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

Versão 4.1

CERTIFICAÇÃO 2013

Editor:
Marcelo Lúcio da Silva

22/10/2013

Conselho Federal de Medicina

Diretoria

Gestão 2009-2014

Presidente:	Roberto Luiz d´Avila
1º Vice-Presidente:	Carlos Vital Corrêa Lima
2º Vice-Presidente:	Aloísio Tibiriçá Miranda
3º Vice-Presidente:	Emmanuel Fortes Silveira Cavalcanti
Secretário-geral:	Henrique Batista e Silva
1º Secretário:	Desiré Carlos Callegari
2º Secretário:	Gerson Zafalon Martins
Tesoureiro:	José Hiran da Silva Gallo
2º Tesoureiro:	Frederico Henrique de Melo
Corregedor:	José Fernando Maia Vinagre
Vice-Corregedor:	José Albertino Souza

Câmara Técnica de Informática em Saúde

Roberto Luiz d'Avila - Coordenador
Alan do Nascimento Santos
Antonio Carlos Endrigo
Antônio César de Azevedo Neves
Beatriz de Faria Leão
Carlos Vital Tavares Corrêa Lima
Claudio Giulliano Alves da Costa
Cristianne da Silva Gonçalves
Desiré Carlos Callegari
Gerson Zafalon Martins
Goethe Ramos
José Mário Morais Mateus
Luciano Mauricio Sampaio Barreto
Marizélia Leão Moreira
Moacyr Perche
Murilo Rezende Melo
Rogério Sugai Mortoza
Ruy Ramos
Sylvain Nahum Levy

Sociedade Brasileira de Informática em Saúde

Diretoria

Gestão 2013-2014

Presidente:	Marco Antonio Gutierrez
Vice-Presidente:	Heimar de Fátima Marin
Secretário:	Marcia Ito
Tesoureiro:	Stanley da Costa Galvão
Diretor Executivo:	Marcelo Lúcio da Silva
Dir. Educação:	Paulo Mazzoncini de Azevedo Marques
Dir. Rel. Institucionais:	Cláudio Giulliano Alves da Costa
Dir. Atend. Associado:	Claudia Maria Cabral Moro Barra
Representante na IMIA:	Lincoln de Assis Moura Jr
Editora-Chefe do JHI:	Heimar de Fátima Marin

Autores desta edição do manual:

Eduardo Pereira Marques
Gislaine Lirian Bueno de Oliveira
Luis Gustavo Gasparini Kiatake
Marcelo Antonio de Carvalho Júnior
Marcelo Lúcio da Silva
Volnys Borges Bernal

Colaboraram nas edições anteriores:

Adilson Eduardo Guelfi
Alex Souza Silveira
Beatriz de Faria Leão
Cláudio Giulliano Alves da Costa
John Lemos Forman
Leopoldo Santana Luz
Luiz Renato Evangelisti
Matteo Nava
Osni Pereira
Stanley da Costa Galvão
Tulio Toshiharu Rodrigues Takemae

Índice

Glossário

ABNT	Associação Brasileira de Normas Técnicas
AC	Autoridade Certificadora
ANS	Agência Nacional de Saúde Suplementar
ANSI	American National Standards Institute
CC	Centro de Certificação da SBIS
CCHIT	Certification Commission for Healthcare Information Technology
CFM	Conselho Federal de Medicina
CNES	Cadastro Nacional de Estabelecimentos e Profissionais de Saúde do SUS
HL7	Health Level Seven
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	International Eletrotechnical Commission
ISO	International Organization for Standardization
ITI	Instituto Nacional de Tecnologia da Informação
MS	Ministério da Saúde
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 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

Nas últimas décadas, a tecnologia afetou significativamente a forma como os indivíduos e organizações lidam com suas informações. Em um processo irreversível, os registros em papel vêm sendo transformados em registros eletrônicos, possibilitando inúmeras vantagens proporcionadas por este meio. O mesmo vem ocorrendo na área da saúde, onde profissionais e instituições, consoantes à evolução tecnológica, vêm adotando cada vez mais os registros eletrônicos em suas atividades.

A área da saúde, contudo, apresenta características e condições bastante específicas, tornando-a única perante as demais atividades profissionais e setores da economia, principalmente naquilo que tange às questões de privacidade e confidencialidade dos indivíduos assistidos, à integridade e segurança das informações e aos recursos mínimos necessários para o perfeito registro dos atos praticados e das condições de saúde dos indivíduos.

Neste cenário, o Conselho Federal de Medicina (CFM) visou as questões concernentes à legalidade da utilização de sistemas informatizados para capturar, armazenar, manusear e transmitir dados do atendimento em saúde, incluindo as condições para a substituição do suporte papel pelo meio eletrônico. Ciente da complexidade do assunto e da necessidade de aprofundar os aspectos técnicos sobre o tema, o CFM, através da Câmara Técnica de Informática em Saúde, 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 nº 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 nº 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 teve 70 sistemas declarados pelos representantes legais das organizações detentoras, como aderentes ao conjunto de requisitos da versão 2.1 do manual (auto-declaração). A Fase 1 teve como objetivo preparar o mercado para o processo de certificação, o que foi plenamente atingido.

A publicação da versão 3.2 (Edição 2008) do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) em agosto de 01/08/2008 encerrou as possibilidades de auto-declaração (Fase 1) e deu início ao processo de auditoria efetiva dos sistemas (Fase 2). 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.

Desde o início da Fase 2, diversos sistemas foram auditados sob este processo, sendo vários destes aprovados. A lista atualizada dos sistemas certificados pode ser consultada no sítio da SBIS na internet (www.sbis.org.br/certificacao).

Em 20/05/2009 foi publicada a versão 3.3 (Edição 2009) deste manual, a qual permanecerá válida até o início da vigência da presente versão. Esta versão (4.1) do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) revoga e substitui, a partir da data de início de sua vigência, 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 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.

2.1.3. 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.

2.1.4. 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.

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.

2.1.5. 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 está organizado em cinco componentes: organizacional, conteúdo e estrutura, representação de conceitos em saúde, 'segurança e privacidade' e comunicação, conforme descrevem as Resoluções Normativas publicadas no sítio da ANS.

A ANS determinou que as normas técnicas estabelecidas pelo CFM 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 *webservices* 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.

2.1.6. Normas ISO TC-215

A norma ISO/TR 20.514[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 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[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.

A norma ISO/DIS 27.799[26] "*Health informatics -- Information security management in health using ISO/IEC 27.002*" detalha e destaca a importância do emprego dos controles de segurança descritos na ISO/IEC 27.002[12] com foco na área de saúde.

2.1.7. Comissão de Estudo Especial de Informática em Saúde (CEEIS) 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: Arquitetura
- GT 2: Comunicação e Interoperabilidade
- GT 3: Conteúdo Semântico
- GT 4: Segurança da Informação e do Paciente

2.1.8. 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 "*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 – "Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação" [13].

A norma ISO/IEC 15.408 "*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.

2.1.9. 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.

2.1.10. 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. 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 banco 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.

Atualmente, o processo de Certificação SBIS-CFM está disponível apenas para algumas categorias mais genéricas de S-RES. No futuro próximo, e considerando a demanda que vier a ser constatada, 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, pode ser submetido ao processo qualquer S-RES que atenda minimamente à seguinte categoria:

- **Básica** – S-RES voltados à assistência à saúde de indivíduos, de forma básica e genérica (não específica), tais como: automação de consultórios clínicos, atendimento ambulatorial, unidades básicas de saúde, atendimento e/ou internação hospitalar, pronto-atendimento, saúde ocupacional, clínicas de imunização, *home care*, serviços de diagnóstico e terapia, etc.

A categoria Básica poderá ser complementada com um ou mais blocos de especialização, que são incrementos voltados a segmentos específicos da assistência à saúde, tais como atendimento ambulatorial, internação hospitalar, pronto-atendimento, saúde ocupacional, etc. Estes blocos deverão ser sempre agregados à categoria Básica. Atualmente, está disponível apenas o bloco Ambulatorial, sendo que posteriormente serão disponibilizados blocos para outros segmentos da assistência.

- **Ambulatorial** – S-RES voltados para a assistência ambulatorial, tais como: automação de consultórios clínicos, clínicas, unidades básicas de saúde, etc., assim como a parte ambulatorial de sistemas hospitalares ou de sistemas integrados de informação em saúde.

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 que o sistema opere sem a geração de registros impressos (sistema sem papel - *paperless*). Adicionalmente, o S-RES deverá ser identificado como sendo um S-RES local ou remoto, refletindo se o mesmo funciona somente no próprio computador onde for instalado (local) ou se pode ser acessado remotamente a partir de estações de trabalho conectadas ao computador (remoto).

Para ser aprovado, um S-RES precisará necessariamente se enquadrar pelo menos na categoria Básica descrita acima, atendendo a todos os requisitos obrigatórios estabelecidos para a mesma, 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, presente nas edições anteriores deste manual, está ausente na presente edição devido ao momento de transição, pela ANS, da versão 2.0 para a versão 3.1 do padrão TISS. Um conjunto atualizado de requisitos ou um novo processo de certificação para a categoria TISS será lançado complementarmente a este manual, quando tal categoria voltará a ser passível de certificação.

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.

As categorias para enquadramento podem ser resumidas, de forma esquemática, conforme disposto na Figura 1 a seguir:

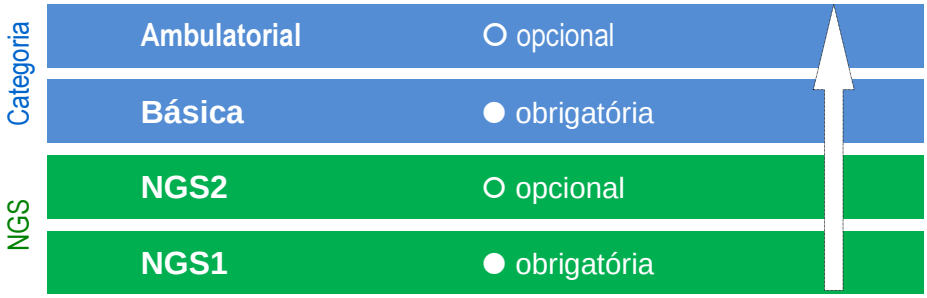

Figura 1: Modelo esquemático das categorias para certificação

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: **Básica** ou **Ambulatorial**

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”. Deve-se, contudo, atentar que necessariamente **a categoria Ambulatorial inclui a Básica**, assim como **o NGS2 inclui o NGS1**.

Caso seja solicitada a certificação para a categoria Ambulatorial e a auditoria apontar não-conformidade aos requisitos da mesma, mas apontar conformidade aos requisitos da categoria Básica, será possível, a critério do Solicitante, a obtenção da certificação na categoria Básica, desde que atingida a conformidade no mínimo ao NGS1.

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, será possível, a critério do Solicitante, a obtenção da certificação no nível NGS1, desde que atingida a conformidade no mínimo à categoria Básica.

4. Conceitos, Normas e Condições da Certificação

4.1. Componentes do 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 SBIS fará a auditoria com base no S-RES identificado e descrito pelo Solicitante, considerando ainda as categorias para as quais a certificação foi 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 de suporte

A seguir apresenta-se uma lista, não exaustiva, dos componentes de suporte que devem ser considerados ao elaborar a descrição do S-RES:

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

4.1.2. Componentes alternativos de suporte

Além dos componentes descritos na auditoria, o Solicitante poderá informar uma lista contendo os componentes de suporte para os quais o S-RES também funciona e que 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 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 reproduza 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 4.4.), 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. Versões de S-RES

Cada certificado está relacionado a uma versão específica do S-RES, testada no processo de auditoria e em total conformidade com os requisitos estabelecidos. Assim, a descrição de um S-RES deverá incluir também a identificação da sua versão.

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 “ajustes não relevantes” ou “ajustes relevantes” no contexto da certificação.

É possível solicitar que a certificação concedida a uma determinada versão de um S-RES seja estendida para outras versões (ver item 4.3.), considerando-se a classificação dos ajustes conforme exposto adiante.

4.2.1. Ajustes Não Relevantes

Entende-se por “ajustes não relevantes” as modificações e atualizações cujo objeto ou alvo não tenham relação direta com qualquer requisito da certificação. Como exemplos de ajustes não relevantes, 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;
- Pequenas modificações na interface com o usuário (esquemas de cores, fontes, estilos de botões, etc.);
- Adição de novas funcionalidades ou módulos 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).

4.2.2. Ajustes Relevantes

Entende-se por "ajustes relevantes" as modificações cujo objeto ou alvo tenham relação direta com algum requisito da certificação, o que pode implicar em risco significativo à manutenção da sua conformidade. 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;
- 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.

4.2.3. 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 4.3.), cabendo integral e exclusivamente ao Solicitante a responsabilidade pela veracidade da declaração de manutenção da conformidade da nova versão do S-RES.

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 4.4.), 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.

4.3. Extensão da Certificação para Outras Versões do S-RES

O Certificado SBIS-CFM é específico para a versão do S-RES nele discriminada.

A SBIS poderá estender a certificação para outras versões de um S-RES já certificado, desde que tal extensão seja obtida durante o período de validade do certificado original. Para tanto, o Solicitante deverá preencher a Ficha de Inscrição para Extensão de Certificação (ver item 4.4.) e submetê-la ao processo descrito no capítulo 5 deste manual.

A solicitação de extensão deverá conter a descrição de todos os ajustes realizados na nova versão ("*release notes*"). Se a nova versão contiver qualquer "ajuste relevante" (ver item 4.2.2), o processo de extensão incluirá auditoria à mesma.

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 4.4.), 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 ajustes não relevantes 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 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 versão na lista dos S-RES certificados, disponível para consulta no sítio da SBIS na internet. Apenas então o Solicitante poderá se referir a esta nova versão como sendo objeto da extensão do certificado pela SBIS.

As 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.

4.4. Validade da Certificação

O Certificado SBIS-CFM será válido por um período calculado da seguinte forma: 02 (dois) anos a partir da emissão, ou 06 (seis) meses a partir da publicação pela SBIS da versão do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-

RES) imediatamente 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 seis meses 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.

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 (noventa) 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.

4.5. Instrumentos Formais

A certificação será formalizada e regulamentada pelos seguintes instrumentos:

- **Ficha de Inscrição para Certificação**: formulário eletrônico 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 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 valores envolvidos, 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.

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

- **Termo de Extensão de Certificado:** documento probatório da extensão do certificado de um determinado S-RES pela SBIS-CFM .

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

4.6. 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, que proporciona ao mesmo unicamente o direito à análise e avaliação de tal ficha pela SBIS e à elaboração do Contrato de Certificação.

- **Taxa de Qualificação para Auditoria:** valor a ser pago pelo Solicitante à SBIS no momento do agendamento da sessão qualificatória, e que proporciona ao mesmo o direito à realização de tal sessão.

- **Taxa de Auditoria e Certificação:** valor a ser pago pelo Solicitante à SBIS no momento do agendamento do 1º ciclo de auditoria, e que proporciona ao mesmo o direito à realização de tal ciclo e, caso venha a ser 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 imediatamente após o envio da Ficha de Inscrição para 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 venha a ser aprovado (obtenha a extensão do certificado), à emissão do Termo de Extensão 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, e que proporciona ao mesmo apenas o direito à execução desta parte do processo.

- **Taxa de Reagendamento:** valor a ser pago pelo Solicitante à SBIS quando houver, a pedido do Solicitante, a necessidade de reagendamento de uma sessão qualificatória ou ciclo de auditoria cujo cronograma tenha sido previamente aprovado entre as partes.

4.6.1. 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, a não qualificação para a auditoria 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

O processo para a obtenção da certificação é constituído pelas seguintes etapas:

a) Preparação
b) Inscrição e formalização
c) Qualificação
d) Auditoria
e) Conclusão

Há, adicional e opcionalmente, o processo para a extensão de uma certificação já concedida.

5.1. Preparação

Os primeiros passos visando a certificação de um S-RES devem ser executados internamente pela organização interessada (Solicitante), que deve:

a) Analisar toda 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 mandatórios para as categorias desejadas;

c) Efetuar os ajustes eventualmente necessários no S-RES para o pleno atendimento aos requisitos mandatórios;

d) Realizar internamente a bateria de testes, conforme descrito no Manual Operacional de Ensaios e Análises para a Certificação de S-RES;

e) Estando a organização interessada segura de que seu S-RES está em condições de ser aprovado na auditoria, proceder à inscrição no processo da Certificação SBIS-CFM.

5.2. Inscrição e Formalização

5.2.1. Envio da Ficha de Inscrição para Certificação

O Solicitante deverá preencher a Ficha de Inscrição para Certificação (ver item 4.5.), disponível para *download* no sítio da Certificação SBIS-CFM na internet, e enviá-la eletronicamente através do e-mail certificacao@sbis.org.br.

5.2.2. Pagamento da Taxa de Inscrição

A SBIS enviará por e-mail ao Solicitante, no prazo máximo de 05 (cinco) dias úteis após o recebimento da Ficha de Inscrição, um boleto bancário referente à Taxa de Inscrição no processo de certificação (ver item 4.6.). 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 no prazo máximo de 10 (dez) dias úteis após o envio do boleto.

5.2.3. Assinatura do 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 4.5.), ainda não assinado. O Solicitante deverá analisar cuidadosamente o contrato, questionando a SBIS sobre qualquer dúvida que porventura seja suscitada.

Caso o Solicitante concorde com todos os termos do contrato, deverá devolvê-lo assinado pelo(s) seu(s) representante(s) legal(is) em 02 (duas) vias à SBIS, que por sua vez também as assinará e enviará uma das vias de volta ao Solicitante.

Caso não ocorra a devolução do contrato assinado à SBIS no prazo de 60 (sessenta) dias após o recebimento do mesmo, o processo será considerado encerrado.

Processos encerrados não poderão ser reativados, devendo o Solicitante, quando necessário, iniciar um novo processo, submetendo nova Ficha de Inscrição.

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 sobre a impossibilidade de execução do processo de certificação, onde serão expostos os motivos para tal rejeição.

5.3. Qualificação

Para que possa ser submetido à auditoria, o S-RES deverá passar por uma sessão qualificatória, onde os auditores verificarão se o mesmo encontra-se minimamente apto para a auditoria e indicarão os principais pontos que deverão ser alvo de atenção e ajustes.

A sessão qualificatória consistirá em uma prévia simplificada das mesmas rotinas que serão executadas na auditoria, onde o Solicitante obterá uma lista preliminar (não-exaustiva) das principais não-conformidades que poderão ser apontadas durante a auditoria, e poderá dirimir eventuais dúvidas de entendimento acerca dos respectivos requisitos.

5.3.1. Solicitação da Qualificação

Concluída a formalização do contrato (ver item 5.2.3), o Solicitante deverá, no prazo máximo de 180 (cento e oitenta) dias, solicitar por e-mail à SBIS o agendamento da sessão qualificatória. Caso tal solicitação não ocorra neste prazo, o processo será considerado encerrado.

5.3.2. Pagamento da Taxa de Qualificação

A SBIS enviará por e-mail ao Solicitante, no prazo máximo de 05 (cinco) dias úteis após o recebimento da solicitação do agendamento, um boleto bancário referente à Taxa de Qualificação para Auditoria (ver item 4.6.). 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 no prazo máximo de 10 (dez) dias úteis após o envio do boleto.

5.3.3. Agendamento da Qualificação

Respeitada a ordem cronológica das solicitações e mediante a disponibilidade de datas, a SBIS enviará ao Solicitante as possibilidades de agendamento para a sessão qualificatória, o qual deverá responder indicando sua aceitação a alguma das opções propostas. Caso nenhuma das opções atenda à disponibilidade do Solicitante, as partes seguirão em negociação até que uma data seja agendada.

Não há prazo máximo pré-determinado para a data da sessão qualificatória, já que tal prazo dependerá da quantidade de solicitações pendentes (“fila de espera”), e observada a capacidade operacional do Centro de Certificação da SBIS.

5.3.4. Execução da Qualificação

A sessão qualificatória será executada na data previamente agendada, quando o Solicitante deverá disponibilizar o produto (S-RES) objeto da certificação e todos os aplicativos e produtos necessários à sua execução através de um dos seguintes meios:
- instalação em computadores portáteis do próprio Solicitante;
- acesso ao sistema através da internet;
- outro meio equivalente, desde que previamente acordado com a SBIS.

O Solicitante deverá, também, disponibilizar de 01 (um) a 03 (três) profissionais para operarem o sistema durante toda a sessão qualificatória. 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 sessão.

A sessão ocorrerá na sede da SBIS, em São Paulo/SP, com duração pré-determinada de 01 (um) a 03 (três) dias, e será executada por 02 (dois) auditores seniores e/ou plenos (ver capítulo 6.3.).

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.

5.3.5. Resultado da Qualificação

Com base nas observações dos auditores obtidas durante a sessão qualificatória, a SBIS emitirá e enviará ao Solicitante, no prazo máximo de 10 (dez) dias úteis após tal sessão, um parecer indicando a possibilidade ou não do S-RES ser submetido à auditoria.

Independentemente dos resultados apresentados, a sessão qualificatória nunca poderá ser entendida como e nem substituirá a auditoria, e tampouco será conclusiva para a concessão da certificação.

5.4. Auditoria

A Certificação SBIS-CFM estabelece a execução de auditoria sobre o S-RES, realizada por equipe especializada, a qual verificará se os requisitos obrigatórios para as categorias selecionadas são realmente atendidos pelo sistema.

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.

5.4.1. Solicitação da Auditoria

Obtido o resultado positivo da qualificação (ver item 5.3.5), o Solicitante deverá, no prazo máximo de 180 (cento e oitenta) dias, solicitar por e-mail à SBIS o agendamento do 1º ciclo de auditoria. Caso tal solicitação não ocorra neste prazo, o processo será considerado encerrado.

5.4.2. Pagamento da Taxa de Auditoria e Certificação

A SBIS enviará por e-mail ao Solicitante, no prazo máximo de 05 (cinco) dias úteis após o recebimento da solicitação do agendamento, um boleto bancário referente à Taxa de Auditoria e Certificação (ver item 4.6.). 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 no prazo máximo de 10 (dez) dias úteis após o envio do boleto.

5.4.3. Agendamento da Auditoria

Respeitada a ordem cronológica das solicitações e mediante a disponibilidade de datas, a SBIS enviará ao Solicitante as possibilidades de agendamento para a auditoria, o qual deverá responder indicando sua aceitação a alguma das opções propostas. Caso nenhuma das opções atenda à disponibilidade do Solicitante, as partes seguirão em negociação até que uma data seja agendada.

Não há prazo máximo pré-determinado para a data da auditoria, já que tal prazo dependerá da quantidade de solicitações pendentes (“fila de espera”), e observada a capacidade operacional do Centro de Certificação da SBIS.

5.4.4. Seleção dos Auditores

A SBIS enviará ao Solicitante a relação e o currículo dos auditores selecionados para a auditoria. A seleção será efetuada de acordo com as normas internas do Centro de Certificação, considerando, entre outros fatores, a rotatividade entre os auditores, a

disponibilidade dos mesmos e eventuais impedimentos por questões éticas ou profissionais.

A auditoria será realizada obrigatoriamente por 03 (três) auditores seniores e/ou plenos, e poderá ser acompanhada por um ou mais auditores *trainees*, cujos papéis encontram-se descritos no capítulo 6.

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 habilitação, não sendo seus registros considerados no resultado da auditoria.

Caso o Solicitante concorde com a relação dos auditores, bastará comunicar por e-mail tal aprovação à SBIS. Caso discorde, deverá comunicar por e-mail tal rejeição à SBIS, justificando explicitamente os motivos.

Na ausência de resposta do Solicitante no prazo de 05 (cinco) dias úteis após o recebimento da relação, a seleção dos auditores será automaticamente considerada aprovada.

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

5.4.5. Execução da Auditoria

A auditoria será executada na data previamente agendada, quando o Solicitante deverá disponibilizar o produto (S-RES) objeto da certificação e todos os aplicativos e produtos necessários à sua execução através de um dos seguintes meios:

- Instalação em computadores portáteis do próprio Solicitante;
- Acesso ao sistema através da internet;
- Outro meio equivalente, desde que previamente acordado com a SBIS.

O Solicitante deverá, também, disponibilizar de 01 (um) a 03 (três) profissionais para operarem o sistema durante toda a 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 sessão.

O Solicitante deverá enviar à SBIS, com antecedência mínima de 05 (cinco) dias úteis do início da auditoria, os seguintes documentos:

- Todos os manuais do S-RES objeto da auditoria;
- Esquema gráfico da estrutura lógica de ligação dos componentes do S-RES, consoante a todas as formas oferecidas para comercialização e/ou implementação.

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

A auditoria ocorrerá na sede da SBIS, em São Paulo/SP, com duração pré-determinada de 02 (dois) a 03 (três) dias. 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.

Durante a auditoria, os auditores solicitarão aos profissionais disponibilizados pelo Solicitante que operem o sistema. Serão executados todos os procedimentos (*scripts*) definidos no Manual Operacional de Ensaios e Análises para Certificação de S-RES 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 auditor líder ao final da auditoria. Caso haja divergência entre os resultados observados por cada auditor na avaliação de um determinado requisito, os auditores debaterão suas conclusões na busca de um consenso, podendo, para tal, consultar a gravação realizada durante a auditoria ou pedir ao Solicitante uma nova verificação. Caso não se obtenha o consenso, prevalecerá o resultado apontado pela maioria, ou seja, por 02 (dois) auditores, o qual passará a ser considerado como resultado final para tal requisito.

Caso a auditoria não seja realizada nas datas previstas devido a qualquer impossibilidade por parte do Solicitante, inclusive por não disponibilizar algum recurso previsto, será elaborado um novo agendamento, mediante o pagamento, pelo Solicitante, da Taxa de Reagendamento de Auditoria (ver item 4.6.).

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.

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.

5.4.6. 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, poderá executar um 2º ciclo de auditoria, ainda dentro do mesmo processo. Caso o Solicitante opte por este procedimento, deverá efetuar o pagamento da Taxa de Realização de 2º Ciclo de Auditoria (ver item 4.6.).

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 auditada, 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 procedimento poderá ser realizado uma única vez dentro de um processo de certificação, não sendo passível de repetição. Caso este 2º ciclo de auditoria ainda aponte para não-conformidades, independentemente da quantidade ou abrangência das mesmas, o S-RES terá sua certificação reprovada.

5.5. Conclusão

Conforme a demanda apresentada, o Comitê de Certificação (ver capítulo 6) se reunirá presencialmente ou à distância 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 (1º ciclo), o Comitê poderá recomendar ao Solicitante a realização de ajustes no S-RES para a execução de um 2º 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.

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, ou à comunicação da reprovação.

5.5.1. Certificação Aprovada

No prazo máximo de 30 (trinta) dias após o término da auditoria, a SBIS emitirá e enviará ao Solicitante o Certificado e o Selo de Certificação SBIS-CFM (ver item 4.5.) em arquivos eletrônicos, e os publicará no sítio da Certificação na internet, encerrando o processo.

5.5.2. Certificação Reprovada

No prazo máximo de 30 (trinta) dias após o término da auditoria, a SBIS comunicará tal fato por escrito ao Solicitante, justificando os motivos e apontando explicitamente os resultados negativos que determinaram tal reprovação.

5.5.3. Interposição de Recurso

Caso não concorde com a reprovação da certificação de seu S-RES, o Solicitante poderá enviar formalmente à SBIS um recurso para revisão do resultado, o qual deverá, necessariamente, conter as justificativas e embasamento para a discordância.

Ao receber um recurso para revisão de resultado, a SBIS reunirá os auditores que executaram a auditoria contestada. A partir dos argumentos expostos pelo Solicitante no recurso 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.

Os recursos para revisão de resultado serão analisados e respondidos pela SBIS no prazo máximo de 60 (sessenta) dias após o seu recebimento.

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

5.6. Extensão da Certificação

Para a obtenção de extensões da certificação para outras versões de um S-RES já certificado (ver item 4.3.), devem ser efetuados os mesmos (ou equivalentes) procedimentos descritos neste capítulo para a inscrição, auditoria e conclusão, 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 4.5.);

b) Deve-se desconsiderar as referências à assinatura e envio do Contrato de Certificação;

c) Toda referência à Taxa de Certificação deve ser substituída pela Taxa de Extensão de Certificação (ver item 4.6.);

d) Para as extensões por ajustes não relevantes (ver 4.2.1) não serão executados os procedimentos referentes à auditoria.

5.7. Apelações, Reclamações e Disputas

Todas as apelações, reclamações e disputas apresentadas à SBIS pelos Solicitantes, outros fornecedores, clientes ou outras partes interessadas, serão registradas e encaminhadas 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.

5.8. 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 não-conformidades 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. 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 do tempo.

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:

- 02 (dois) membros indicados pela Diretoria da SBIS;
- 01 (um) membro representante do CFM.

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. Gerência 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.

A Gerência do Centro de Certificação poderá, a critério da Diretoria da SBIS, ser exercida pelo seu Diretor ou Gerente Executivo.

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 pleno ou sênior, 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, serão publicadas 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 apoia seus membros, especialmente o Gerente, nas atividades relacionadas à certificação.

A Secretaria do Centro de Certificação poderá, a critério da Diretoria da SBIS, ser exercida pela sua Secretária Administrativa.

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 e supervisionar as políticas relativas à operação da certificação;
- 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.

7. Uso da Informação Relacionada com a Certificação

A certificação de S-RES foi concebida como uma maneira de melhorar a qualidade dos softwares e a segurança dos profissionais e instituições de saúde no uso dos mesmos, assim como garantir a legalidade da substituição dos registros em papel pelos seus respectivos registros eletrônicos.

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.

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 organizações 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, a organização deverá indicar claramente:

- O nome da organização
- 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 organização) 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 2013”.

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, 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 consultas e 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.

Grande parte dos requisitos da Certificação SBIS-CFM foram elaborados com base nos 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
- Requisitos para GED (para aplicação futura)

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
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 importante, porém ainda não obrigatório. Possui alta probabilidade de tornar-se obrigatório nas próximas versões deste manual. **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.).

A numeração (ID) dos requisitos e respectivos grupos mantém compatibilidade com as versões anteriores deste manual. Assim, é comum observarem-se lacunas na numeração causadas pela remoção, nesta versão, de itens existentes nas versões anteriores.

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 requisitos recomendados 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 obrigatoriamente 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 aplicável a S-RES que **não** pretendem eliminar a impressão dos registros em papel. Assim, mantém 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.

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

Conforme já exposto no item 3.1. , a categoria Básica aplica-se a qualquer S-RES voltado à assistência à saúde de indivíduos. Adicionalmente, um S-RES poderá ser complementado pelo bloco de requisitos para atendimento Ambulatorial. Sistemas voltados a outros tipos de atendimento assistencial, como sistemas de informação hospitalar, pronto-atendimento e saúde ocupacional serão gradualmente contemplados com categorias específicas em futuras versões deste manual.

Neste conjunto de requisitos, a coluna "Presença" está representada por duas colunas:

- **BAS = Básica**: aplicável a todo e qualquer S-RES assistencial;
- **AMB = Ambulatorial**: aplicável exclusivamente a S-RES Ambulatorial.

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.

Encontra-se publicado nesta versão do manual somente um conjunto mínimo preliminar de requisitos para referência, os quais serão expandidos quando esta categoria tornar-se passível de certificação.

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

NGS1.01 - Controle de versão do software

ID	Título	Requisito	Local	Remoto
NGS1.01.01	Versão do software	O S-RES (conjunto de componentes principais) deve possuir minimamente na tela inicial informações de versão do software, contendo obrigatoriamente o nome do software, nome do fornecedor, identificação da versão e/ou *release* e/ou *build*. Esta versão será utilizada como referência na certificação do produto.	M	M
NGS1.01.02	Código fonte	Possibilitar, a partir do número de versão do S-RES, o resgate dos códigos-fonte correspondentes, possibilitando a rastreabilidade dos arquivos fontes que o geraram. Deve ser possível efetuar operações de roll-back para versões anteriores. Indicações de eventual incompatibilidade com versões anteriores devem ser exibidas em forma de aviso ao usuário antes da execução de atualizações e/ou correções e registradas em trilha de auditoria.	R	R
NGS1.01.04	Repositório de versões	Manter um repositório estruturado com todas as versões do S-RES (executáveis e códigos-fonte) que foram utilizadas em produção em algum momento, permitindo demonstrações tais como em auditorias, avaliações ou ações judiciais.	R	R

NGS1.02 - Identificação e autenticação de pessoas

ID	Título	Requisito	Local	Remoto
NGS1.02.01	Identificação e autenticação de pessoa	Identificar e autenticar toda pessoa deve ser antes de qualquer acesso a dados do S-RES.	M	M

NGS1.02.02	Método de autenticação de pessoa	Utilizar, no mínimo, um dos seguintes métodos de autenticação: • Usuário e senha; • Certificado digital e senha/PIN (Personal Identifier Number); • Validação Biométrica. Nota 1: OTP (one-time password), Captcha ou outros métodos de comprovação de interação humana são considerados complementares e podem ser utilizados apenas em conjunto com um dos métodos supracitados. Nota 2: Outros métodos de autenticação podem ser utilizados, devendo ser avaliados individualmente. Neste caso, deve ser apresentada documentação que demonstre nível de segurança equivalente ou superior ao mecanismo baseado em usuário e senha. Nota 3: Recomenda-se a utilização de um método de autenticação forte, adotando-se minimamente dois dos seguintes fatores: • Algo que o usuário conhece (ex: senha); • Algo que o usuário detém (ex: cartão ou token PKI, OTP); • Algo que comprove a presença do usuário (ex.: biometria).	M	M
NGS1.02.03	Proteção dos parâmetros de autenticação	Armazenar de forma protegida todos os dados ou parâmetros utilizados no processo de autenticação de pessoa. Método: Usuário e senha • A senha deve ser armazenada de forma codificada por algoritmo de hash aberto (público) de no mínimo 160 bits. • As codificações das senhas devem ser protegidas contra acesso não autorizado. Método: Biometria • Os templates biométricos dos usuários devem ser protegidos contra acesso não autorizado. • As amostras biométricas coletadas e transmitidas durante o processo de autenticação devem ser protegidas contra acesso não autorizado. Método: One-time password (OTP) • As sementes de geração dos valores numéricos devem ser protegidas contra acesso não autorizado. Nota: No caso do uso de biometria, recomenda-se que parâmetros de erro, como Crossover Error Rate (CER), sejam baixos.	M	M

NGS1.02.04	Segurança de senhas	Condição: Utilização de autenticação baseada no método de usuário e senha. Utilizar os seguintes controles de segurança: • Qualidade da senha: deve ser verificada 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 alfabético e 1 numérico; • Periodicidade de troca de senhas: deve ser obrigatória a troca de senhas pelos usuários, em um período máximo configurável (vide ESTR.02.11) que não exceda a 6 meses. • Os processos de troca de senha devem exigir que a nova senha seja diferente da imediatamente anterior. • Quando da geração de senha que não seja definida pelo próprio usuário, tal processo deve impedir sua visualização por terceiros. • Recomenda-se a implementação de técnicas de SALT para a codificação da senha.	M	M
NGS1.02.05	Controle de tentativas de login	Possuir mecanismos para bloquear a conta do usuário após um número máximo configurável (vide ESTR.02.11) de tentativas inválidas de login que não exceda a 10 tentativas.	M	M
NGS1.02.06	Identidade única da pessoa	Toda pessoa usuária do S-RES deve possuir um identificador único. Campos de identificação unívoca devem ser validados para garantir tal unicidade. Para isso, no momento da inclusão ou edição, o sistema deve verificar a existência de duplicidade, comparando os identificadores unívocos deste usuário (ex: RG, CPF, número de identificação profissional, etc) com a base de usuários já existentes. Nota: Caso o S-RES opere na modalidade "S-RESaaS" (S-RES as a Service), a unicidade do identificador da pessoa deve ser por organização.	M	M
NGS1.02.07	Autenticação para operações sensíveis	Toda pessoa usuária deve ser novamente autenticada no momento da realização de operações sensíveis, tais como registro de dados clínicos, troca de senha, delegação de poder, etc.	R	R
NGS1.02.08	Informações na autenticação	Assim que completada uma autenticação de sucesso, o sistema deve exibir à pessoa usuária as seguintes informações: • data e hora da última autenticação com sucesso; • data e hora das tentativas de autenticação sem sucesso depois da última autenticação com sucesso.	M	M

NGS1.03 - Controle de sessão de usuário

ID	Título	Requisito	Local	Remoto
NGS1.03.01	Bloqueio ou encerramento por inatividade	A sessão de usuário deve ser bloqueada ou encerrada após período de inatividade. O período máximo de inatividade deve ser configurável (vide ESTR.02.11) no sistema. Não deve ser possível para o usuário do sistema desativar ou desabilitar tais controles. Nota: No caso de encerramento da sessão, recomenda-se que os dados inseridos e não salvos sejam preservados para reutilização no acesso seguinte.	M	M
NGS1.03.02	Segurança contra roubo de sessão de usuário	A sessão de comunicação remota deve possuir controles de segurança a fim de não permitir o roubo da sessão do usuário. Não deve ser permitido ao usuário desabilitar tais controles. Nota 1: O S-RES não deve ser suscetível a ataques de *replay e covert-channel.* Nota 2: 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 de pessoas

ID	Título	Requisito	Local	Remoto
NGS1.04.01	Impedir acesso por pessoas não autorizadas	Impedir acesso ao RES, S-RES, SGBD e GED por pessoas não autorizadas.	M	M
NGS1.04.02	Mecanismo de controle de acesso ao RES	Garantir que o acesso aos dados do S-RES seja somente possível por meio de canais de interação pré-definidos (ex.: web, console local, interface entre aplicativos), com atuação obrigatória de mecanismos de controle de acesso.	M	M
NGS1.04.03	Gerenciamento de usuários e papéis	Permitir o gerenciamento (criação, inativação e modificação) de usuários e papéis (perfis), de forma a possibilitar o controle de acesso às funções conforme os papéis aos quais o usuário possui. Um usuário pode possuir um ou mais papéis.	M	M

NGS1.04.05	Configuração de controle de acesso	Disponibilizar mecanismos necessários para que seja possível implementar a política de controle de acesso através da configuração das permissões e restrições de acesso, considerando os papéis de usuário, funções e tipos de operação (consulta, inclusão e alteração). Cada papel (perfil) gerenciado deve permitir a associação com toda e qualquer função disponível no S-RES. Nota: Recomenda-se a possibilidade de configuração do controle de acesso dos papéis relacionados à T.I. com os seguintes objetivos (não necessariamente com estes nomes): • Administrador: configuração dos parâmetros de TI do S-RES; • Operador de cópias de segurança: realização e restauração de cópias de segurança; • Operador: iniciação e encerramento do sistema, monitoração do sistema. • Gestor de usuários: gerenciamento de usuários do sistema; gerenciamento dos perfis de usuários do sistema; gerenciamento de permissões aos serviços do sistema. • Auditor: auditoria dos registros do sistema.	M	M
NGS1.04.06	Concessão de autorizações	Garantir que haja ao menos um usuário responsável pela gestão de usuários, concessão de autorização e controle de acesso aos recursos de acordo com o escopo de atuação, a política organizacional e legislação.	M	M

NGS1.04.07	Delegação de poder	Condição: Intenção de fornecer suporte à delegação de poder.
		
		Sendo o delegante aquele que delega um poder a um delegado, então:
		• A delegação de poder deve ser permitida somente em caráter temporário, sendo a mesma concedida por período de tempo ou até a conclusão de uma determinada ação;
		• A delegação de poder deve ser registrada no sistema, contendo minimamente os seguintes dados:
		  • O delegante;
		  • O delegado;
		  • O motivo;
		  • O instante da concessão;
		  • O período de vigência;
		  • O objeto da delegação (ação delegada).
		
		O S-RES deve considerar a delegação de poder no controle de acesso.
		
		Nota 1: Considera-se delegação de poder o ato no qual uma pessoa (delegante) transfere determinado poder (permissão) a outra pessoa (delegado) por um determinado período, criando a correspondente corresponsabilidade pelas ações efetuadas. A delegação aplica-se quando o delegado não detém o poder que se pretende delegar.
		
		Nota 2: Como exemplo de delegação, pode-se citar a delegação do atendimento de um paciente pelo médico responsável a um outro médico quando da necessidade do mesmo ausentar-se do local de atendimento.
			M	M

NGS1.04.08	Acesso ao RES pelo paciente	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, deve existir um papel de usuário que permita realizar esta atividade em nome do paciente. Estas informações poderão ser geradas em formato eletrônico ou impresso. O sistema deverá disponibilizar uma interface para impressão de declaração do usuário (vide FUNC.25.02) de que está recebendo suas informações.	M	M
NGS1.04.10	Gerenciamento de grupos	Permitir o gerenciamento (criação, inativação e modificação) de grupos de usuários, de forma a possibilitar o controle de acesso a dados conforme os grupos aos quais o usuário pertence. Um usuário poderá pertencer a um ou mais grupos.	R	R

NGS1.05 - Disponibilidade do RES

ID	Título	Requisito	Local	Remoto
NGS1.05.01	Cópia de Segurança	O S-RES deve gerar cópia de segurança atendendo aos seguintes requisitos: • exportar os atributos de segurança e metadados em conjunto com os dados; • garantir, na restauração de uma cópia de segurança, 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	Integridade na recuperação de dados	Possuir controle que garanta a verificação da integridade das informações na geração e na restauração da cópia de segurança, gerando um alerta caso ocorra alguma falha.	M	M
NGS1.05.03	Alerta de limiar de ocupação	O S-RES deve gerar alerta quando o espaço para armazenamento de registros atingir um limiar de ocupação a fim de possibilitar aos operadores a realização de medidas preventivas.	M	M

NGS1.06 - Componentes distribuídos

ID	Título	Requisito	Local	Remoto
NGS1.06.01	Segurança da comunicação com componente de interação com o usuário	A sessão de comunicação entre o componente de interação com o usuário (ex.: browser ou executável cliente) e os outros componentes do S-RES (ex.: servidor de aplicação, banco de dados, etc) deve oferecer os seguintes serviços de segurança: autenticação do servidor, integridade dos dados e confidencialidade dos dados. Nota: Como exemplo, pode-se citar a utilização do protocolo HTTPS (HTTP + SSL/TLS).	X	M
NGS1.06.02	Controle de acesso do cliente ao servidor	Em S-RES de acesso remoto, o acesso ao sistema deve ser restrito somente aos clientes autorizados. Nota: Este controle de acesso pode ser realizado, por exemplo: • em browser: autenticação do usuário; • em executável cliente: restrição pelo endereço IP e porta.	X	M
NGS1.06.03	Restrição de dados transmitidos	Em S-RES de acesso remoto, os dados transmitidos ao componente cliente (lado do usuário) devem ser somente aqueles que serão apresentados ao usuário.	X	M

NGS1.06.04	Segurança da comunicação entre componentes	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 (ambas as partes), integridade dos dados e confidencialidade dos dados. A segurança pode ser aplicada ao canal de comunicação ou às mensagens trocadas.	X	M
NGS1.06.05	Controle de acesso entre componentes	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	Condição: haver troca de dados direta entre S-RES distintos. A comunicação entre S-RES deve oferecer os seguintes serviços de segurança: autenticação de parceiro (ambas as partes) utilizando certificados digitais, integridade dos dados e confidencialidade dos dados.	M	M
NGS1.06.07	Confirmação de entrega	Condição: haver troca de dados direta automática entre sistemas (não via interface). 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
NGS1.06.08	Integridade e origem de componentes dinâmicos	Caso o S-RES utilize componentes que exijam download para sua execução (ex.: ActiveX, Applet, aplicações para tablet, etc), estes devem possuir controle de integridade e possibilidade de verificação da origem (ex.: pelo uso de assinatura digital do componente).	M	M
NGS1.06.09	Método de autenticação de parceiro de comunicação	Deve ser utilizado o método de chaves assimétricas com certificado digital para autenticação de parceiro de comunicação.	R	R

NGS1.07 - Segurança de Dados

ID	Título	Requisito	Local	Remoto
NGS1.07.01	Importação de dados	Condição: possibilidade de importação de dados de outros S-RES. Os dados importados de outro S-RES devem estar relacionados a um paciente, um médico responsável pelo paciente, um médico responsável pela geração da informação, e local e momento (data e hora) da importação. Caso os dados sejam importados manualmente, registrar o profissional que está realizando a importação.	M	M

NGS1.07.03	Impedir exclusão e alteração	Não permitir exclusão ou alteração de dados já existentes no RES. Ações de correção ou edição devem preservar os dados previamente inseridos. Nota: Como exemplo, pode haver a troca de estado dos dados previamente inseridos para “inativos”, com os novos dados "ativos".	M	M
NGS1.07.04	Verificação de integridade dos dados	Devem existir controles para verificação de integridade dos dados do RES de forma a prevenir que qualquer ação do usuário, falha do sistema, inserção ou remoção indevida de dados possa causar inconsistência da base de dados.	R	R
NGS1.07.05	Utilização de SGBD	O RES deve ser armazenado e protegido por um Sistema de Gerenciamento de Banco de Dados (SGBD) ou Sistema de Gerenciamento Eletrônico de Documentos (GED).	M	M
NGS1.07.06	Impedir acesso direto ao SGBD	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. O SGBD não deve permitir acesso direto pelos usuários do S-RES.	M	M
NGS1.07.07	Impedir reconstrução do RES	Impedir a reconstrução do RES por meio de acessos não autorizados à base de dados.	R	R
NGS1.07.09	Manipuladores RES	Componentes que manipulam dados do RES para fins de interoperabilidade, visualização, assinatura e outros, não devem manter tais dados fora do SGBD após o término da operação. Nota: como exemplos, pode-se citar o cache de arquivos PDF após a sua a visualização, e resquícios de arquivos XML (Estensible Markup Language) ou DICOM (Digital Imaging and Communications) após o seu processamento.	R	R
NGS1.07.10	Validação de dados de entrada	Os dados inseridos pelo usuário nos campos de entrada devem ser validados antes de serem processados, de forma a prevenir ataques de buffer overflow e injeção de dados. Nota: por exemplo, em aplicações baseadas em interface web, efetuar a validação de dados de forma a evitar os ataques descritos na seção de Data Validation Testing da metodologia OWASP Testing Guide[27].	M	M
NGS1.07.11	Segregação dos dados por organização	Condição: o S-RES ser operado na modalidade "S-RESaaS" (S-RES as a Service). Todos os dados do RES devem ser segregados por organização, ou seja, nenhum dado do RES de uma organização pode ser acessado ou visualizado por usuário de outra organização.	M	M

NGS1.08 – Auditoria

ID	Título	Requisito	Local	Remoto
NGS1.08.01	Auditoria contínua	Gerar registros de auditoria de forma contínua e permanente, não sendo permitida a sua desativação ou interrupção, ainda que temporária.	M	M
NGS1.08.02	Proteção dos registros de auditoria	Os registros de auditoria devem ser protegidos contra acesso não autorizado e contra qualquer tipo de alteração.	M	M

NGS1.08.04	Eventos e informações registradas	As trilhas de auditoria devem conter informações relacionadas minimamente aos seguintes eventos: Quanto ao RES: • Criação e consulta a registros do RES • Importação e exportação de dados • Impressão de registros do RES Quanto às ações de usuário: • Tentativas de autenticação de usuário, com ou sem sucesso • Tentativas de troca de senha, com ou sem sucesso • Realização de assinatura digital • Encerramento e bloqueio de sessão de usuário Quanto às ações operacionais: • Inicio e parada do sistema • Atividades de gerenciamento de usuários, papéis e grupos • Geração de senha para usuário • Acesso aos registros de auditoria • Realização de backup e restore Quanto às interações entre sistemas: • Transmissão e recepção de dados • Erros de integridade e autenticação de mensagens • Erros de autenticação de parceiros Quanto às situações especiais: • Delegação de poder • Autorizações excepcionais (acesso de emergência) Com relação aos eventos citados acima, os registros de auditoria devem possuir, no mínimo, as seguintes informações para cada evento: • Data e hora do evento; • Nível de criticidade (ex.: crítico, alerta, erro, informação, etc. Referência: RFC 5424); • Evento; • Identificação do componente gerador do evento (ex.: nome do componente, endereço IP, dispositivo do usuário, ponto de acesso, etc); • Identificação do usuário gerador do evento, quando aplicável; • Indicação de atividade realizada por delegação, quando aplicável; • Descrição (detalhes do evento, ex.: identificação do registro consultado). Nota 1: Recomendada-se registrar também os eventos relacionados à pesquisa de registros. Nota 2: Deve-se atentar ao requisito NGS1.07.11 na visualização dos registros de auditoria.	M	M

NGS1.08.05	Visualização dos registros de auditoria	Possuir uma interface de visualização dos registros de auditoria em ordem cronológica. Permitir a filtragem de registros por data, evento e usuário. Tal interface deve possuir acesso restrito a usuários autorizados.	M	M
NGS1.08.06	Exportação dos registros de auditoria	Possibilitar a exportação dos registros de auditoria em formato aberto, de tal forma que possam ser visualizados em aplicativo externo.	M	M
NGS1.08.07	Armazenamento dos registros de auditoria	Os registros de auditoria devem ser armazenados e protegidos por um SGBD.	M	M

NGS1.09 - Documentação

ID	Título	Requisito	Local	Remoto
NGS1.09.01	Documentação	O S-RES deve possuir manuais que apresentem minimamente as seguintes informações: • Instruções de uso do S-RES para os usuários; • Visão geral do S-RES, incluindo formas de operação, requisitos do ambiente, papéis de usuários relevantes (por exemplo: administrador, operador, operador de backup, etc); • Instalação e configuração do S-RES; • Instalação e configuração dos componentes complementares (ex: SGBD,sistema operacional, etc); • Recomendação sobre a forma de configuração segura do S-RES e componentes complementares, e forma de operação segura do S-RES.	M	M
NGS1.09.02	Referência à versão do software na documentação	Todos os manuais devem indicar claramente, no início do documento, seu versionamento e a versão do S-RES a que se referem.	M	M
NGS1.09.04	Operador de backup	O manual de instalação deve informar como realizar a configuração de um usuário com perfil de operador de backup no SGBD. Além disso, o manual de instalação deve informar como configurar o SGBD de forma que as atividades de exportação e restauração de uma cópia de segurança dos dados possa ser realizada somente pelo usuário com papel de operador de *backup*. Os manuais pertinentes devem conter indicações de cautela caso existam outros usuários com permissão de geração ou restauração de cópia de segurança (ex.: usuário 'sa' ou equivalente).	M	M

NGS1.09.05	Restrição de acesso a entidades não autenticadas e autorizadas	O manual de instalação deve informar como configurar o SGBD e todos os demais componentes do S-RES de forma a impedir o acesso de entidades (usuários ou outros sistemas) não autenticadas ou não autorizadas pelo controle de acesso.	M	M
NGS1.09.07	Configuração da segurança da comunicação entre componentes	O manual de instalação deve informar que a comunicação entre os componentes de um S-RES distribuído deve implementar os serviços de segurança de autenticação de parceiro, integridade dos dados e confidencialidade dos dados, e dar orientações para tal configuração.	M	M
NGS1.09.08	Sincronização de relógio	O manual de administração e operação deve informar ao administrador que os componentes do S-RES devem estar com seus relógios sincronizados e referenciados ao UTC (Coordinated Universal Time). O manual deve também informar as formas para que a sincronização possa ser configurada no ambiente.	M	M
NGS1.09.09	Guarda da mídia de cópia de segurança	O manual de operação deve informar que as mídias que contenham cópias de segurança do RES devem ser guardadas em repositório provido de controle de acesso.	M	M
NGS1.09.10	Segregação dos componentes	O manual de instalação deve informar que o S-RES deve possuir uma segregação lógica do componente de banco de dados de seus demais componentes. O manual deve exemplificar uma ou mais arquiteturas de configuração.	M	M
NGS1.09.11	Importação de dados de dispositivos externos de saúde	Condição: possibilidade de importação automática de dados de dispositivos externos de saúde. O manual deve indicar que, em caso de importação de dados de dispositivos externos de saúde, é necessário que exista um termo de responsabilidade referente à aferição e calibração periódica desses dispositivos, ou que haja um profissional de saúde que valide essas informações antes de sua aceitação pelo S-RES. Nota: consideram-se dispositivos externos de saúde aqueles que coletam dados clínicos dos pacientes, tais como monitores multiparamétricos com interfaces ASTM.	M	M
NGS1.09.12	Idioma	Deve haver versão em Português do Brasil para todos os manuais do S-RES.	M	M
NGS1.09.13	Alertas sobre configurações inseguras	Os manuais devem conter informações e alertas sobre configurações inseguras do S-RES.	M	M
NGS1.09.14	Histórico de alteração	Gerar e manter documento contendo o histórico descritivo das alterações realizadas em cada versão do S-RES ("*release notes*"), contendo a data, modificações, impacto (módulos, funções, serviços afetados,etc), restrições de compatibilidade e o responsável pela alteração.	M	M

NGS1.10 - Tempo

ID	Título	Requisito	Local	Remoto
NGS1.10.1	Uniformidade da representação de tempo para auditoria	Todo registro de tempo para fins de auditoria deve ser exibido no formato RFC 3339.	M	M
NGS1.10.3	Fonte temporal	Basear todo registro de tempo em uma fonte de referência temporal sob controle do S-RES, ou seja, utilizar a referência de tempo do servidor e não da estação do usuário. Nota: Na implantação do S-RES em uma organização, a fonte temporal deverá ser sincronizada ao UTC (Coordinated Universal Time), utilizando um protocolo de sincronismo de tempo (ex.: NTP).	M	M

NGS1.11 – Notificação de Ocorrências

ID	Título	Requisito	Local	Remoto
NGS1.11.01	Interface para notificação	Possuir uma interface para que o usuário possa notificar e acompanhar a ocorrência de incidentes de segurança, problemas, melhoramentos ou sugestões.	R	R

NGS1.12 – Privacidade

ID	Título	Requisito	Local	Remoto
NGS1.12.01	Concordância com termos de uso	Exibir imediatamente após o primeiro acesso do usuário no sistema, um termo de concordância sobre o uso apropriado das informações de saúde, alertando para o devido cuidado visando a confidencialidade dos dados e as consequências do uso inadequado dos mesmos. O usuário só deve poder prosseguir após aceitar explicitamente as condições ali dispostas	M	M
NGS1.12.02	Consentimento do paciente	Registrar o consentimento do paciente referente ao propósito de uso das informações pessoais de saúde, assim como de quem poderá ter acesso a tais informações, incluindo a possibilidade de acesso de emergência.	R	R
NGS1.12.03	Associação do consentimento à informação de saúde	Em situações em que informações pessoais de saúde, em formato eletrônico, forem transmitidas para fora do domínio da instituição, as informações de consentimento devem acompanhar os dados, de forma a permitir que o sistema receptor respeite as diretivas do consentimento.	R	R

NGS1.12.04	Acesso de emergência	Permitir o acesso de emergência às informações pessoais de saúde somente a pessoas autorizadas, e seu uso deve ser registrado nas informações de auditoria.	R	R
NGS1.12.05	Propósito de uso	Registrar o propósito de uso das informações pessoais de saúde, e utilizar tais informações somente para os propósitos consentidos.	R	R
NGS1.12.06	Restrição de exportação por propósito de uso	A exportação ou impressão de informações pessoais de saúde devem respeitar o propósito de uso e consentimento.	R	R
NGS1.12.07	Restrições para transmissão e exportação de RES	A exportação de dados do S-RES, incluindo sua impressão, deve ser permitida somente nas seguintes situações: • para transmissão para um outro S-RES; • cópia de segurança; • para o paciente, a pedido do mesmo, 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 exportação de RES devem ser registradas.	M	M
NGS1.12.08	Restrições de acesso ao RES adicionadas pelo paciente	Permitir que o paciente possa adicionar ou solicitar adição de restrições de acesso a uma determinada parte ou à totalidade de seu RES. Esta restrição pode ser inclusive relacionada a um ou mais profissionais de saúde usuários do sistema.	R	R

NGS1.13 – Certificado Digital

Requisitos aplicáveis somente quando da utilização de certificado digital para autenticação de usuário e/ou assinatura digital.

ID	Título	Requisito	Local	Remoto
NGS1.13.01	Certificado digital	Utilizar certificado digital ICP-Brasil para o processo de autenticação de usuário e/ou assinatura digital de documentos eletrônicos no S-RES.	M	M
NGS1.13.02	Atendimento à ICP-Brasil	Atender às normas de uso definidas pela ICP-Brasil na utilização de certificados digitais.	M	M
NGS1.13.03	Validação do certificado digital antes do uso	Validar o certificado digital e sua cadeia de certificação antes de sua utilização ou imediatamente após sua utilização. A validação do certificado digital envolve a validação criptográfica, verificação de validade e revogação, inclusive dos certificados da sua cadeia de certificação. Registrar no log períodos de indisponibilidade de comunicação que impeçam a verificação da revogação do certificado digital.	M	M

NGS1.13.04	Configuração de certificados raiz do S-RES	Permitir a configuração do conjunto de certificados raiz de confiança do S-RES. Suportar controles de segurança que garantam a integridade e evite alteração não autorizada da relação de certificados raiz de confiança. Nota: Em algumas situações, pode existir um conjunto de certificados raiz de confiança do S-RES e outro conjunto de certificados raiz no contexto do ambiente operacional do usuário. Caso as operações de validação de certificado ocorram no ambiente operacional do usuário, tais certificados devem ser revalidados no contexto do conjunto de certificados raiz do S-RES, o qual pode ser alterado somente por usuários autorizados.	M	M

NGS1.14 – Autenticação de usuário utilizando certificado digital

Requisitos aplicáveis somente quando da utilização de certificado digital para autenticação.

ID	Título	Requisito	Local	Remoto
NGS1.14.01	Verificação do propósito do certificado digital para autenticação	Verificar, antes da realização de uma autenticação de usuário, se o certificado digital a ser utilizado é um certificado digital ICP-Brasil de assinatura tipo A1, A2, A3 ou A4.	M	M
NGS1.14.02	Irretratabilidade da autenticação realizada	A autenticação realizada por meio de certificado digital deve gerar prova de forma a garantir a irretratabilidade da autenticação realizada. O elemento de prova deve ser armazenado no sistema, em formato compatível com o disposto na DOC-ICP-15, da ICP-Brasil, que trata sobre a normalização de assinatura digital, para o padrão de “assinatura digital com referências básicas (AD-RB)”, sendo recomentado a utilização do padrão de “assinatura digital com referências para validação (AD-RV), com os objetos referenciados estando no domínio da instituição, ou padrão de “assinatura digital com referências completas (AD-RC)”.	M	M
NGS1.14.03	Tipos de usuários para autenticação com certificação digital	Todos os usuários que realizam assinatura digital ICP-Brasil devem se autenticar com seus certificados digitais ICP-Brasil.	R	R
NGS1.14.04	Homologação ICP-Brasil	O componente do S-RES que realiza autenticação de usuário utilizando certificado digital deve ser homologado pela ICP-Brasil.	R	R

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

NGS2.02 – Assinatura Digital

ID	Título	Requisito	Presença
NGS2.02.01	Formato de assinatura	O S-RES deve gerar assinaturas digitais nos formatos AD-RT (Assinatura Digital com Referências de Tempo), com a inclusão de todos os objetos necessários à validação (certificados dos signatários, cadeias de certificação, objetos de revogação, etc). Opcionalmente, tais objetos podem não ser incluídos, desde que: • Os objetos referenciados (certificados digitais, objetos de revogação, etc) estiverem armazenados localmente ao S-RES; • For garantida a disponibilidade do armazenamento e a recuperação futura de todos os objetos necessários para realizar a validação; • O S-RES for capaz de incluir na assinatura AD-RT todos os objetos necessários para realizar a validação (necessário, por exemplo, quando um registro assinado for exportado). Nota: Recomenda-se o uso dos formatos AD-RV (Assinatura Digital com Referências de Validação) e AD-RC (Assinatura Digital com Referências Completas). Neste caso, o formato AD-RV (que inclui as referências aos objetos relevantes à validação - certificados e objetos de revogação - na estrutura de atributos da assinatura digital) pode ser utilizado somente quando: • Os objetos referenciados (certificados digitais, objetos de revogação, etc) estiverem armazenados localmente ao S-RES; • For garantida a disponibilidade do armazenamento e a recuperação futura dos objetos necessários para recompor a assinatura no formato AD-RC; • O S-RES for capaz de transformar a assinatura AD-RV em uma assinatura AD-RC, ou seja, for capaz de recompor o documento assinado digitalmente com estrutura de atributos de assinatura aderente à especificação AD-RC (necessário, por exemplo, quando um registro assinado for exportado).	M
NGS2.02.02	Verificação do propósito do certificado digital para assinatura	Antes da realização de uma assinatura digital, o S-RES deve verificar se o certificado digital a ser utilizado possui propósito de uso de assinatura digital, ou seja, se possui o campo *key usage* definido como *Digital Signature* e *NonRepudiation* e verificar se é certificado digital ICP-Brasil de assinatura tipo A1, A2, A3 ou A4.	M

NGS2.02.03	Referência temporal para revogação	O S-RES deve ser capaz de requisitar e incluir o carimbo de tempo após a realização de uma assinatura. O carimbo de tempo deve ser incluído tão logo seja possível. Toda assinatura digital realizada no âmbito do S-RES deve incluir um carimbo de tempo compatível com a ICP-Brasil a ser utilizado como referência temporal nas atividades de verificação de revogação do certificado digital. No momento da inclusão do carimbo de tempo, a assinatura deve ser revalidada. Nota: Enquanto não houver oferta disseminada do serviço de carimbo de tempo ICP-Brasil será permitido o uso de outros provedores de serviço de carimbo de tempo, inclusive interno.	M
NGS2.02.04	Validação da assinatura digital	Realizar a validação da assinatura minimamente nas seguintes situações: • Antes de sua inclusão no sistema; • Na geração da assinatura digital: a assinatura deve ser validada imediatamente após sua geração; • Na importação de registro assinado: a assinatura deve ser validada antes de iniciar sua inclusão no RES; • Por vontade e ação do usuário ao ter acesso a todo e qualquer documento assinado, durante pesquisa ou consulta. A validação da assinatura de um documento inclui a validação das assinaturas de cada signatário (co-assinatura). A validação de uma assinatura inclui: • A validação do carimbo de tempo, quando presente: verificação da assinatura do carimbo de tempo, do certificado da autoridade de carimbo de tempo e dos certificados da cadeia de certificação, conforme requisitos da ICP-Brasil e da RFC 3161; • A verificação do certificado do signatário e dos certificados da cadeia de certificação; • A verificação do estado de revogação do certificado do signatário e dos certificados da cadeia de certificação, utilizando como referência temporal o instante presente no carimbo de tempo, e utilizando LCR (Lista de Certificados Revogados) [RFC 5280] ou Resposta OCSP (*Online Certificate Status Protocol*) [RFC 2560]. Caso o objeto de revogação (LCR ou resposta OCSP) não esteja presente, obtê-lo e incluí-lo na assinatura no momento da validação. Retrocompatibilidade: Na validação da assinatura de documentos/registros antigos do S-RES sem a presença de carimbo de tempo, a referência temporal a ser utilizada para verificação de revogação é o instante presente no atributo “momento de assinatura” (*signingtime*).	M

NGS2.02.06	Propósito da assinatura	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. O S-RES deve incluir o atributo de propósito de assinatura (atributo *commitment-type-indication)*. O propósito da assinatura deve ser requisitado ao usuário antes da aplicação da assinatura ou ser pré-definido naquela situação. Neste último caso, o S-RES deve informar ao usuário o tipo de propósito que será incluído na assinatura: prova de aprovação ou prova de criação. Quando a assinatura representa o compromisso do signatário com o conteúdo assinado, deve ser utilizado o propósito "prova de aprovação" (*proof of approval*) . [RFC 5126]	R
NGS2.02.07	Visualização das informações a serem assinadas	Permitir a visualização da informação a ser assinada antes da sua assinatura.	M
NGS2.02.08	Homologação ICP-Brasil	Os componentes de um S-RES que utilizam certificação digital para assinatura digital devem estar homologados pela ICP-Brasil.	R
NGS2.02.09	Exportação de registros assinados	Na exportação de registros assinados, utilizar o formato AD-RC (Assinatura Digital com Referências Completas) ou AD-RT (Assinatura Digital com Referências de Tempo), incluindo todos os objetos necessários à validação (certificados dos signatários, cadeias de certificação, dados de revogação, certificados de atributos, etc).	M
NGS2.02.11	Resultado da verificação da assinatura digital	O sistema deve, a qualquer tempo, prover meios para validação e exibição do estado de validade de um documento assinado digitalmente. O resultado da verificação de uma assinatura digital deve retornar um dos seguintes estados: • Válida: assinatura valida; • Inválida: assinatura inválida; • Indeterminada: quando não é possível determinar se a assinatura está válida ou inválida, geralmente devido a falta de objetos críticos (ex: certificado, objeto de revogação, carimbo de tempo, certificado da cadeia, atributos obrigatórios, etc). Exceto para o estado válido, a causa deverá ser indicada.	M
NGS2.02.12	Validação com objeto de revogação ideal	Revalidar o registro assinado com o objeto de revogação obtido após a próxima publicação ("next update") do estado de revogação do certificado pela AC. Caso essa validação indique que a assinatura foi realizada com um certificado revogado: • uma mensagem imediata deve ser enviada aos responsáveis da instituição e do profissional cujo certificado foi revogado; • o registro deve ser colocado na lista de registros pendentes de assinatura.	R

NGS2.02.13	Indisponibilidade de acesso a LCR no momento da assinatura	No momento da assinatura, caso não haja disponibilidade da OCSP ou da LCR publicada imediatamente antes da assinatura, o S-RES deve realizar a assinatura com a última LCR disponível correspondente, se existir. A assinatura ficará pendente de atualização do objeto de revogação (LCR ou OCSP), devendo ser atualizada tão logo haja disponibilidade. Neste caso, o sistema deve sinalizar pendência.	M
NGS2.02.14	Validação e adequação da assinatura de documentos recebidos	No momento de recebimento de um registro externo assinado digitalmente, o S-RES deve: • Validar sua assinatura; • Complementar, quando necessário, a estrutura de atributos de forma a estar aderente ao formato AD-RT, AD-RV ou AD-RC (inclusão de objetos estado de revogação, inclusão de carimbo de tempo, etc).	M
NGS2.02.15	Instante da assinatura	Incluir em toda assinatura realizada o atributo *CMS/CAdES id-signingTime* ou a propriedade *XMLDSIG/XAdES SigningTime*. Este atributo representa o instante de assinatura acordado com o signatário.	M
NGS2.02.16	Inclusão e validação de certificado de Atributo	O S-RES deve: • Possibilitar a inclusão e validação de certificado de atributo (RFC 5126) para qualificação do signatário, de acordo com a DOC-ICP-16. • Ser capaz de incluir, no momento da assinatura, um certificado de atributo como um atributo assinado "atributos do signatário" (*signer attributes*). • Ser capaz de validar certificados de atributos incluídos em uma assinatura.	R
NGS2.02.17	Informações sobre assinatura	O documento a ser assinado deve exibir ao usuário e incluir a seguinte mensagem: "Documento assinado digitalmente conforme MP 2.200-2 de 24/08/2001, Resolução CFM 1821/2007, no sistema certificado SBIS nº XXX-Y". XXX-Y deve ser o número fornecido no processo de certificação de S-RES SBIS-CFM para o sistema em questão. Este requisito não se aplica aos episódios individuais de checagem de enfermagem.	M
NGS2.02.18	Encadeamento de registros assinados digitalmente	Garantir a ordem temporal de assinatura e presença de todos os registros assinados para cada paciente.	R
NGS2.02.19	Verificação do encadeamento de registros	Possuir funcionalidade para que o usuário, a qualquer momento, consiga validar o encadeamento dos registros assinados digitalmente.	R

NGS2.02.20	Indisponibilidade da chave privada	Em caso de não disponibilidade da chave privada de assinatura do profissional de saúde, o S-RES deve assinar o documento com a finalidade de garantir a integridade e o instante de geração do documento. Esta assinatura deve ser realizada com o certificado da instituição com o atributo assinado "commitment-type-indication" com o propósito genérico "id-cti-ets-proofOfReceipt". Esse documento ficará pendente de assinatura pelo profissional cuja chave privada estava indisponível.	M
NGS2.02.21	Aviso de registro pendente de assinatura	Caso o usuário possua alguma assinatura pendente (vide NGS2.02.16), exibir imediatamente após a autenticação do usuário no sistema a relação de documentos pendentes e possibilitar tais assinaturas, eventualmente após a exibição de outras mensagens de segurança e privacidade.	M

NGS2.04 – Digitalização de Documentos

Requisitos aplicáveis somente para S-RES da categoria GED.

ID	Título	Requisito	Presença
NGS2.04.01	Assinatura digital do sistema de GED	Todo documento digitalizado deve ser assinado pelo componente de digitalização com certificado digital especificado no NGS2.04.08, com o propósito de garantia de integridade e de indicação de que a imagem assinada foi originada em um processo de digitalização. Este propósito deve 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	O operador de digitalização deve assinar digitalmente o documento digitalizado, com certificado ICP-Brasil de acordo com NGS2.01.05, com o propósito de conferência, garantindo a verificação do enquadramento e a qualidade da imagem digitalizada em comparação à original, refazendo o processo de digitalização em casos de imperfeições. Este propósito deve 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 sistema de GED.	M
NGS2.04.03	Assinatura digital do responsável	O responsável deve assinar digitalmente o documento digitalizado, com certificado ICP-Brasil de acordo com NGS2.01.05, com o propósito de criação, garantindo a autenticidade da imagem digitalizada em comparação à original. Este propósito deve ser estabelecido incluindo o atributo assinado "commitment-type-indication" com o propósito genérico "id-cti-ets-proofOfCreation", enquanto não seja definido um propósito mais específico. Essa assinatura deve ser aposta como uma contra-assinatura da assinatura do sistema de GED.	M
NGS2.04.06	Termo de conduta para digitalização	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	Os componentes de um S-RES que utilizam certificação digital para autenticação e assinatura digital devem ser homologados pela ICP-Brasil.	R

NGS2.04.08	Certificado digital do sistema GED	Todo componente de digitalização deve possuir um par de chaves assimétricas e certificado digital associado, com propósito de uso de chave (*KeyPuposeID*) para autenticação de servidor definido no *extended key usage* como *server authentication* (1.3.6.1.5.5.7.3.1), com *common name* emitido conforme o Registro de Domínios para a Internet no Brasil (Registro.br) para a instituição de saúde. Recomenda-se que seja emitido um certificado com subdomínio exclusivo para o processo de digitalização, por exemplo: “ged.hospitalexemplo.com.br”.	M

NGS2.05 - Carimbo de tempo

ID	Título	Requisito	Presença
NGS2.05.01	Carimbo de tempo ICP-Brasil	O S-RES deve suportar: • a requisição e inclusão de carimbo de tempo no momento da geração da assinatura; • o uso de carimbo de tempo no procedimento de validação de uma assinatura. Nota: Enquanto não houver oferta disseminada do serviço de carimbo de tempo ICP-Brasil será permitido o uso de outros provedores de serviço, inclusive interno.	M
NGS2.05.02	Verificação do carimbo de tempo	A verificação de um carimbo de tempo deve incluir a verificação do certificado de assinatura do carimbo de tempo, seguindo NGS2.02.04. O certificado de assinatura do carimbo de tempo deve: • Ser um certificado ICP-Brasil tipo T3 ou T4. • Possuir o propósito de uso de chave (*KeyPurposeID*) “assinatura de carimbo de tempo” definido no *extended key usage* como *timestamping* (OID 1.3.6.1.5.5.7.3.8). Nota: Enquanto não houver oferta disseminada do serviço de carimbo de tempo ICP-Brasil será permitido o uso de outros provedores de serviço, inclusive interno.	M
NGS2.05.03	Indisponibilidade do serviço de carimbo de tempo	No momento da geração de uma assinatura digital, caso não seja possível obter o carimbo de tempo de assinatura, o S-RES deve: • Gerar registros de auditoria informando sobre a impossibilidade de obtenção dos dados de verificação de revogação de certificado digital; • Gerar alerta ao administrador do sistema e gestor do sistema informando sobre a situação. Assim que houver o retorno do serviço, o carimbo de tempo deve ser obtido e incluído na assinatura.	M

NGS2.06 - Certificado de atributo

ID	Título	Requisito	Presença
NGS2.06.01	Configuração das fontes de autoridade	O S-RES deve: • Permitir a configuração das fontes de autoridade, para cada classe de privilégio (relação <privilégio, fonte_de_autoridade>, exemplo: <médico, Conselho Regional de Medicina>); • Implementar controles de segurança que garantam a integridade e detecte alteração não autorizada da relação de fontes de autoridade configuradas.	R
NGS2.06.02	Tratamento de certificado de atributo	O S-RES deve ser capaz de tratar certificados de atributo segundo a ICP-Brasil (DOC-ICP-16), a RFC 5755 e X.509, para as seguintes atividades: • Verificação de certificado de atributo, incluindo revogação; • Geração de assinaturas com a inclusão de certificado de atributo; • Verificação de assinatura com presença de certificado de atributo; • Delegação.	R

NGS2.07 – Impressão de Registro Assinado Digitalmente

ID	Título	Requisito	Presença
NGS2.07.01	Impressão de registros assinados digitalmente	Imprimir os registros assinados digitalmente utilizando ao menos uma das seguintes opções: • mensagem de rodapé: impressa em cada registro assinado digitalmente (vide NGS2.07.02), e/ou; • relatório de assinaturas: impresso para um conjunto de registros assinados digitalmente (vide NGS2.07.03).	M

NGS2.07.02	Impressão de mensagem de rodapé	Condição: Impressão de mensagem de rodapé. Em caso de impressão de mensagem de rodapé (em cada registro assinado digitalmente), os mesmos devem ser validados no momento da impressão e deve ser adicionada a seguinte mensagem na parte inferior de cada página. Os dados variáveis (nome, CPF, data e hora) deverão ser extraídos da assinatura. A hora e a data são respectivamente referentes ao *signingtime*. Assinado por: <nome do signatário>, CPF <número do CPF do signatário>, <papel, extraído do certificado de atributo, se presente>, às < HH:MM+-fuso de DIA/MÊS/ANO, extraído do atributo *signing time*>. Caso haja mais de uma assinatura, os mesmos dados devem ser apresentados para os outros signatários na sequência. A exibição das figuras é opcional.	M

NGS2.07.03	Impressão de relatório de assinaturas	Condição: Impressão de relatório de assinaturas. Em caso de impressão de relatório de assinaturas (para um conjunto de registros asinados digitalmente), todos os registros assinados devem ser validados no momento da geração do relatório e da impressão dos registros, e a seguinte mensagem deve ser impressa: “Os registros a seguir estão assinados digitalmente de acordo com a ICP-Brasil, MP-2.200-2/2001, Resolução CFM 1821/2007, A lista abaixo indica o número do documento e seu(s) signatário(s).”  Em seguida, deverá vir a lista dos registros assinados digitalmente, numerados e paginados sequencialmente, e para cada registro, indicar: Seu número sequencial, as páginas a que se referem, Assinado por: <nome do signatário>, CPF <número do CPF do signatário>, <papel, extraído do certificado de atributo, se presente>, às < HH:MM+-fuso de DIA/MÊS/ANO, extraído do atributo *signing time*>. Caso haja mais de uma assinatura, os mesmos dados devem ser apresentados para os outros signatários na sequência. A exibição das figuras é opcional.	M

8.4. Requisitos de Estrutura e Conteúdo

ESTR.01 - Estrutura do RES

ID	Título	Requisito	BAS	AMB
ESTR.01.01	Navegação e consultas	Organizar os dados e informações do RES em diferentes seções para facilitar a navegação e consultas em tela, segundo os papéis do usuário e suas necessidades e expectativas.	M	M
ESTR.01.03	Compartilhamento com independência	Garantir o compartilhamento do RES com independência de hardware, software (aplicativos, sistemas operacionais, linguagens de programação), bancos de dados, redes, sistemas de codificação e linguagens naturais. Exemplo: parâmetros de regras de validação no banco de dados e não embutidos no código dos aplicativos (vide ESTR.02.11).	M	M
ESTR.01.04	Recuperação de dados	Possibilitar que os dados e informações estejam organizados e passíveis de recuperação de tal forma que facilite os usos secundários do RES, tais como: vigilância epidemiológica, gestão de processos, auditoria de processos, faturamento de procedimentos e pesquisa científica, entre outros.	M	M

ESTR.02 - Dados estruturados

ID	Título	Requisito	BAS	AMB
ESTR.02.01	Armazenamento em listas	Armazenar em listas todos os dados, que possuam registro de tempo, de tal forma que a ordem cronológica esteja preservada sempre que os dados forem apresentados, como por exemplo em uma consulta em tela ou impressão em PDF.	M	M
ESTR.02.02	Preservação de relacionamento de dados	Registrar dados em tabelas representando matrizes, quando aplicável, de tal forma que os relacionamentos dos dados com as linhas e colunas estejam preservados no banco de dados, com total independência dos aplicativos. Exemplo: audiograma; registros de pressões arteriais de membros superiores e inferiores com paciente em pé, sentado e deitado; e odontograma.	M	M
ESTR.02.03	Hierarquia de nodos	Registrar os dados em hierarquias, quando aplicável, preservando o relacionamento dos nodos pais com os nodos filhos, de forma que possibilite a navegação, busca e consulta destes dados. Exemplo: familiograma.	M	M
ESTR.02.04	Associação do nome e valor dado	Registrar dados simples, preservando a associação entre nome do dado e respectivo valor. Exemplo: a pressão sistólica deve estar associada ao campo correspondente.	M	M

ESTR.02.05	Armazenamento de múltiplos valores	Registrar múltiplos valores coletados sequencialmente para uma mesma observação, durante um mesmo contato ou em diferentes contatos e locais. O contexto no qual os dados foram coletados deve ser preservado, tais como o tipo de ferramenta e metodologia utilizada e quem os coletou. Estes valores devem ser exibidos quando solicitados, e ordenados de diferentes formas. Exemplo: registro sequencial da pressão arterial braquial; registro sequencial da pressão sonora em um ambiente de trabalho.	M	M
ESTR.02.06	Inclusão de comentários em texto livre	Permitir a inclusão de texto livre complementar para melhor qualificar as opções de campos estruturados, quando o negócio assim o exigir, garantindo a associação destes comentários com os dados ou informações estruturadas originais (vide ESTR.02.08).	M	M
ESTR.02.07	Busca	Fazer pesquisa (de texto e dados numéricos) em todos os campos (estruturados e de texto livre).	M	M
ESTR.02.08	Inclusão de comentários em texto estruturado	Permitir a inclusão de campo estruturado complementar para melhor qualificar o conteúdo de um campo de texto livre, quando o negócio assim o exigir, garantindo a associação deste campo estruturado com o texto livre original (vide ESTR.02.08).	M	M
ESTR.02.09	Ênfase nos comentários e dados	Permitir enfatizar comentários ou dados registrados segundo as necessidades do negócio. Exemplo: ativação de um *flag* e/ou alteração de atributos da fonte (negrito, cor, etc.) a semelhança do uso de um marca-texto em papel.	M	M
ESTR.02.10	Validação da cronologia	Parametrizar regras de validação de cronologia de dados ou informações que possuam registro de tempo. Exemplo: alarmar se a data de óbito for anterior à data de nascimento; alertar se data de resultado de exame complementar for anterior à data de sua solicitação.	M	M
ESTR.02.11	Independência de dado e código	Armazenar parâmetros, configurações e classificações/codificações em banco de dados e não em linhas de código da aplicação. Exemplos: período máximo de validade de senha; período máximo de inatividade para bloqueio de sessão; e limites de temperatura axilar para validação (vide NGS1.02.04, NGS1.02.05, NGS1.03.01, e ESTR.01.03).	M	M

ESTR.03 - Dados Administrativos

ID	Título	Requisito	BAS	AMB
ESTR.03.03	Episódios de atenção	Registrar os episódios de atenção e os seus processos, preservando a associação dos dados registrados a cada um destes episódios. Exemplo: associação de uma prescrição medicamentosa a uma consulta; evolução clínica específica; resultado de exame complementar a uma sua solicitação específica; execução de procedimento cirúrgico; internação hospitalar; e realização de exame invasivo de imagenologia ou avaliação de risco ambiental.	M	M

ESTR.03.04	Informações financeiras e comerciais	Registrar dados e informações financeiras e comerciais, tais como operadoras de planos de saúde e respectivas elegibilidades, coberturas, responsável por despesas, custos, taxas e utilização. Exemplo: informações padronizadas nas mensagens entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde no âmbito da TISS	X	M
ESTR.03.05	Identificação do guardião ou representante do paciente	Identificar univocamente o representante ou guardião do sujeito da atenção, sua situação legal e documento comprobatório.	X	M
ESTR.03.06	Vigilância	Realizar consultas sobre diagnósticos e emitir relatórios para atender às demandas da vigilância epidemiológica, sanitária e doenças de notificação compulsória em pacientes externos ou internados. Deverão ser contemplados, no mínimo, os agravos constantes da Portaria n. 104, de 25 de Janeiro de 2011 (ou outro documento oficial mais recente) do Ministério de Saúde e das autoridade sanitária das demais esferas, quando aplicáveis (vide FUNC.04.03).	X	M
ESTR.03.07	Identificação unívoca do paciente e profissional	Identificar univocamente o sujeito da atenção e os profissionais envolvidos no processo assistencial (incluindo seus respectivos papéis bem como o registro de tempo inicial e final do evento). A identificação do sujeito da atenção e dos profissionais responsáveis pela assistência e pela entrada dos dados utilizará a plenitude dos padrões de identificação do Ministério da Saúde, como os do Cartão Nacional de Saúde e do CNES (vide NGS1.02.06).	X	M
ESTR.03.08	Registro de identificação do estabelecimento	Identificar univocamente utilizando o código do Cadastro Nacional de Estabelecimentos de Saúde – CNES. Para 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.	X	M
ESTR.03.09	Identificação do ambiente ou local de assistência	Identificar univocamente o local da assistência (por exemplo via pública, embarcação, aeronave, residência, consultório, leito ou quarto) ou ambiente ocupacional, segundo parâmetros dependentes da instituição naquele contexto.	X	M

ESTR.04 - Dados clínicos

ID	Título	Requisito	BAS	AMB
ESTR.04.01	Conjunto essencial de dados	Armazenar dados clínicos estruturados e não estruturados.	M	M

ESTR.04.02	Laudos e resultados de exames	Registrar os resultados de investigação (exemplo: exames complementares), com a descrição de como foi realizado, o método utilizado, a registro do tempo da realização, o profissional responsável pelo laudo/resultado e conclusão.	X	M
ESTR.04.03	Envio eletrônico de dados	Possuir funcionalidade de envio eletrônico de dados. Exemplo: mensagem via *webservices*.	M	M
ESTR.04.04	Estrutura de dados clínicos	Definir estrutura de dados clínicos. Exemplo: arquétipo de pressão arterial estruturado segundo a openEHR.	X	R
ESTR.04.05	Arquitetura de documentos	Estruturar a arquitetura de dados usando modelos de referência. Exemplo: HL7/CDA, ASTM/CCR	X	R
ESTR.04.06	Conjunto avançado de dados	Atender a plenitude dos dados clínicos constantes da resolução CFM 1638/2002 (ou mais recente).	X	M

ESTR.05 - Tipos de dados

ID	Título	Requisito	BAS	AMB
ESTR.05.01	Dados numéricos e quantificáveis	Possuir estrutura lógica de representação de dados numéricos e quantificáveis, incluindo o gerenciamento e conversão automática parametrizável entre unidades. Exemplos: interconverter quilograma em grama; grau Celsius em Farhenheit; miligrama por decilitro para miliosmol por litro; hora em minutos; miligrama em grama, litro para mililitro, e centímetro de mercúrio em milímetro de mercúrio.	M	M
ESTR.05.02	Precisão da medida	Armazenar o grau de precisão de medidas de quantidades de acordo com o método utilizado. Exemplo: intervalo de confiança de medida de peso corpóreo em balança antropométrica.	R	R
ESTR.05.03	Percentagem e valor absoluto	Expressar as percentagens também em valores absolutos.	R	R
ESTR.05.04	Limites	Parametrizar a estrutura lógica de representação de intervalos, ou seja, a representação de limites inferior e superior para dados quantificáveis adequados ao contexto, garantindo a escolha da ação (alerta, alarme, bloqueio, etc.). Exemplo: peso e altura de recém-nascido; frequência cardíaca em adulto; e potássio sérico em paciente em uso de diurético.	X	M
ESTR.05.05	Lógica dos valores fracionados	Representar a lógica de valores fracionados. Exemplo: Relação Colesterol total / HDL-Colesterol.	X	M

ESTR.05.06	Registro do tempo	Definir a estrutura lógica de representação dos valores de registro de tempo, incluindo dia, mês, ano, hora, minuto, segundo, milissegundo, fuso horário e horário de verão (vide ESTR.05.07 e ESTR.05.10, ESTR.05.13).	M	M
ESTR.05.07	Definições incompletas de tempo	Definir a estrutura lógica de representação dos valores de tempo que permita definições incompletas ou aproximadas, tais como: - datas aproximadas – Exemplo: ontem; semana passada. - datas parciais – Exemplo: ??/Maio/1997; ??/??/1928.	R	R
ESTR.05.08	Eventos e ações futuras	Registrar eventos ou ações planejadas para o futuro. Exemplos: 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; e períodos alternados de datas/horas: alternadamente a cada 8 horas, todas as segundas, quartas e sextas-feiras, todos os sábados, todo terceiro domingo.	R	R
ESTR.05.09	Linha de tempo	Registrar com acurácia o tempo associado a um determinado evento (vide NGS1.03.01). O registro do tempo do momento de registro no banco de dados deverá ser automático. O registro do tempo do evento poderá ser editável, possibilitando, por exemplo, o registro retroativo de ações passadas. Exemplo: registro de uma consulta ocorrida em momento de falha no fornecimento de energia elétrica à unidades prestadora de serviços.	M	M
ESTR.05.10	Fuso horário	Registrar o fuso horário do local de ocorrência de um determinado evento.	M	M
ESTR.05.11	Precisão do registro de tempo	Registrar todos os campos de tempo com precisão de pelo menos milissegundo.	R	R
ESTR.05.12	Tipos de dados padronizados	Utilizar uma estrutura lógica de representação de tipos de dados padronizados. Exemplo: DICOM em imagens médicas e odontológicas.	X	M
ESTR.05.13	Formato da representação do tempo em registros eletrônicos para exportação	Todo registro de tempo deve ser exportado no formato da ISO 8601:2004 e RFC 3339, incluindo o horário local e sua diferença para o UTC (*Coordinated Universal Time*, que representa o fuso horário). Exemplo: evento no dia 12 de abril de 1985, ocorrido às 10 horas, 15 minutos e 30 segundos no horário de Brasília, fora do horário de verão, que corresponde a 3 horas atrás do UTC. Sintaxe: 1985-04-12T10:15:30-03:00 (vide ESTR.05.06).	M	M
ESTR.05.14	Formato da exibição do tempo	Para exibição, o S-RES deve apresentar opção de formatos NBR 5892, ISO 8601:2004 entre outros. A exibição do fuso local deve ser configurável pelo S-RES, podendo ser inibida em sistemas locais.	M	M

ESTR.07 - Dados contextuais

ID	Título	Requisito	BAS	AMB
ESTR.07.01	Registro de tempo de uma ocorrência	Registrar o contexto associado ao registro do tempo em que o evento ocorreu. Exemplo: atendimento do paciente durante a falta de energia elétrica na unidade.	R	R
ESTR.07.02	Registro de tempo de gravação	Registrar o contexto associado ao registro do tempo em que o evento foi gravado no SRES. Exemplo: registro do atendimento ocorrido há 6 horas atrás quando não havia energia elétrica na unidade prestadora de serviços em saúde.	R	R
ESTR.07.03	Motivo ou assunto	Registrar o contexto associado ao motivo/assunto do evento. Exemplo: impressão do prontuário realizada por imposição de autoridade judicial; troca de nome de medicação comercial devido a indisponibilidade temporária.	R	R
ESTR.07.04	Responsável pelo registro	Registrar o contexto associado à pessoa responsável pelo registro do evento. Exemplo: diretor clínico da unidade de saúde efetuando o registro por ausência do profissional de saúde habitual do paciente.	R	R
ESTR.07.05	Ambiente físico da ocorrência	Registrar o contexto associado ao estabelecimento (ambiente físico) onde ocorreu o evento. Exemplo: atendimento realizado em via pública, consultório, enfermaria ou salão da caldeira; acidente do trabalho no trajeto empresa residência. (vide ESTR.03.08).	R	R
ESTR.07.06	Localização do registro	Registrar o contexto associado ao local onde o evento foi registrado. Exemplo: registro efetuado na unidade matriz de um serviço de atendimento domiciliar.	R	R
ESTR.07.07	Contexto e razão	Registrar o contexto associado à razão do registro. Exemplo: registro de mudança do status do prontuário para inativo por não comparecimento do paciente na unidade de atendimento após 20 anos da última consulta.	R	R
ESTR.07.08	Protocolo associado	Registrar o contexto associado ao protocolo associado à informação registrada. Exemplo: registro disparado por procedimento, rotina ou protocolo de pesquisa clínica na unidade de atendimento do paciente.	R	R

ESTR.08 - Associações

ID	Título	Requisito	BAS	AMB
ESTR.08.01	Associação semântica	Representar a associação semântica entre diferentes dados e informações no RES, através de um serviço de terminologias. Exemplo: relações semânticas dos tipos semânticos do UMLS.	X	R
ESTR.08.02	Dados referenciados externamente	Associar “dados referenciados externamente” quando estes não puderem ser representados no RES, desde que a segurança dos dados do paciente não seja comprometida. Exemplo: *link* de imagem médica/odontológica registrada em um outro sistema.	X	R

ESTR.09 - Representação de conceitos

ID	Título	Requisito	BAS	AMB
ESTR.09.01	Múltiplos sistemas de codificação	Utilizar múltiplos sistemas de codificação (terminologias de entrada ou interface, terminologias de referência e classificações) e o mapeamento entre eles.	X	R
ESTR.09.02	Captura de código	Registrar o código, a descrição do sistema de classificação/codificação utilizado, a versão, o idioma original e a descrição original no registro de um código de um sistema de classificação/codificação. Exemplo: ao se registrar um código do CID ou LOINC, associar ao registro dados relativos ao sistema utilizado (CID ou LOINC), versão, idioma original, o descritivo original no sistema de codificação em questão.	M	M
ESTR.09.03	Vocabulário padrão e de origem	Registrar dados a partir de vocabulários padrão, preservando-se a informação do vocabulário de origem. O registro de diagnósticos deverá utilizar obrigatoriamente o vocabulário de versão mais recente padronizada pelo Ministério da Saúde (vide ESTR.09.02). Exemplo: CID versão 10 em português.	X	M
ESTR.09.04	Ambiguidade	Garantir que todo dado apresentado em mais de um lugar ou mais de uma maneira seja sempre referenciado ao mesmo *label,* evitando ambiguidade de interpretação. Exemplo: garantir que “pulsos pediosos: não” tem o mesmo significado que “pulsos pediosos: ausentes”.	M	M
ESTR.09.05	Mapeamentos	Utilizar mapeamentos entre modelos de informação e de referência com base em um conjunto de conceitos bem definidos num vocabulário de referência ou modelo conceitual.	X	R
ESTR.09.06	Serviços de terminologia	Utilizar um serviço de terminologia. Exemplo: HL7 CTS; serviços que usem UMLS ou SNOMED-CT.	X	R
ESTR.09.07	Padrões de terminologia em saúde	Utilizar os padrões oficiais de terminologia em saúde. Exemplo: TUSS na TISS.	X	R

ESTR.10 - Representação de texto

ID	Título	Requisito	BAS	AMB
ESTR.10.01	Texto original	Preservar o texto original de campos estruturados conforme escolhido pelo usuário do RES, quando a informação for traduzida da linguagem estrangeira para português do Brasil, ou quando os termos forem mapeados de um sistema de codificação/classificação para outro. Exemplo: mostrar descritivos traduzidos versus os originais do LOINC ou de arquétipos do openEHR.	X	R

8.5. Requisitos de Funcionalidades

FUNC.01 - Suporte aos processos de atenção

ID	Título	Requisito	BAS	AMB
FUNC.01.01	Evento	Registrar qualquer tipo de evento, encontro ou episódio relevante à assistência à saúde do paciente.	M	M
FUNC.01.02	Processos de apoio	Criar, acompanhar e fazer a manutenção dos processos que apoiam as atividades de seus usuários.	M	M
FUNC.01.03	Continuidade de processos	Consultar o status de um processo e modificar um processo já existente, facilitando a continuidade do cuidado. Exemplo: status de um exame complementar ou de um levantamento (vide FUNC.05.01); e status de uma perícia.	M	M
FUNC.01.04	Processos incompletos	Registrar processos em aberto ou incompletos. Exemplos: exame ou procedimento solicitado nunca realizado pelo paciente; e levantamento de ambiente de trabalho incompleto.	M	M

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

ID	Título	Requisito	BAS	AMB
FUNC.02.01	Condição holística do paciente	Registrar a condição holística da situação da saúde do indivíduo, situação funcional, problemas, condições, circunstâncias e outras questões que possam afetar a sua saúde e caracterizar seu estado num dado momento.	X	M
FUNC.02.02	Estrutura de dados orientada por problemas	Registrar e apresentar dados em estrutura orientada por problemas, incluindo o status dos problemas (subjetivos e objetivos), análise, planos de solução e metas (SOAP). Possibilitar também a apresentação dos dados em estruturas como as orientadas cronologicamente, por episódios, e por processos (vide ESTR.02.01 e ESTR.03.03).	X	R
FUNC.02.03	Período de vida do indivíduo	Registrar longitudinalmente todo o período de vida do indivíduo, incluindo a condição de saúde e intervenções, que devem obrigatoriamente ser visualizadas de forma cronológica (vide ESTR.02.01). O RES é simultaneamente: • retrospectivo: oferece visão histórica das condições de saúde e intervenções. Exemplo: eventos ou atos 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).	X	M

FUNC.03 - Raciocínio Clínico

ID	Título	Requisito	BAS	AMB
FUNC.03.01	Raciocínio clínico	Registrar do raciocínio clínico para todos diagnósticos e avaliações (provisórios ou definitivos), conclusões e ações a respeito da assistência ao paciente, incluindo aqueles realizados por processos automatizados. Exemplo: usar o formato SOAP (subjetivo, objetivo, análise e programa), ou registrar o nexo causal em um acidente do trabalho ou doença profissional.	X	R

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

ID	Título	Requisito	BAS	AMB
FUNC.04.01	Alertas e lembretes	Apresentar automaticamente alertas, lembretes e avisos parametrizáveis. Exemplos: alergias e outras comorbidades, resultados urgentes, condição de infecção, precauções terapêuticas, interações medicamentosas, toxicidade potencializada por comorbidade, intervenções importantes e resultados urgentes, riscos ambientais (NR9) e uso de equipamentos de proteção individual (NR6), os quais deverão ser necessariamente exibidos sempre que se abrir o prontuário do paciente, fazer prescrições/orientações, consultar telas ou gerar relatórios pertinentes.	X	M
FUNC.04.02	Alertas e lembretes em vigilância	Incorporar lembretes e chamadas sobre os programas de vigilância epidemiológica e outras ações de saúde pública. Exemplo: programas de imunização, levantamentos de massa e outras campanhas (vide ESTR.03.06).	X	M
FUNC.04.03	Notificação de agravos	Emitir automaticamente a notificação de agravos, acidentes do trabalho ou doenças relacionadas ao trabalho conforme prevê o gestor federal, estadual e municipal de saúde. Deverão ser contemplados, no mínimo, os agravos constantes da Portaria n. 104, de 25 de Janeiro de 2011 (ou mais recente) do Ministério de Saúde. (vide ESTR.03.06).	X	M
FUNC.04.04	Diretrizes e protocolos	Incorporar diretrizes, protocolos e sistemas de apoio à decisão usando metodologias dedicadas, como por exemplo sintaxe de Arden.	X	R
FUNC.04.05	Restrição e obrigatoriedade	Representar restrições e dados obrigatórios (ambos parametrizáveis) ao processo de apoio à decisão. Exemplo: restrições de sexo X diagnóstico, medicação X diagnóstico, preparo para exame X medicação, atividade X restrição à prescrição de medicação que tenha alergia informada, e interação medicamentosa (vide FUNC.04.01).	X	M
FUNC.04.06	Mensagens do sistema	Apresentar clara e objetivamente as mensagens do sistema, em linguagem não técnica ao usuário, em português do Brasil. Exemplo: evitar mensagens de sistemas operacionais, componentes de segurança, bancos de dados sem tratamento pela aplicação.	M	M

FUNC.04.07	Rótulos	Apresentar rótulos de campos mostrados em tela e relatórios da forma clara e legível a qualquer momento do uso da tela, incluindo durante a sua rolagem, e em listas, *combos* etc.	M	M

FUNC.05 – Gerenciamento de status

ID	Título	Requisito	BAS	AMB
FUNC.05.01	Gerenciamento de status	Permitir o gerenciamento do status de diferentes atividades. Exemplos de status: solicitado, agendado, em realização, suspenso, em pendência, completo, verificado, cancelado, recebido, autorizado, glosado, complementado, encerrado, etc. (vide FUNC.01.03).	M	M

FUNC.06 - Prescrição e processamento de exames, investigações e solicitações

ID	Título	Requisito	BAS	AMB
FUNC.06.01	Registro e acompanhamento	Permitir o registro e acompanhamento de prescrições, ordens ou orientações dos profissionais de saúde, solicitação de exames complementares, investigações, levantamentos, interconsultas e encaminhamentos (vide ESTR.04.01).	X	M
FUNC.06.02	Associação	Associar um procedimento solicitado com o realizado e o respectivo resultado (vide ESTR.04.02). Exemplo: resultado de exame associado à sua solicitação; e mensagem de envio de recurso de glosas e as mensagens associadas de resposta de recurso de glosas e de recebimento do recurso de glosas na TISS.	M	M

FUNC.07 - Assistência integral

ID	Título	Requisito	BAS	AMB
FUNC.07.01	Assistência integral	Registrar o processo de assistência integral incluindo cuidados multidisciplinares e em diferentes níveis de atenção à saúde. Exemplo: primário, secundário, terciário, quaternário, especializado, internação hospitalar, cuidados e hospitalização domiciliar, urgência / emergência, pronto atendimento, odontológico, saúde do trabalhador ou saúde ambiental.	X	M

FUNC.08 - Garantia de qualidade

ID	Título	Requisito	BAS	AMB
FUNC.08.01	Performance operacional	Registrar e consultar dados com medidas (indicadores) de performance operacional, aderentes aos padrões de melhores práticas, com o objetivo de garantir a qualidade e medir os resultados dos processos. Exemplo: registro de objetivos, indicadores, metas e iniciativas.	R	R

FUNC.09 - Captura de dados

ID	Título	Requisito	BAS	AMB
FUNC.09.01	Entrada e acréscimo de dados	Possuir regras claras e consistentes para a entrada, manutenção, transmissão, recepção, tradução e substituição de dados. Este requisito jamais implicará em exclusão ou deleção de registros. Exemplo: regras para marcação de um registro ou campo (parcial ou total) com o status de inativo por lançamento inadvertido, etc. (vide FUNC.20.01 e FUNC.22.01).	M	M
FUNC.09.02	Validação de dados	Implementar regras de validação dos dados em consonância às melhores práticas. Exemplo: limites ou faixas de validade (vide ESTR.05.04).	M	M
FUNC.09.03	Pesquisa com filtros	Permitir o uso de filtros na pesquisa de dados já registrados.	M	M

FUNC.11 - Apresentação dos dados

ID	Título	Requisito	BAS	AMB
FUNC.11.01	Sumário clínico	Gerar automaticamente o sumário clínico a partir de cada campo de dado clínico marcado através de um *flag* parametrizável. O sumário clínico será parametrizável e deverá conter minimamente flags nos campos de diagnóstico provisórios e definitivos, medicamentos prescritos, exames complementares solicitados com resultados, atendimentos programados e/ou realizados, alergias e procedimentos realizados.	X	R
FUNC.11.02	Resolução para interpretação clínica	Alertar sobre a resolução mínima necessária para a interpretação clínica de imagens médicas ou odontológicas, ou seja, a matriz de pixeis/voxeis, o número de bits de cores e frames no tempo.	X	M
FUNC.11.03	Imagens médicas e odontológicas	Ao exibir imagens médicas ou odontológicas, exibir uma mensagem informando qual a matriz de pixeis/voxeis, número de bits de cores e frames no tempo da imagem original, e quando não disponíveis alertar para a indisponibilidade dessas informações.	X	M

FUNC.12 - Escalabilidade e performance

ID	Título	Requisito	BAS	AMB
FUNC.12.01	Eficiência de processamento	Processar eficientemente mesmo quando lidando com registros numerosos e/ou grandes, garantindo escalabilidade.	M	M

FUNC.13 - Protocolos de mensagens

ID	Título	Requisito	BAS	AMB
FUNC.13.01	Exportação e importação de dados	Exportar e importar dados recebidos por meio de protocolos de mensagens tais como HL7 e DICOM. Exemplo: sistemas de radiologia digital usando DICOM para troca de arquivos de imagem.	X	R
FUNC.13.02	Mensageria	Utilizar protocolos de mensagens padronizados pelas autoridades sanitárias oficiais. Exemplo: última versão dos padrões de troca de mensagem TISS.	X	R

FUNC.14 - Troca de registros

ID	Título	Requisito	BAS	AMB
FUNC.14.01	Serialização	Serializar dados com propósito de interoperabilidade. Exemplo: XML Schema na TISS.	X	R
FUNC.14.02	Regras de troca	Prover regras de troca de dados que sejam as mesmas tanto para apenas um extrato do RES ou para o RES completo. Exemplos: padrão TISS de troca de autorização de procedimentos, de cobrança de serviços de saúde, de comunicação de internação ou alta, de recurso de glosa, e de e emissão de demonstrativos de retorno.	X	R
FUNC.14.03	Interoperabilidade semântica	Promover a interoperabilidade semântica de conceitos clínicos entre sistemas objetivando processamento automático dos dados no S-RES receptor. (vide ESTR.08.01 e ESTR.09.06). Exemplo: uso de UMLS ou SNOMED.	X	R
FUNC.14.04	Interoperabilidade sintática	Promover a interoperabilidade sintática na troca de mensagens com autoridades sanitárias. Exemplo: uso de mensagem totalmente aderentes a última versão dos formatos padronizados do TISS (XML Schema).	X	R

FUNC.16 - Consentimento

ID	Título	Requisito	BAS	AMB
FUNC.16.01	Consentimento informado	Registrar os consentimentos informados do sujeito da atenção ou seu representante legal.	M	M
FUNC.16.02	Situação do consentimento informado	Obter, registrar e acompanhar a situação do consentimento informado para acessar parte ou todo o RES, para propósitos previamente definidos.	M	M
FUNC.16.03	Propósito do consentimento informado	Registrar os propósitos pelos quais o consentimento foi obtido.	M	M
FUNC.16.04	Instante do consentimento informado	Gravar o registro de tempo de cada consentimento.	M	M

FUNC.17 - Médico-legal

ID	Título	Requisito	BAS	AMB
FUNC.17.01	Cronologia de eventos	Assegurar a cronologia dos eventos e informações (vide ESTR.02.01, ESTR.05.06, ESTR.05.11). Exemplo: impressão de prontuário por solicitação de autoridade judiciária.	M	M
FUNC.17.02	Precisão e acurácia de visão cronológica	Visualizar com precisão e acurácia todo e qualquer dado do RES desde o momento do seu registro, garantindo compatibilidade retrógrada com versões anteriores (vide FUNC 20.02 e FUNC 23.02).	M	M

FUNC.18 - Atores

ID	Título	Requisito	BAS	AMB
FUNC.18.03	Identificação de fornecedor de informação	Identificar univocamente os usuários que atestam ou registram qualquer informação específica no RES (vide NGS1.02.01 e NGS1.02.06).	R	R

FUNC.18.04	Identificação do indivíduo	Identificar continuamente o indivíduo objeto da atenção, mesmo que este mude qualquer atributo de identificação. Isto tem que permitir que pesquisas ou relatórios acusem claramente as alterações desses atributos. Exemplo: alteração de nome; profissão; sexo ou endereço (vide FUNC 18.02).	M	M
FUNC.18.06	Registro do papel dos profissionais de saúde	Registrar o papel de todos os profissionais responsáveis por qualquer atividade registrada no RES (vide NGS1.02.01 e NGS1.02.06).	M	M
FUNC.18.07	Data do registro	Garantir que todo registro seja datado e seu autor responsável univocamente identificado (vide NGS1.02.01 e NGS1.02.06).	M	M
FUNC.18.08	Identificação de responsável pela informação no RES	Garantir que toda a informação registrada no RES seja atribuída a um ator responsável, independentemente se este foi o autor da informação ou não. Exemplo: na transcrição posterior de uma prescrição original em papel, o sistema deve identificar univocamente a pessoa que está digitando a informação e o autor da mesma (vide NGS1.02.01).	R	R
FUNC.18.09	Responsabilidade sobre contribuição aos registros	Nos sistemas que admitem preceptoria, garantir que todos os dados fornecidos ao RES sejam atestados ou validados pela pessoa responsável univocamente identificada. Exemplo: preceptor validando entradas de pós-graduandos em treinamento em ambiente acadêmico (vide NGS1.02.01 e NGS1.02.06).	M	M
FUNC.18.10	Responsabilidade sobre emendas e adições	Garantir que adição de dados, em situações excepcionais, seja atribuída à pessoa responsável, e que o registro de tempo e a razão para tal adição sejam gravados.	R	R

FUNC.19 - Competência e governança clínica

ID	Título	Requisito	BAS	AMB
FUNC.19.01	Competência técnica e responsabilidade	Registrar os dados de credenciamento, registro profissional e responsabilidade técnica dos profissionais de saúde. Exemplo: credencial de diretor técnico de uma unidade de saúde segundo o CRM local.	X	R

FUNC.20 – Fé Pública

ID	Título	Requisito	BAS	AMB
FUNC.20.01	Substituição de dados	Garantir que as novas informações inseridas em substituição a outras previamente registradas não apaguem as anteriores. O sistema deve manter histórico acessível das informações anteriores de forma segregada das atuais. Jamais um registro ou campo (total ou parcial) poderá ser deletado (vide FUNC.09.01 e FUNC.22.01).	M	M

FUNC.20.02	Situação de registro	Possibilitar a impressão da exata situação do registro em um dado ponto no tempo desde a criação original do RES (vide FUNC.17.02 e FUNC.23.02). Exemplo: impressão do SRES por solicitação do paciente ou autoridade judicial do prontuário em uma determinada data.	M	M

FUNC.21 - Preservação de contexto

ID	Título	Requisito	BAS	AMB
FUNC.21.02	Associação da informação do contexto clínico	Manter a associação da informação do contexto clínico e elementos de dados relevantes independentemente de como os dados tenham sido estruturados.	X	R

FUNC.23 - Controle de versão

ID	Título	Requisito	BAS	AMB
FUNC.23.01	Controle de versões	Suportar o versionamento das informações/dados armazenados no RES, explicitando o status de cada informação/dado (exemplo: ativo ou inativo).	M	M
FUNC.23.02	Medidas de discernimento	Visualizar o versionamento das informações/dados contidos no RES, sempre que aplicável (exemplos: mudança de nome; endereço, profissão e sexo) (vide FUNC.17.02 e FUNC.20.02).	M	M

FUNC.24 - Ética

ID	Título	Requisito	BAS	AMB
FUNC.24.01	Registro de justificativa ética	Registrar em campo específico da justificativa ética e da aprovação para uso secundário de informações extraídas do RES para uso *offline*. Exemplo: solicitação de cópia parcial ou total do prontuário por autoridade judiciária; e uso para pesquisa científica.	M	M

FUNC.25 - Direitos do paciente

ID	Título	Requisito	BAS	AMB
FUNC.25.01	Visão orientada para o paciente	Garantir o direito de acesso *online* ou *offline* do sujeito da atenção ao seu RES (vide ESTR.01.01 e ESTR.01.04). Exemplo: impressão do conteúdo do SRES, atendendo a cronologia natural dos eventos, com a sincronia de atualização cadastral e eventos clínicos.	M	M

FUNC.25.02	Direito de acesso	Garantir o direito de acesso do paciente ou seu representante legal às todas as informações do RES. O acesso pode ser direto ou via impressão em papel ou arquivo (por exemplo no formato PDF) obedecendo a cronologia dos eventos. Todas as informações deverão estar em português (vide NGS01.04.08). Um recibo será emitido pelo S-RES para registrar a solicitação do paciente ou seu representante legal e o recebimento das informações do RES. O recibo deverá conter o registro do tempo do período das informações do RES, identificação do paciente ou seu representante legal, identificação do profissional, registro do tempo e local da ocorrência, e espaço para assinatura pelo paciente ou seu representante legal.	M	M
FUNC.25.03	Informações dos pacientes	Permitir a incorporação no RES de informações dos pacientes sobre “autocuidado”, ponto de vista pessoal sobre as questões de saúde, níveis de satisfação, expectativas e comentários, quando assim o paciente desejar.	X	R

FUNC.27 - Evolução

ID	Título	Requisito	BAS	AMB
FUNC.27.01	Compatibilidade retroativa	Garantir compatibilidade com arquiteturas e versões antigas dos S-RES, de forma que possa processar os dados registrados nessas versões.	M	M
FUNC.27.03	Novos conhecimentos	Incorporar o registro de informação relacionada a novos conhecimentos, novas disciplinas, novas práticas e processos.	R	R

FUNC.28 - Acesso

ID	Título	Requisito	BAS	AMB
FUNC.28.01	Direito de acesso	Garantir acesso apenas aos profissionais ou entidades autorizadas pelo sujeito da atenção como os responsáveis pela guarda e manuseio do seu RES (vide NGS1.02.01), bloqueando o acesso aos não autorizados (vide NGS1.04.01).	M	M

8.6. Requisitos para GED

SGED.01 – Gerais

ID	Título	Requisito	Presença
SGED.01.01	Utilização de banco de dados	Utilizar base de dados adequada para o armazenamento dos arquivos digitalizados, em banco de dados relacional.	M
SGED.01.02	Método de Indexação	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	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	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	Permitir o armazenamento de vários formatos de documentos (PDF, DOCX, JPG, PNG, GIF, XLSX, PPTX,TIFF, KEY, ODT, etc.).	M
SGED.01.06	Integração com sistemas externos	Permitir a integração com sistemas de informação externos, tais como sistemas integrados de gestão.	R

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.

[26] ISO 27.799:2008 Health informatics -- Information security management in health using ISO/IEC 27002. Disponível em: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41298

[27] OWASP Testing Guide v4. Disponível em: https://www.owasp.org/index.php/OWASP_Testing_Project