
# Manual para Avaliação de Conformidade de Sistema de Prontuário Eletrônico para Unidades Básicas de Saúde

Versão 1.0

# Sociedade Brasileira de Informática em Saúde

## Diretoria 2017-2018

| | |
|---|---|
| Presidente: | Beatriz de Faria Leão |
| Vice-Presidente: | Zilma Silveira Nogueira Reis |
| Secretário: | Luiz Roberto de Oliveira |
| Tesoureiro: | Luiz Renato Evangelisti |
| Diretor Executivo: | Marcelo Lúcio da Silva |
| Diretoria de Educação: | Juliana Pereira de Souza Zinader e<br>Luiz Aparecido Virginio Jr. |
| Editor-Chefe do JHI: | Marco Antônio Gutierrez |

Editor deste manual: Marcelo Lúcio da Silva

Publicado em 24 de outubro de 2017

# Índice

# Glossário

| | |
|---|---|
| **Controle de Acesso** | Mecanismos utilizados para garantir que os recursos de um sistema de processamento de dados só possam ser acessados por entidades autorizadas e de forma autorizada. (Fonte: ISO/IEC 2382-8:1998, definição 08.04.01) |
| **Delegação de Poder** | Permissão dada por um usuário para que outro possa desempenhar funções em papéis que originalmente não tenha. Deve ocorrer por tempo limitado e, preferencialmente, serem respeitadas as limitações legais e dos órgãos de classe. |
| **Papel** | Função ou cargo desempenhado por uma entidade em uma determinada atividade. |
| **Perfil de acesso** | Permissão de acesso ou execução no sistema de um conjunto de funcionalidades e transações que podem ser baseadas na categoria funcional ou no grupo aos quais o usuário pertence. O perfil de acesso do usuário deve ser feito de forma discricionária pelo gestor de acesso ou administrador do sistema. |
| **Permissão de Acesso** | Relação de atividades que o usuário poderá executar no sistema de acordo com os processos definidos pela instituição ou de acordo com a legislação vigente ou regras do conselho de classe pertinente. |
| **Representante legal** | Pessoa com poderes para representar juridicamente o solicitante, conforme designação em seu estatuto ou contrato social ou em procuração. |
| **Restrição de Acesso** | Tecnologia de segurança que proíbe seletivamente ou não certos tipos de acesso a dados com base na identidade da entidade de acesso e no objeto de dados que está sendo acessado. |
| **Solicitante** | Organização solicitante (contratante) da avaliação de conformidade. |
| **Usuário** | Agente externo ao sistema que usufrui da tecnologia para realizar determinada atividade, podendo ser desde usuários comuns do sistema até administradores ou técnicos. |

# 1. Introdução

A informatização da gestão e da assistência é uma realidade crescente na área da saúde brasileira, possibilitando inúmeros benefícios aos profissionais, instituições, órgãos governamentais e, principalmente, aos cidadãos.

No sentido de ampliar e otimizar a informatização ao nível da Atenção Básica (AB), o Ministério da Saúde pretende credenciar empresas interessadas em fornecer e implantar sistemas de Prontuário Eletrônico nas Unidades Básicas de Saúde (UBS) do Sistema Único de Saúde (SUS).

Visando estabelecer critérios mínimos de qualidade para os sistemas de Prontuário Eletrônico a serem utilizados pelas UBS, a Sociedade Brasileira de Informática em Saúde (SBIS) definiu, em parceria com o Ministério da Saúde, um conjunto mínimo de requisitos a serem contemplados pelos referidos sistemas, cuja adoção será verificada por meio de um processo de avaliação de conformidade realizada por auditoria.

Este manual apresenta os requisitos e o processo de avaliação acima citados, descrevendo-os e detalhando-os de forma a possibilitar às empresas interessadas a implementação dos recursos necessários em seus sistemas de Prontuário Eletrônico para o pleno atendimento de tais requisitos, assim como viabilizar a realização da avaliação de conformidade junto à SBIS.

Este processo de avaliação de conformidade tem como objetivo garantir que um conjunto mínimo de requisitos seja atendido para responder à necessidade de implantação em larga escala de sistemas de Prontuário Eletrônico em todas as Unidades Básicas de Saúde do País. Os requisitos aqui definidos não são equivalentes ao bem estabelecido processo de Certificação de Sistemas de Registro Eletrônico em Saúde SBIS-CFM, voltado para, entre outros objetivos, possibilitar a exclusão de documentos em papel, finalidade esta que o presente processo não atende.

O processo proposto neste documento visa garantir que haja, de imediato, segurança da informação e que se pavimente o caminho para melhores práticas de qualidade e segurança de dados.

Os sistemas de Prontuário Eletrônico que demonstrarem, durante suas auditorias, total conformidade com os requisitos deste processo, receberão da SBIS uma Declaração de Conformidade, a qual deverá ser obrigatoriamente apresentada como parte da documentação exigida pelo Ministério da Saúde para o credenciamento da empresa fornecedora no Programa de Informatização das UBS, conforme definido em edital específico.

Deve-se observar que esta versão deste Manual, que dá início ao processo de avaliação de conformidade, apresenta um conjunto mínimo de requisitos restritos à análise da segurança da informação como um passo inicial deste processo, mas já com a perspectiva de ampliação de tal conjunto e extensão dos mesmos para requisitos de estrutura, conteúdos e funcionalidades mínimas nos próximos passos, os quais serão sempre anunciados e publicados com a devida antecedência necessária à adequação dos sistemas postulantes à obtenção ou atualização da Declaração de Conformidade.

Deve-se, por fim, ressaltar que o presente processo destina-se exclusivamente a sistemas de Prontuário Eletrônico cujas empresas detentoras pretendam credenciar-se no Programa de Informatização das Unidades Básicas de Saúde do SUS, conforme edital específico do Ministério da Saúde, tendo as respectivas Declarações de Conformidade o propósito único de atendimento aos critérios de credenciamento no referido Programa, sem relação ou efeito para os fins previstos pelo processo de Certificação de Sistemas de Registro Eletrônico em Saúde SBIS-CFM[1] também realizado por esta Sociedade.

[1] *Partes do conteúdo deste Manual foram obtidas e/ou adaptadas do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde SBIS-CFM - versão 4.2, publicado pela SBIS em 14/06/2016.*

# 2. Definições

A norma ISO 18308:2011 define Registro Eletrônico em Saúde (RES) como:

> "Um ou mais repositórios, física ou virtualmente integrados, de informação em forma processável por computadores, relevantes para o bem-estar, saúde e assistência à saúde de um indivíduo, capaz de ser armazenado e transmitido de forma segura e de ser acessível por múltiplos usuários autorizados, representado de acordo com um modelo de informação lógico padronizado ou comumente acordado. Seu objetivo principal é o apoio à atenção em saúde ao longo da vida do indivíduo de forma integrada, efetiva, com alta qualidade e segura."

Esta mesma norma define Sistema de Registro Eletrônico em Saúde (S-RES) como:

> "Sistema para registro, recuperação e manipulação das informações de Registros Eletrônicos em Saúde."

Desta forma, considera-se o Prontuário Eletrônico como um S-RES, ou seja:

> Um sistema informatizado para registro, recuperação e manipulação das informações relevantes para o bem-estar, saúde e assistência à saúde de um indivíduo, capaz de ser armazenado e transmitido de forma segura e de ser acessível por múltiplos usuários autorizados, representado de acordo com um modelo de informação lógico padronizado ou comumente acordado.

# 3. Princípios Adotados

## 3.1. Imparcialidade

Para que a SBIS possa oferecer um processo de avaliação que proporcione confiança, é necessário que o mesmo seja imparcial e percebido como tal. Todas as atividades e decisões deste processo serão baseadas em evidências objetivas de conformidade e as decisões não serão influenciadas por interesses espúrios.

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

## 3.2. Competência

Para que o processo de avaliação ofereça confiança, é necessário que o mesmo utilize apenas recursos humanos competentes, entendendo-se por competência a capacidade demonstrada de aplicar conhecimentos e habilidades.

A SBIS utilizará neste processo somente recursos humanos comprovadamente competentes e autorizados, e manterá registros de formação, experiência, habilidade e treinamento dos mesmos.

## 3.3. Responsabilidade

Para que o processo de avaliação ofereça confiança, é necessário que o solicitante entenda e assuma que é ele, e não a SBIS, quem possui a responsabilidade pela conformidade com os requisitos. Assim, diante de uma reclamação de um usuário do sistema avaliado, esta avaliação jamais poderá ser invocada como evidência objetiva de que o sistema não apresenta a deficiência apontada pelo usuário.

A SBIS é responsável por avaliar evidências objetivas suficientes nas quais possa basear sua declaração de conformidade aos requisitos expressos neste manual, com base nos resultados das auditorias realizadas no sistema.

## 3.4. Transparência

Transparência é um princípio de acesso ou divulgação de informações. Para obter e manter confiança, a SBIS oferecerá acesso público sobre seu processo de avaliação, exceto informações de natureza confidencial, tais como as informações privadas das partes envolvidas.

## 3.5. Confidencialidade

A confidencialidade é um princípio que proporciona à SBIS obter confiança da empresa solicitante de que esta não terá sua imagem ou seus interesses, de alguma forma, prejudicados por submeter seu sistema a este processo de avaliação.

Para que possa obter acesso privilegiado às informações necessárias para avaliar adequadamente a conformidade do sistema com os requisitos, a SBIS compromete-se a manter a confidencialidade de todas as informações privadas das empresas solicitantes e seus produtos, com exceção dos dados cadastrais essenciais da empresa, do sistema avaliado e da validade da avaliação, os quais serão publicados no sítio da SBIS na internet e/ou outros meios pertinentes.

# 4. Escopo da Avaliação

O presente processo de avaliação de conformidade destina-se única e exclusivamente a sistemas de Prontuário Eletrônico cujas empresas detentoras pretendam credenciar-se no Programa de Informatização das Unidades Básicas de Saúde do SUS, conforme edital específico do Ministério da Saúde.

Considera-se como sistema de Prontuário Eletrônico, para efeito de avaliação no presente processo, o conjunto completo que compreende o sistema principal e seus subsistemas e componentes (ex.: SGBD, sistema operacional, navegador, bibliotecas, etc.), devidamente configurados de forma a atender os requisitos especificados neste manual.

É importante ressaltar que é dever do fornecedor do sistema indicar para seus clientes e usuários todas as interdependências entre os subsistemas e componentes necessários para que o sistema esteja configurado e funcione corretamente, especialmente quando os subsistemas ou componentes não forem fornecidos juntamente com produto principal, cabendo ao cliente/usuário contratar o licenciamento destes separadamente.

## 4.1. Itens Condicionais

A lista de requisitos apresenta alguns itens condicionais, os quais serão aplicáveis somente quando a referida condição for verdadeira para o sistema sob avaliação, sendo desconsiderados caso contrário.

Em vários destes requisitos, a condição de aplicabilidade se dará pela declaração do solicitante através de um questionário que lhe será enviado previamente à auditoria. Todas as condições para as quais o solicitante declarar atendidas pelo sistema terão seus respectivos requisitos considerados aplicáveis e, assim, terão que demonstrar conformidade nos testes durante a auditoria para a devida aprovação.

Deve-se ressaltar que, caso uma determinada condição tenha sido declarada como não atendida pelo solicitante, mas que seja observada como atendida durante a auditoria, esta passará a ser considerada válida, tornando seus respectivos requisitos aplicáveis para os devidos testes.

Caso o sistema tenha a sua avaliação aprovada, constará na respectiva Declaração de Conformidade tanto as condições consideradas válidas como as inválidas, de forma que aqueles que a consultarem possam identificar quais requisitos condicionais foram atendidos ou não testados.

# 5. Conceitos e Condições

## 5.1. Componentes do sistema

Para submeter um sistema à avaliação de conformidade, o solicitante deve identificá-lo e descrever cada um de seus componentes. A descrição deve incluir a infraestrutura necessária para o sistema funcionar corretamente, incluindo todos os componentes de hardware e software que serão utilizados no processo de avaliação, além dos respectivos parâmetros que devam ser eventualmente ajustados.

A SBIS fará a auditoria com base no sistema identificado e descrito pelo solicitante. É importante lembrar que a descrição fornecida pelo solicitante deverá ser fiel à versão do sistema que será efetivamente submetida ao processo de avaliação.

### 5.1.1. Componentes de suporte

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

- Sistema operacional (servidor e estação)
- SGBD (Banco de Dados) e conectores
- Arquitetura do S-RES (cliente/servidor, *web*, SaaS, etc.)
- Arquitetura de rede (centralizada, distribuída, em nuvem, etc.)
- Componentes dinâmicos do tipo *web* (a*pplets, ActiveX, etc.*)
- Sistema de diretórios (AD, LDAP, etc.)
- Navegador (*browser*), no caso de sistemas baseados na *web*

### 5.1.2. Componentes alternativos de suporte

Além dos componentes utilizados na auditoria, o solicitante poderá informar uma lista contendo os componentes de suporte para os quais o sistema também funciona e que produzem exatamente os mesmos efeitos no que tange à conformidade aos requisitos deste manual.

Sendo o sistema aprovado na auditoria, a SBIS publicará sua descrição na Declaração de Conformidade e na lista de sistemas aprovados 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 sistema 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 Serviços de Avaliação Técnica (ver item 5.5), as quais poderão incluir o cancelamento da Declaração de Conformidade.

## 5.2. Versões do sistema

Cada Declaração de Conformidade está relacionada a uma versão específica do sistema, testada no processo de auditoria e em total conformidade com os requisitos estabelecidos. Assim, a descrição do sistema deverá incluir também a identificação da sua versão.

Para efeito deste processo, uma nova versão de um sistema 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 tais ajustes podem ser classificados como “não relevantes” ou “relevantes” no contexto deste processo.

É possível solicitar que a Declaração de Conformidade concedida a uma determinada versão de um sistema de Prontuário Eletrônico seja estendida para outras versões do mesmo sistema (ver item 5.3), considerando-se a classificação dos ajustes conforme exposto adiante.

### 5.2.1. Ajustes não relevantes

Entende-se por “ajustes não relevantes” as modificações e atualizações cujo objeto ou alvo não tenham relação direta com qualquer requisito deste processo. Como exemplos de ajustes não relevantes, lembrando que eles não podem afetar, modificar ou remover uma ou mais funcionalidades ou características necessárias para a aprovação da conformidade, podem ser citados:

- Modificações no nome do produto;
- Modificações na interface com o usuário (esquemas de cores, fontes, estilos de botões, etc.);
- Adição de novas funcionalidades ou módulos fora do escopo da avaliação;
- Correções ou alterações em funcionalidades fora do escopo da avaliação.

### 5.2.2. Ajustes relevantes

Entende-se por "ajustes relevantes" as modificações cujo objeto ou alvo tenham relação direta com algum requisito deste processo, 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 sistema consideradas no processo de avaliação, podem ser citados:

- Remoção de qualquer funcionalidade ou módulo essencial para a obtenção da conformidade;
- Substituição de bibliotecas ou componentes de software (por exemplo, substituindo um editor de textos desenvolvido internamente e utilizado na edição do prontuário 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 sistema que, mesmo possuindo interfaces ou características padronizadas, oferecem características específicas utilizadas para obter a conformidade (por exemplo, substituição de SGBD cujo módulo de criptografia de dados era utilizado para garantir aspectos de segurança da informação avaliados no processo).

## 5.3. Extensão da Declaração de Conformidade para outras versões do sistema

A Declaração de Conformidade é específica para a versão do sistema de Prontuário Eletrônico nela discriminada.

A SBIS poderá estender a Declaração para outras versões de um sistema já aprovado, desde que tal extensão seja obtida durante o período de validade da Declaração original. Para tanto, o solicitante deverá preencher a Ficha de Inscrição para Extensão de Declaração (ver item 5.5) e submetê-la ao processo descrito no capítulo 6.5 deste manual.

A solicitação de extensão deverá conter a descrição de todos os ajustes realizados na nova versão do sistema ("*release notes*"). Se a nova versão contiver qualquer "ajuste relevante" (ver item 5.2.2), o processo de extensão incluirá nova auditoria do sistema.

No caso de nova versão de um sistema já aprovado que contenha ajustes relevantes, uma das seguintes alternativas deverá ser observada:

- Caso a versão deste Manual de Avaliação de Conformidade vigente à época da solicitação de extensão for a mesma utilizada na avaliação da versão anterior do sistema, este deverá passar por uma auditoria para Extensão de Declaração. 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 sistema. No caso da nova versão ser aprovada nesta nova auditoria, o prazo de validade da Declaração passará a ser contado a partir desta última auditoria.

- Caso a versão deste Manual de Avaliação de Conformidade vigente à época da solicitação de extensão for diferente daquela utilizada na avaliação da versão anterior do sistema, o solicitante deverá submeter o sistema a uma nova avaliação completa, não podendo ser efetuado o processo de extensão da declaração.

Mesmo nos casos onde é possível estender a Declaração de Conformidade de um sistema 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 sistema previamente aprovado é também aprovado, sem antes obter formalmente tal extensão da SBIS. Ao conceder tal extensão, a SBIS irá incluir a nova versão na lista dos sistemas aprovados, 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 de declaração pela SBIS.

## 5.4. Validade da Declaração de Conformidade

A Declaração de Conformidade será válida pelo prazo definido pelo Ministério da Saúde a partir da publicação pela SBIS da versão deste Manual de Avaliação de Conformidade imediatamente posterior à que serviu de base para a Declaração original, sendo tal prazo limitado a 30 (trinta) meses da data de emissão da respectiva Declaração.

## 5.5. Instrumentos Formais

O processo de Avaliação de Conformidade será formalizado e regulamentado pelos seguintes instrumentos:

- **Ficha de Inscrição para Avaliação**: formulário eletrônico a ser preenchido e enviado pelo solicitante à SBIS para indicar a intenção de submeter um sistema ao processo de avaliação.

- **Ficha de Inscrição para Extensão de Declaração**: formulário eletrônico a ser preenchido e enviado pelo solicitante à SBIS para indicar a intenção de submeter um sistema já aprovado ao processo de extensão da declaração.

- **Contrato de Prestação de Serviços de Avaliação Técnica**: contrato firmado entre o solicitante e a SBIS antes do início da auditoria do sistema, o qual regulamenta tanto a execução do processo de avaliação quanto as normas a serem cumpridas pelas partes após tal processo, seja o sistema aprovado 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 da Declaração de Conformidade), e os devidos termos jurídicos referentes ao contexto pactuado.

- **Declaração de Conformidade**: documento probatório da aprovação do sistema no processo de Avaliação de Conformidade pela SBIS.

- **Termo de Extensão de Declaração:** documento probatório da extensão da Declaração de Conformidade para uma nova versão de um sistema já aprovado anteriormente no processo de Avaliação de Conformidade pela SBIS.

## 5.6. Taxas e Preços

Serão cobradas do solicitante as seguintes taxas, cujos valores encontram-se disponíveis para consulta no sítio da SBIS na internet. A SBIS se reserva o direito de alterar os valores a qualquer momento de acordo com critérios próprios, sob aviso prévio mínimo de 30 (trinta) dias da alteração.

- **Taxa de Inscrição**: valor a ser pago pelo solicitante à SBIS imediatamente após o envio da Ficha de Inscrição para Avaliação, que proporciona ao mesmo unicamente o direito à

análise e avaliação de tal ficha pela SBIS e à elaboração do Contrato de Serviços de Avaliação Técnica.

- **Taxa de Avaliação de Conformidade:** valor a ser pago pelo solicitante à SBIS entre a celebração do contrato e a realização da auditoria (ciclo inicial), e que proporciona ao mesmo o direito à realização de tal ciclo e, caso venha a ser aprovado, à emissão da Declaração de Conformidade.

- **Taxa de Extensão de Declaração:** valor a ser pago pelo solicitante à SBIS imediatamente após o envio da Ficha de Inscrição para Extensão de Declaração, e que proporciona ao mesmo o direito ao processo de análise e/ou auditoria do sistema e, caso venha a ser aprovado, à emissão do Termo de Extensão de Declaração.

- **Taxa de Realização de Ciclo Adicional de Auditoria:** valor a ser pago pelo solicitante à SBIS para a realização, quando necessário, de um ciclo adicional de auditoria dentro de um processo de Avaliação de Conformidade, e que proporciona ao mesmo somente 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 um ciclo de auditoria cujo cronograma tenha sido previamente aprovado entre as partes.

### 5.6.1. 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 ou a não aprovação do sistema ao final de sua 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.

# 6. Processo de Avaliação de Conformidade

O processo de Avaliação de Conformidade é constituído pelas seguintes etapas:

a) Preparação
b) Inscrição e formalização
c) Auditoria (um ou mais ciclos)
d) Conclusão

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

Todos os prazos regimentais especificados nas etapas abaixo que dependam da SBIS representarão a melhor tentativa, e podem variar em função de eventos ou problemas inesperados ou fora do seu controle, tais como excesso de demanda, conflitos com a realização de eventos, etc., e não poderão ser objeto de exigência estrita contratual por parte do solicitante.

## 6.1. Preparação

Os primeiros passos visando a avaliação de um sistema devem ser executados internamente pela empresa interessada (solicitante), que deve:

a) Analisar toda a documentação sobre o processo de avaliação disponível no sítio da SBIS na internet;

b) Verificar se o sistema a ser avaliado atende a todos os requisitos deste Manual;

c) Efetuar os ajustes eventualmente necessários no sistema para o pleno atendimento aos requisitos;

d) Realizar internamente a bateria de testes, conforme descrito no Manual Operacional de Ensaios e Análises para a Avaliação de Conformidade de Sistema de Prontuário Eletrônico para Unidades Básicas de Saúde, publicado pela SBIS;

e) Estando a empresa interessada segura de que seu sistema está em condições de ser aprovado na auditoria, só então deverá proceder à inscrição no presente processo de Avaliação de Conformidade.

## 6.2. Inscrição e formalização

### 6.2.1. Envio da Ficha de Inscrição para Avaliação

O solicitante deverá preencher a Ficha de Inscrição para Avaliação (ver item 5.5), disponível no sítio da SBIS na internet, e enviá-la eletronicamente através do e-mail certificacao@sbis.org.br.

### 6.2.2. Pagamento da Taxa de Inscrição

A SBIS enviará por e-mail ao solicitante, no prazo máximo de um dia útil após o recebimento da Ficha de Inscrição para Avaliação, um boleto bancário referente à Taxa de Inscrição no processo (ver item 5.6). 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 dez dias úteis após o envio do boleto.

### 6.2.3. Assinatura do contrato

Caso a análise da Ficha de Inscrição pela SBIS não aponte qualquer restrição à participação do solicitante e do sistema inscrito no processo, o solicitante receberá da SBIS, no prazo máximo de dois dias úteis após o pagamento da Taxa de Inscrição, o Contrato de Prestação de Serviços de Avaliação Técnica (ver item 5.5), 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 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 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 sistema inscrito no processo, o solicitante receberá da SBIS, no prazo máximo de cinco dias úteis após o pagamento da Taxa de Inscrição, um comunicado sobre a impossibilidade de execução do processo, onde serão expostos os motivos para tal rejeição.

## 6.3. Auditoria

A Avaliação de Conformidade estabelece a execução de auditoria sobre o sistema, realizada por equipe especializada, a qual verificará se os requisitos são realmente atendidos pelo sistema.

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

### 6.3.1. Solicitação

Concluída a formalização do contrato (ver item 6.2.3), o solicitante deverá, no prazo máximo de 60 dias, solicitar por e-mail à SBIS o agendamento da auditoria de seu sistema. Caso tal solicitação não ocorra neste prazo, o processo será considerado encerrado.

### 6.3.2. Pagamento da Taxa de Avaliação de Conformidade

A SBIS enviará por e-mail ao solicitante, no prazo máximo de dois dias úteis após o recebimento do contrato assinado, um boleto bancário referente à Taxa de Avaliação de Conformidade (ver item 5.5). 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 dez dias úteis após o envio do boleto.

### 6.3.3. Agendamento

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.

### 6.3.4. 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 da SBIS, 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 dois auditores seniores e/ou plenos, e poderá ser acompanhada por um ou mais auditores *trainees*, 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 cinco dias úteis após o envio da relação, a seleção dos auditores será automaticamente considerada aprovada.

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

### 6.3.5. Preparação para a auditoria

Estando com a auditoria programada, recomenda-se ao solicitante que realize exaustivamente os testes apresentados no Manual Operacional de Ensaios e Análises para Avaliação de Conformidade de Sistema de Prontuário Eletrônico para Unidades Básicas de Saúde, bem como quaisquer testes adicionais que julgar pertinentes.

A fim de otimizar o andamento da auditoria, recomenda-se também que o solicitante documente, para cada requisito e/ou script de teste, os dados a serem acessados e procedimentos a serem

executados no sistema para a demonstração da conformidade. Esses dados e procedimentos incluem, mas não se limitam a:

- Usuários e respectivas senhas de acesso necessários para execução dos testes;
- Caminhos ou sequência de passos para acesso a determinadas funções ou dados no sistema, especialmente para as funções e dados de difícil acesso, tais como parâmetros de configuração;
- Scripts SQL necessários para demonstrações que exijam acesso à base de dados;
- Outras informações e anotações que agilizem a execução dos testes.

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

- Todos os manuais do sistema objeto da auditoria, preferivelmente em formato eletrônico (PDF ou semelhante, mas não na forma de HELP);
- Esquema gráfico da estrutura lógica de ligação dos componentes do sistema, 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, que deverá providenciá-lo.

Por fim, o solicitante deverá instalar e/ou preparar o sistema no ambiente computacional onde os testes serão executados, incluindo todos os aplicativos e produtos adicionais necessários à sua execução, para uso de uma das seguintes formas:

- Em computadores portáteis ou desktops do próprio solicitante, que deverão ser levados fisicamente para o local da auditoria;
- Acesso ao sistema por meio da internet.

A SBIS disponibiliza no local da auditoria uma rede de área local (LAN) com roteador TCP/IP com e sem fio, e conectividade em banda larga à internet, para uso compartilhado pelo solicitante. O solicitante poderá, a seu critério, utilizar um roteador próprio, desde que permita aos auditores conectarem-se nesta rede para fins de execução dos testes de conformidade aos requisitos deste Manual.

### 6.3.6. Execução da auditoria

A auditoria ocorrerá na sede da SBIS ou em outro local definido por esta, mas nunca nos escritórios do solicitante, com duração pré-determinada de quatro horas. 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 sistema auditado.

O solicitante deverá estar presente no local da auditoria com um ou dois profissionais para operarem o sistema durante todo o período. Tais profissionais deverão, conjuntamente, estar aptos a operar todos os módulos e funcionalidades do sistema pertinentes aos requisitos da avaliação, assim como acessar o Sistema de Gerenciamento de Banco de Dados (SGBD) utilizado no sistema na condição de administrador, e deverão atender às orientações e solicitações efetuadas pelos auditores durante toda a sessão.

Durante a auditoria, os auditores solicitarão aos profissionais disponibilizados pelo solicitante que operem o sistema. Serão executados todos testes necessários à verificação da conformidade do sistema a todos os requisitos, tendo como orientação os procedimentos (*scripts*) definidos no Manual Operacional de Ensaios e Análises para Avaliação de Conformidade de Sistema de Prontuário Eletrônico para Unidades Básicas de Saúde, verificando-se a obtenção ou não dos resultados esperados.

É importante salientar que os *scripts* e respectivos procedimentos de testes constituem um roteiro básico que visa verificar a aderência do sistema aos requisitos, não contemplando, contudo, testes exaustivos em todo o sistema e em todas as situações possíveis. Assim, a qualquer momento durante o processo de auditoria, os auditores poderão reprovar um determinado requisito caso seja identificada qualquer inconformidade às suas exigências, mesmo que esta não tenha sido constatada por meio dos *scripts* ou ainda que este requisito já tenha sido aprovado anteriormente.

Deve-se ainda ressaltar que a conformidade refere-se à aderência do sistema aos requisitos do presente Manual, sendo o referido Manual Operacional de Ensaios e Análises tão somente um guia orientador dos testes, podendo os auditores executar outros testes que considerarem necessários, desde que pertinentes aos requisitos em questão.

Após a execução de cada teste, cada auditor registrará o seu parecer em sua planilha de resultados, sendo estes consolidados 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.

A duração estipulada pela SBIS para a auditoria será inflexível, constituindo-se de tempo suficientemente hábil para a execução de todos os testes aplicáveis. Eventuais interrupções nas sessões de auditoria provocados pelos profissionais do solicitante, seja para ajustes no sistema ou qualquer outro motivo, consumirão parte do tempo disponível, não constituindo prerrogativa para extensão da duração pré-definida. Assim, qualquer requisito que deixe de ser testado por falta de tempo em decorrência de tais interrupções será considerado como não-conforme. Excetuam-se as situações em que a falta de tempo para a conclusão dos testes for decorrente de eventuais falhas na infraestrutura oferecida pela SBIS.

Caso a auditoria não seja realizada nas datas previstas devido a qualquer impossibilidade por parte do solicitante, inclusive por não disponibilizar quaisquer recursos previstos, será elaborado um novo agendamento, mediante o pagamento, pelo Solicitante, da Taxa de Reagendamento de Auditoria (ver item 5.6).

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

Todos os custos e despesas decorrentes da disponibilização pelo solicitante dos recursos físicos e humanos aqui citados, tais como despesas de viagem, hospedagem e alimentação, serão de responsabilidade total e exclusiva do próprio solicitante, e não serão passíveis de qualquer tipo de remuneração, auxílio financeiro ou reembolso por parte da SBIS.

### 6.3.7. Ciclos adicionais de auditoria

Caso, ao final de um ciclo de auditoria de um sistema, o mesmo não seja aprovado, será proporcionada ao solicitante a oportunidade para que este realize os ajustes necessários no sistema para a solução das não-conformidades apontadas, com consequente execução de um novo ciclo de auditoria, ainda dentro do mesmo processo. Caso o solicitante opte por este procedimento, deverá efetuar o pagamento da Taxa de Realização de Ciclo Adicional de Auditoria (ver item 5.6).

O prazo máximo para a realização dos ajustes será de 60 dias a partir da comunicação da SBIS ao solicitante para o primeiro ciclo adicional e de 30 dias para o segundo e terceiro ciclos adicionais, devendo a nova auditoria (ciclo adicional) ser realizada na data mais próxima disponível após este período. A nova auditoria será realizada obrigatoriamente sobre o mesmo sistema 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.

A execução dos ciclos adicionais seguirão os mesmos procedimentos definidos para o ciclo inicial (ver item 6.3.6 acima), com exceção da duração que será pré-determinada entre uma a quatro horas.

Este procedimento poderá ser realizado até três vezes dentro de um mesmo processo. Caso, ao final do terceiro ciclo adicional, a auditoria ainda aponte para não-conformidades, independentemente da quantidade ou abrangência das mesmas, o sistema terá sua avaliação reprovada.

## 6.4. Conclusão

A Diretoria da SBIS avaliará o resultado da auditoria, emitindo um parecer que poderá indicar a aprovação ou reprovação naquele ciclo. Após cada ciclo de auditoria, a SBIS poderá recomendar ao solicitante a realização de ajustes no sistema para a execução de um ciclo adicional de auditoria (até o limite máximo de 3 ciclos adicionais), ainda dentro do mesmo processo original, cujo parecer final indicará a aprovação ou reprovação do sistema.

Conforme já exposto anteriormente, para que seja aprovado, o sistema deverá demonstrar, em sua auditoria, conformidade a todos os requisitos deste Manual.

### 6.4.1. Sistema aprovado

No prazo máximo de cinco dias após o término da auditoria, a SBIS emitirá e enviará ao solicitante a Declaração de Conformidade (ver item 5.5) em arquivo eletrônico, e a publicará no sítio da SBIS na internet, encerrando o processo.

### 6.4.2. Sistema reprovado

No prazo máximo de cinco 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.

### 6.4.3. Interposição de recurso

Caso não concorde com a reprovação de seu sistema, 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 30 dias após o seu recebimento.

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

## 6.5. Extensão de Declaração

Para a obtenção de extensões de declaração para outras versões de um sistema já aprovado (ver item 5.3), devem ser efetuados os mesmos procedimentos (ou equivalentes) descritos neste capítulo para a inscrição, auditoria e conclusão, exceto nos pontos destacados a seguir:

a) Toda referência à Ficha de Inscrição para Avaliação deve ser substituída pela Ficha de Inscrição para Extensão de Avaliação (ver item 5.5);

b) Deve-se desconsiderar as referências à assinatura e envio do Contrato de Prestação de Serviços de Avaliação Técnica;

c) Toda referência à Taxa de Avaliação de Conformidade deve ser substituída pela Taxa de Extensão de Declaração (ver item 5.6);

d) Para as extensões por ajustes não relevantes (ver 5.2.1) não serão executados os procedimentos referentes à auditoria.

## 6.6. 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.

Todas as 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 uma empresa fornecedora de sistema aprovado, esta será comunicada formalmente e será intimada a apresentar resposta formal, sob pena de aplicação de sanção, que irá desde a advertência até a eventual suspensão de sua Declaração de Conformidade, a critério da Diretoria da SBIS.

# 7. Uso da Informação Relacionada

As informações relacionadas à Avaliação de Conformidade deverão seguir as diretrizes aqui apresentadas. Estas diretrizes devem ser observadas para a confecção de qualquer material de marketing ou comercial (folhetos, folders, embalagens, manuais, brindes, cartões de visita, prospectos, contratos, etc.), incluindo todas as formas de comunicação com o mercado (mídia impressa, rádio, televisão, internet, etc.).

Apenas as empresas fornecedoras de sistemas de Prontuário Eletrônico aprovados no presente processo poderão divulgar o respectivo sistema como sendo aprovado pela SBIS, sendo que esta divulgação somente poderá ocorrer após a publicação da Declaração de Conformidade no sítio da SBIS na internet. Caso tal declaração seja revogada ou tenha sua validade expirada, os materiais de marketing ou comercial que façam referência à mesma não poderão ser distribuídos ou divulgados.

Não é permitido o uso antecipado de informações acerca de uma possível ou pretensa obtensão da Declaração de Conformidade, como, por exemplo, a promessa da empresa de que obterá a declaração unicamente com base no fato de estar inscrita no processo, aguardando a auditoria, aguardando ciclos adicionais de auditoria ou aguardando a emissão da respectiva declaração, mesmo que esta esteja em vias de publicação.

As pessoas ou empresas que divulgarem informações relacionadas com a Avaliação de Conformidade de modo não previsto nestas diretrizes serão chamados a responder por tais atos. Caso trate-se de um sistema aprovado, o mesmo poderá ter sua Declaração de Conformidade revogada.

## 7.1. Referências ao estado de sistema aprovado

Ao fazer qualquer referência a um sistema aprovado no presente processo, a empresa deverá indicar claramente:

- O nome da empresa fornecedora
- O nome do sistema aprovado
- A versão do sistema aprovado
- A versão deste Manual utilizada como referência para a avaliação do sistema

A empresa fornecedora do sistema não poderá nunca utilizar-se da Declaração de Conformidade de seu sistema como um endosso à sua organização ou aos seus produtos de maneira geral, devendo limitar tal uso ao sistema e à versão efetivamente aprovados.

# 8. Requisitos de Conformidade

Uma parte significativa dos requisitos do presente processo foi elaborada a partir de normas e padrões nacionais e internacionais, enquanto outros foram criados com base na experiência de seus autores, e que atendem necessidades específicas consideradas fundamentais para os requisitos mínimos ou recomendados para os sistemas de Prontuário Eletrônico no Brasil.

Este capítulo apresenta todos os requisitos que compõem o processo de Avaliação de Conformidade, exibidos de forma tabular com as seguintes informações:

| Coluna | Descrição |
|---|---|
| ID | Identificação do requisito, codificada no seguinte padrão:<br>*Sigla-da-área.Número-do-capítulo.Número-do-requisito*<br>Exemplo: NGS1.01.01 |
| Título | Título (nome) do requisito |
| Requisito | Descrição do requisito, incluindo exemplos quando apropriado.<br>Adicionalmente, pode incluir notas explicativas para melhor elucidação de seu conteúdo. |

Nos requistos iniciados com uma expressão de "**Condição**", a obrigatoriedade será válida desde que a referida condição seja verdadeira, caso contrário o requisito será desconsiderado.

A numeração (ID) dos requisitos e respectivos grupos apresentam compatibilidade com a numeração do Manual para Certificação de S-RES SBIS-CFM, tanto para a sua versão atual como as anteriores. Assim, é comum observarem-se lacunas na numeração causadas pela remoção de itens existentes nas versões daquele manual. Da mesma forma, itens inteiramente novos receberam numeração adicional em relação ao mesmo.

O Manual Operacional de Ensaios e Análises para Avaliação de Conformidade de Sistema de Prontuário Eletrônico para Unidades Básicas de Saúde apresenta os *scripts* de teste para verificação da conformidade de todos os requisitos.

Para a aprovação do sistema e consequente emissão da Declaração de Conformidade, é necessário que o sistema demonstre conformidade com a totalidade dos requisitos aqui dispostos. Qualquer ausência de conformidade, independentemente da quantidade ou complexidade dos requisitos em questão, será fator impeditivo para a obtenção da Declaração de Conformidade objeto deste processo.

Todas as citações a "S-RES" nos requisitos referem-se ao Sistema de Registro Eletrônico em Saúde, que neste processo trata-se do Sistema de Prontuário Eletrônico submetido à avaliação de conformidade.

## 8.1. Requisitos do Nível de Garantia de Segurança 1 (NGS1)

**NGS1.01 - Controle de versão do software**

| ID | Título | Requisito |
|---|---|---|
| NGS1.01.01 | Versão do software | a) O S-RES (conjunto de componentes principais) deve apresentar minimamente as informações de identificação do software, contendo obrigatoriamente o nome do software, nome do fornecedor, identificação completa da versão e/ou *release* e/ou *build*. Essas informações deverão corresponder à da versão aprovada do produto, e será utilizada como referência em todos os documentos relacionados.<br><br>b) Essas informações deverão estar disponíveis minimamente:<br>▪ na tela inicial do S-RES;<br>▪ nas telas de cada módulo (por exemplo, cabeçalho, rodapé ou ainda em um item de um menu), de modo que quando o sistema esteja em uso essas informações estejam sempre visíveis. |

**NGS1.02 - Identificação e autenticação de pessoas**

| ID | Título | Requisito |
|---|---|---|
| NGS1.02.01 | Identificação e autenticação de usuário | Todo usuário do S-RES deve ser identificado e autenticado antes de qualquer acesso a dados ou funcionalidades do S-RES. |
| NGS1.02.02 | Método de autenticação de pessoa | a) Utilizar, em todos os processos autenticação de pessoa, no mínimo um dos seguintes métodos de autenticação de pessoa:<br>▪ Digitação de um nome de usuário e senha secreta de acesso;<br>▪ Certificado digital e senha/PIN (Personal Identifier Number);<br>▪ Validação biométrica;<br>▪ ou uma combinação dos métodos acima.<br><br>b) As credenciais para autenticação no S-RES devem ser validadas após a submissão das mesmas ao serviço de autenticação do sistema no lado do servidor, evitando que a validação ocorra on-the-fly no lado do cliente.<br><br>Nota: Quaisquer outras técnicas diferentes das exigidas acima, tais como OTP (one-time password) e Captcha são considerados complementares e podem ser utilizados apenas em conjunto com um dos métodos supracitados. |

| | | |
|---|---|---|
| NGS1.02.03 | Proteção dos parâmetros de autenticação de usuário | Armazenar de forma protegida todos os dados ou parâmetros utilizados no processo de autenticação de usuário.<br><br>Método: Nome de usuário e senha<br>a) A senha deve ser armazenada em banco de dados, de forma codificada por algoritmo de *hash* aberto (público) de no mínimo 160 bits.<br>b) As codificações das senhas de acesso dos usuários devem ser protegidas contra acesso não autorizado. Apenas o usuário do banco de dados utilizado pela aplicação deve ter acesso aos mesmos.<br><br>Método: Biometria (condição: somente para pessoas)<br>c) Os *templates* biométricos das pessoas devem ser protegidos contra acesso não autorizado. Apenas o usuário do banco de dados utilizado pela aplicação deve ter acesso aos mesmos.<br>d) As amostras biométricas coletadas e transmitidas durante o processo de autenticação devem ser protegidas contra acesso não autorizado.<br><br>Método: One-time password (OTP)<br>e) As sementes de geração dos valores numéricos devem ser protegidas contra acesso não autorizado. Apenas o usuário do banco de dados utilizado pela aplicação deve ter acesso aos mesmos. |
| NGS1.02.04 | Segurança de senhas | Condição: Utilização de autenticação baseada no método de usuário e senha.<br><br>Utilizar os seguintes controles mínimos de segurança de senhas:<br><br>a) **Qualidade da senha:** deve ser verificada a qualidade da senha no momento de sua definição, obrigando a utilização de, no mínimo, 8 caracteres sendo ao menos 1 caractere alfabético e 1 numérico.<br>b) **Troca de senha:** o usuário do S-RES deve ser capaz de efetuar troca de senha de seu usuário no sistema.<br>c) **Troca forçada de senha:** o S-RES deve ser capaz de solicitar a troca de senha de usuário(s) no próximo *login* por solicitação do administrador ou gestor de acessos (ex. caso de comprometimento da segurança do banco de dados e/ou aplicação).<br>d) **Periodicidade de troca de senhas:** deve ser obrigatória a troca de senhas pelos usuários, em um período máximo configurável que não exceda a 6 meses. O controle de tempo para periodicidade de senha deve ser realizado pelo servidor.<br>e) **Igualdade de senha:** os processos de troca de senha devem exigir que a nova senha seja diferente da imediatamente anterior àquela já utilizada pelo usuário.<br>f) **Visualização de senhas por terceiros:** quando da geração |

| | | |
|---|---|---|
| | | ou alteração de senha que não seja definida pelo próprio usuário, tal processo deve impedir sua visualização por terceiros (administradores ou outros usuários com perfil permitindo execução destas funcionalidades). |
| NGS1.02.05 | Controle de tentativas de login | a) O S-RES deve possuir, em todos os processos de autenticação de usuário, independentemente do método de autenticação utilizado, mecanismos para bloquear a conta deste usuário no S-RES (ou seja, bloquear seu acesso ao S-RES) após um número máximo configurável de tentativas consecutivas de *login* com autenticação inválida, que não exceda a 10 tentativas.<br>b) Após o bloqueio de conta de um usuário, o sistema só deve permitir *login* deste após o desbloqueio de sua conta de usuário. |
| NGS1.02.06 | Identidade única da pessoa e responsabiliza-ção | a) **Identidade única:** toda pessoa usuária do S-RES deverá ser identificada individualmente.<br>b) **Vinculação a número legal e único:** toda pessoa usuária do S-RES deverá ser vinculada minimamente a um documento de identificação pessoal unívoco segundo a legislação brasileira vigente (por exemplo, Número de Cadastro de Pessoa Física - CPF).<br>c) **Unicidade de identificação de usuários:** a informação de identificação de tal documento deverá ser validada em todos os processos de inclusão ou alteração de pessoas para garantir a unicidade, ou seja ,o S-RES não deve permitir a associação de um mesmo documento de identificação a dois usuários no sistema.<br>d) **Exclusão de usuários:** Para fins de responsabilização, não deve ser possível remover o cadastro ou vínculo de usuários e profissionais de saúde do sistema, caso alguma operação tenha sido realizada pelo mesmo.<br>e) **Unicidade em modalidade SaaS:** caso o S-RES opere na modalidade "S-RESaaS" (S-RES as a Service), a unicidade do identificador da pessoa deve ser por organização. |

**NGS1.03 - Controle de sessão de usuário**

| ID | Título | Requisito |
|---|---|---|
| NGS1.03.01 | Bloqueio ou encerramento por inatividade | a) A sessão de usuário deve ser automaticamente bloqueada ou encerrada forçadamente pelo aplicativo após um período de inatividade.<br>b) O período máximo de inatividade deve ser configurável e armazenado no banco de dados (vide ESTR.02.11).<br>c) Caso o S-RES possibilite ao usuário o desbloqueio de sessão, essa operação deve ser permitida apenas quando o desbloqueio for realizado pelo mesmo usuário bloqueado. Para que o desbloqueio de sessão seja realizado, o sistema deve requerer novo processo de autenticação do usuário bloqueado.<br>d) Após o bloqueio ou encerramento da sessão de usuário, as informações em tela não deverão mais estar visíveis, sendo necessária uma nova autenticação para a retomada da atividade.<br>e) Não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles. |
| NGS1.03.02 | Segurança contra roubo de sessão de usuário | A sessão de comunicação remota entre cliente e servidor deve possuir controles de segurança que impeçam o roubo ou reuso da sessão do usuário.<br>a) As credenciais de acesso não devem ser transmitidas entre as partes na forma de texto claro.<br>b) Devem haver controles que impeçam o reuso de identificadores de sessão do usuário (ataques de *replay e covert-channel)* e roubo da sessão.<br>c) Não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles. |
| NGS1.03.03 | Retomada de atividade do usuário | Condição: S-RES bloqueia a sessão de usuário por inatividade.<br><br>O S-RES deverá permitir a retomada da atividade do usuário após bloqueio de sessão. Essa operação é permitida apenas quando o desbloqueio for realizado pelo mesmo usuário bloqueado. Para que o desbloqueio de sessão seja realizado, o sistema deve requerer novo processo de autenticação do usuário bloqueado. |

**NGS1.04 - Autorização e controle de acesso de pessoas**

| ID | Título | Requisito |
|---|---|---|
| NGS1.04.01 | Impedir acesso por pessoas não autorizadas | Impedir acesso ou visualização do RES por pessoas não autorizadas no S-RES. |

| | | |
|---|---|---|
| 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. |
| NGS1.04.03 | Gerenciamento de usuários e papéis | O S-RES deve permitir o gerenciamento (criação, ativação/inativação e modificação) de usuários e papéis (perfis), por meio da aplicação, de forma a possibilitar o controle de acesso às funcionalidades do S-RES conforme os papéis aos quais o usuário possui. Um usuário pode possuir um ou mais papéis. |
| NGS1.04.04 | Papéis relacionados à T.I. | O S-RES deve suportar a criação minimamente dos seguintes papéis específicos relacionados à T.I. e seus respectivos objetivos (não necessariamente com estes nomes):<br>▪ Administrador: acesso a todas as funcionalidades do S-RES, exceto aquelas relacionadas ao acesso a dados clínicos reais (não fictícios ou pseudonomizado);<br>▪ Gestor de acessos: acesso restrito às funcionalidades de gerenciamento de usuários, perfis e grupos do sistema. |
| 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 (autorização), considerando os papéis de usuário, funções e tipos de operação (consulta, inclusão e alteração) disponíveis.<br><br>Nota: Para dados clínicos e demográficos de sujeitos da atenção, considera-se como “alteração” atividades de acréscimo e substituição a dados já previamente inseridos. |
| NGS1.04.08 | Acesso ao RES pelo sujeito da atenção | Condição: S-RES oferecer acesso direto ao RES pelo sujeito da atenção ou seu responsável legal como usuário do sistema.<br><br>O sujeito da atenção ou seu responsável legal deverá ter acesso unicamente ao seu prontuário, não podendo o mesmo ter acesso a informações de outros sujeitos da atenção. No caso de acesso ao prontuário pelo responsável legal, o acesso à funcionalidade de visualização e impressão poderá ser realizada tanto para seu prontuário quanto para o do sujeito da atenção sob sua responsabilidade. |
| NGS1.04.12 | Inserção de dados pelo sujeito da atenção | Condição: S-RES permite que o sujeito da atenção registre diretamente suas informações de saúde.<br><br>Qualquer registro inserido diretamente pelo sujeito da atenção no S-RES deverá ser realizado em uma área restrita e identificado distintamente dos dados inseridos pelos profissionais de saúde. |
| NGS1.04.13 | Acesso a dados de RES no SGBD | O SGBD deverá ser capaz de impedir que seus usuários tenham acesso a dados de saúde identificados no banco de dados. |

**NGS1.05 - Disponibilidade do RES**

| ID | Título | Requisito |
|---|---|---|
| NGS1.05.01 | Cópia de Segurança | O S-RES deve gerar cópia de segurança ("*backup full*"), contendo informações suficientes para restauração, atendendo aos seguintes requisitos:<br>a) Exportar os atributos de segurança e metadados em conjunto com os dados;<br>b) Garantir, na restauração de uma cópia de segurança, que os atributos de segurança e metadados sejam automaticamente recuperados, sem a intervenção do administrador.<br><br>Nota: Considera-se como atributos de segurança todos os parâmetros e configurações existentes. |
| NGS1.05.02 | Integridade na restauração da cópia de segurança | a) O S-RES deve possuir controle de integridade da cópia de segurança.<br>b) A verificação da integridade deverá ocorrer durante a restauração da cópia, gerando um alerta caso ocorra alguma falha. O processo de restauração deve garantir a atomicidade de forma que toda informação seja restaurada. Caso haja algum erro durante a restauração, nenhuma informação deverá então ser restaurada, retornando-se, portanto, ao estado anterior (rollback). |

**NGS1.06 – Comunicação entre componentes do S-RES**

| ID | Título | Requisito |
|---|---|---|
| NGS1.06.01 | Segurança da comunicação com componente de interação com o usuário | a) A sessão de comunicação entre o componente de interação com o usuário (ex.: browser ou executável cliente) e os outros componentes do S-RES (ex.: servidor de aplicação, banco de dados, etc) deve oferecer os seguintes serviços de segurança: autenticação do servidor, integridade dos dados e confidencialidade dos dados.<br>b) O serviço de segurança empregado deve implementar criptografia dos dados em trânsito. |
| NGS1.06.02 | Controle de acesso do cliente ao servidor | a) O S-RES deve ser capaz de identificar a origem de uma solicitação de acesso e decidir sobre sua autorização, de forma que apenas origens autorizadas possam ter acesso ao S-RES.<br>b) O S-RES deve possuir recursos que permitam configurar as origens permitidas ou proibidas, tais como uma lista de números de MACs ou IPs dos clientes. |

| | | |
|---|---|---|
| NGS1.06.03 | Processamento de dados no lado servidor | a) Todo processamento (modificação) de dados de RES deve ocorrer no lado do servidor. Todos os dados apresentados no lado cliente devem ter sido gerados e processados no lado servidor.<br><br>b) Todos os processos de validação de dados devem ser realizados no lado do servidor.<br><br>Nota: Opcionalmente, por questões de performance, poderá haver validação de dados inicialmente no lado cliente desde que seguida de validação no lado do servidor. |
| NGS1.06.04 | Segurança da comunicação entre componentes | Condição: S-RES ser composto por componentes distribuídos.<br><br>A comunicação entre componentes distribuídos (como, por exemplo, entre a aplicação e o banco de dados) deve oferecer os seguintes serviços de segurança: autenticação mútua de parceiros (ambas as partes), integridade dos dados e confidencialidade dos dados (criptografia).<br><br>Nota: A segurança pode ser aplicada ao canal de comunicação ou às mensagens trocadas. |
| NGS1.06.05 | Controle de acesso entre componentes | Condição: S-RES ser composto por componentes distribuídos.<br><br>Na comunicação entre componentes distribuídos (como, por exemplo, entre a aplicação e o banco de dados), o acesso ao componente deve ser restrito somente aos parceiros (componentes) previamente autorizados. |

**NGS1.07 - Segurança de dados**

| ID | Título | Requisito |
|---|---|---|
| NGS1.07.05 | Utilização de SGBD | Todos os dados de RES em S-RES devem ser armazenados integral e exclusivamente por um Sistema de Gerenciamento de Banco de Dados (SGBD). |
| NGS1.07.06 | Impedir acesso direto ao SGBD | a) 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.<br>b) O SGBD não deve permitir acesso direto pelos usuários do S-RES. |
| NGS1.07.10 | Validação de dados de entrada | Os dados inseridos pelo usuário nos campos de entrada (inputs, caixas de texto, etc) devem ser validados antes de serem processados, de forma a prevenir ataques de buffer overflow e injeção de dados. |

| | | |
|---|---|---|
| NGS1.07.11 | Segregação dos dados por organização | Condição: S-RES ofertado na modalidade "S-RESaaS" (S-RES as a Service).<br><br>Todos os dados do RES devem ser segregados por organização, ou seja, nenhum dado do RES de uma organização pode ser acessado ou visualizado por usuário de outra organização, salvo quando consentido pelo sujeito da atenção segundo acordo de privacidade.<br><br>Nota: A regra não se aplica obrigatoriamente para usuários de TI ou administrativos que sejam responsáveis pela gestão e controle centralizado (multi-organização). |

**NGS1.08 – Auditoria**

| ID | Título | Requisito |
|---|---|---|
| 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. |
| 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. |
| NGS1.08.04 | Eventos e informações registradas na trilha de auditoria | As trilhas de auditoria devem conter informações relacionadas minimamente aos seguintes tipos de eventos:<br><br>a) Quanto ao RES:<br>▪ Criação, consulta, acréscimo ou substituição de registros do RES.<br><br>b) Quanto às ações de usuário:<br>▪ Tentativas de autenticação de usuário, com ou sem sucesso;<br>▪ Troca de senha;<br>▪ Encerramento e bloqueio de sessão de usuário;<br>▪ Desbloqueio de sessão de usuário (aplicável apenas caso o S-RES permita o desbloqueio de sessões de usuário bloqueadas por inatividade);<br>▪ Aceitação do termo de concordância de uso (vide NGS1.12.01).<br><br>c) Quanto às ações operacionais:<br>▪ Atividades de configuração do sistema (por exemplo, parâmetros de configuração de senha e limite de tentativas de login);<br>▪ Atividades de gerenciamento de usuários e papéis, incluindo inativação/bloqueio e ativação/desbloqueio de conta de usuário;<br>▪ Geração de senha para usuário;<br>▪ Acesso aos registros de auditoria;<br>▪ Realização de cópia de segurança.<br><br>d) Com relação aos eventos citados acima, os registros de |

| | | |
|---|---|---|
| | | auditoria devem possuir, no mínimo, as seguintes informações para cada evento:<br>▪ Data e hora do evento;<br>▪ Tipo de evento (por exemplo, “troca de senha”, “autenticação de usuário”, etc.);<br>▪ Identificação do componente gerador do evento (ex.: nome do componente, endereço IP, dispositivo do usuário, ponto de acesso, etc);<br>▪ Identificação do usuário gerador do evento, quando aplicável;<br>▪ Identificador único e permanente do registro afetado pelo evento, quando aplicável (por exemplo, identificador do sujeito da atenção).<br><br>e) Dados clínicos ou demográficos não deverão ser registrados na trilha de auditoria (por exemplo, registrar os dados anteriores e posteriores à uma alteração de anamnese).<br><br>Nota: Deve-se atentar ao requisito NGS1.07.11 na visualização dos registros de auditoria. |

**NGS1.09 – Documentação**

Todas as instruções constantes deste grupo de requisitos devem estar detalhadas nos manuais, de forma a possibilitar a execução das atividades de instalação e configuração por eles descritos.

| ID | Título | Requisito |
|---|---|---|
| NGS1.09.01 | Documentação | a) O S-RES deve possuir manuais que apresentem minimamente as seguintes informações:<br>▪ Instruções de uso do S-RES para os usuários contemplando todos os perfis/papéis existentes (por exemplo: administrador, operador, operador de backup, etc);<br>▪ Visão geral do S-RES, incluindo formas de operação, requisitos do ambiente computacional;<br>▪ Instalação e configuração do S-RES.<br><br>b) Os manuais poderão ser apresentados em documentos separados ou em um mesmo documento dividido em diferentes capítulos, em suporte em papel e/ou eletrônico. Essa separação deve incluir minimamente os temas: instalação, operação e administração. |
| NGS1.09.12 | Idioma | Deve haver versão em Português do Brasil para todos os manuais do S-RES. |

**NGS1.10 – Tempo**

| ID | Título | Requisito |
|---|---|---|
| NGS1.10.03 | Fonte temporal | Todo registro de tempo do S-RES deverá ser baseado em uma fonte de referência temporal configurável, ou seja, utilizar a referência de tempo do servidor e não da estação do usuário. |

**NGS1.12 – Privacidade**

| ID | Título | Requisito |
|---|---|---|
| NGS1.12.01 | Concordância com termos de uso | a) O S-RES deve exibir imediatamente após o primeiro acesso do usuário no sistema, um termo de concordância sobre o uso apropriado das informações de saúde, alertando para o devido cuidado visando a confidencialidade dos dados e as consequências do uso inadequado dos mesmos.<br>b) O usuário só deve poder prosseguir após aceitar explicitamente as condições ali dispostas. |