos aspectos administrativos e burocráticos do Centro, e apóia seus membros, especialmente o Gerente, nas atividades relacionadas à certificação.

Enquanto o volume de trabalho assim o permitir, a Secretaria do Centro de Certificação será realizada pela Secretária Administrativa da SBIS.

Compete também à Secretaria:

- Controlar todos os documentos, dados e registros relativos à certificação, garantindo o controle do acesso e da distribuição das informações às pessoas

autorizadas e garantindo a confidencialidade, integridade e atualidade das informações mantidas. Os documentos obsoletos e o registros devem ser mantidos por um período de tempo não inferior a cinco anos;

- Manter registros de qualificação, treinamento e experiência e compromisso pertinentes de cada pessoa envolvida no processo de certificação.

6.5. Diretoria da SBIS

Compete à Diretoria da SBIS, concomitantemente e sem prejuízo de suas atribuições estatutárias:

- Garantir a existência de estrutura interna que salvaguarde a imparcialidade da SBIS na certificação e que permita a participação de todas as partes com interesse significativo no desenvolvimento de políticas e princípios relativos ao conteúdo e funcionamento do sistema de certificação;
- Formular políticas relativas à operação da certificação;
- Supervisionar a implementação de suas políticas;
- Definir as bases técnicas para conceder a certificação;
- Nomear recursos humanos e estruturas internas envolvidos no processo de certificação e determinar suas respectivas autoridades e responsabilidades, empregando um número suficiente de pessoas que tenham a necessária formação, treinamento, conhecimento técnico e experiência para desempenhar as funções de certificação, sob a responsabilidade do Gerente do Centro de Certificação;
- Garantir que os recursos humanos e as estruturas envolvidas estejam livres de quaisquer pressões comerciais, financeiras e outras que possam influenciar os resultados do processo de certificação;
- Garantir que os recursos humanos e as estruturas envolvidas mantenham a confidencialidade das informações obtidas através das atividades de certificação, em todos os níveis da organização, incluindo também comitês, organismos externos ou pessoas atuando em seu nome;
- Estabelecer instruções documentadas para a equipe envolvida na certificação, conforme necessário, descrevendo seus deveres e responsabilidades;
- Exigir que os recursos humanos envolvidos no processo de certificação assinem Termos de Compromisso de Conduta no qual se comprometem a: i) obedecer às regras definidas pela SBIS, inclusive aquelas relativas à confidencialidade e independência de interesses comerciais e outros interesses; ii) declarar qualquer associação, presente ou passada, direta ou indireta, da sua parte com o Solicitante para cuja avaliação ou certificação venha a ser designado;
- Elaborar as decisões finais sobre a concessão, manutenção, extensão, suspensão e cancelamentos dos certificados;
- Estabelecer políticas e procedimentos para a solução de reclamações, apelações e disputas recebidas de fornecedores ou de outras partes, sobre o tratamento dado à certificação ou quaisquer outras matérias relacionadas;
- Supervisionar as finanças da SBIS e a garantia de existência de estabilidade financeira e recursos necessários para a operação do sistema de certificação, incluindo mecanismos adequados para cobrir responsabilidades legais decorrentes das suas operações e/ou atividades de certificação;
- Realizar análises críticas documentadas do sistema de certificação, em intervalos definidos, que sejam suficientemente breves para assegurar a contínua adequação e eficácia em satisfazer aos requisitos e às políticas.

7. Uso da Informação Relacionada com a Certificação

A certificação de S-RES foi inicialmente concebida como uma maneira de garantir a legalidade da substituição do papel por sistemas computadorizados quando da captura, armazenamento, manuseio e transmissão de dados identificados em saúde.

Dentre os benefícios que a Certificação SBIS/CFM traz para o mercado de saúde no Brasil, destacam-se:

- Conscientizar o mercado quanto à importância de funcionalidades básicas em S-RES;
- Diminuir o risco enfrentado por médicos e instituições de saúde na seleção e compra de S-RES;
- Redirecionar as prioridades de investimentos em informática em saúde, considerando aspectos relevantes para a melhoria da qualidade, segurança e eficiência de sistemas informatizados;
- Contribuir para a confidencialidade e privacidade das informações de saúde ao demandar que os S-RES atendam requisitos de segurança adequados, e garantir a legalidade das informações armazenadas nestes sistemas pelo uso de tecnologia reconhecida no país (ICP/Brasil);
- Aumentar o uso da informática em saúde no Brasil, e consequentemente melhorar a eficiência e a eficácia do sistema de saúde brasileiro.

Apesar do processo de certificação ser voluntário, a expectativa é que desenvolvedores de S-RES busquem a certificação como forma de diferenciação dos seus softwares no mercado, utilizando o fato do sistema ter sido certificado como parte importante de suas estratégias de marketing. De forma análoga, espera-se que médicos e instituições de saúde privilegiem S-RES certificados.

A informação relacionada à Certificação SBIS/CFM deverá ser utilizada de acordo com as diretrizes apresentadas abaixo. Estas diretrizes devem ser observadas para a confecção de qualquer material de marketing (folhetos, folders, embalagens, manuais, brindes, etc.), incluindo todas as formas de comunicação com o mercado (mídia impressa, rádio, televisão, internet, etc.).

No caso de *press releases* mencionando a SBIS, CFM ou a Certificação SBIS/CFM, é obrigatória a consulta prévia à SBIS, sendo necessária autorização desta por escrito para a divulgação do material à imprensa.

Apenas os Clientes Certificados poderão divulgar o respectivo S-RES como sendo certificado pela SBIS/CFM. Caso tal certificado seja revogado ou tenha sua validade expirada, os materiais de marketing que façam referência ao mesmo não poderão ser distribuídos ou divulgados.

As pessoas ou instituições que divulgarem informações relacionadas com a Certificação SBIS/CFM de modo não previsto nestas diretrizes serão chamados a responder por tais atos. Caso trate-se de um S-RES certificado, o mesmo poderá ter sua certificação revogada.

7.1. Referências ao Estado de S-RES Certificado

Ao fazer qualquer referência a um S-RES certificado pela SBIS/CFM, uma empresa ou instituição deverá indicar claramente:

- O nome da empresa ou instituição
- O nome do produto (S-RES) certificado
- A versão do produto (S-RES) certificado
- O ano-base dos requisitos considerados na certificação (ano que aparece no selo de certificação)
- As categorias certificadas

Desta forma, é válido o seguinte exemplo de citação: “O (nome do S-RES e versão) desenvolvido pela (Nome da empresa) recebeu a Certificação SBIS/CFM na(s) categoria(s) (indicar categorias) com base nos requisitos de (ano-base requisitos)". Exemplo: “O sistema YYY, versão 9.99 da ZZZ LTDA recebeu a Certificação SBIS/CFM na categoria Ambulatorial NGS1 com base nos requisitos de 2009”.

É vetado ao Cliente Certificado usar a certificação de maneira a prejudicar a imagem da SBIS ou do CFM, assim como fazer qualquer declaração sobre a certificação que a SBIS ou o CFM possa considerar indevida ou não autorizada.

A Certificação SBIS/CFM indica que um S-RES foi testado em relação a um conjunto de requisitos de segurança, estrutura, conteúdo e funcionalidade, bem como a aderência ao padrão TISS, e que durante a auditoria todos os requisitos especificados em cada categoria apontada no Selo de Certificação foram integralmente verificados. Estes requisitos para a certificação são um conjunto objetivo de critérios a serem considerados em um processo de avaliação de qualquer S-RES, facilitando o processo de busca e comparação entre sistemas disponíveis no mercado, e diminuindo os riscos enfrentados por qualquer organização interessada em adotar um novo S-RES.

7.2. Uso do Selo de Certificação SBIS/CFM

Figura 2: Modelo ilustrativo do Selo de Certificação SBIS/CFM

Apenas os S-RES que tenham sido certificados pela SBIS/CFM terão o direito, não exclusivo, de utilizar o selo SBIS/CFM em seus respectivos manuais e materiais promocionais durante o período de vigência do respectivo certificado (ver item 4.4.).

O selo deverá ser utilizado de modo que fique legível, mantendo as mesmas proporções, cores e aparência do selo original, não podendo ser de qualquer modo estilizado. O selo não poderá, em nenhuma hipótese, ser apresentado com destaque maior do que o nome do S-RES ou da organização responsável por sua comercialização.

Se o selo for utilizado em uma página *web*, é necessário identificar claramente dentre os produtos apresentados na página, quais são os S-RES e respectivas versões que estão de fato certificados e quais não estão. Além disto, o selo deverá fornecer um *link* vinculado à sua imagem que, ao ser acionado ("clicado"), remeta o usuário à página do sítio da SBIS na internet onde sejam apresentadas as informações do S-RES detentor de tal selo.

7.3. Referências ao Processo de Certificação

A Certificação SBIS/CFM foi elaborada com base no estado da arte em certificação de sistemas de informação e as mais recentes normas e recomendações sobre características e funcionalidades necessárias para constituir um S-RES. Foram consideradas inúmeras referências nacionais e internacionais, assim como a realidade brasileira, gerando como produto um conjunto de requisitos compatível com o estágio atual do mercado brasileiro, assegurando níveis apropriados de segurança, confiabilidade e sofisticação.

Todo o processo foi amplamente debatido com a sociedade, através de inúmeras apresentações em congressos e seminários, além de audiências públicas realizadas especificamente para validar e aprimorar todas as etapas da certificação. Merece destaque o empenho do Grupo de Interesse em Certificação de Software e Padrões da SBIS, composto por voluntários que dedicaram inúmeras horas para contribuir com a melhoria e aperfeiçoamento da certificação como um todo.

A auditoria realizada em um S-RES será feita com base em cenários reais de utilização de sistemas de registro eletrônico em saúde, concebidos de modo a testá-los de forma rigorosa, garantindo o nível de funcionalidade e segurança demandados pela sociedade em geral.

A Certificação SBIS/CFM contribui para o aumento na adoção das Tecnologias da Informação na área da saúde, facilitando a escolha de sistemas por instituições, médicos e outros profissionais da saúde que não são especialistas em TI. Ao mesmo tempo, indica as características e funcionalidades necessárias para a construção de sistemas úteis e confiáveis, ajudando os desenvolvedores de S-RES a evoluírem na direção de sistemas cada vez mais efetivos, seguros e completos.

7.4. Reclamações de Solicitantes e Clientes Certificados

Os Solicitantes e os Clientes Certificados deverão:

- Manter os registros de todas as reclamações de qualquer parte interessada trazidas ao seu conhecimento relativas à conformidade do produto com os requisitos da Certificação SBIS/CFM e das ações subsequentes tomadas, que deverão ser disponibilizados à SBIS sempre que solicitados;

- Tomar ações apropriadas com respeito às reclamações e quaisquer deficiências encontradas no produto ou serviços que afetem o atendimento aos requisitos para certificação.

8. Requisitos de Conformidade

O capítulo 2.1. apresenta uma descrição resumida de cada um dos padrões utilizados na elaboração dos requisitos. Vários destes padrões descrevem características e funcionalidades que idealmente devem estar presentes em um S-RES, independentemente do seu nicho de aplicação. As características e funcionalidades existentes em padrões respeitados nacional ou internacionalmente podem e devem ser utilizadas como base para facilitar a avaliação de um S-RES, bem como para o planejamento de novas versões de S-RES ao longo do tempo (incorporando características e funcionalidades existentes no padrão, mas ainda não disponíveis no sistema).

Do ponto de vista do processo de certificação, é necessário estabelecer critérios objetivos que possam ser utilizados de modo uniforme em cada auditoria, garantindo que os S-RES avaliados tenham as mesmas chances de serem ou não aprovados no processo, independentemente dos auditores envolvidos.

Os requisitos obrigatórios da Certificação SBIS/CFM foram extraídos dos padrões acima mencionados. Destes padrões foram selecionados os requisitos mais adequados à realidade brasileira. Vários requisitos obrigatórios no cenário internacional foram definidos como recomendáveis ou opcionais neste manual. Estes devem ser vistos como funcionalidades ou características desejáveis para futuros desenvolvimentos.

Os requisitos da certificação SBIS/CFM foram agrupados da seguinte forma:

- Requisitos de Segurança
- Requisitos de Estrutura, Conteúdo e Funcionalidades para S-RES Assistencial
- Requisitos para GED
- Requisitos para TISS

Os próximos capítulos apresentam todos os requisitos que compõem a Certificação SBIS/CFM, exibidos de forma tabular com as seguintes informações:

Coluna	Descrição
ID	Identificação do requisito, utilizando codificação padronizada
Requisito	Nome do requisito
Referência	Padrão de referência que deu origem ao requisito
Conformidade	Descrição do requisito, incluindo exemplos sempre que apropriado. Adicionalmente, pode incluir indicações de como o requisito será avaliado durante a auditoria
Presença	**M – Mandatório**: Deve ser obrigatoriamente atendido pelo S-RES. **R – Recomendado**: Requisito com alta probabilidade de tornar-se obrigatório nas próximas versões. **O – Opcional**: Requisito relevante, porém de adoção opcional. **X – Não se aplica**: Requisito não aplicável à situação apresentada.

Os requisitos com a presença "R" (Recomendado) tratam-se, geralmente, de requisitos já obrigatórios nos padrões de referência, como os da CEE-IS/ABNT e do Comitê ISO/TC 215. Porém, encontram-se aqui apenas como "recomendados" com o objetivo de preparar o mercado desenvolvedor e permitir que sejam implementados gradualmente. É indicado, portanto, que os desenvolvedores adotem ações para atender estes requisitos nas próximas versões de seus S-RES.

Nos requisitos do Nível de Garantia de Segurança 1 (NGS1), a coluna "Presença" está dividida entre "Local" e "Remoto", refletindo como cada requisito deve ser considerado de acordo com o enquadramento do S-RES que está sendo auditado (ver item 8.1.).

O Manual Operacional de Ensaios e Análises para Certificação de S-RES apresenta os *scripts* de teste para verificação da conformidade de todos os requisitos mandatórios (M). Os demais requisitos (recomendados e opcionais) somente terão *scripts* de teste divulgados a partir do momento em que tornarem-se mandatórios.

8.1. Introdução aos Requisitos

8.1.1. Segurança

Os requisitos de segurança de um S-RES são fundamentais para garantir a privacidade, confidencialidade e integridade da informação identificada em saúde. Uma das principais motivações do CFM ao participar deste processo de certificação foi o de garantir o sigilo profissional, ou seja, que o acesso à informação identificada só possa ser feito por pessoas autorizadas. Aos interessados em eliminar o registro das informações em papel, é obrigatória a conformidade ao Nível de Garantia de Segurança 2 (NGS2), que contempla o uso de certificados digitais, conforme descrito abaixo.

O Processo de Certificação SBIS/CFM classifica os S-RES, do ponto de vista de segurança da informação, em dois Níveis de Garantia de Segurança (NGS):

- **NGS1** - categoria constituída por S-RES que **não** contemplam o uso de certificados digitais ICP-Brasil para assinatura digital das informações clínicas, consequentemente sem amparo para a eliminação do papel e com a necessidade de impressão e aposição manuscrita da assinatura;

- **NGS2** - categoria constituída por S-RES que viabilizam a eliminação do papel nos processos de registros de saúde. Para isso, especifica a utilização de certificados digitais ICP-Brasil para os processos de assinatura e autenticação. **Para atingir o NGS2 é necessário que o S-RES atenda aos requisitos já descritos para o NGS1 e apresente ainda total conformidade com os requisitos especificados para o Nível de Garantia 2**.

Recomenda-se, para ambos os níveis, a observância das boas práticas para a gestão da segurança da informação descritas na norma NBR ISO/IEC 27.002[13] publicada pela ABNT, adaptadas às necessidades organizacionais de cada instalação do S-RES.

A Certificação SBIS/CFM considera no seu processo de auditoria o nível de segurança para o qual o S-RES se declara em conformidade, já que o NGS2 incorpora todos os requisitos do NGS1, e prevê um conjunto adicional de requisitos.

Os S-RES auditados no NGS1 devem possuir todas as características necessárias para que uma perícia técnica possa tirar conclusões satisfatórias sobre a validade ou não das informações por ele armazenadas. As conclusões da perícia levarão em consideração também a forma como o sistema está sendo utilizado, já que o S-RES, por si só, não será suficiente para garantir a legitimidade de qualquer informação. Por exemplo, o S-RES possui mecanismos para validar seus usuários através de identificação e senha, mas este mecanismo se torna irrelevante na medida em que todos os usuários do sistema usam a mesma identificação e senha para acessar o sistema.

Já os S-RES classificados como NGS2 estarão, a princípio, autorizados a substituir o papel, em conformidade com a ICP-Brasil, desde que atendam integralmente aos requisitos obrigatórios de estrutura, conteúdo e funcionalidades (ver item 8.1.2). Recomenda-se que as instituições que queiram substituir o papel façam também a certificação de aderência à Norma ABNT NBR ISO/IEC 27.001:2006[20] junto a Organismos Acreditados de Certificação.

O uso efetivo de certificados digitais, em conjunto com a observância dos demais requisitos de segurança, dependerá também da forma como o S-RES for utilizado por seus usuários.

Para efeito da certificação SBIS/CFM, os S-RES foram classificados em:

- **Acesso Local** - todo S-RES instalado num único computador, com acesso ao sistema apenas neste equipamento. Além disso, um S-RES de acesso local não deverá permitir o acesso simultâneo por mais de um usuário.

- **Acesso Remoto** - todo S-RES que permite o acesso simultâneo ao sistema, no computador onde o S-RES está instalado, ou em computador remoto, através de algum tipo de conexão (rede local, conexão sem-fio, internet, etc.).

8.1.2. Estrutura, Conteúdo e Funcionalidades para S-RES Assistencial

Conforme já exposto no item 3.1. , a categoria S-RES Assistencial está voltada para S-RES ambulatoriais nesta versão do manual. Sistemas voltados a outros tipos de atendimento assistencial, como sistemas de informação hospitalar, vigilância epidemiológica, medicina ocupacional, e SADT serão gradualmente contemplados nesta categoria em futuras versões do manual.

8.1.3. GED

Os requisitos para sistemas de GED (Gerenciamento Eletrônico de Documentos) contemplam as necessidades básicas a este tipo de recurso para a digitalização, guarda e manuseio dos prontuários em meio eletrônico, atendendo fundamentalmente a Resolução CFM Nº 1821/2007.

8.1.4. TISS

Os requisitos específicos para verificar a aderência ao padrão TISS refletem o conteúdo da RN 153, de 29/05/2007, da ANS. Os requisitos foram agrupados em conteúdo, estrutura e comunicação de dados, para que assim um sistema possa ser considerado em conformidade com o TISS. Além disto, é preciso distinguir se o S-RES tem como foco a automação de operadoras de planos de saúde (médico e/ou odontológico) ou a automação de prestadores de serviços de saúde (categorias 1, 2 e 3). Esta subdivisão respeitou os agrupamentos adotados pela ANS, conforme apresentado no item 3.1.

Cabe ainda lembrar que na definição dos requisitos de conteúdo e estrutura para S-RES utilizados por Prestadores pertencentes ao Grupo 1, foi ainda necessário distinguir entre S-RES para SADTs isolados, e S-RES para todos os demais tipos de instituição contidos neste grupo.

Os conjuntos de requisitos TISS devem ser atendidos conforme o seguinte esquema (Tabela 2), considerando-se o tipo do serviço prestado e as categorias descritas no item 3.1. :

Tabela 2 - Esquema de conjuntos de requisitos TISS

	A	**B**	**C**	**D**
	Prestador	**Comunicação "Lado" Prestador**	**Comunicação "Lado" Operadora**	**Operadora**
Grupo 1	TISS.01	TISS.06	TISS.08	TISS.04
Grupo 2	TISS.02			
Grupo 3	TISS.03	TISS.07	TISS.09	TISS.05

Para facilitar o entendimento do esquema acima, podem ser consideradas as seguintes possibilidades:

- Sistemas voltados ao uso dos Prestadores devem atender os requisitos da coluna A;
- Sistemas voltados ao uso dos Prestadores e que também efetuam a comunicação com as Operadoras, devem atender os requisitos das colunas A e B;
- Sistemas voltados ao uso das Operadoras devem atender os requisitos da coluna D;
- Sistemas voltados ao uso das Operadoras e que também efetuam a comunicação com os Prestadores, devem atender os requisitos das colunas C e D;
- Sistemas voltados apenas à comunicação entre Prestadores e Operadoras (caso típico das empresas de conectividade) devem atender os requisitos das colunas B e C.

Delimitadas as colunas aplicáveis, deve-se então cruzá-las com as devidas linhas da tabela, conforme os grupos definidos pela ANS (ver Tabela 1), para se obter os conjuntos de requisitos a serem atendidos para a certificação.

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

NGS1.01 - Controle de versão do software

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.01.01	Versão software	HL7 ERH-S FM IN4.2 ABNT NBR ISO/IEC 27001:2006 A.12.5	Todos os componentes do S-RES devem possuir versão do software associada a uma única referência (nome, fornecedor e número de versão) e não ambígua. O S-RES deve possuir funcionalidade que permita a visualização da versão de seus componentes de software por parte do usuário.	M	M
NGS1.01.02	Código fonte	HL7 ERH-S FM IN5.2 ABNT NBR ISO/IEC 27001:2006 A.12.5	Deve ser possível, a partir do número de versão de cada componente do S-RES, resgatar os códigos-fonte correspondentes, possibilitando a rastreabilidade dos arquivos fontes que o geraram.	R	R
NGS1.01.03	Histórico de alteração	HL7 ERH-S FM IN4.2	Manter histórico descritivo de todas as alterações realizadas em cada versão, contendo a data e o responsável pela alteração.	R	R
NGS1.01.04	Repositório de versões	HL7 ERH-S FM IN4.2	Ter um repositório estruturado com todas as versões dos componentes (executáveis e códigos-fonte) que foram utilizadas em produção em algum momento, permitindo voltar versões anteriores em casos de atualizações mal sucedidas.	R	R
NGS1.01.05	Dependências dos componentes	HL7 ERH-S FM IN5.2	Para cada versão de cada componente, indicar no manual de instalação e requisitos de sistema quais são as dependências com outros componentes do S-RES ou do ambiente, e os requisitos de operação. Por exemplo, informar que uma determinada versão de componente é compatível com o padrão HL7 versão 2.x (requisito de operação), que roda em um determinado sistema operacional (requisito de ambiente), que depende de um específico sistema de diretório para autenticação de usuários.	R	R

NGS1.02 - Identificação e autenticação de usuário

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.02.01	Identificação e autenticação do usuário	HL7 ERH-S FM IN1.1; ABNT NBR ISO/IEC 27001:2006 A.11.5.2	Todo usuário deve ser identificado e autenticado antes de qualquer acesso a dados do S-RES.	M	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.02.02	Método de autenticação	HL7 ERH-S FM IN1.1 ABNT NBR ISO/IEC 27001:2006 A.11.5.1	Utilizar, no mínimo, um dos seguintes métodos de autenticação: • Usuário e senha; • Certificado digital; • *One Time Password* (OTP); e/ou • Biometria. Nota: Na utilização de outro método de autenticação, este será avaliado.	M	M
NGS1.02.03	Proteção dos parâmetros de autenticação	SBIS	Todos os dados ou parâmetros utilizados no processo de autenticação de usuário devem ser armazenados de forma protegida. Por exemplo, armazenar somente o código *hash* da senha do usuário e garantir que o local de armazenamento possua restrições de acesso. Deve ser utilizado algoritmo reconhecidamente seguro como, por exemplo: • SHA-1; • SHA-2. Nota: Em tecnologias que utilizam o conceito de semente para geração de código, a semente deve ser protegida contra acesso não autorizado e alteração.	M	M
NGS1.02.04	Segurança de senhas	ABNT NBR ISO/IEC 27001:2006 A.11.5.3	Condição: Utilização de autenticação baseada em usuário/senha. Utilizar os seguintes controles de segurança: • Qualidade da senha: verificar a qualidade da senha no momento de sua definição pelo usuário, obrigando a utilização de, no mínimo, 8 caracteres dos quais, no mínimo, 1 caractere deve ser não alfabético; • Periodicidade de troca de senhas: o S-RES deve ter funcionalidade de obrigar a troca de senhas pelos usuários, em um período máximo configurável; • Armazenar a senha de forma codificada. Como exemplo, armazenar somente o código *hash.*	M	M
NGS1.02.05	Controle de tentativas de *login*	ABNT NBR ISO/IEC 27001:2006 A.11.5.1	O S-RES deve ter mecanismos para bloquear o usuário após um número máximo configurável de tentativas inválidas de *login*.	M	M

NGS1.03 - Controle de sessão de usuário

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.03.01	Encerramento por inatividade	ABNT NBR ISO/IEC 27001:2006 A.11.5.5	Sessão de usuário deve ser encerrada após período configurável de inatividade, invalidando o parâmetro de controle da sessão como, por exemplo, o *cookie*.	M	M
NGS1.03.02	Segurança contra roubo de sessão de usuário	ABNT NBR ISO/IEC 27001:2006 A.10.8	A sessão de comunicação deve possuir controles de segurança a fim de não permitir o roubo da sessão do usuário. Nota:O roubo de sessão pode ser possível inclusive em sessões protegidas (ex. SSL/TLS). Por exemplo, se o controle de sessão for realizado através de *cookie* na URL, em determinadas situações, a URL da sessão de um usuário pode ser obtida e utilizada por outro usuário, personificando o usuário anterior.	X	M

NGS1.04 - Autorização e controle de acesso

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.04.01	Impedir acesso por entidades não autorizadas	HL7 ERH-S FM IN1.2 ABNT NBR ISO/IEC 27001:2006 A.11.6.1	Impedir acesso ao RES, S-RES e SGBD por entidades não autenticadas e não autorizadas.	M	M
NGS1.04.02	Mecanismo de controle de acesso ao RES	HL7 ERH-S FM IN1.2	Garantir que o acesso ao RES seja somente possível através do mecanismo de controle de acesso.	M	M
NGS1.04.03	Gerenciamento de usuários	HL7 ERH-S FM IN1.2 ISO/TS 18308:2004(E) PRS3.2	Permitir o gerenciamento de usuários (criação, inativação e modificação), gerenciamento de papéis (criação, inativação e modificação) e gerenciamento de grupos (criação, Inativação e modificação).	M	M
NGS1.04.04	Papéis relacionados à TI	SBIS	Suportar funcionalidades que permitam, no mínimo, as seguintes atividades: • Auditoria dos registros das atividades do sistema; • Configuração do sistema; • Gerenciamento de permissões; • Gerenciamento de usuários; • Realização e restauração de cópia de segurança.	R	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.04.05	Configuração de controle de acesso	HL7 ERH-S FM IN1.2; ABNT NBR ISO/IEC 27001:2006 A.11.6 ISO/TS 18308:2004(E) PRS3.3	Disponibilizar mecanismos necessários para que seja possível implementar a política de controle de acesso através da configuração dos perfis de acesso, considerando os papéis de usuário, dos grupos e das operações que podem ser realizadas, inclusive a diferenciação de operações de consulta e de inclusão/alteração. Considerar que um mesmo usuário pode possuir mais de um papel.	M	M
NGS1.04.06	Concessão de autorizações	HL7 ERH-S FM IN1.2	Garantir que haja ao menos um usuário responsável pela concessão de autorização e pelo controle de acesso aos recursos de acordo com o escopo de atuação, a política organizacional e legislação. Nota: Preferencialmente um usuário dedicado a esta atividade.	M	M

NGS1.04.07	Delegação de poder	SBIS	Condição: Intenção de fornecer suporte à delegação de poder.
			
			Sendo o atribuidor aquele responsável por autorizar a delegação de poder e o delegado aquele quem recebe a delegação de poder, então:
			• O atribuidor deve ser previamente autorizado para conceder tais autorizações;
			• A delegação de poder deve ser registrada no sistema;
			• A delegação de poder deve informar:
			  • O atribuidor;
			  • O delegado;
			  • O motivo
			  • O instante da concessão
			  • O período de vigência
			
			Nota: Como exemplo de delegação pode-se citar um médico que delega poder de entrada de informações ao RES de um paciente para uma enfermeira.
				M	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.04.08	Acesso ao RES pelo paciente.	HL7 ERH-S FM IN1.4	Garantir que o paciente possa ter acesso a todas as suas informações pessoais e clínicas armazenadas no S-RES. Caso o S-RES não permita acesso direto do próprio paciente ao S-RES, deve existir um papel de usuário que permita realizar esta atividade em nome do paciente. O paciente deverá poder levar consigo estas informações em formato eletrônico ou impresso. O sistema deverá disponibilizar uma interface para impressão de declaração do usuário de que está recebendo suas informações. Tanto no caso do paciente acessar diretamente as informações, quanto no caso da existência de um responsável direto pelo acesso a estas informações, as atividades de exportação de dados e impressão da declaração de recebimento devem ser registrada com, no mínimo, as seguintes informações: • Usuário que executou a atividade • Nome completo do paciente • Local e instante da operação	M	M
NGS1.04.09	Restrições de acesso ao RES adicionadas pelo paciente	HL7 ERH-S FM IN1.4	Permitir que o paciente possa adicionar restrições de acesso a uma determinada parte ou à totalidade de seu RES.	O	O

NGS1.05 - Disponibilidade do RES

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.05.01	Cópia de Segurança	ABNT NBR ISO/IEC 27001:2006 A.10.5	O S-RES deve permitir que a cópia de segurança atenda aos seguintes requisitos: • exportar os atributos de segurança em conjunto com os dados; • garantir na restauração de uma cópia de segurança e arquivamento que os atributos de segurança e suas associações sejam automaticamente recuperados, sem a intervenção do administrador; • assegurar que somente o usuário com papel de operador de backup possa exportar e restaurar uma cópia de segurança, garantindo que este usuário não tenha acesso direto às informações.	M	M
NGS1.05.02	Verificação de integridade na recuperação de dados	ABNT NBR ISO/IEC 27001:2006 A.10.5	Deve haver controle que garanta a verificação da integridade das informações na geração e na restauração da cópia de segurança.	M	M

NGS1.06 - Comunicação remota

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.06.01	Segurança da comunicação entre cliente e servidor	ABNT NBR ISO/IEC 27001:2006 A.10.9.2	A sessão de comunicação entre o componente cliente (do lado do usuário) e o componente servidor deve oferecer os seguintes serviços de segurança: autenticação do servidor, integridade dos dados e confidencialidade dos dados. Nota: Como exemplo, pode-se citar a utilização de protocolos como HTTPS (HTTP + SSL/TLS) e IPSEC.	X	M
NGS1.06.02	Controle de acesso do cliente ao servidor	ABNT NBR ISO/IEC 27001:2006 A.10.9.2	Em S-RES de acesso remoto, o acesso ao sistema deve ser restrito somente aos clientes previamente autorizados. Este controle de acesso pode ser realizado, por exemplo, pelo endereço IP do cliente.	X	R
NGS1.06.03	Restrição de dados transmitidos	ABNT NBR ISO/IEC 27001:2006 A.10.9.2	Em S-RES de acesso remoto os dados transmitidos ao componente cliente (lado do usuário) devem ser somente aqueles que serão apresentados ao usuário. Ou seja, todo e qualquer processamento relacionado à seleção de dados deve ser realizado no lado servidor.	X	M
NGS1.06.04	Segurança da comunicação entre componentes	ABNT NBR ISO/IEC 27001:2006 A.10.9.2	Em S-RES composto por diversos componentes distribuídos (localizados em computadores diferentes), a comunicação entre tais componentes (como, por exemplo, com o banco de dados) deve oferecer os seguintes serviços de segurança: autenticação de parceiro (cliente e servidor), integridade dos dados e confidencialidade dos dados.	X	M
NGS1.06.05	Controle de acesso entre componentes	ABNT NBR ISO/IEC 27001:2006 A.10.9.2	Em S-RES composto por diversos componentes distribuídos (localizados em computadores diferentes), na comunicação entre tais componentes (como, por exemplo, com o banco de dados), o acesso ao componente deve ser restrito somente aos parceiros (componentes) previamente autorizados.	X	M
NGS1.06.06	Comunicação entre S-RES.	HL7 ERH-S FM IN1.7	O canal de comunicação entre S-RES deve oferecer os seguintes serviços de segurança: autenticação de parceiro (cliente e servidor) utilizando certificados digitais, integridade dos dados e confidencialidade dos dados.	M	M

NGS1.07 - Segurança de Dados

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.07.01	Importação de dados	HL7 ERH-S FM IN1.6	Os dados importados de outro S-RES devem estar relacionados a um paciente e um médico responsável, local e momento (data e hora) da importação e profissional usuário do sistema que realiza a importação.	M	M
NGS1.07.02	Restrições para transmissão e exportação de RES	SBIS	A transmissão e exportação de RES de um S-RES deve ser permitida somente nas seguintes situações: • para transmissão para um outro sistema; • cópia de segurança; • para o paciente, a pedido do paciente, podendo ser realizada de forma eletrônica ou impressa; • em processos nos quais seja necessária a impressão de parte ou todo do RES; • para atendimento ao requisito legal de manter documentação em papel através da impressão. Todas as atividades de transmissão e exportação de RES devem ser registradas.	M	M
NGS1.07.03	Impedir exclusão e alteração	SBIS	Não permitir exclusão ou alteração de dados já existentes no RES. Ações de correção devem preservar os dados antigos.	M	M
NGS1.07.04	Verificação de integridade dos dados	SBIS	Devem existir controles para verificação de integridade dos dados RES de forma a prevenir que qualquer ação do usuário ou falha do sistema possa originar uma inconsistência nos dados.	R	R
NGS1.07.05	Utilização de SGBD	SBIS	O RES deve ser armazenado e protegido por um Sistema de Gerenciamento de Banco de Dados.	M	M
NGS1.07.06	Impedir acesso direto ao SGBD	SBIS	O SGBD não deve permitir acesso direto pelos usuários do S-RES. O acesso de usuários ao RES deve ser permitido somente por intermédio do componente de autenticação e controle de acesso do S-RES, nunca diretamente pelo SGBD, exceto nas atividades de cópia de segurança.	M	M
NGS1.07.07	Dados de identificação do paciente criptografados	SBIS	Os dados de identificação do paciente devem ser criptografados a fim de impedir a reconstrução do seu RES através de acessos não autorizados à base de dados do S-RES ou à cópia de segurança (gerado na salvaguarda dos dados).	R	R
NGS1.07.08	Confirmação de entrega	SBIS	A troca de dados entre S-RES deve possuir controles de confirmação de entrega/recebimento dos dados. Nota: Como exemplo podemos citar o TISS.	M	M

NGS1.08 – Auditoria

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.08.01	Auditoria de acesso	ISO/TS 18308:2004(E) PRS5.1	Suportar o registro de dados para auditoria de autenticação, acesso e manutenção de dados em parte ou no todo do S-RES	M	M
NGS1.08.02	Integridade das trilhas de auditoria	ABNT NBR ISO/IEC 27001:2006 A.10.10.3	Os recursos e informações de trilhas de auditoria devem ser protegidos contra acesso não autorizado e alteração por parte de nenhum usuário.	M	M
NGS1.08.03	Acesso às trilhas de auditoria	ABNT NBR ISO/IEC 27001:2006 A.10.10.1	Garantir que o acesso às trilhas de auditoria somente seja permitido ao usuário responsável pela auditoria.	M	M
NGS1.08.04	Trilha de auditoria	ABNT NBR ISO/IEC 27001:2006 A.10.10.1 ISO/TS 18308:2004(E) PRS5.3	As trilhas de auditoria devem conter informações relacionadas minimamente aos seguintes eventos: • tentativas de autenticação de usuário; • atividades de gerenciamento de usuários, papéis e grupos; • atividades de administração do sistema; • operações realizadas pelos usuários; • interação com outros sistemas, incluindo outros S-RES; • troca (transmissão e recepção) de dados; • cópia de segurança; • acessos à base de dados. Com relação aos eventos citados acima, as trilhas de auditoria devem possuir, no mínimo, as seguintes informações adicionais para cada evento: • data/hora • local • usuário	M	M

NGS1.09 - Documentação

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.09.01	Documentação	SBIS	Possuir no(s) manual(is) as seguintes informações: • Instalação e requisitos de sistemas; • Administração e operação do sistema; • Mecanismos e práticas de segurança.	M	M
NGS1.09.02	Referência à versão do software na documentação	SBIS	Todos os manuais devem indicar claramente, no início do documento, a versão a que se referem.	M	M
NGS1.09.03	Alteração Documentação	SBIS	Informar e manter histórico de todas as alterações nos manuais, para que o usuário possa consultar todas as alterações realizadas até a última versão disponível.	O	O
NGS1.09.04	Operador de backup	ABNT NBR ISO/IEC 27001:2006	O manual de instalação deve informar como realizar a configuração de um usuário com perfil de operador de backup no SGBD. Além disso, 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 papel de operador de *backup*.	R	R
NGS1.09.05	Restrição de acesso a entidades não autenticadas e autorizadas	SBIS	O manual de instalação deve informar como configurar o SGBD de forma a impedir o acesso de entidades (usuários ou outros sistemas) não autenticadas e não autorizadas pelo componente de autenticação e controle de acesso do S-RES.	R	R
NGS1.09.06	Verificação da integridade dos dados	SBIS	O manual de instalação ou operação deve informar que, quando houver geração e restauração de cópia de segurança, o sistema deve realizar a verificação da integridade dos dados.	R	R
NGS1.09.07	Configuração da Segurança da comunicação entre componentes	SBIS	O manual de instalação e operação deve informar que a comunicação entre os componentes de um S-RES distribuído deve implementar os serviços de segurança de autenticação de parceiro (cliente e servidor), integridade dos dados e confidencialidade dos dados.	X	M
NGS1.09.08	Sincronização de relógio	ABNT NBR ISO/IEC 27001:2006 10.10	O manual de administração e operação deve informar ao administrador que os componentes do S-RES devem estar com seus relógios sincronizados e referenciados a uma única e mais confiável fonte temporal. O manual deve também informar as formas para que a sincronização possa ser configurada no ambiente.	O	R

NGS1.10 - Tempo

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.10.1	Uniformidade da representação de tempo para controle e auditoria	SBIS	Todo registro de tempo para fins de controle e auditoria deve estar no mesmo formato em todo o S-RES.	M	M
NGS1.10.2	Formato da representação de tempo para controle e auditoria em registros exportados	ISO 8601:2004	Todo registro de tempo para fins de controle e auditoria presente em registros exportados deve ser representado no formato da ISO 8601:2004, com exceção do carimbo de tempo, que segue RFC 3161.	O	O
NGS1.10.3	Fonte temporal	ABNT NBR ISO/IEC 27001:2006	Todo registro de tempo para fins de controle e auditoria em todo o S-RES deve ser baseado em uma única e mais confiável fonte temporal, que não tenha acesso de configuração pelo usuário a não ser pelo administrador do sistema.	X	M

NGS1.11 – Notificação de Ocorrências

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Local	Remoto
NGS1.11.01	Interface para notificação	ABNT NBR ISO/IEC 27002:2006 13.1.1	Disponibilizar uma interface para que usuários possam notificar ocorrência de incidentes de segurança, problemas, melhoramentos ou sugestões.	O	R

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

NGS2.01 – Certificação Digital

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
NGS2.01.01	Certificado digital	ICP-Brasil; Resolução CFM	Utilização de certificado digital emitido por AC credenciada à ICP-Brasil para os processos de autenticação de usuários e para assinatura digital de documentos eletrônicos no S-RES.	M
NGS2.01.02	Atendimento à ICP-Brasil	ICP-Brasil; Resolução CFM	Atender às normas de uso definidas pela ICP-Brasil na utilização de certificados digitais.	M
NGS2.01.03	Validação do certificado digital antes do uso	ICP-Brasil	Antes da utilização de um certificado digital deve ser realizada sua validação. A validação do certificado digital envolve a validação criptográfica, verificação de validade, inclusive dos certificados da sua cadeia de certificação. A verificação da revogação do certificado e sua cadeia de certificação deve ser realizada antes de sua utilização ou imediatamente após sua utilização.	M
NGS2.01.04	Configuração de certificados raiz	ICP-Brasil	O S-RES deve permitir a configuração do conjunto de certificados raiz de confiança. Deve, também, possuir controles de segurança sobre esse conjunto de certificados raiz de confiança.	M

NGS2.02 – Assinatura Digital

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
NGS2.02.01	Formato de assinatura	SBIS	Utilizar formatos abertos a fim de garantir a interoperabilidade dos dados. Neste sentido, a assinatura digital deverá utilizar estruturas compatíveis com o formato CMS [RFC 3852] ou XMLDSIG [RFC 3275].	M
NGS2.02.02	Verificação do propósito do certificado digital para assinatura digital	X.509	Verificar, antes da realização de uma assinatura digital, se o certificado digital a ser utilizado possui propósito de uso para assinatura digital (*Digital Signature* e *Non-Repudiation* no campo *key usage*).	M
NGS2.02.03	Referência temporal para revogação	ETSI TS 101 733	Toda assinatura digital ICP-Brasil realizada no âmbito do S-RES deve incluir um carimbo de tempo (RFC 3161) que deve ser utilizado como referência temporal nas atividades de verificação de revogação.	R
NGS2.02.04	Validação da assinatura digital	SBIS	Para cada assinatura digital a ser realizada, incluindo os casos de duas ou mais assinaturas, deve ser efetuada a validação criptográfica e verificação de revogação da(s) assinatura(s) digital(is) e da cadeia dos certificados digitais associados a cada uma das assinaturas.	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
NGS2.02.05	Validação da assinatura a qualquer momento	ETSI TS 101 733	Manter os elementos necessários (informações sobre certificados raiz, cadeias de certificação, certificados dos signatários e informações de revogação) a fim de possibilitar que a assinatura digital possa ser validada a qualquer momento futuro. Esses elementos podem estar incluídos no registro assinado digitalmente ou referenciado por este e armazenado no S-RES.	M
NGS2.02.06	Propósito da assinatura e papel do signatário	ETSI TS 101 733	Incluir, em toda assinatura digital realizada, o propósito da assinatura (atributo *commitment-type-indication*), ou seja, o tipo de comprometimento que o signatário assume no momento de firmar a assinatura digital, e o papel do signatário (atributo *role*) no S-RES.	R
NGS2.02.07	Visualização das informações a serem assinadas	SBIS	Sempre permitir a visualização da informação a ser assinada.	M
NGS2.02.08	Homologação ICP-Brasil	ICP-Brasil	Os componentes de um S-RES que utilizam certificação digital para assinatura digital devem ser homologados pela ICP-Brasil.	R
NGS2.02.09	Exportação de registros assinados	SBIS	Todos os registros assinados digitalmente exportados, por exemplo, para outros S-RES, devem conter todos os elementos necessários para sua validação (informações sobre certificados raiz, cadeias de certificação, certificados dos signatários e informações de revogação).	M
NGS2.02.10	Política de assinatura	ICP-Brasil	As assinaturas firmadas nos registros assinados digitalmente devem utilizar política de assinatura.	R

NGS2.03 – Autenticação de usuário utilizando certificado digital

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
NGS2.03.01	Verificação do propósito do certificado digital para autenticação	ICP-Brasil	Condição: S-RES que utiliza certificado digital para autenticação. Verificar, antes da realização de uma autenticação, se o certificado digital a ser utilizado possui propósito de uso para autenticação (*client authentication*).	M
NGS2.03.02	Irretratabilidade da autenticação realizada	SBIS	Condição: S-RES que utiliza certificado digital para autenticação. A autenticação realizada através de certificado digital deve gerar prova de forma a garantir a irretratabilidade da autenticação realizada. O elemento de prova deve ser armazenado em registros de segurança do sistema, em formatos compatíveis com os padrões CMS [RFC 3852] ou XMLDSIG [RFC 3275] e deve ser possível agregar todos os elementos necessários para sua validação (informações sobre certificados raiz, cadeias de certificação, certificados dos signatários e informações de revogação) no S-RES.	M
NGS2.03.03	Tipos de usuários para autenticação com certificação digital	SBIS	Condição: S-RES que utiliza certificado digital para autenticação. Todos os usuários que realizam assinatura digital ICP-Brasil devem se autenticar com seus certificados digitais ICP-Brasil.	R
NGS2.03.04	Homologação ICP-Brasil	ICP-Brasil	Condição: S-RES que utiliza certificado digital para autenticação. Os componentes de um S-RES que utilizam certificação digital para autenticação devem ser homologados pela ICP-Brasil.	R

NGS2.04 – Digitalização de Documentos (Aplicável somente para S-RES da categoria GED)

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
NGS2.04.01	Assinatura digital do software	SBIS	Todo componente de digitalização deve possuir um par de chaves assimétricas e certificado digital associado. Todo documento digitalizado deve ser assinado pelo componente de digitalização com esta chave, utilizando o propósito "garantia de envio". O propósito de garantia de envio pode ser estabelecido incluindo o atributo assinado "commitment-type-indication" com o propósito genérico "id-cti-ets-proofOfDelivery", enquanto não seja definido um propósito mais específico.	M
NGS2.04.02	Assinatura digital do operador	SBIS	O operador de digitalização deve assinar digitalmente o documento digitalizado, com certificado ICP-Brasil tipo A3 ou A4, utilizando o propósito "garantia de recebimento". O propósito de garantia de recebimento pode ser estabelecido incluindo o atributo assinado "commitment-type-indication" com o propósito genérico "id-cti-ets-proofOfReceipt", enquanto não seja definido um propósito mais específico. Essa assinatura deve ser aposta como uma contra-assinatura da assinatura do software. O operador deve necessariamente verificar o enquadramento e a qualidade da imagem digitalizada em comparação à original, e ser capaz de repetir do processo de digitalização em casos de imperfeições.	M
NGS2.04.03	Assinatura digital do responsável	Resolução CFM	O responsável deve assinar digitalmente o documento digitalizado, com certificado ICP-Brasil utilizando o propósito "aprovação". O propósito de aprovação pode ser estabelecido incluindo o atributo assinado "commitment-type-indication" com o propósito genérico "id-cti-ets-proofOfApproval", enquanto não seja definido um propósito mais específico. Essa assinatura deve ser aposta como uma contra-assinatura da assinatura do software.	M
NGS2.04.04	Autenticação	SBIS	O operador, responsável e administrador do sistema de assinatura devem se autenticar no sistema segundo o NGS2.03.	M
NGS2.04.05	Instante da assinatura	SBIS	Toda assinatura de documento digitalizado deve incluir o atributo signing-time, contendo o instante da assinatura no formato UTC.	M
NGS2.04.06	Termo de conduta para digitalização	SBIS	Permitir ao usuário a realização de operações de digitalização somente após a assinatura digital do "Termo de conduta para digitalização" que deve conter requisitos sobre confidencialidade das informações e sobre a responsabilidade do processo.	M
NGS2.04.07	Homologação ICP-Brasil	ICP-Brasil	Os componentes de um S-RES que utilizam certificação digital para autenticação e assinatura digital devem ser homologados pela ICP-Brasil.	R

8.4. Requisitos de Estrutura e Conteúdo para S-RES Assistencial

ESTR.01 - Estrutura do RES

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
ESTR.01.01	Navegação e consultas	ABNT ISO/TS 18308 EST1.1	Possibilitar que a informação do RES esteja organizada em diferentes seções que devem se refletir nos mecanismos de navegação e consultas.	M
ESTR.01.02	Estrutura mínima	ABNT ISO/TS 18308 EST1.2 CFM 1638/2002	Assegurar que a estrutura do RES esteja aderente ao conjunto de especificações estabelecidas pela resolução 1638/2002 do CFM, aos padrões de identificação de usuário, profissional de saúde e estabelecimento conforme descritos no Cadastro Nacional de Usuários, e adotados no Cartão Nacional de Saúde e no Cadastro Nacional de Estabelecimentos de Saúde. A identificação do Estabelecimento Assistencial de Saúde (EAS) deverá utilizar o código do Cadastro Nacional de Estabelecimentos de Saúde – CNES. Em se tratando de consultórios particulares que não possuam o número CNES, deverá utilizar o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), ou a identificação do profissional responsável conforme padrões de identificação do profissional de saúde no CNES. Para a área de saúde suplementar, assegurar que os requisitos de informação da ANS estejam contemplados, conforme descritos no padrão TISS. Links pertinentes: ftp://ftp.datasus.gov.br/cartaosus/CadNacional/manuais/Manual%20Cad.Nacional%20030801.zip http://cnes.datasus.gov.br/Mod_DownLoad_Manuais_Simplificado.asp	M
ESTR.01.03	Independência	ABNT ISO/TS 18308 EST1.3	Suportar o compartilhamento de RES com independência de hardware, software (aplicativos, sistemas operacionais, linguagens de programação), bancos de dados, redes, sistemas de codificação e linguagens naturais.	R
ESTR.01.04	Recuperação de dados	ABNT ISO/TS 18308 EST1.4	Possibilitar que a informação esteja organizada e passível de recuperação de tal forma que facilite os usos secundários do RES, tais como: vigilância epidemiológica, gestão, faturamento e pesquisa.	R
ESTR.01.05	Armazenamento do RES	ABNT ISO/TS 18308 EST1.5	Suportar o armazenamento do RES.	M

ESTR.02 - Dados estruturados

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
ESTR.02.01	Armazenamento em listas	ABNT ISO/TS 18308 EST2.1	Permitir o armazenamento em listas de todos os dados que possuam registro de tempo, de tal forma que a ordem cronológica esteja preservada sempre que a informação for apresentada.	M
ESTR.02.02	Preservação de relacionamento de dados	ABNT ISO/TS 18308 EST2.2	Permitir o registro de dados em tabelas de tal forma que os relacionamentos dos dados com as linhas e colunas estejam preservados.	M
ESTR.02.03	Hierarquia de nodos	ABNT ISO/TS 18308 EST2.3	Permitir o registro de dados em hierarquias, preservando o relacionamento dos nodos pais com os nodos filhos, de forma que possibilite a navegação, busca e consulta destes dados.	M
ESTR.02.04	Associação do nome e valor dado	ABNT ISO/TS 18308 EST2.4	Possibilitar o registro de dados simples, preservando a associação entre nome do dado e respectivo valor.	M
ESTR.02.05	Armazenamento de múltiplos valores	ABNT ISO/TS 18308 EST2.5	Possibilitar o registro de múltiplos valores para a mesma observação coletada sequencialmente, em curtos intervalos de tempo, durante um mesmo contato ou em diferentes contatos e locais. O contexto no qual as medidas foram realizadas deve ser preservado, tais como o tipo de ferramenta e metodologia utilizada e quem as coletou. Estes valores devem ser exibidos quando solicitados, e ordenados de diferentes formas.	M
ESTR.02.06	Texto livre	ABNT ISO/TS 18308 EST2.6 ERH-S FM- IN 2.5.1	Incorporar a inclusão de texto livre.	M
ESTR.02.07	Busca e inclusão	ABNT ISO/TS 18308 EST2.7	Possibilitar a busca em dados não-estruturados (texto e não-texto) e inclusão de texto estruturado nestes dados.	M
ESTR.02.08	Inclusão de comentários	ABNT ISO/TS 18308 ISO EST2.8	Possibilitar a inclusão de comentários nos dados armazenados, permitindo que o profissional de saúde os complemente, preservando a associação dos comentários com os respectivos dados.	R
ESTR.02.09	Ênfase nos comentários e dados	ABNT ISO/TS 18308 EST2.9	Oferecer mecanismos que possibilitem ao profissional de saúde enfatizar os comentários ou dados fornecidos, devendo tal ênfase ser apresentada junto ao respectivo dado.	R

ESTR.03 - Dados Administrativos

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
ESTR.03.01	Registro de identificação do paciente	ABNT/TS18308 EST2.11 SUS	Possibilitar que, além dos dados constantes do requisito ESTR.01.02, a identificação do paciente contenha a pessoa para contato e o responsável legal (quando for o caso).	M
ESTR.03.02	Padrões do CNS, CNES, CNPJ	ABNT/TS18308 EST2.12	Possibilitar a representação de forma não ambígua do sujeito da atenção, dos profissionais envolvidos no processo assistencial (incluindo seus respectivos papéis), o local da assistência, bem como a data e hora inicial e final do evento. Conforme definido no requisito ESTR.01.02, a identificação do sujeito da atenção e dos profissionais responsáveis pela assistência e pela digitação dos dados deverá utilizar os padrões de identificação do Cartão Nacional de Saúde e do CNES.	R
ESTR.03.03	Episódios de atenção	ABNT/TS18308 EST2.13	Suportar a administração dos processos em saúde e episódios de atenção, bem como a organização de cada evento e seus dados.	M
ESTR.03.04	Informações financeiras e comerciais	ABNT/TS18308 EST2.14	Suportar o registro das informações financeiras e outras informações comerciais, tais como operadoras de planos de saúde e respectivas elegibilidades, coberturas, responsável por despesas, custos, taxas e utilização.	R
ESTR.03.05	Situação legal	ABNT/TS18308 EST2.15	Suportar o registro da situação legal e consentimentos relevantes para o cuidado do paciente (ex: situação legal do guardião, consentimento para cirurgia e outros procedimentos). Este registro deverá conter minimamente a identificação do signatário do consentimento, bem como a data e hora da assinatura.	R
ESTR.03.06	Vigilância	ABNT/TS18308 EST2.16	Possibilitar a realização de consultas e a emissão de relatórios para atender às demandas da vigilância epidemiológica, sanitária e doenças de notificação compulsória. Deverão ser contemplados, no mínimo, os agravos constantes da Portaria N.º 5, de 21/02/2006 da Secretaria de Vigilância em Saúde.	M

ESTR.04 - Dados clínicos

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
ESTR.04.01	Dados estruturados ou não	ABNT ISO/TS 18308 EST2.10 CFM 1638/2002	Suportar o armazenamento de dados estruturados e não estruturados que atendam minimamente: ▪ Anamnese (história do paciente) ▪ Exame físico ▪ Antecedentes mórbidos pessoais (psicológicos, sociais, ambientais) e familiares ▪ Alergias e outras informações de relevância clínica ▪ Imunizações e medidas preventivas e outras intervenções no estilo de vida ▪ Investigação diagnóstica, intervenções terapêuticas tais como medicamentos e procedimentos ▪ Evoluções clínicas, interpretações, decisões e raciocínio clínico ▪ Solicitação de exames, tratamentos e encaminhamentos ▪ Hipóteses Diagnósticas, Lista de Problemas, Diagnósticos, Questões relevantes, preferências e expectativas ▪ Consentimentos informados (não mandatório quando NGS1) ▪ Operadora de plano de saúde ▪ Sumário de alta com as condições funcionais e de saúde ▪ Informações a respeito de próteses ou implantes: fornecedor, modelo	M
ESTR.04.02	Laudos e resultados de exames	ABNT ISO/TS 18308 EST2.10 SUS	Suportar o registro de resultados de exames, com a descrição do que foi realizado, método utilizado, data e hora da realização, profissional responsável pelo laudo/resultado e conclusão.	R
ESTR.04.03	Envio eletrônico de dados	ABNT ISO/TS 18308 EST2.10 SUS	Suportar o envio eletrônico de dados de faturamento, produção e vigilância conforme as exigências do SUS / Ministério da Saúde e Agência Nacional de Saúde Suplementar.	R

ESTR.05 - Tipos de dados

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
ESTR.05.01	Dados numéricos e quantificáveis	ABNT ISO/TS 18308 EST3.1	Incorporar uma definição de estrutura lógica para representar dados numéricos e quantificáveis, incluindo o manuseio de unidades.	M
ESTR.05.02	Precisão da medida	ABNT ISO/TS 18308 EST3.2	Suportar o armazenamento do grau de precisão de medidas de quantidades de acordo com o método utilizado.	R
ESTR.05.03	Percentagem e valor absoluto	ABNT ISO/TS 18308 EST3.3	Suportar que as percentagens estejam expressas também em valores absolutos.	R

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
ESTR.05.04	Limites	ABNT ISO/TS 18308 EST3.4	Incorporar uma definição de estrutura lógica para representar intervalos, ou seja, a representação de limites inferior e superior para dados quantificáveis adequados ao contexto clínico. Ex.: peso e altura de recém-nascido.	M
ESTR.05.05	Lógica dos valores fracionados	ABNT ISO/TS 18308 EST3.5	Incorporar uma representação lógica de valores fracionados. Ex.: Relação Colesterol total / HDL-Colesterol.	R
ESTR.05.06	Lógica de data e hora	ABNT ISO/TS 18308 EST3.6	Incorporar a definição de estrutura lógica para representar valores data e hora.	M
ESTR.05.07	Definições incompletas	ABNT ISO/TS 18308 EST3.7	Suportar que a estrutura lógica para representar os valores de data e hora aceite definições incompletas ou aproximadas, tais como: - datas aproximadas – ex: ontem; semana passada - datas parciais – ex: ??/Maio/1997; ??/??/1928	R
ESTR.05.08	Eventos e ações futuras	ABNT ISO/TS 18308 EST3.8	Suportar o registro de eventos ou ações planejadas para o futuro, tais como: - Períodos do dia ou de tempo: manhã, tarde, noite, enquanto acordado; - Momentos aproximados de datas ou horas: ao acordar, durante as refeições (café da manhã, almoço, jantar), ao deitar; - Momentos relativos de datas ou horas: antes do café da manhã, após o almoço, dois dias após a alta, uma semana depois da última dose; - Períodos alternados de datas/horas: alternadamente a cada 8 horas, todas as segundas, quartas e sextas-feiras, todos os sábados, todo terceiro domingo.	R
ESTR.05.09	Linha de tempo	ABNT ISO/TS 18308 EST3.9	Suportar o registro do tempo em um dado instante, o tempo decorrido desde um determinado evento e/ou sua respectiva duração.	R
ESTR.05.10	Fuso horário	ABNT ISO/TS 18308 EST3.10	Suportar o registro do fuso horário do local onde o RES foi realizado.	R
ESTR.05.11	Precisão de milissegundos	ABNT ISO/TS 18308 EST3.11	Suportar o registro de unidades de tempo com precisão de milissegundos.	R
ESTR.05.12	DICOM, MIME e ECG	ABNT ISO/TS 18308 EST3.12	Incorporar uma estrutura lógica para representar tipos de dados padronizados, tais como: DICOM, MIME e ECG.	R

ESTR.06 - Dados de referência

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
ESTR.06.01	Dados de referência	ABNT ISO/TS 18308 EST3.13	Suportar o registro de dados de referência, tais como faixas de normalidade e os atributos e contexto relevantes a uma observação ou mensuração específica. Ex.: medida de pressão arterial em membros inferiores ou superiores; medida de temperatura em paciente em incubadora.	R

ESTR.07 - Dados contextuais

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
ESTR.07.01	Eventos já ocorridos	ABNT ISO/TS 18308 EST3.14	Suportar o registro de dados contextuais associados com a data/hora em que o evento ocorreu.	M
ESTR.07.02	Contexto e tempo	ABNT ISO/TS 18308 EST3.15	Suportar o registro de dados contextuais associados com a data/hora em que o evento foi armazenado no SRES.	M
ESTR.07.03	Contexto e assunto	ABNT ISO/TS 18308 EST3.16	Suportar o registro de dados contextuais associados ao sujeito da assistência.	R
ESTR.07.04	Contexto e responsável	ABNT ISO/TS 18308 EST3.17	Suportar o registro de dados contextuais associados com a pessoa responsável pelo registro do evento.	R
ESTR.07.05	Contexto e ambiente físico	ABNT ISO/TS 18308 EST3.18	Suportar o registro de dados contextuais associados ao estabelecimento de saúde.	R
ESTR.07.06	Contexto e localização	ABNT ISO/TS 18308 EST3.19	Suportar o registro de dados contextuais associados ao local onde o evento foi registrado.	R
ESTR.07.07	Contexto e razão	ABNT ISO/TS 18308 EST3.20	Suportar o registro de dados contextuais associados ao motivo do registro da informação associada ao evento.	R
ESTR.07.08	Contexto e protocolo	ABNT ISO/TS 18308 EST3.21	Suportar o registro de dados contextuais associados ao protocolo associado à informação registrada.	R

ESTR.08 - Associações

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
ESTR.08.01	Associação semântica	ABNT ISO/TS 18308 EST3.22	Representar a associação semântica entre diferentes informações no RES, através de um serviço de terminologias.	R
ESTR.08.02	Dados referenciados externamente	ABNT ISO/TS 18308 EST3.23	Possibilitar a associação a “dados referenciados externamente” quando estes não puderem ser representados no RES, desde que a segurança dos dados do paciente não seja comprometida.	R

ESTR.09 - Representação de conceitos em saúde

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
ESTR.09.01	Múltiplos sistemas de codificação	ABNT ISO/TS 18308 EST 4.1	Suportar múltiplos sistemas de codificação (terminologias de entrada ou interface, terminologias de referência e classificações) e o mapeamento entre eles.	R
ESTR.09.02	Captura de código	ABNT ISO/TS 18308 EST4.2 HL7 CNS	Ao registrar um código que representa um sistema de classificação/codificação, deverão ser registrados o código, a descrição do sistema de classificação/codificação utilizado, a versão, o idioma original e a descrição original.	M
ESTR.09.03	Vocabulário padrão e de origem	ABNT ISO/TS 18308 EST4.3 CNS	Suportar o registro de dados a partir de vocabulários padrão, preservando-se a informação do vocabulário de origem. O registro de diagnósticos deverá utilizar obrigatoriamente o CID-10.	M
ESTR.09.04	Ambiguidade	ABNT ISO/TS 18308 EST4.4	Suportar regras explícitas para evitar ambiguidades sempre que o dado não for registrado de apenas uma maneira ou em um único lugar. Ex.: deixar claro que [pulsos pediosos: não] é igual a [pulsos pediosos ausentes].	R
ESTR.09.05	Mapeamentos	ABNT ISO/TS 18308 EST4.5	Suportar os mapeamentos entre modelos de informação e de inferência com base em um conjunto de conceitos bem definidos num vocabulário de referência ou modelo conceitual.	R
ESTR.09.06	Serviços de terminologia	ABNT ISO/TS 18308 EST 4.1 HL7 DIS 27951 Lexicon Query Service Specification	Incorporar um serviço de terminologia clínica.	R

ESTR.10 - Representação de texto

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
ESTR.10.01	Texto original	ABNT ISO/TS 18308 EST 4.6	Preservar o texto original conforme fornecido pelo profissional de saúde no RES, quando a informação for traduzida da linguagem natural para outra, ou quando os termos forem mapeados de um sistema de codificação/classificação para outro.	R

8.5. Requisitos de Funcionalidades para S-RES Assistencial

FUNC.01 - Suporte aos processos clínicos

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.01.01	Evento clínico	ABNT ISO/TS 18308 PRO1.1	Capacidade de registrar qualquer tipo de evento clínico, encontro ou episódio relevante à assistência à saúde do paciente.	R
FUNC.01.02	Processos de apoio clínico	ABNT ISO/TS 18308 PRO1.2	Suportar a criação, acompanhamento e manutenção dos processos clínicos que apóiam as atividades de seus usuários.	M
FUNC.01.03	Continuidade de processos clínicos	ABNT ISO/TS 18308 PRO1.3	Suportar a continuidade do processo clínico (assistência ao paciente), possibilitando consultar o status de um processo, aditar um processo já existente e verificar se um processo foi completado. Ex.: status de um exame de laboratório.	M
FUNC.01.04	Processos clínicos incompletos	ABNT ISO/TS 18308 PRO1.4	Acomodar a existência de processos clínicos em aberto / incompletos (ex.: solicitação de exames nunca realizados).	M

FUNC.02 - Problemas / condições de saúde e outras questões

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.02.01	Condição holística do paciente	ABNT ISO/TS 18308 PRO1.5	Suportar o registro da condição holística da situação da saúde do indivíduo, situação funcional, problemas, condições, circunstâncias ambientais e outras questões que possam afetar a sua saúde.	R
FUNC.02.02	Estrutura de dados orientada por problemas	ABNT ISO/TS 18308 PRO1.6	Suportar o registro e apresentação os dados em estrutura orientada por problemas incluindo o status dos problemas, planos de solução e metas. Possibilitar também a apresentação dos dados em estruturas como as orientadas cronologicamente, por episódios, e por processos.	R
FUNC.02.03	Período de vida do paciente	ABNT ISO/TS 18308 PRO1.7	Suportar todo o período de vida do paciente, com registro longitudinal da condição de saúde e intervenções, que devem ser visualizadas de forma cronológica. O RES é simultaneamente: • retrospectivo: oferece visão histórica das condições de saúde e intervenções (ex: eventos ou atos em saúde realizados); • atual: visão da condição atual de saúde e intervenções ativas ou em andamento; e • prospectivo: planejamento das ações futuras (eventos ou atos em saúde pendentes ou agendados).	M

FUNC.03 - Raciocínio Clínico

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.03.01	Raciocínio clínico	ABNT ISO/TS 18308 PRO1.8	Suportar o registro do raciocínio clínico para todos os diagnósticos, conclusões e ações a respeito da assistência à saúde do paciente, incluindo aqueles realizados por processos automatizados.	R

FUNC.04 - Suporte à decisão, protocolos clínicos e alertas.

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.04.01	Alertas e lembretes	ABNT ISO/TS 18308 PRO1.9	Suportar a apresentação automática de alertas, lembretes e avisos, tais como alergias, resultados urgentes, condição de infecção, precauções terapêuticas, intervenções importantes e resultados urgentes, os quais deverão ser necessariamente exibidos sempre que se abrir a ficha do paciente e ao fazer prescrições.	R
FUNC.04.02	Alertas e lembretes em vigilância	ABNT ISO/TS 18308 PRO1.10	Incorporar lembretes e chamadas sobre os programas de vigilância epidemiológica e outras ações de saúde pública, tais como programas de imunização ou outras campanhas.	R
FUNC.04.03	Notificação de agravos	SUS	Incorporar a emissão automática da notificação de agravos conforme prevê o gestor federal, estadual e municipal de saúde. Deverão ser contemplados, no mínimo, os agravos constantes da Portaria N.º 5, de 21/02/2006 da Secretaria de Vigilância em Saúde.	M
FUNC.04.04	Diretrizes e protocolos	ABNT ISO/TS 18308 PRO1.11	Suportar a incorporação de diretrizes, protocolos e sistemas de apoio à decisão.	R
FUNC.04.05	Restrição e obrigatoriedade	ABNT ISO/TS 18308 PRO1.12	Suportar a representação de restrições e dados obrigatórios ao processo de apoio à decisão. Por ex.: restrições de sexo X diagnóstico, medicação X diagnóstico, restrição à prescrição de medicação que tenha alergia informada.	R

FUNC.05 - Planejamento Terapêutico

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.05.01	Planejamento terapêutico	ABNT ISO/TS 18308 PRO1.13	Incorporar o planejamento terapêutico incluindo gerenciamento da situação dos diferentes processos (ex: solicitado, agendado, em realização, suspenso, em pendência, completo, verificado, cancelado, complementado).	M

FUNC.06 - Prescrição e processamento de exames

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.06.01	Registro e acompanha-mento	ABNT ISO/TS 18308 PRO1.14	Suportar o registro e o acompanhamento de todas as prescrições médicas e de outros profissionais de saúde (quando for o caso), solicitação de exames e encaminhamentos.	R
FUNC.06.02	Associação	ABNT ISO/TS 18308 PRO1.15	Associar o procedimento solicitado com o realizado e o respectivo resultado.	R

FUNC.07 - Assistência integral

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.07.01	Assistência integral	ABNT ISO/TS 18308 PRO1.16	Suportar o registro do processo de assistência integral incluindo cuidados multidisciplinares e em diferentes níveis de atenção em saúde: primário, especializado, internação hospitalar, cuidados e hospitalização domiciliar, urgência / emergência.	R

FUNC.08 - Garantia de qualidade

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.08.01	Performance clínica e operacional	ABNT ISO/TS 18308 PRO1.17	Suportar o registro e consulta de dados com medidas (indicadores) de performance clínica e operacional, aderentes aos padrões de assistência com o objetivo de garantir a qualidade e medir os resultados dos processos em saúde.	R

FUNC.09 - Captura de dados

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.09.01	Entrada e acréscimo de dados	ABNT ISO/TS 18308 PRO2.1	Incorporar regras claras e consistentes para a entrada, manutenção, transmissão, recepção, tradução e substituição de dados. Este requisito não implica em exclusão de registros. Regras locais para a retenção de dados deverão ser aplicadas.	M
FUNC.09.02	Validação de dados	ABNT ISO/TS 18308 PRO2.2	Implementar regras de validação dos dados em todos os campos estruturados.	M
FUNC.09.03	Pesquisa com filtros	ABNT ISO/TS 18308 PRO2.3	Suportar a habilidade de recuperar informações de todos os tipos registradas no passado, inclusive através do uso de pesquisas com filtros durante o processo de entrada de dados.	R

FUNC.10 - Recuperação/ consultas e visões

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.10.01	Visões	ABNT ISO/TS 18308 PRO2.4	Suportar visões diferenciadas e recuperação seletiva para a mesma informação para atender demandas específicas, tais como apoio à decisão, análise de dados, financeiro, administrativo, etc.	M

FUNC.11 - Apresentação dos dados

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.11.01	Sumário clínico	ABNT ISO/TS 18308 PRO2.5	Suportar a apresentação de dados marcados como sumário clínico de forma automática, sem a necessidade de pesquisa manual. O sumário clínico deverá conter, minimamente, os diagnósticos, medicamentos, exames, atendimentos, alergias e outros dados que sejam considerados relevantes.	R
FUNC.11.02	Resolução para interpretação clínica	ABNT ISO/TS 18308 PRO2.6	Garantir a resolução necessária para a interpretação clínica (p.ex., manter a mesma resolução e quantidade de cores do original).	R
FUNC.11.03	Imagens médicas	SBIS	Ao exibir imagens médicas, exibir uma mensagem informando qual a resolução mínima e/ou adequada para a resolução diagnóstica.	R

FUNC.12 - Escalabilidade e performance

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.12.01	Eficiência de processamento	ABNT ISO/TS 18308 PRO2.5	Processar eficientemente mesmo quando lidando com registros numerosos e/ou grandes.	R

FUNC.13 - Protocolos de mensagens

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.13.01	Exportação e importação de dados	ABNT ISO/TS 18308 COM2.1	Suportar a exportação e a importação de dados recebidos por meio de protocolos de mensagens tais como HL7, UN/EDIFACT e DICOM.	R

FUNC.14 - Troca de registros

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.14.01	Serialização	ABNT ISO/TS 18308 COM2.2	Suportar a serialização de dados com propósito de interoperabilidade (ex: via XML, SOAP, CORBA, .Net, etc.).	R
FUNC.14.02	Regras de troca	ABNT ISO/TS 18308 COM2.5	Prover regras de troca que sejam as mesmas para apenas um extrato do RES ou para o RES completo.	R
FUNC.14.03	Interoperabilidade semântica	ABNT ISO/TS 18308 COM2.6	Suportar a interoperabilidade semântica de conceitos clínicos entre sistemas objetivando processamento automático dos dados no S-RES receptor.	R

FUNC.16 - Consentimento

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.16.01	Consentimento informado	ABNT ISO/TS 18308 PRS2.1	Suportar o registro de consentimento informado.	R
FUNC.16.02	Situação do consentimento informado	ABNT ISO/TS 18308 PRS2.2	Suportar a obtenção, registro e acompanhamento da situação do consentimento informado para acessar parte ou todo o RES, para propósitos previamente definidos.	R
FUNC.16.03	Propósito do consentimento informado	ABNT ISO/TS 18308 PRS2.3	Suportar o registro dos propósitos pelos quais o consentimento foi obtido.	R
FUNC.16.04	Instante do consentimento informado	ABNT ISO/TS 18308 PRS2.4	Suportar o registro do instante de cada consentimento.	R

FUNC.17 - Médico-legal

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.17.01	Cronologia de eventos	ABNT ISO/TS 18308 MEL1.1	O RES deve assegurar a acurácia da cronologia dos seus eventos clínicos e das suas informações.	M
FUNC.17.02	Precisão de visão cronológica	ABNT ISO/TS 18308 MEL1.2	Suportar a visualização precisa com acurácia de qualquer dado do RES desde a sua criação.	M

FUNC.18 - Atores

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.18.02	Atributos clínicos relevantes	ABNT ISO/TS 18308 MEL2.2	Suportar o registro dos atributos apropriados para a identificação do paciente e de atributos clínicos relevantes tais como data de nascimento, sexo, etnia, etc.	M
FUNC.18.03	Identificação de fornecedor de informação	ABNT ISO/TS 18308 MEL2.3	Garantir que usuários que atestam ou registram qualquer informação específica no RES sejam identificados de maneira confiável e unívoca.	R
FUNC.18.04	Identificação de usuário	ABNT ISO/TS 18308 MEL2.4	Suportar a capacidade contínua de identificação do usuário, mesmo que este mude seu nome, profissão, sexo ou endereço.	M
FUNC.18.05	Identificação dos profissionais de saúde	ABNT ISO/TS 18308 MEL2.5	Suportar medidas que assegurem que todos os profissionais de saúde referidos em um RES sejam distintamente identificados.	M
FUNC.18.06	Registro do papel dos profissionais de saúde	ABNT ISO/TS 18308 MEL2.6	Suportar o registro do papel de todos os profissionais de saúde responsáveis por qualquer atividade assistencial registrada no RES.	R
FUNC.18.07	Data do registro	ABNT ISO/TS 18308 MEL2.7	Suportar medidas que assegurem que todo registro seja datado e seu autor responsável identificado.	M
FUNC.18.08	Identificação de responsável pela informação no RES	ABNT ISO/TS 18308 MEL2.8	Suportar medidas que assegurem que toda a informação registrada no RES seja atribuída a um ator responsável na área da saúde, independentemente se este foi o autor da informação ou não. Ex.: na digitação posterior de uma prescrição original em papel, o sistema deve identificar univocamente a pessoa que está digitando a informação e o autor da mesma.	R
FUNC.18.09	Responsabilidade sobre contribuição aos registros	ABNT ISO/TS 18308 MEL2.9	Suportar medidas que assegurem que todos os dados fornecidos ao RES sejam atestados ou validados pela pessoa responsável.	R
FUNC.18.10	Responsabilidade sobre emendas e adições	ABNT ISO/TS 18308 MEL2.10	Suportar medidas que assegurem que adições de dados sejam atribuídas à pessoa responsável, e que a hora/data e a razão (quando aplicável) para tal adição sejam registradas.	M

FUNC.19 - Competência e governança clínica

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.19.01	Competência técnica e responsabilidade	ABNT ISO/TS 18308 MEL3.1	Suportar a demonstração dos dados de credenciamento, registro profissional e responsabilidade técnica dos profissionais de saúde.	R

FUNC.20 – Fé Pública

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.20.01	Substituição de dados	ABNT ISO/TS 18308 MEL4.1	Assegurar que as novas informações/dados inseridas para substituição de outras previamente registradas, sejam coletadas separadamente e atestadas como em substituição àquelas previamente registradas, as quais devem ser mantidas.	M
FUNC.20.02	Situação de registro	ABNT ISO/TS 18308 MEL4.2	Assegurar que a exata situação do registro possa ser recriada em um dado ponto no tempo desde a criação original do RES.	R

FUNC.21 - Preservação de contexto

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.21.01	Preservação da linguagem original do registro	ABNT ISO/TS 18308 MEL5.1	Suportar que textos originais sejam preservados no idioma original, sempre que o texto ou termos codificados no RES tenham sido traduzidos ou mapeados.	R
FUNC.21.02	Associação da informação do contexto clínico	ABNT ISO/TS 18308 MEL5.2	Manter a associação da informação do contexto clínico e elementos de dados relevantes independentemente de como os dados tenham sido estruturados.	R

FUNC.22 - Permanência

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.22.01	Permanência	ABNT ISO/TS 18308 MEL6.1	Impedir a alteração ou exclusão de qualquer informação armazenada no RES.	R

FUNC.23 - Controle de versão

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.23.01	Controle de versões	ABNT ISO/TS 18308 MEL7.1	Suportar o versionamento das informações/dados armazenados no RES.	R
FUNC.23.02	Medidas de discernimento	ABNT ISO/TS 18308 MEL7.2	Suportar a visualização do versionamento das informações/dados contidos no RES, sempre que aplicável (ex. mudança de nome, sexo, etc.).	R

FUNC.24 - Ética

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.24.01	Registro de justificativa ética	ABNT ISO/TS 18308 ETH1.1	Suportar o registro da justificativa ética e da aprovação para uso secundário da informação do paciente constante no RES.	R

FUNC.25 - Direitos do paciente

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.25.01	Visão orientada para o paciente	ABNT ISO/TS 18308 COC1.1	Suportar o direito de acesso do paciente ao seu RES.	R
FUNC.25.02	Direito de acesso	ABNT ISO/TS 18308 COC1.2	Suportar o direito de acesso a todas as informações do RES sujeitas a questões legais.	M
FUNC.25.03	Informações dos pacientes	ABNT ISO/TS 18308 COC1.3	Suportar a incorporação no RES de informações dos pacientes sobre “auto-cuidado”, ponto de vista pessoal sobre as questões de saúde, níveis de satisfação, expectativas e comentários, quando assim o desejarem.	R

FUNC.26 - Questões culturais

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.26.01	Interoperabili-dade	ABNT ISO/TS 18308 COC2.1	Suportar a interoperabilidade de tal forma que seja realmente global, respeitando, contudo, os costumes e cultura locais. O processo deve ser sempre simples e adaptável a diferentes ambientes legais.	R

FUNC.27 - Evolução

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
FUNC.27.01	Compatibilida-de retroativa	ABNT ISO/TS 18308 EVO1.1	Ser compatível com arquiteturas e versões antigas dos S-RES, de forma que possa processar dados criados nessas versões.	R
FUNC.27.03	Novos conhecimentos	ABNT ISO/TS 18308 EVO1.3	Ser capaz de incorporar o registro de informação relacionada a novos conhecimentos clínicos, novas disciplinas clínicas, e novas práticas e processos clínicos.	R

8.6. Requisitos para GED

SGED.01 - Gerais

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
SGED.01.01	Utilização de banco de dados	Resolução CFM 1821/2007	Utilizar base de dados adequada para o armazenamento dos arquivos digitalizados, em banco de dados relacional.	M
SGED.01.02	Método de Indexação	Resolução CFM 1821/2007	Possuir método de indexação que permita criar um arquivamento organizado, possibilitando a pesquisa de maneira simples e eficiente.	M
SGED.01.03	Organização dos documentos	Resolução CFM 1821/2007	Permitir a organização dos documentos em pastas e sub-pastas, de forma a representar a estrutura de seções de um Prontuário.	M
SGED.01.04	Qualidade	Resolução CFM 1821/2007	O documento digitalizado deve reproduzir todas as informações dos documentos originais. Em caso de digitalização de registros multimídia, tais como imagens, vídeos e áudios, é responsabilidade da comissão de prontuários analisar os algoritmos e formatos utilizados no processo, que eventualmente causem redução da qualidade das imagens. As assinaturas do software, do operador e do responsável devem ser apostas no registro final que será armazenado (pós-processado). O sistema deve armazenar os algoritmos utilizados no processamento dos registros.	M
SGED.01.05	Formatos de arquivo	SBIS	Permitir o armazenamento de vários formatos de documentos (PDF, DOC, JPG, PNG, GIF, XLS, PPT, etc.).	M
SGED.01.06	Integração com sistemas externos	SBIS	Permitir a integração com sistemas de informação externos, tais como sistemas de gestão hospitalar, ambulatorial, SADT, etc.	R

8.7. Requisitos para TISS

TISS.01 – Conteúdo e Estrutura para Prestadores do Grupo 1

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Grupo 1*	SADT s
TISS.01.01	Guia de Consulta TISS	ANS – RN 153, 29/05/2007	O S-RES deve ser capaz de capturar e/ou gerar os dados da **Guia de Consulta** TISS, conforme: http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/consulta/Guia_Consulta.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M	X
TISS.01.02	Guia de Serviços Profissionais / SADT	ANS – RN 153, 29/05/2007	O S-RES deve ser capaz de capturar e/ou gerar os dados da Guia de Serviços Profissionais / Serviço Auxiliar Diagnóstico e Terapia (SP/SADT) TISS, conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/sp-sadt/Guia_SADT.xls http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/sp-sadt/Guia_SADT.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M	X
TISS.01.03	Guia TISS de Solicitação de Internação	ANS – RN 153, 29/05/2007	O S-RES deve ser capaz de capturar os dados da Guia TISS de Solicitação de Internação, conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/solicita%20interna%E7%E3o/Guia_Solicitacao_Internacao.xls e gerar este conteúdo em XML para compor a mensagem eletrônica "SOLICITACAO_PROCEDIMENTOS" conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M	X
TISS.01.04	Guia TISS de Resumo de Internação	ANS – RN 153, 29/05/2007	O S-RES deve ser capaz de capturar os dados da Guia TISS de Resumo de Internação, conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/resumo%20e%20interna%E7%E3o/Guia_Resumo_Internacao.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M	X

* Grupo 1 – inclui todos os S-RES no Grupo 1 da Tabela 1 (item 3.1.), EXCETO S-RES para SADT isolados.

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	Grupo 1*	SADT s
TISS.01.05	Guia TISS de Honorário Individual	ANS – RN 153, 29/05/2007	O S-RES deve ser capaz de capturar os dados da Guia TISS de e Honorário Individual conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/Honor%E1rio%20Individual/Guia_Honorario_Individual.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M	R
TISS.01.06	Guia TISS de Outras Despesas	ANS – RN 153, 29/05/2007	O S-RES deve ser capaz de capturar os dados da Guia TISS de Outras Despesas conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/outras%20despesas/Guia_Outras_Despesas.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	O	R

TISS.02 – Conteúdo e Estrutura para Prestadores do Grupo 2

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
TISS.02.01	Guia de Consulta TISS	ANS – RN 153, 29/05/2007	O sistema de informações de prestadores da categoria 2 deve ser capaz de capturar e/ou gerar os dados da **Guia de Consulta** TISS, conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/consulta/Guia_Consulta.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.02.02	Guia TISS de Solicitação de Internação	ANS – RN 153, 29/05/2007	O sistema de informações de prestadores da categoria 2 deve ser capaz de capturar os dados da **Guia TISS de Solicitação de Internação**, conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/solicita%20interna%E7%E3o/Guia_Solicitacao_Internacao.xls e gerar este conteúdo em XML para compor a mensagem eletrônica "SOLICITACAO_PROCEDIMENTOS" conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.02.03	Guia de Serviços Profissionais / SADT	ANS – RN 153, 29/05/2007	O sistema de informações de prestadores da categoria 2 deve ser capaz de capturar e/ou gerar os dados da **Guia de Serviços Profissionais / Serviço Auxiliar Diagnóstico e Terapia (SP/SADT)** TISS, conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/sp-sadt/Guia_SADT.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M

TISS.03 – Conteúdo e Estrutura para Prestadores do Grupo 3

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
TISS.03.01	Guia de Tratamento Odontológico - Solicitação	ANS – RN 153, 29/05/2007	O sistema de informações de prestadores da categoria 3 deve ser capaz de capturar os dados da **Guia TISS de Tratamento Odontológico - Solicitação** conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/tratamento%20odontol%F3gico/Guia_Solicitacao_odontologia.xls e gerar este conteúdo em XML para compor a mensagem eletrônica AUTORIZACAO_ODONTOLOGIA conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M
TISS.03.02	Guia de Tratamento Odontológico - Cobrança	ANS – RN 153, 29/05/2007	O sistema de informações de prestadores da categoria 3 deve ser capaz de capturar os dados da Guia TISS de Tratamento Odontológico - Cobrança conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/tratamento%20odontol%F3gico/Guia_Cobranca_odontologia.xls e gerar este conteúdo em XML para compor a mensagem eletrônica ENVIO_GUIAS conforme o esquema XML publicado em http://www.ans.gov.br/padroes/tiss/esquemas	M

TISS.04 – Conteúdo e Estrutura para Operadoras de Planos de Assistência Médica (Grupos 1 e 2)

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
TISS.04.01	Demonstrativo de Pagamento	ANS – RN 153, 29/05/2007	O sistema de informações das operadoras de planos de assistência medica deverá gerar os dados do **Demonstrativo de Pagamento**, conforme: http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/demonstrativos/Demonstrativo.doc	M
TISS.04.02	Demonstrativo de Análise de Conta Médica	ANS – RN 153, 29/05/2007	O sistema de informações das operadoras de planos de assistência medica deverá gerar os dados do **Demonstrativo de Análise de Conta Médica** conforme http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/demonstrativos/Demonstrativo_Conta_Medica.doc	M

TISS.05 – Conteúdo e Estrutura para Operadoras exclusivamente de Planos Odontológicos (Grupo 3)

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
TISS.05.01	Guia de Tratamento Odontológico - Demonstrativo de Pagamento	ANS – RN 153, 29/05/2007	O sistema de informações das operadoras de planos exclusivamente odontológicos deverá gerar os dados do **Guia de Tratamento Odontológico - Demonstrativo de Pagamento**, conforme: http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/guias/tratamento_odontol%F3gico/Guia_demonstrativo_pagamento_Odonto.xls	M

TISS.06 – Comunicação para Prestadores dos Grupos 1 e 2

Nota 1: Observar que o conteúdo das mensagens em XML deve obedecer aos esquemas descritos acima nos requisitos de conteúdo, de acordo com o grupo no qual o S-RES se enquadra, conforme classificação da ANS. Por exemplo, em se tratando de S-RES de consultório médico este deverá enviar as Guias de Faturamento de seu contexto, ou seja, as Guias de Consulta. Portanto, não será exigido que um S-RES de consultório seja capaz de enviar Guias de Resumo de Internação.

Nota 2: Conforme o Manual de Comunicação e Segurança das Mensagens TISS, a comunicação prestador operadora poderá ser: via *WebServices* (preferencialmente), via troca de arquivos em diretórios de entrada e saída, também definidos pelo padrão TISS, ou, ainda através de *upload* no sítio das operadoras na internet. Cada uma das mensagens abaixo descritas deverá, portanto, obedecer a pelo menos um destes métodos de comunicação para que o S-RES nesta categoria venha a ser certificado.

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
TISS.06.01	Guias de Faturamento	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de gerar o conteúdo em XML da Mensagem TISS ENVIO_LOTE_GUIAS conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.06.02	Protocolo de Recebimento Lote de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem TISS "PROTOCOLO_RECEBIMENTO" conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.06.03	Solicitação do Status do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de gerar o conteúdo em XML da Mensagem TISS SOLIC_STATUS_PROTOCOLO conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.06.04	Recebimento da Situação do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem SITUACAO_PROTOCOLO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.06.05	Solicitação de Procedimentos	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de gerar o conteúdo em XML da Mensagem TISS SOLICITACAO_PROCEDIMENTOS , conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.06.06	Recebimento Autorização de Procedimentos	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem AUTORIZACAO_PROCEDIMENTOS, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.06.07	Solicitação do Status da Autorização	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS SOLICITA_STATUS_AUTORIZACAO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
TISS.06.08	Solicitação dos Demonstrativos de Retorno	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS SOLIC_DEMONSTRATIVO_RETORNO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.06.09	Recebimento de demonstrativos de pagamento, da análise de contas médicas e de odontologia	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber as mensagens TISS "DEMONSTRATIVO_PAGAMENTO" e "DEMONSTRATIVO_ANALISE_CONTA_MEDICA" conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.06.10	Reapresentação de guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS ENVIO_LOTE_GUIAS incorporando a RE_APRESENTACAO_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.06.11	Cancelamento de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS CANCELA_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.06.12	Verificação de Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS VERIFICA_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	O
TISS.06.13	Recebimento da resposta a Verificação Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem TISS SITUACAO_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	O

TISS.07 – Comunicação para Prestadores do Grupo 3

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
TISS.07.01	Guias de Faturamento	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de gerar o conteúdo em XML da Mensagem TISS ENVIO_LOTE_GUIAS conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.07.02	Protocolo de Recebimento do Lote de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem TISS “PROTOCOLO_RECEBIMENTO” conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.07.03	Solicitação do Status do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de gerar o conteúdo em XML da Mensagem TISS SOLIC_STATUS_PROTOCOLO conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
TISS.07.04	Recebimento da Situação do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem SITUACAO_PROTOCOLO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.07.05	Solicitação de Autorização Procedimentos Odontologia	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de gerar o conteúdo em XML da Mensagem TISS AUTORIZACAO_ODONTOLOGIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.07.06	Recebimento da Autorização de Procedi-mentos	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem AUTORIZACAO_PROCEDIMENTOS, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.07.07	Solicitação do Status da Autorização	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS SOLICITA_STATUS_AUTORIZACAO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.07.08	Solicitação dos Demonstrativos de Retorno Odontologia	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS SOLIC_DEMONSTRATIVO_RETORNO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.07.09	Recebimento, Demonstrativo de Odontologia	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber as mensagens TISS "DEMONSTRATIVO_ODONTOLOGIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.07.10	Reapresen-tação de guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS ENVIO_LOTE_GUIAS incorporando a RE_APRESENTACAO_GUIA , conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.07.11	Cancelamento de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS CANCELA_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.07.12	Verificação de Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar as operadoras a mensagem TISS VERIFICA_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	O
TISS.07.13	Recebimento da resposta a Verificação Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber das operadoras a mensagem TISS SITUACAO_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	O

TISS.08 – Comunicação para Operadoras de Planos de Assistência Médica (Grupos 1 e 2)

Nota: Além dos requisitos abaixo, as Operadoras devem atender também ao disposto na Nota Esclarecedora DIDES/GGSUS Nº 001/2008, disponível em: http://www.ans.gov.br/portal/site/_hotsite_tiss/nota_esclarecedora_001_2008.htm

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
TISS.08.01	Guias de Faturamento	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores o conteúdo em XML da Mensagem TISS : ENVIO_LOTE_GUIAS conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.08.02	Protocolo de Recebimento do Lote de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar às operadoras a mensagem TISS "PROTOCOLO_RECEBIMENTO" conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.08.03	Solicitação do Status do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores o conteúdo em XML da Mensagem TISS SOLIC_STATUS_PROTOCOLO conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.08.04	Envio da Situação do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores a mensagem SITUACAO_PROTOCOLO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.08.05	Solicitação de Procedimentos	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a Mensagem TISS SOLICITACAO_PROCEDIMENTOS , conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.08.06	Envio da Autorização de Procedimentos	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz enviar aos prestadores a mensagem TISS AUTORIZACAO_PROCEDIMENTOS, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.08.07	Solicitação do Status da Autorização	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS SOLICITA_STATUS_AUTORIZACAO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.08.08	Solicitação dos Demonstrativos de Retorno	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS SOLIC_DEMONSTRATIVO_RETORNO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.08.09	Envio de Demonstrativo de Pagamento e da Análise de contas Médicas	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores as mensagens TISS "DEMONSTRATIVO_PAGAMENTO" e "DEMONSTRATIVO_ANALISE_CONTA_MEDICA", conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.08.10	Reapresen-tação de guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS ENVIO_LOTE_GUIAS incorporando a RE_APRESENTACAO_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
TISS.08.11	Cancelamento de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS CANCELA_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.08.12	Verificação de Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS VERIFICA_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	O
TISS.08.13	Resposta a Verificação Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores a mensagem TISS SITUACAO_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	O

TISS.09 – Comunicação para Operadoras exclusivamente de Planos Odontológicos (Grupo 3)

Nota: Além dos requisitos abaixo, as Operadoras devem atender também ao disposto na Nota Esclarecedora DIDES/GGSUS Nº 001/2008, disponível em: http://www.ans.gov.br/portal/site/_hotsite_tiss/nota_esclarecedora_001_2008.htm

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
TISS.09.01	Guias de Faturamento	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores o conteúdo em XML da Mensagem TISS ENVIO_LOTE_GUIAS conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.09.02	Protocolo de Recebimento do Lote de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores a mensagem TISS "PROTOCOLO_RECEBIMENTO" conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.09.03	Solicitação do Status do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores o conteúdo em XML da Mensagem TISS SOLIC_STATUS_PROTOCOLO conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.09.04	Envio da Situação do Protocolo	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores a mensagem SITUACAO_PROTOCOLO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.09.05	Solicitação de Procedimentos Odontologia	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a Mensagem TISS AUTORIZACAO_ODONTOLOGIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.09.06	Envio da Autorização de Procedimentos	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz enviar aos prestadores a mensagem TISS AUTORIZACAO_PROCEDIMENTOS, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M

ID	REQUISITO	REFERÊNCIA	CONFORMIDADE	PRESENÇA
TISS.09.07	Solicitação do Status da Autorização	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS SOLICITA_STATUS_AUTORIZACAO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.09.08	Solicitação dos Demonstrativos de Retorno	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS SOLIC_DEMONSTRATIVO_RETORNO, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.09.09	Envio de Demonstrativo de Pagamento e da Análise de contas Médicas	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores as mensagens TISS DEMONSTRATIVO_ODONTOLOGIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.09.10	Reapresen-tação de guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS ENVIO_LOTE_GUIAS incorporando a RE_APRESENTACAO_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.09.11	Cancelamento de Guias	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS CANCELA_GUIA, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	M
TISS.09.12	Verificação de Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de receber dos prestadores a mensagem TISS VERIFICA_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	O
TISS.09.13	Envio da resposta a Verificação Elegibilidade	ANS – RN 153, 29/05/2007 e IN nº 26, de 10/05/2007	O S-RES deve ser capaz de enviar aos prestadores a mensagem TISS SITUACAO_ELEGIBILIDADE, conforme esquemas descritos em http://www.ans.gov.br/padroes/tiss/schemas	O

9. Referências

[1] CFM. Resolução 1638/2002. On-line. Disponível em: http://www.portalmedico.org.br/resolucoes/cfm/2002/1638_2002.htm

[2] CFM. Resolução 1639/2002. On-line. Disponível em: http://www.portalmedico.org.br/resolucoes/cfm/2002/1639_2002.htm

[3] CFM. Resolução 1821/2007. On-line. Disponível em: http://www.portalmedico.org.br/resolucoes/cfm/2007/1821_2007.htm

[4] MEDIDA PROVISÓRIA No 2.200-2, DE 24 DE AGOSTO DE 2001. On-line. Disponível em: https://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm

[5] Cadastro Nacional de Usuários do Sistema Único de Saúde. Disponível em: http://cartaonet.datasus.gov.br/

[6] Cadastro Nacional de Estabelecimentos e Profissionais de Saúde – CNES. Disponível em: http://www.datasus.gov.br/cnes

[7] Padrão TISS. Disponível em: http://www.ans.gov.br/portal/site/_hotsite_tiss

[8] ISO/TR 20.514:2005 Technical Report - Health informatics -- Electronic health record -- Definition, scope and context. Disponível em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39525

[9] ISO/TS 18.308:2004 - Health informatics -- Requirements for an electronic health record architecture. Disponível em: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33397

[10] ABNT ISO/TR 20.514 – Informática em saúde - Registro eletrônico de saúde - Definição, escopo e contexto. Disponível em: http://www.abntnet.com.br/fidetail.aspx?FonteID=41192

[11] ABNT ISO/TS18.308 - Informática em saúde - Requisitos para uma arquitetura do registro eletrônico. Disponível em: http://www.abntnet.com.br/fiprint.aspx?FonteID=41190

[12] ISO/IEC 27.002:2005 - Information technology -- Security techniques -- Code of practice for information security management. Disponível em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

[13] ABNT NBR ISO/IEC 27.002:2005 (antiga NBR ISO/IEC 17799:2005) - Código de Prática para a Gestão da Segurança da Informação. Disponível em: http://www.abntnet.com.br/ecommerce/default.aspx

[14] ISO/IEC 15.408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model. Disponível em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40612

[15] ISO/IEC 15.408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements. Disponível em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40613

[16] ISO/IEC FCD 15.408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements. Disponível em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40614

[17] HL7 – Health Level 7 – http://www.hl7.org

[18] HL7 -EHR Functional Model. Disponível em: http://www.hl7.org/EHR/

[19] CCHIT. Commercial Certification Handbook. Ambulatory EHR Products. Disponível em: http://www.cchit.org/files/Ambulatory_Domain/2007AEHRCertificationHandbookV2_1.pdf

[20] ABNT NBR ISO/IEC 27.001:2006 Sistemas de Gestão de Segurança da Informação – Requisitos. Disponível em: http://www.abntnet.com.br/ecommerce/default.aspx

[21] ISO/FDIS - 21549-7 - Health informatics - Patient healthcard data - Part 7: Medication data - Final draft 2007

[22] Mon, Donald T.. “Difference Between the EHR Standard and Certification.“ Journal of AHIMA 77, no.5 (May 2006): 66,68,70.

[23] ETSI TS 101 733: ETSI. "Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats".

[24] ABNT ISO/IEC GUIA 65/1997 Requisitos para Organismos que Operam Sistemas de Certificação de Produtos.

[25] ABNT NBR ISO/IEC 17021:2007 Avaliação de Conformidade – Requisitos para Organismos que Fornecem Auditoria e Certificação de Sistemas de Gestão.