



PROJETO SREI

Sistema de Registro Eletrônico Imobiliário

PA 1.9 - Análise dos processos de certificação de software existentes

Título	PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes
Versão	Versão 1.1 release 3
Data da liberação	15/12/2011
Classificação	LSI-TEC:Restrito
Autores	Gislaine Bueno e Volnys Bernal
Propriedade	LSI-TEC
Restrições de acesso	LSI-TEC

Sumário

1	INTRODUÇÃO	4
2	ALGUNS PROCESSOS DE CERTIFICAÇÃO DE SOFTWARE EXISTENTES	5
3	CERTIFICAÇÃO DE SISTEMA DE REGISTROS ELETRÔNICOS DE SAÚDE	6
3.1	MOTIVAÇÃO	6
3.2	OBJETIVO	6
3.3	ESCOPO	7
3.4	PRINCÍPIOS DO PROCESSO DE CERTIFICAÇÃO	8
3.5	CERTIFICAÇÃO	8
3.6	VALIDADE DO CERTIFICADO	9
3.7	INSTRUMENTOS FORMAIS	9
3.8	PREÇO DA CERTIFICAÇÃO	9
3.9	AMBIENTE DE AVALIAÇÃO	10
3.10	DURAÇÃO DA AUDITORIA DO S-RES	11
3.11	FLUXO DE CERTIFICAÇÃO S-RES	11
3.12	ESTRUTURA DO CENTRO DE CERTIFICAÇÃO.....	12
3.13	TIPOS DE REQUISITOS.....	13
3.14	REQUISITOS QUE REMETEM A OUTRAS CERTIFICAÇÕES.....	14
3.15	REQUISITOS DE CONFORMIDADE	14
3.16	REQUISITOS DE SEGURANÇA	14
3.17	REQUISITOS DE ESTRUTURA, CONTEÚDO E FUNCIONALIDADE PARA S-RES ASSISTENCIAL	16
3.18	REQUISITOS PARA GED.....	19
3.19	REQUISITOS PARA TISS	19
4	O PROCESSO DE HOMOLOGAÇÃO DE PRODUTOS DA ICP-BRASIL	21
4.1	OBJETIVO DO PROCESSO DE HOMOLOGAÇÃO	21
4.2	ORGANIZAÇÃO DA ICP-BRASIL.....	21
4.2.1	<i>Comitê Gestor.....</i>	23
4.2.2	<i>Instituto Nacional de Tecnologia da Informação</i>	23
4.2.3	<i>Laboratório de Ensaio e Auditoria</i>	23
4.3	NÍVEIS DE CONFIABILIDADE DA HOMOLOGAÇÃO	24
4.4	O PROCESSO DE HOMOLOGAÇÃO DA ICP-BRASIL.....	24
4.4.1	<i>Depósito dos ativos de ensaio.....</i>	26
4.4.2	<i>Análise quantitativa e qualitativa</i>	26
4.4.3	<i>Realização dos ensaios técnicos</i>	26
4.4.4	<i>Homologação do produto</i>	26

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	2 / 36

4.5	FLUXO DAS ATIVIDADES PARA HOMOLOGAÇÃO NO LEA.....	26
4.6	ESPECIFICAÇÃO DOS ENSAIOS.....	28
4.7	INFRAESTRUTURA DO LEA.....	31
4.7.1	Controles de segurança	31
4.7.2	Controles de qualidade.....	31
4.8	ESTIMATIVA DE PRAZO E CUSTO	31
5	ANÁLISE COMPARATIVA	33
6	CONCLUSÃO.....	35
	REFERÊNCIAS.....	36

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	3 / 36

1 Introdução

Este documento descreve o processo de certificação de software SREI (Sistema de Registro Eletrônico Imobiliário). São apresentados dois processos de certificação existentes atualmente no Brasil: a certificação de Sistema de Registro Eletrônico de Saúde (S-RES) e o processo de homologação de produtos da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Também, é apresentada uma análise comparativa dos modelos existentes, visando demonstrar as características inerentes a cada modelo e ainda evidenciar a diferença entre eles. E concluindo, é enfatizado como o estudo de processos existentes pode auxiliar na definição do Processo de Certificação do Sistema de Registro Eletrônico Imobiliário.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	4 / 36

2 Alguns processos de certificação de *software* existentes

Atualmente, existem processos de certificação de *software* em alguns segmentos de mercado. O objetivo principal desses processos é avaliar os sistemas em relação às suas funcionalidades, interoperabilidade, segurança e documentação.

No âmbito nacional, destacam-se dois processos: o processo de certificação de Sistemas de Registros Eletrônicos de Saúde (S-RES), desenvolvido e controlado pelo convênio Sociedade Brasileira de Informática em Saúde (SBIS) / Conselho Federal de Medicina (CFM), e o processo de homologação de produtos no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), definido pela ICP-Brasil, controlado pelo Instituto Nacional de Tecnologia de Informação (ITI) e executado pelo Laboratório de Ensaios e Auditoria (LEA). As seções 3 e 4 apresentam detalhadamente as especificações de ambos os processos.

Além dos processos de certificação de sistema de *software* relacionados anteriormente, pode-se citar outros em segmentos próximos, como o processo de avaliação de qualidade de *software* como o MPS.Br (Melhoria Processos de *Software* Brasileiro) e *Capability Maturity Model Integration* (CMMI).

O CMMI é um modelo de referência que contém práticas necessárias à maturidade em disciplinas específicas: *Systems Engineering* (SE), *Software Engineering* (SW), *Integrated Product and Process Development* (IPPD), *Supplier Sourcing* (SS). Desenvolvido pelo SEI (*Software Engineering Institute*) da Universidade Carnegie Mellon, o CMMI é uma evolução do CMM e procura estabelecer um modelo único para o processo de melhoria corporativo, integrando diferentes modelos e disciplinas.

O MPS.Br, baseado no CMMI SW, é um programa para melhoria da qualidade de *software* e um modelo de qualidade de processos, voltados a pequenas e médias empresas desenvolvedoras de *software*.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de <i>software</i> existentes	v1.1.r.3	LSITEC:Restrito	5 / 36

3 Certificação de Sistema de Registros Eletrônicos de Saúde

O Conselho Federal de Medicina (CFM) e a Sociedade Brasileira de Informática em Saúde (SBIS) formaram um convênio de cooperação técnica visando desenvolver o processo de certificação de Sistemas de Registros Eletrônicos de Saúde (S-RES).

O processo de certificação é baseado em requisitos que avaliam os sistemas em relação à segurança, estrutura, conteúdo e funcionalidade. As avaliações verificam como são capturados, armazenados, manuseados e transmitidos os dados do paciente gerados nos atendimentos em saúde.

Outro desafio do processo de certificação é avaliar a aderência do sistema em relação ao formato eletrônico de documento que, caso utilize assinatura digital, possibilita a eliminação do papel.

O primeiro produto elaborado pela parceria SBIS/CFM foi a resolução n.º 1639/2002 que contemplava "*Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico*". Em 2007, uma nova resolução foi aprovada, vindo substituir a anterior. A resolução 1821/2007 aprovou "*Normas Técnicas Concernentes à Digitalização e Uso dos Sistemas Informatizados para Guarda e Manuseio dos Documentos dos Prontuários dos Pacientes Autorizando a Eliminação do Papel e Troca de Informação Identificada em Saúde*".

3.1 Motivação

O processo de certificação para S-RES teve como motivadores principais a necessidade de eliminação do prontuário em papel e a necessidade de padronização desta classe de sistemas, de forma a garantir sua interoperabilidade e seu correto funcionamento.

3.2 Objetivo

O objetivo principal do processo de certificação desenvolvido pela SBIS/CFM é a melhoria da qualidade dos Sistemas de Registro Eletrônico em Saúde pela contribuição da privacidade e confidencialidade dos dados (ao estabelecer requisitos de segurança) e a aderência ao uso correto da tecnologia de assinatura digital.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	6 / 36

3.3 Escopo

O escopo do processo de certificação abrange todos os subsistemas e componentes do sistema de registro eletrônico em saúde. A empresa solicitante da certificação deve identificar o sistema e descrever todos os componentes, assim como a infraestrutura necessária para o funcionamento do sistema.

Segundo o Manual de Certificação, além da própria aplicação incluem-se outros subsistemas e componentes avaliados como: sistema operacional, SGBD (Banco de Dados), conectores, arquitetura do S-RES (cliente/servidor, ASP, Mainframe), componente do tipo Web dinâmico (Applet, Active X) e sistemas de diretório (AD e LDAP).

A certificação abrange, atualmente, as seguintes categorias de S-RES:

- **Assistencial:** Voltados para registro de atendimentos em saúde, tais como: sistemas de automação de consultórios clínicos, sistemas de informação hospitalar e ambulatorial, sistemas de vigilância epidemiológica, etc.;
- **Sistema de gerenciamento eletrônico de documentos (GED):** Utilizados para o armazenamento e visualização de documentos relacionados à informação de saúde;
- **Troca de Informação em Saúde Suplementar (TISS):** Dirigida ao atendimento do padrão TISS da ANS, de forma que o TISS é responsável pelo registro e intercâmbio de dados entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde.

A certificação pode ser aderente a um dos seguintes Níveis de Garantia de Segurança:

- **Nível de Garantia de Segurança 1 (NGS1):** Utiliza documentação eletrônica, porém não utiliza assinatura digital. O S-RES deve obrigatoriamente manter também cópias em papel;
- **Nível de Garantia de Segurança 2 (NGS2):** Utiliza assinatura digital sendo, neste caso, permitida a eliminação do papel.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	7 / 36

Para ser aprovada a certificação, o S-RES deve atender todos os requisitos obrigatórios estabelecidos para a categoria em que está enquadrado e também estar aderente, no mínimo, aos requisitos de segurança obrigatórios do NGS1.

O processo de certificação para S-RES está em amadurecimento. Aproximadamente, a cada ano é lançada uma nova versão do manual. Além disso, para atender as demandas do mercado de *software* na área de saúde, voltados a outros tipos de atendimentos assistenciais como sistemas de informação hospitalar, vigilância epidemiológica, medicina ocupacional, e SADT, novos requisitos e alterações são estudados para que isso ocorra de forma gradual.

3.4 Princípios do processo de certificação

O processo de certificação de Sistemas de Registros Eletrônicos em Saúde é realizado considerando requisitos essenciais de imparcialidade, competência, transparência, responsabilidade e confidencialidade.

3.5 Certificação

O certificado emitido refere-se a uma configuração específica de S-RES avaliada no processo de auditoria juntamente com os subsistemas e componentes e em completa aderência aos requisitos obrigatórios estabelecidos.

O processo de certificação SBIS/CFM considera como uma nova versão quando o S-RES sofre ajustes em relação a versões anteriores. Esses ajustes podem ser classificados como "pequenos ajustes" ¹ ou "ajustes relevantes" ²

A declaração da manutenção da conformidade pode ser declarada pelo cliente, a qual, perante afirmação, não necessita de abertura de processo para a análise de extensão de certificação.

¹ Segundo o Manual de Certificação SBIS/CFM, pequenos ajustes são "*as modificações e atualizações que não afetam a conformidade do S-RES aos requisitos da certificação;*"

² Já como ajustes relevantes entende-se "*as modificações que impliquem em risco significativo de afetar a conformidade do S-RES aos requisitos da certificação*".

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	8 / 36

No caso do processo de extensão de certificação vários fatores devem ser analisados, dentre eles os ajustes realizados e qual a versão do Manual de Certificação utilizada para ocasião da emissão do certificado e a atual.

3.6 Validade do Certificado

A certificação S-RES emitida pela SBIS/CFM tem validade de dois anos. No entanto, no caso de lançamento de uma nova versão do Manual de Certificação de Sistemas de Registro Eletrônico de Saúde a validade do certificado será de um ano após a publicação do certificado.

3.7 Instrumentos formais

O processo de certificação utiliza os seguintes documentos para formalizar as ações tomadas:

- Ficha de inscrição para a certificação;
- Ficha de inscrição para extensão da certificação;
- Contrato de Certificação;
- Termo de Extensão de Certificação;
- Certificado (Diploma de Certificação);
- Selo de Certificação SBIS/CFM.

3.8 Preço da certificação

O preço para a realização de um processo de certificação SBIS/CFM contempla as taxas listadas no Quadro 1 seguir: (fonte: www.sbis.org.br – 09/03/2011).

Quadro 1 – Preço do processo de certificação S-RES SBIS/CFM.

Descrição	Valor
Taxa de Inscrição	R\$ 100,00

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	9 / 36

Taxa de Certificação	Considerar o Quadro 2
Taxa de Extensão de Certificação (pequenos ajustes)	3% da taxa de certificação
Taxa de Extensão de Certificação (ajustes relevantes)	20% a 80% da taxa de certificação
Taxa de Realização de 2º Ciclo de Auditoria	20% a 50% da taxa de certificação
Taxa de Reagendamento de Auditoria	10% da taxa de certificação

Quadro 2 – Taxa de certificação.

Descrição	Valor
Valor base (valor inicial para o cálculo)	R\$ 3.600,00
NGS2	+ R\$ 7.200,00
S-RES Assistencial (Ambulatorial)	+ R\$ 7.200,00
TISS sem comunicação	+ R\$ 1.800,00
TISS com comunicação	+ R\$ 3.600,00

As taxas são baseadas no enquadramento o qual o S-RES está inserido. Exemplos:

- Valor base + S-RES Assistencial (Ambulatorial) + NGS1 = R\$ 14.400,00
- Valor base + S-RES Assistencial (Ambulatorial) + NGS2 = R\$ 18.000,00

3.9 Ambiente de avaliação

O processo de certificação exige que o solicitante disponibilize o S-RES através de um dos meios descritos no Manual de Certificação, por exemplo:

- Instalação do sistema no equipamento disponibilizado pela SBIS ou pelo próprio solicitante (ambiente montado localmente);
- Acesso direto ou indireto via *Internet*, ou outro meio previamente acordado entre as duas partes.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	10 / 36

Cabe ao solicitante, disponibilizar de um a três profissionais para operar o sistema durante período de auditoria.

Somente o áudio da auditoria é gravado, registrando todos os sons do ambiente e as imagens da tela (navegação e operação) do S-RES auditado.

3.10 Duração da Auditoria do S-RES

O processo de auditoria do S-RES, geralmente, é realizado em um período de 3 dias, totalizando aproximadamente 24 horas. A auditoria é acompanhada por três auditores seniores e pelo gerente de certificação. Esta ainda pode ser acompanhada por auditores *trainees*, porém suas avaliações servem apenas para aprendizado e não são consideradas no momento da elaboração do parecer.

O período estipulado para a auditoria pode variar, dependendo da(s) categoria(s) em que o S-RES estiver classificado.

Caso o S-RES não atenda completamente os requisitos das categorias que foi previamente enquadrado, o solicitante tem um prazo de 90 dias para efetivar as correções propostas e realizar o segundo ciclo de auditoria.

3.11 Fluxo de certificação S-RES

O processo de certificação contempla que a auditoria seja realizada por uma equipe especializada que verifica a aderência do S-RES a todos os requisitos obrigatórios, na categoria na qual está enquadrado.

Existem dois fluxos possíveis no processo de certificação: processo padrão e processo para extensão da certificação.

O Manual Operacional de Ensaio e Análises do S-RES é utilizado para orientar o processo de auditoria. As etapas do processo padrão de certificação estão apresentadas na Figura 1 (fonte: Manual de Certificação de S-RES):

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	11 / 36

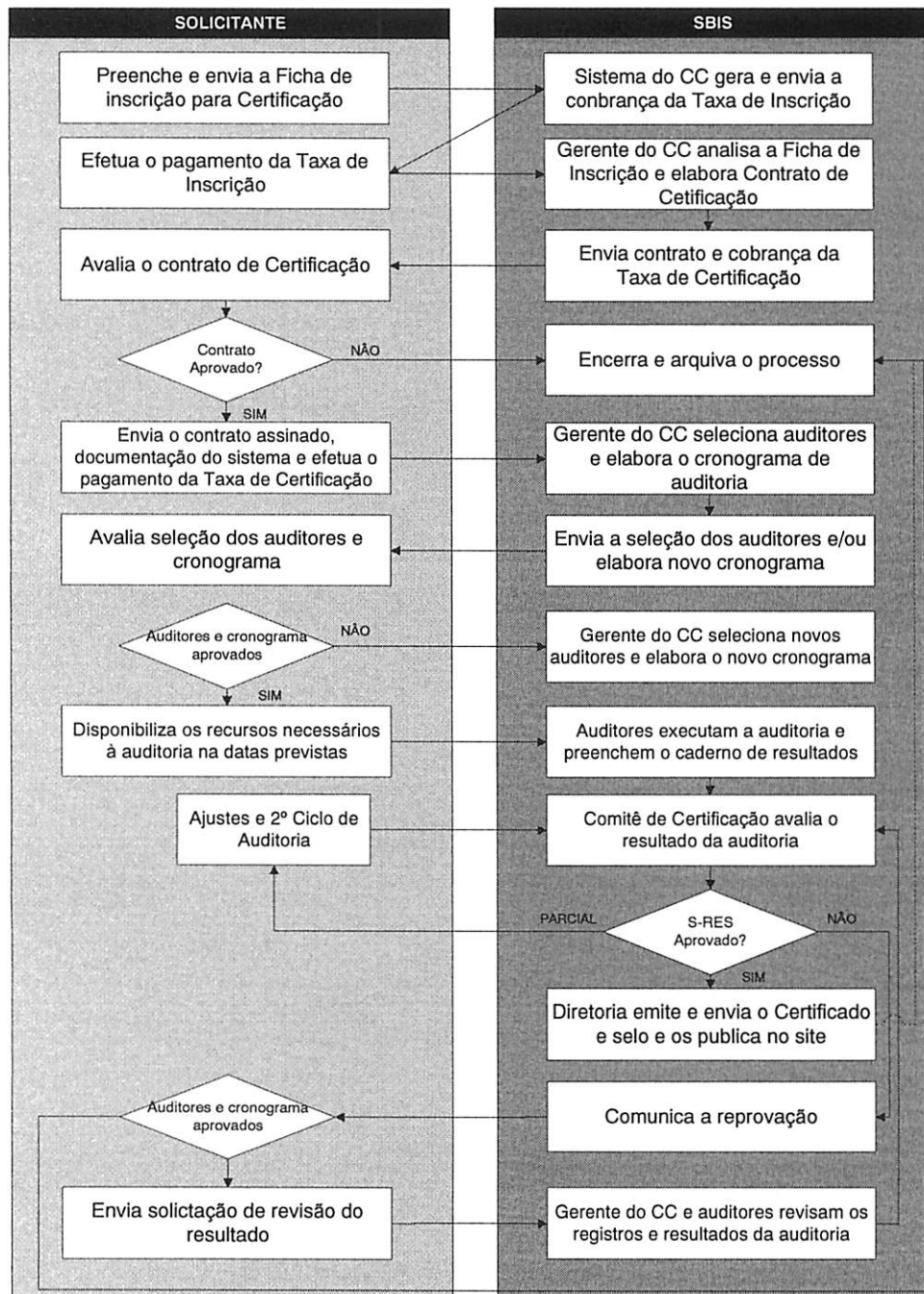


Figura 1 – Etapas do processo de certificação S-RES.

3.12 Estrutura do Centro de Certificação

O departamento responsável para operacionalizar o processo de certificação é denominado Centro de Certificação. É composto por colaboradores de dedicação não-exclusiva, porém subordinado à Diretoria da SBIS.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	12 / 36

Os papéis e responsabilidades desempenhados pelos participantes do Centro de Certificação são:

- **Comitê de Certificação:** analisa os atos durante o processo de auditoria, garantindo fundamentalmente o cumprimento do princípio da imparcialidade e assegura a transparência e a imagem pública do processo de certificação, além de avaliar os atos tomados pelo gerente de certificação;
- **Gerente de certificação:** gerencia todo o processo de certificação analisando as solicitações, elaborando contratos, contatando os auditores e interação com a Diretoria da SBIS nas questões relativas à certificação;
- **Auditores:** realiza auditorias e documenta os resultados conforme regras estabelecidas pela SBIS. Também assegura a imparcialidade e o sigilo sobre as auditorias realizadas;
- **Secretaria:** responsável pelos aspectos administrativos do Centro de Certificação, auxiliando principalmente o Gerente de Certificação;
- **Diretoria SBIS:** garante e supervisiona implementações de políticas e infraestrutura a fim de suportar todo o processo de certificação.

3.13 Tipos de requisitos

Os requisitos presentes no Manual de Certificação para S-RES SBIS/CFM são classificados em três tipos: mandatórios, recomendados ou opcionais. A classificação do requisito refere-se como o S-RES deve atendê-lo:

- **Mandatório:** o S-RES obrigatoriamente deve estar em conformidade com todos os requisitos que possuem essa classificação;
- **Recomendado:** os requisitos que possuem essa classificação tendem a se tornar mandatório nas próximas versões do Manual de Certificação. Esses requisitos são baseados em padrões de referência onde já são aceitos, porém serão implementados de forma gradual, possibilitando ao mercado desenvolvedor a preparação necessária para atendê-los.
- **Opcional:** esses requisitos tratam de questões relevantes, porém da mesma forma que os requisitos recomendados para a implementação será realizada de forma gradual a fim de preparar o mercado de S-RES.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	13 / 36

3.14 Requisitos que remetem a outras certificações

Existem requisitos que remetem a outros processos de certificação. É o caso dos requisitos relacionados à biblioteca criptográfica utilizada na assinatura digital. Atualmente existe um requisito que recomenda que esta biblioteca seja homologada pela ICP-Brasil. Provavelmente na próxima versão do manual de certificação, será obrigatório o uso de bibliotecas homologadas.

3.15 Requisitos de Conformidade

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

- Requisitos de Estrutura, Conteúdo e Funcionalidade (ECF);
- Requisitos TISS (Troca de Informações de Saúde Suplementar);
- Requisitos GED (Gerenciamento Eletrônico de Documentos);
- Requisitos de segurança:
 - Requisitos de segurança NGS1;
 - Requisitos de segurança NGS2.

A avaliação da aderência de um requisito leva em consideração a denominação apresentada no Manual da Certificação de S-RES: M - mandatório R- recomendado, O – opcional e X – Não se aplica.

Os sistemas também são classificados quanto ao tipo de acesso: de acesso local (L) ou de acesso remoto (R)

3.16 Requisitos de Segurança

Um dos objetivos principais do CFM ao estabelecer a parceria do processo de certificação foi o de garantir o sigilo das informações do paciente, ou seja, garantir o sigilo do profissional permitindo que o acesso aos dados do paciente possa ser realizado apenas por pessoas autorizadas.

O processo de certificação classifica o S-RES em dois níveis de segurança:

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	14 / 36

- Nível de Garantia de Segurança 1 (NGS1): não contempla o uso de certificados digitais ICP-Brasil para assinatura de informações clínicas, impossibilitando a eliminação do papel.
- Nível de Garantia de Segurança 2 (NGS2): O NGS2 através da assinatura digital utilizando certificados ICP-Brasil, possibilita a eliminação do papel. No entanto, é necessário que o S-RES também esteja em conformidade com todos os requisitos do NGS1, estrutura, conteúdo e funcionalidade (ECF).

O S-RES também pode ser classificado como:

- Acesso Local: o S-RES e seus componentes são instalados em uma única máquina, não permitindo acesso a mais de um usuário;
- Acesso Remoto: o S-RES e seus componentes são instalados de forma distribuída permitindo o acesso simultâneo de vários usuários.

No Quadro 3 e no Quadro 4 é possível visualizar os grupos de requisitos de segurança que devem ser aplicados ao S-RES.

Quadro 3 – Requisitos NGS1: Quantidade de requisitos em cada grupo.

Grupo de requisitos	*Totais (53)
NGS1.01 - Controle de versão do software	5
NGS1.02 - Identificação e autenticação de usuário	5
NGS1.03 - Controle de sessão de usuário	2
NGS1.04 – Autorização e controle de acesso	9

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	15 / 36

NGS1.05 - Disponibilidade do RES	2
NGS1.06 - Comunicação remota	6
NGS1.07 - Segurança de Dados	8
NGS1.08 – Auditoria	4
NGS1.09 – Documentação	8
NGS1.10 – Tempo	3
NGS1.11 – Notificação de Ocorrências	1

Quadro 4 – Requisitos NGS2: Quantidade de requisitos em cada grupo

Grupo de requisitos	*Totais (25)
NGS2.01 – Certificação Digital	4
NGS2.02 – Assinatura Digital	10
NGS2.03 – Autenticação de usuário utilizando certificado digital	4
NGS2.04 – Digitalização de Documentos (Aplicável somente para S-RES da categoria GED)	7

* Considerando todos os requisitos: mandatórios, recomendados e opcionais.

3.17 Requisitos de Estrutura, Conteúdo e Funcionalidade para S-RES Assistencial

Os requisitos utilizados para avaliação da estrutura, conteúdo e funcionalidade (ECF) são utilizados para avaliar S-RES voltados à assistência ambulatorial, como por exemplos, sistemas de automação de consultórios clínicos ou ainda como parte ambulatorial de sistemas hospitalares.

Os requisitos para estrutura e conteúdo visam avaliar como o S-RES realiza a manipulação e tratamento dos dados e assegurar que a estrutura do sistema esteja aderente ao conjunto de especificações estabelecidas pela resolução 1638/2002.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	16 / 36

Em relação às funcionalidades do S-RES, através dos requisitos descritos no Manual de Certificação, é possível avaliar se o S-RES contempla de forma correta as operações básicas realizadas no sistema de saúde.

No Quadro 5 é possível visualizar os grupos de requisitos de estrutura e conteúdo e no Quadro 6 os grupos referentes à funcionalidade.

Quadro 5 – Requisitos de estrutura e conteúdo: quantidade de requisitos em cada grupo.

Grupo de requisitos	*Totais (53)
ESTR.01 - Estrutura do RES	5
ESTR.02 - Dados estruturados	9
ESTR.03 - Dados administrativos	6
ESTR.04 - Dados clínicos	3
ESTR.05 - Tipos de dados	12
ESTR.06 - Dados de referência	1
ESTR.07 - Dados contextuais	8
ESTR.08 - Associações	2
ESTR.09 - Representação de conceitos em saúde	6
ESTR.10 - Representação de texto	1

Quadro 6 – Requisitos de Funcionalidade: quantidades de requisitos em cada grupo.

Grupo de requisitos	*Totais (61)
FUNC.01 - Suporte aos processos clínicos	4
FUNC.02 - Problemas / condições de saúde e outras questões	3
FUNC.03 – Raciocínio clínico	1
FUNC.04 - Suporte à decisão, protocolos clínicos e alertas.	5

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	17 / 36

FUNC.05 - Planejamento Terapêutico	1
FUNC.06 - Prescrição e processamento de exames	2
FUNC.07 - Assistência integral	1
FUNC.08 - Garantia de qualidade	1
FUNC.09 - Captura de dados	3
FUNC.10 - Recuperação/ consultas e visões	1
FUNC.11 - Apresentação dos dados	3
FUNC.12 - Escalabilidade e performance	1
FUNC.13 - Protocolos de mensagens	1
FUNC.14 - Troca de registros	3
FUNC.16 - Consentimento	4
FUNC.17 - Médico-legal	2
FUNC.18 – Atores	10
FUNC.19 - Competência e governança clínica	1
FUNC.20 – Fé pública	2
FUNC.21 - Preservação de contexto	2
FUNC.22 - Permanência	1
FUNC.23 - Controle de versão	2
FUNC.24 – Ética	1
FUNC.25 - Direitos do paciente	3
FUNC.26 - Questões culturais	1
FUNC.27 – Evolução	2

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	18 / 36

* Considerando todos os requisitos: mandatórios, recomendados e opcionais.

3.18 Requisitos para GED

Os requisitos voltados ao gerenciamento eletrônico de documentos são utilizados para avaliar o armazenamento e visualização de documentos relacionados à informação de saúde, os quais devem avaliar se o S-RES atende a resolução CFM Nº 1821/2007.

Além dos requisitos específicos para GED o S-RES deve apresentar conformidade total aos requisitos NGS1 e NGS2.

Quadro 7 – Requisitos GED: quantidade de requisitos em cada grupo.

Grupo de requisitos	*Totais (6)
SGED.01 - Gerais	6

* Considerando todos os requisitos: mandatórios, recomendados e opcionais

3.19 Requisitos para TISS

Os requisitos voltados para TISS (Quadro 8) visam avaliar os S-RES em relação à conformidade das trocas de informações de operadoras de planos de saúde e prestadores de serviços de saúde.

Os requisitos TISS devem ser atendidos respeitando grupo no qual está enquadrado o S-RES (conforme mencionado na página 51 do Manual de Certificação de S-RES).

Quadro 8 – Requisitos TISS: quantidade de requisitos em cada grupo.

Grupo de requisitos	*Totais (66)
TISS.01 – Conteúdo e Estrutura para Prestadores do Grupo 1	6
TISS.02 – Conteúdo e Estrutura para Prestadores do Grupo 2	3
TISS.03 – Conteúdo e Estrutura para Prestadores do Grupo 3	2
TISS.04 – Conteúdo e Estrutura para Operadoras de Planos de Assistência Médica (Grupos 1 e 2)	2
TISS.05 – Conteúdo e Estrutura para Operadoras exclusivamente de Planos Odontológicos (Grupo 3)	1

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	19 / 36

TISS.06 – Comunicação para Prestadores dos Grupos 1 e 2	13
TISS.07 – Comunicação para Prestadores do Grupo 3	13
TISS.08 – Comunicação para Operadoras de Planos de Assistência Médica (Grupos 1 e 2)	13
TISS.09 – Comunicação para Operadoras exclusivamente de Planos Odontológicos (Grupo 3)	13

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	20 / 36

4 O processo de homologação de produtos da ICP-Brasil

4.1 Objetivo do processo de homologação

O objetivo do processo de homologação de produtos no âmbito da ICP-Brasil é garantir a aderência a requisitos de segurança, interoperabilidade e documentação de produtos que utilizem certificado digital.

Atualmente, o escopo de homologação abrange os seguintes tipos de produtos:

- Cartões criptográficos (*smart cards*);
- *Tokens* criptográficos;
- Leitora de cartões criptográficos;
- *Software* de assinatura digital;
- *Software* de autenticação;
- *Software* de sigilo;
- *Software* de autoridades certificadoras e de registro;
- Equipamentos de HSM (Hardware Security Module)³;
- Bibliotecas criptográficas;
- CSP's (Provedores de Serviços Criptográficos);
- *Software* de carimbo de tempo.

4.2 Organização da ICP-Brasil

No Brasil o sistema de certificação digital foi implantado com a publicação da Medida Provisória 2.200, em junho de 2001. A MP 2.200 instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) com o objetivo de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras, conforme seu artigo 1º.

³ HSM é um equipamento criptográfico capaz de armazenar chaves de *assinatura digital* de maneira segura.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	21 / 36

A infraestrutura normativa e técnico-administrativa é formada pelas seguintes entidades (Figura 2):

- Comitê Gestor da ICP-Brasil (CG);
- Comissão Técnica Executiva (COTEC);
- Instituto Nacional de Tecnologia da Informação (ITI);
- Prestadores de serviço de certificação:
 - Autoridade Certificadora (ACs);
 - Autoridade de Registro (ARs);
 - Laboratório de Ensaio e Auditoria (LEA);
 - Outros prestadores de serviço.

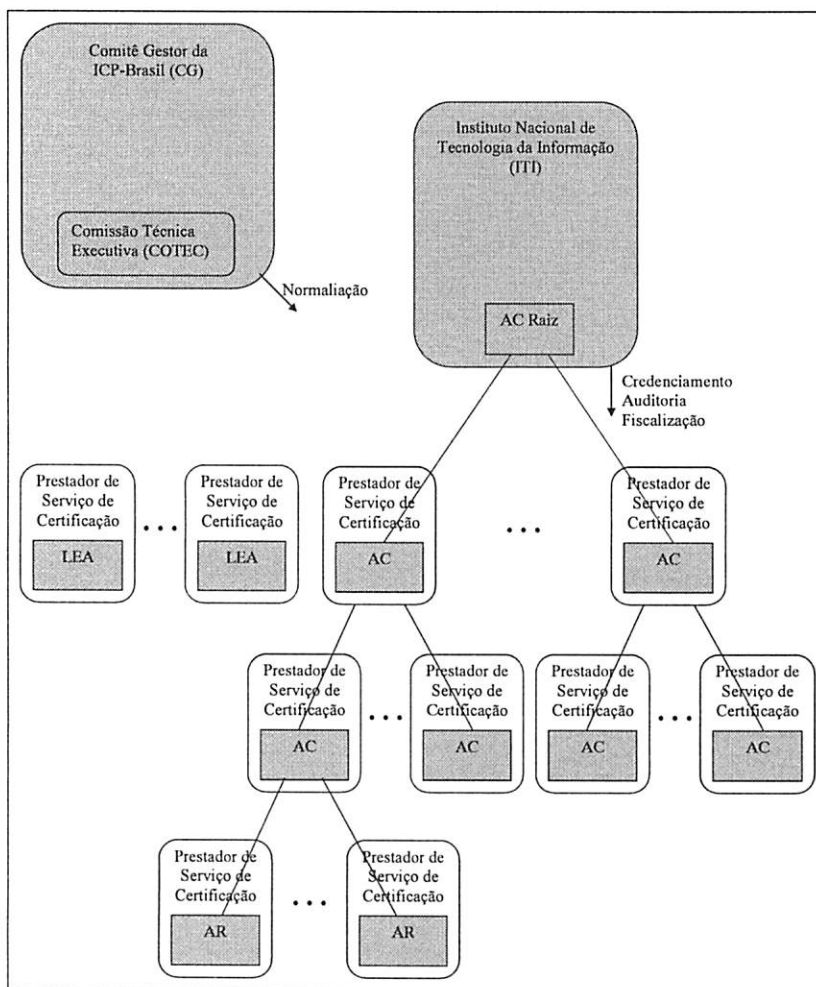


Figura 2 – Estrutura da ICP-Brasil.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	22 / 36

4.2.1 Comitê Gestor

O Comitê Gestor da ICP-Brasil, conforme o disposto na MP 2.200-2, é responsável pela regulamentação e coordenação da sua implantação e da sua operação. As regulamentações, realizadas através das resoluções da ICP-Brasil, tratam, por exemplo: do estabelecimento dos critérios e das normas para o credenciamento das entidades que integram a cadeia de certificação; das diretrizes e normas técnicas para a formulação de políticas de certificados; regras operacionais das Autoridades Certificadoras (ACs) e das Autoridades de Registro (ARs); e regras de outros prestadores de serviço de certificação, como prestadores de serviço de carimbo de tempo e de Laboratório de Ensaios e Auditoria (LEA). O Comitê Gestor da ICP-Brasil é composto por doze integrantes, não remunerados, sendo sete representantes de órgãos governamentais e outros cinco representantes da sociedade civil.

4.2.1.1 Comissão Técnica Executiva

A Comissão Técnica Executiva (COTEC) assiste e dá suporte técnico ao CG – órgão deliberativo. Os integrantes da COTEC são indicados individualmente pelos membros do CG.

4.2.2 Instituto Nacional de Tecnologia da Informação

Instituto Nacional de Tecnologia da Informação (ITI) é a entidade designada como executora de algumas atividades da ICP-Brasil, como, por exemplo, a operação da AC Raiz da ICP-Brasil. O art. 1º, I, do Decreto Nº 4.689, de 07 de maio de 2003, atribui competência ao Instituto Nacional de Tecnologia da Informação (ITI) para executar as políticas de certificação e as normas técnicas e operacionais aprovadas pelo CG.

4.2.3 Laboratório de Ensaio e Auditoria

A ICP-Brasil possui um processo de homologação de sistemas e equipamentos de certificação. A homologação é realizada pelos Laboratórios de Ensaio e Auditoria (LEA). A homologação de produto (sistema ou dispositivo), por sua vez, consiste em verificar a aderência a um conjunto de requisitos de segurança e de interoperabilidade definidos para cada classe de equipamentos.

Até maio de 2010 o serviço de homologação era subsidiado pelo governo. Em maio de 2010 o sistema de homologação da ICP-Brasil recebeu novas regras do Comitê

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	23 / 36

Gestor da ICP-Brasil. As principais mudanças foram: a obrigatoriedade da homologação dos produtos e sistemas utilizados no âmbito da ICP e a assunção dos custos do processo por parte dos interessados, que até então era mantido pelo ITI de forma gratuita.

Até maio de 2010 existia somente um Laboratório de Ensaios e Auditoria credenciado pela ICP-Brasil, o LEA LSI-TEC, que operava através de convênio com o ITI. A partir desta data, os LEAs passaram a ser credenciados. Assim, outros LEAs podem ser credenciados, desde que atendam às especificações editadas pelo Comitê Gestor.

Os LEAs passam, também, por auditorias periódicas, a exemplo do que ocorre com as Autoridade Certificadoras, as de Carimbo de Tempo e as de Registro.

4.3 Níveis de confiabilidade da homologação

A homologação pode ser realizada em 3 níveis de segurança:

- **Nível de Segurança de Homologação 1 (NSH1):** não requer o depósito ou análise do código fonte associado ao produto em homologação;
- **Nível de Segurança de Homologação 2 (NSH2):** requer depósito e análise apenas do código fonte de componentes específicos associados ao produto em homologação;
- **Nível de Segurança de Homologação 3 (NSH3):** requer depósito e análise de código fonte completo associado ao produto em homologação.

4.4 O processo de homologação da ICP-Brasil

A homologação de produtos no âmbito da ICP-Brasil é realizada por um Laboratório de Ensaios e Auditoria (LEA) credenciado.

O fornecedor, fabricante ou representante do produto, denominado Parte Interessada (PI), contrata o serviço de avaliação de conformidade junto a um LEA credenciado pela ICP-Brasil. O preço é negociado livremente entre fornecedor e LEA, que realiza a avaliação da conformidade do produto em relação aos requisitos técnicos estabelecidos utilizando os procedimentos de testes definidos. Ao final, o LEA emite um Laudo de Conformidade com o resultado da avaliação de

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	24 / 36

conformidade. A Parte Interessada encaminha o Laudo de Conformidade ao ITI que, subsidiado pelos resultados apresentados, pode homologar o produto e autorizar o uso do selo ICP-Brasil.

As homologações realizadas pelo LEA estão baseadas nos requisitos e seus respectivos ensaios descritos nos Manuais de Conduta Técnicas (MCTs). Para cada objeto de homologação há dois MCTs:

- O Volume I que apresenta o conjunto de requisitos técnicos que os produtos devem atender, envolvendo requisitos de segurança, requisitos funcionais, requisitos de interoperabilidade e requisitos de documentação;
- O Volume II que descreve o conjunto de procedimentos que devem ser executados para a avaliação de conformidade de cada requisito técnico.

O conjunto de MCTs existentes atualmente foi elaborado pelo LEA LSI-TEC, por solicitação do ITI (Instituto de Tecnologia da Informação) e estão publicados no site do ITI (www.iti.gov.br).

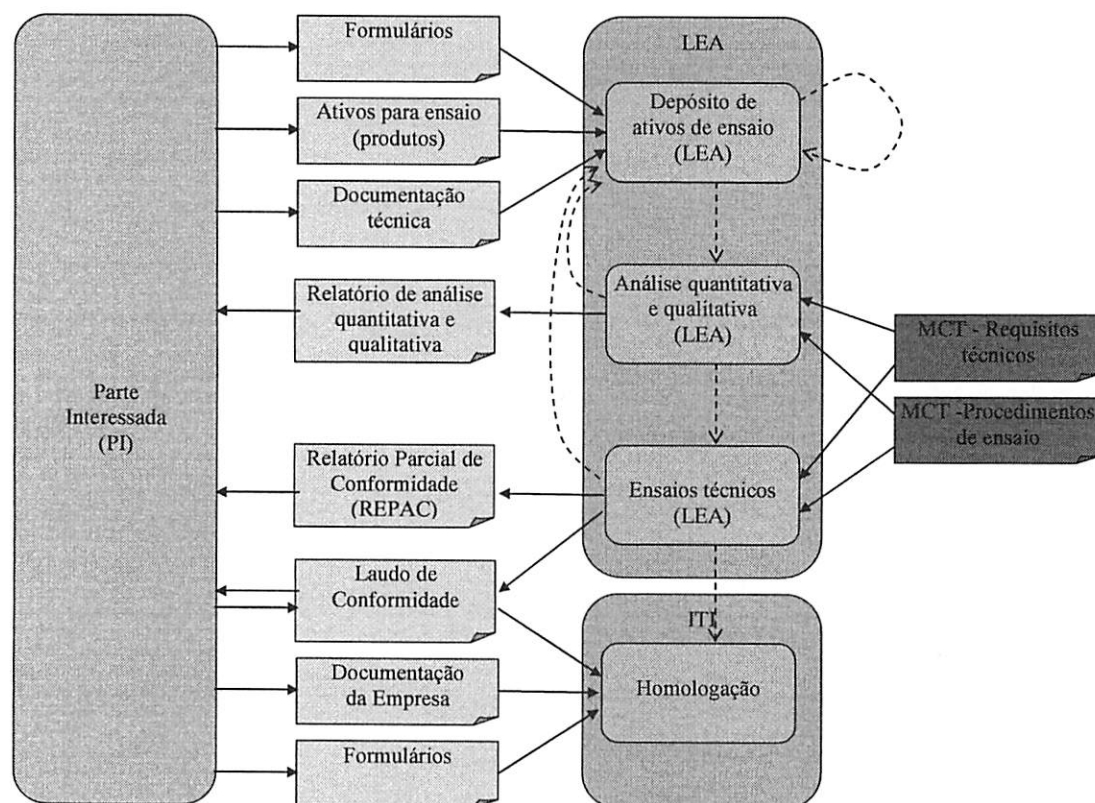


Figura 3 – Etapas do processo de homologação da ICP-Brasil.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	25 / 36

4.4.1 Depósito dos ativos de ensaio

A Parte Interessada (PI) deve depositar no LEA os ativos de ensaio, ou seja, um conjunto de amostras dos produtos a serem homologados, junto com sua documentação técnica (como, por exemplo, documentação do projeto e manuais).

4.4.2 Análise quantitativa e qualitativa

Após o depósito, os ativos de ensaio passam por análises quantitativas e qualitativas, gerando relatórios que informam se os materiais depositados pela PI são suficientes e adequados para dar início aos ensaios de conformidade. Novos depósitos de materiais podem ser necessários sempre que um relatório apontar que os materiais depositados pela PI não foram suficientes ou adequados para dar condições de realizar os ensaios de conformidade. Os depósitos de materiais pela PI podem ser feitos pessoalmente, via email, ou então via SEDEX.

4.4.3 Realização dos ensaios técnicos

Uma vez que os materiais depositados são considerados suficientes e adequados, os ensaios são realizados para avaliar a conformidade do objeto de homologação. Caso seja identificado algum requisito que não esteja em conformidade ou não seja atendido pelo objeto de homologação durante o processo de avaliação de conformidade, um REPAC (Relatório Parcial de Conformidade) é gerado para informar a PI sobre a não conformidade encontrada. Se nenhum problema for apontado, a avaliação de conformidade transcorre normalmente até sua conclusão.

Como resultado da avaliação de conformidade, o LSITEC LEA emite à PI um Laudo de Conformidade.

4.4.4 Homologação do produto

A PI encaminha o Laudo de Conformidade ao ITI que, subsidiado pelas informações do Laudo, tem condições de realizar o deferimento ou indeferimento da homologação ICP-Brasil.

4.5 Fluxo das atividades para homologação no LEA

O resumo do fluxo de atividades de avaliação de conformidade realizado nas dependências do LEA segue as seguintes etapas:

- Definição do escopo: Identificação do objeto da avaliação de conformidade;

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	26 / 36

- Avaliação de capacidade de fornecimento do serviço ao cliente: avalia a carga de trabalho atual e as necessidades de prazo do cliente;
- Elaboração da proposta comercial;
- Assinatura do NDA (quando for o primeiro projeto do cliente);
- Estabelecimento do contrato;
- O LEA informa a lista de materiais e documentações necessárias para depósito junto ao LEA;
- Depósito dos ativos de ensaio (materiais): O cliente encaminha amostras e documentação sobre o produto ao LEA para a realização dos ensaios;
- Análise qualitativa dos ativos de ensaio: verificação se os ativos depositados são suficientes para a realização dos ensaios. Se houver falta de materiais, é requisitado ao cliente o depósito dos materiais faltantes;
- Realização dos ensaios segundo o respectivo MCT;
- Elaboração dos relatórios de ensaio;
- Elaboração do Laudo de Conformidade, contendo um resumo dos resultados dos testes realizados;
- Encaminhamento ao cliente, por e-mail, do relatório assinado digitalmente;
- Publicação do documento de declaração de identificação do objeto homologado no site do LEA.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	27 / 36

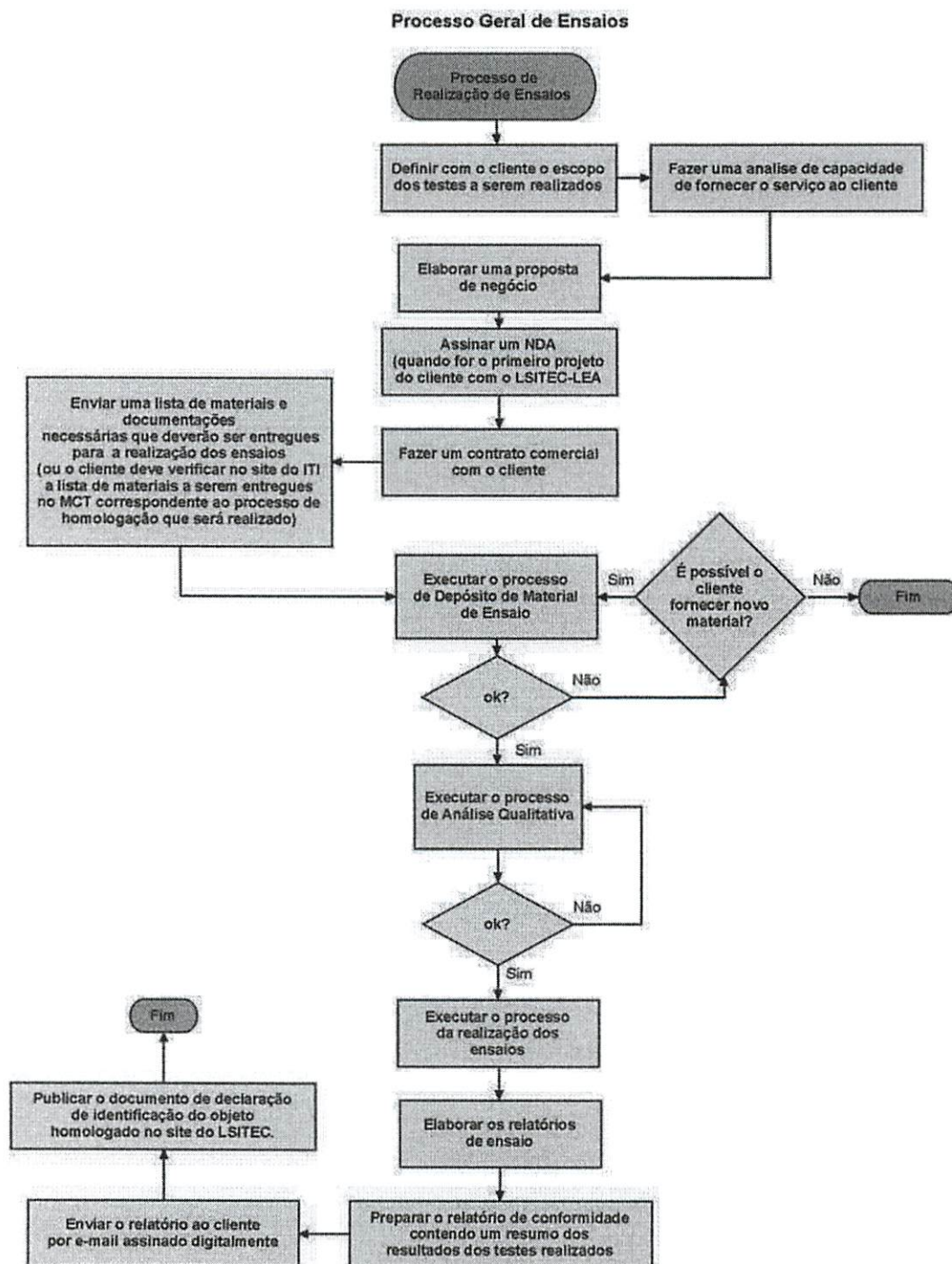


Figura 4 – Resumo do fluxo das atividades de avaliação de conformidade no LEA.

4.6 Especificação dos ensaios

O processo de especificação dos ensaios, incluídos no Manual de Condutas Técnicas (MCT), segue as etapas:

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	28 / 36

- Atribuir os requisitos necessários para a elaboração dos ensaios aos analistas de ensaio;
- Elaborar e descrever as etapas a serem cumpridas para cada um dos ensaios no documento específico de Procedimentos de Ensaios;
- Desenvolver, testar e validar as ferramentas (softwares) a serem aplicadas na realização dos ensaios baseado nos processos do Sistema de Gestão da Qualidade do LSITEC-LEA;
- Validar os métodos de ensaio baseado nos processos do Sistema de Gestão da Qualidade do LSITEC-LEA;
- Fazer a revisão técnica e gramatical dos procedimentos de ensaio, verificando as alterações necessárias;
- Elaborar a versão final dos procedimentos de ensaio;
- Fazer o treinamento dos analistas de ensaio que irão executar os ensaios elaborados.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	29 / 36

Procedimento de Elaboração de Ensaios

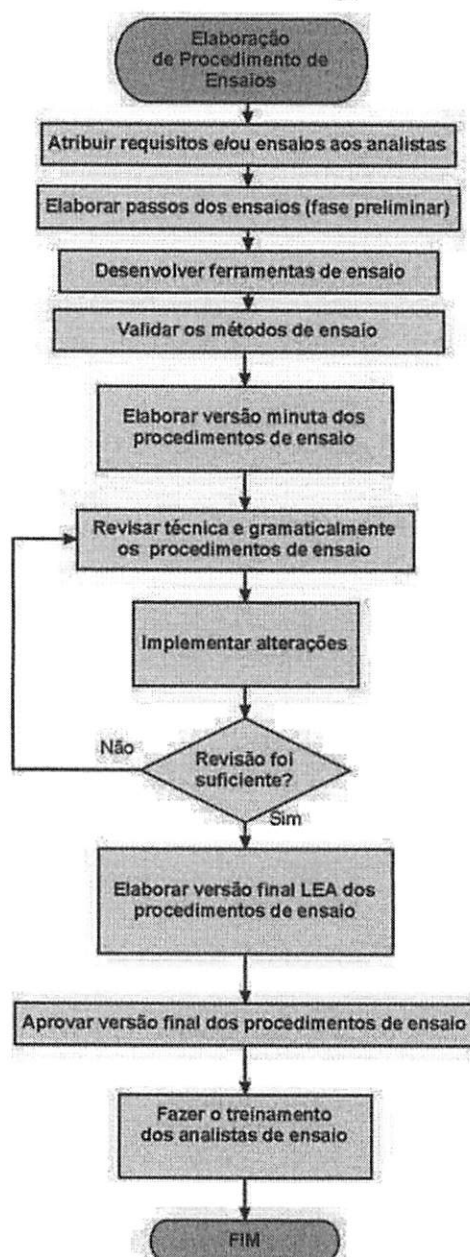


Figura 5 – Procedimento de Elaboração de Ensaio

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	30 / 36

4.7 Infraestrutura do LEA

Um LEA, para ser credenciado pelo ITI, deve atender a alguns requisitos de segurança, de qualidade e de capacitação técnica.

4.7.1 Controles de segurança

O LEA possui uma série de controles de segurança: controles de segurança lógica, controle de segurança física, incluindo sistema de controle de acesso físico e circuito fechado de TV, controles contra ameaças ambientais e controle climático.

Controles específicos são implementados nas áreas reservadas à realização de ensaios e para armazenamento de ativos de ensaio. O acesso a essas áreas é controlado por um sistema de controle de acesso que determina que somente pessoas autorizadas acessem determinadas áreas.

Os computadores utilizados para a elaboração dos relatórios de ensaios e para a realização dos ensaios estão segregados em uma rede isolada das outras dependências do LEA. Os ativos de ensaio entregues pelos clientes são armazenados em uma sala (com armários individuais para cada processo de homologação, trancado com chave), de forma que o acesso a estes ativos só é possível se, no mínimo, duas pessoas autorizadas fizerem a solicitação ao sistema de controle de acesso. Todos os acessos a esses materiais são devidamente registrados.

4.7.2 Controles de qualidade

O LEA também implementa um sistema de gestão da qualidade, baseado na norma ISO 17025 – Requisitos gerais de competência de laboratórios de ensaio e calibração, a fim de garantir a qualidade dos processos de homologação realizados.

Para atender a esta norma, os equipamentos utilizados nos ensaios são mantidos calibrados.

4.8 Estimativa de prazo e custo

A Tabela 1 apresenta uma estimativa de prazos e custos das homologações de produtos realizadas no processo da ICP-Brasil.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	31 / 36

Tabela 1 – Prazos e custos das homologações na ICP-Brasil.

Objeto	Prazo estimado (meses)	Custo estimado (R\$)
Cartões criptográficos (smart cards)	3	R\$ 50 a 100 mil
Tokens criptográficos	3	R\$ 50 a 100 mil
Leitora de cartões criptográficos	1,5	< R\$ 50 mil
Software de assinatura digital	2	< R\$ 50 mil
Software de autenticação	1	< R\$ 50 mil
Software de sigilo	1	< R\$ 50 mil
Software de AC e de AR	4	R\$ 50 a 100 mil
HSM	6	> R\$ 100 mil
Bibliotecas criptográficas	2	< R\$ 50 mil
CSPs (Provedores de Serviços Criptográficos)	2	< R\$ 50 mil
Carimbadoras de tempo	6	> R\$ 100 mil

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	32 / 36

5 Análise comparativa

O Quadro 9 apresenta uma análise comparativa entre o processo de Certificação S-RES e o processo de homologação ICP-Brasil.

Quadro 9 – Comparação da certificação S-RES e da homologação ICP-Brasil.

	Certificação S-RES	Homologação ICP-Brasil
Órgão responsável pelo processo	SBIS/CFM	ICP-Brasil
Objeto da avaliação	Sistemas de saúde	Módulos e sistemas criptográficos
Tipos de objeto de avaliação	Assistencial GED TISS	Cartões criptográficos Tokens criptográficos Leitora de cartões criptográficos Software de assinatura digital Software de autenticação Software de sigilo Software de autoridades certificadoras e de registro HSM; Bibliotecas criptográficas; CSP Software de carimbo de tempo.
Escopo principal	Funcionalidades	Segurança
Escopo secundário	Segurança e interoperabilidade	Interoperabilidade
Organização dos requisitos	Por tipo de sistema	Por tipo de produto
Profundidade da avaliação	Baixa	Alta
Duração média da avaliação	3 dias	60 dias
Custo aproximado	R\$ 5.400,00 a R\$ 30.000,00	R\$ 20.000,00 a R\$ 150.000,00
Remete a outras certificações	Sim, homologação de biblioteca criptográfica ICP-Brasil	Não
Níveis de segurança de avaliação	Não possui	NSH1 NSH2 NSH3
Avaliadores	3 profissionais certificados	Entidade credenciada
Seleção dos avaliadores	SBIS	Livre escolha

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	33 / 36

O modelo de processo de certificação desenvolvido pelo LEA é robusto e requer avaliações e requisitos mais complexos. Já o modelo desenvolvido pelo convênio SBIS/CFM, é um tanto mais simples o que possibilita que a fase de auditoria seja efetivada em um período menor, porém não deixa de atender os princípios fundamentais da certificação.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	34 / 36

6 Conclusão

O estudo dos processos existentes possibilita um melhor entendimento dos requisitos mínimos necessários para que um sistema possa ser aceito e se tornar certificado.

Pode proporcionar maior familiaridade nas atividades desenvolvidas durante todas as fases, que compreende desde o processo de submissão da ficha de inscrição da empresa que deseja ter o sistema avaliado até a fase final de divulgação do sistema certificado.

As diferenças, vantagens e desvantagens observadas de cada processo existentes possibilita que ao criar um novo processo de certificação, as adequações sejam feitas de uma forma mais clara, levando em consideração as características e necessidades específicas do negócio.

Diante das análises e comparações realizadas, o Processo de Certificação SREI será baseado no Processo de Certificação SBIS/CFM, porém considerando as regras de negócios inerentes ao Registro Eletrônico Imobiliário.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	35 / 36

Referências

SBIS, 2009a. Sociedade Brasileira de Informática em Saúde e Conselho Federal de Medicina ***Manual de Certificação para Sistemas de Registros Eletrônicos de Saúde (SRES)*** versão 3.3. São Paulo. 2009.

SBIS, 2009b. Sociedade Brasileira de Informática em Saúde e Conselho Federal de Medicina. ***Manual de Operacional de Ensaio e Análises para Sistemas de Registros Eletrônicos de Saúde (SRES)*** versão 1.2. São Paulo. 2009.

ABNT Associação Brasileira de Normas Técnicas. ***NBR ISO/IEC 17025: Requisitos gerais para a competência de laboratórios de ensaio e calibração.*** Rio de Janeiro. 2006

ICP-BRASIL. COMITÊ GESTOR DA ICP-BRASIL. ***ESTRUTURA NORMATIVA DA ICP-BRASIL.*** Versão 3.4. Brasília. 2010.

Título	Versão	Classificação	Página
PROJETO SREI: PA 1.9 - Análise dos processos de certificação de software existentes	v1.1.r.3	LSITEC:Restrito	36 / 36