Thiago de Barros Silva

Projeto arquitetural de aplicações para área da saúde em dispositivos móveis

São Paulo

2015

Thiago de Barros Silva

Projeto arquitetural de aplicações para área da saúde em dispositivos móveis

Monografia apresentada ao PECE – Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para conclusão do curso de MBA em Tecnologia de Software.

Área de Concentração: Tecnologia de Software

Orientador: Profa. Dra. Gabriela Maria Cabel Barbarán

São Paulo

2015

Atutorização para Reprodução

Ficha catalográfica

Catalogação-na-publicação

Silva, Thiago de Barros
Projeto arquitetural de aplicações para área da saúde em dispositivos móveis / T. B. Silva -- São Paulo, 2015.
51 p.

Monografia (MBA em Tecnologia de Software) - Escola Politécnica da Universidade de São Paulo. PECE – Programa de Educação Continuada em Engenharia.

1.Arquitetura de software 2.Padrões arquiteturais 3.Dispositivos móveis 4.Registro Eletrônico em Saúde I.Universidade de São Paulo. Escola Politécnica. PECE – Programa de Educação Continuada em Engenharia II.t.

DEDICATÓRIA

Dedico este trabalho a minha futura esposa Viviana Sayão Gabriel, aos meus pais Mauro Pereira da Silva e Edileusa Cordeiro de Barros e ao meu irmão Matheus de Barros Silva.

AGRADECIMENTOS

À minha futura esposa Viviana Sayão Gabriel que me apoiou durante todo este trabalho, entendendo minhas ausências e oferecendo todo suporte que precisei para concluir este trabalho.

Ao meu pai Mauro Pereira da Silva que demonstrou que não há limites para continuar aprendendo, concluindo sua segunda graduação, me inspirando, incentivando e servindo de exemplo.

Aos meus familiares, que me apoiaram, incentivaram e entenderam minhas ausências em diversos eventos.

Ao corpo docente do PECE, por todo conhecimento transmitido e suporte para conclusão do curso, em especial à minha orientadora Profa. Dra. Gabriela Maria Cabel Barbarán que teve muita paciência durante este trabalho.

Aos meus amigos e colegas de trabalho por todo auxílio, suporte e incentivo durante este trabalho, em especial ao Wallas dos Santos Souza pelas opiniões expressadas, à Beatriz Cristina Munhoz pela companhia em tardes de estudos e ao Daniel Marques Gomes de Morais pelos conhecimentos acadêmicos compartilhados.

Resumo

Este trabalho propõe um projeto arquitetural para atender aplicações corporativas na área da saúde que utilizam dispositivos móveis como interface do sistema. Para isto foi realizada uma pesquisa bibliográfica em livros e artigos relacionados com a descrição de aplicações corporativas, estilos e padrões arquiteturais para o desenvolvimento destas aplicações. O projeto leva em consideração os requisitos funcionais e não funcionais de um sistema de registro eletrônico em saúde utilizando dispositivos móveis. Com base no levantamento realizado obteve-se um projeto arquitetural utilizando o estilo arquitetural cliente-servidor e os padrões arquiteturais cliente-servidor multicamadas e agentes móveis em conjunto, considerado o mais adequado para atender os requisitos funcionais e não funcionais propostos em um escopo definido.

Palavras-chave: Arquitetura de software, Padrões arquiteturais, Dispositivos móveis, Registro Eletrônico em Saúde

Abstract

This work proposes an architectural design to meet enterprise applications in healthcare using mobile devices as system interface. A bibliographic research was done in books and articles related to the description of enterprise applications, styles and architectural patterns for the development of these applications. The proposed architectural design took into account the functional and non-functional requirements of an electronic health record system using mobile devices. Based on this research, an architectural project using the architectural style client-server and the architectural patterns client-server, multi layered and mobile agents was designed, taking into account the most adequate to meet the functional and non-functional requirements proposed on a defined scope.

Keywords: Software architectural, Architectural patterns, Mobile devices, Electronic health record

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

ABNT	Associação Brasileira de Normas Técnicas
CFM	Conselho Federal de Medicina
C/A/S	Client/Agent/Server
C/I/S	Client/Intercept/Server
C/S	Client/Server
HTML	HyperText Markup Language
HTTPS	Hyper Text Transfer Protocol Secure
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
MVC	Modelo Vista Controlador
NGS1	Nível de Garantia de Segurança 1
NGS2	Nível de Garantia de Segurança 2
SBIS	Sociedade Brasileira de Informática em Saúde
SGBD	Sistema Gerenciador de Banco de Dados
S-RES	Sistema de Registro Eletrônico em Saúde

Sumário

Capítulo 1

Introdução

1.1 Motivações

Com o surgimento de uma nova geração de dispositivos móveis, apoiados por aplicações móveis que aumentam as possibilidades além de apenas comunicação por voz, o desafio dos desenvolvedores aumentou, são eles:

- Diversidade dos dispositivos
- Intermitência do sinal das redes móveis
- Capacidade de armazenamento
- Capacidade de processamento
- Limite e diferentes tamanhos de telas

Tais desafios devem ser considerados para o desenvolvimento de aplicativos móveis, pode-se destacar a necessidade de acesso a fontes de dados externas ao dispositivo para atender a complexidade da aplicação devido às limitações citadas. Para alcançar o objetivo proposto são utilizados servidores e/ou *middlewares* para fornecer estes dados para aplicações móveis.[1]

De acordo com Sommerville (2011), sistema é o trabalho em conjunto realizado por softwares e hardwares. Acrescentando pessoas e processos a este sistema permite que tarefas complexas possam ser executadas para alcançar algum propósito humano, social ou empresarial e define esse conceito mais amplo como sistemas sociotécnicos. [2]

1.2 Objetivo

Este trabalho tem como objetivo descrever padrões arquiteturais de software para o desenvolvimento de aplicações corporativas em dispositivos móveis e identificar um padrão arquitetural que atenda a necessidade de comunicação entre a aplicação móvel e as fontes de dados utilizadas pelas empresas do setor de saúde.

1.3 Justificativas

O crescimento do mercado de dispositivos e aplicativos móveis foi impulsionado em 2007, com surgimento de uma nova geração de dispositivos com novos conceitos como o iPhone produzido pela Apple. Segundo Giessmann, Stanoevska-Slabeva e Visser (2012) em especial as lojas de aplicativos móveis em um período de 2009 a 2014 presenciaram um aumento de 677%, movimentando uma enorme quantidade de dinheiro, cerca de 10,9 trilhões de dólares

em 2010. Motivados por esta demanda os dispositivos móveis com maior capacidade e processamento são lançados no mercado a cada ano. [3]

Neste cenário as empresas estão procurando formas de ganhar valor utilizando aplicativos móveis. Melhorando o atendimento de seus clientes, auxiliando em seus processos internos, tendo benefícios como oferta de serviços mais rápidos e disponíveis a qualquer momento online através dos dispositivos móveis de empregados ou clientes, reduzindo custos e aumentando o desempenho do negócio.

Existem diferentes tipos de softwares para diferentes propósitos, conforme Fowler (2006), cada um com seus desafios e complexidades. As aplicações corporativas trabalham com grande quantidade de dados aliados com regras de negócios com diferentes níveis de complexidade de acordo com o ramo da empresa.

Estas aplicações necessitam de dados persistentes por vários anos, disponíveis em múltiplas execuções na maioria das vezes o software durará mais que o hardware. Com a evolução, a estrutura de dados será alterada para armazenamento de novas informações e não poderá alterar as já existentes, tendo que haver a migração dos dados para a nova estrutura ou aplicação.

A concorrência de acesso aos dados em muitas vezes é tratada pelas ferramentas de controle de transações, evitando que

duas pessoas não alterem o mesmo dado ao mesmo tempo ocasionando erros, mas com os sistemas baseados na Web disponibilizando acesso a uma grande quantidade pessoas os desenvolvedores precisam intervir.

As aplicações corporativas em sua grande maioria comunicam-se com outras aplicações corporativas, podendo ser de tecnologias diferentes, utilizando uma tecnologia comum de comunicação para integração, muitas vezes por falta de padronização as integrações são desenvolvidas de diversas formas diferentes. Outro fator implicante na comunicação entre aplicações é a diferença conceitual dos dados, ocasionado por áreas de atuações diferentes. [4]

De acordo com a SBIS (Sociedade Brasileira de Informática em Saúde) o uso da tecnologia na área da saúde está em grande expansão, auxiliando os profissionais, aumentando a segurança dos pacientes e armazenando informações em computadores, o que antes era armazenado em papel. Para garantir a segurança das informações e a legalidade de S-RES (Sistema de Registro Eletrônico em Saúde) que é responsável por capturar, armazenar, processar, exibir, imprimir e transmitir dados do atendimento em saúde a SBIS em conjunto com o CFM (Conselho Federal de Medicina) propôs um manual de certificação destes sistemas detalhando os requisitos de segurança, estrutura, conteúdo e funcionalidades que devem ser atendidos. [5]

Existem algumas abordagens de arquitetura de software para suprir as necessidades da melhor forma possível, como *client-server* (C/S), *client-agent-server* (C/A/S), *client-intercept-server* (C/I/S), ponto a ponto e outras que são utilizadas no desenvolvimento de aplicações móveis.[1]

Normalmente divididas nas camadas de interface com usuário, negócio e dados as aplicações são bem atendidas nas estruturas C/A/S e C/I/S. Onde no modelo C/A/S, toda comunicação com a aplicação no dispositivo móvel passa por um *middleware* também chamado de agente que faz a conexão com a fonte de dados, trazendo vantagens como aumento de segurança na rede sem fio aplicando tratativas no agente, melhorando a qualidade do serviço com baixo custo computacional otimizando somente o *middleware*. Porém, nessa arquitetura caso o dispositivo não possua conexão não permitirá interações.

Na arquitetura C/I/S são implantados agentes do lado do servidor e do cliente, este modelo tem como vantagem poder realizar otimizações nos dados transmitidos entre os agentes possibilitando a redução de dados trafegados na rede sem fio e permite o funcionamento do aplicativo mesmo não conectado a rede devido ao agente do lado do cliente.

Neste sentido este trabalho pretende analisar padrões arquiteturais para atender as necessidades de aplicações corporativas na

área da saúde para dispositivos móveis e propor um projeto arquitetural para auxiliar os desenvolvedores com os desafios citados.

1.4 Estrutura do trabalho

O Capítulo 1 INTRODUÇÃO apresenta a motivação, o objetivo, a justificativa e a estrutura do trabalho.

O Capítulo 2 REVISÃO BIBLIOGRÁFICA apresenta a definição de aplicações corporativas e seus tipos, descreve arquitetura de software, exemplifica estilos e padrões arquiteturais, decisões de projeto de arquitetura e os requisitos de qualidade de software da ISO 9126-1.

O Capítulo 3 PADRÃO ARQUITETURAL apresenta informática em saúde, a certificação para sistemas de registro eletrônico em saúde e seus requisitos funcionais e não funcionais, define o escopo da aplicação, apresenta o projeto arquitetural e justifica as decisões tomadas.

O Capítulo 4 ANÁLISE DO PROJETO ARQUITETURAL analisa o projeto arquitetural proposto.

O Capítulo 5 CONSIDERAÇÕES FINAIS concluí o trabalho. É divido em duas partes, a primeira descreve as conclusões obtidas com o projeto arquitetural proposto e a segunda parte aponta evoluções a seguir em trabalhos futuros.

REFERÊNCIAS relaciona os trabalhos, artigos, livros e demais referências usadas neste trabalho.

ANEXO A apresenta a descrição dos requisitos para certificação de Sistemas de Registro Eletrônico em Saúde definidos pela Sociedade Brasileira de Informática em Saúde.

Capítulo 2

Revisão Bibliográfica

2.1 Aplicações Corporativas

Segundo Araujo (2013), aplicações corporativas são softwares que auxiliam as empresa na resolução de problemas, normamente concebidos para integração ou interface para outras aplicações. [6]

Existem diferentes tipos de softwares para diferentes propósitos, conforme Fowler (2006), cada um com seus desafios e complexidades. As aplicações corporativas trabalham com grande quantidade de dados aliados a regras de negócios com diferentes níveis de complexidade de acordo com o ramo da empresa.

Estas aplicações necessitam de dados persistentes por vários anos, disponíveis em múltiplas execuções na maioria das vezes, o software durará mais que o hardware. Com a evolução, a estrutura de dados será alterada para armazenamento de novas informações e não poderá alterar as já existentes, tendo que haver a migração dos dados para a nova estrutura ou aplicação.

A concorrência de acesso aos dados em muitas vezes é tratada

pelas ferramentas de controle de transações, evitando que duas pessoas alterem o mesmo dado ao mesmo tempo ocasionando erros, mas com os sistemas baseados na Web disponibilizando acesso a uma grande quantidade de pessoas os desenvolvedores precisam intervir.

As aplicações corporativas em sua grande maioria comunicam-se umas com as outras, podendo ser de tecnologias diferentes, mas utilizando uma tecnologia comum de comunicação para integração, muitas vezes por falta de padronização as integrações são desenvolvidas de diversas formas diferentes. Outro fator implicante na comunicação entre aplicações é a diferença conceitual dos dados, ocasionado por áreas de atuações diferentes. [4]

2.1.1 Tipos de aplicações

Para Fowler (2006) as aplicações corporativas são diferentes umas das outras, sendo necessário conhecer as alternativas para escolher a melhor solução frente aos desafios distintos.

No caso de uma loja virtual que pode ter uma grande quantidade de usuários simultâneos, por exemplo, possuir um fluxo de negócio direto com lista de produtos, obter o pedido, cálculos de preço e frete e notificações de envio. Neste cenário é necessária uma interface Web bastante genérica disponibilizando o conteúdo para maior quantidade de navegadores possíveis, sendo uma aplicação

eficiente no uso de recursos e escalonável, permitindo adicionar mais hardware conforme a demanda. Utilizará um banco de dados para armazenar os pedidos e possivelmente uma comunicação com o sistema de estoque para consultar disponibilidade e entrega.

Comparando a loja virtual com um sistema que automatize o processo de contratos de *leasing* a quantidade de usuários é menor, o que o torna mais simples em relação a algumas implementações. Porém, a lógica de negócio é mais complexa, tendo que realizar cálculos mensais, pagamentos atrasados, planejar reservas de contratos e diversas regras arbitrárias que são exigidas pelo domínio do negócio. Essa aplicação necessita de uma interface para o usuário mais sofisticada e em maior quantidade para atender diferentes interações e visões e um banco de dados complexo com diversas tabelas e relações para suprir demandas das regras de negócio.

Na criação de um sistema de controle de gastos de uma empresa pequena se espera um desenvolvimento rápido comparando-o aos exemplos anteriores, onde uma interface Web simples e poucas tabelas no banco de dados suprem a necessidade. Porém, este sistema pode crescer com as necessidades da empresa incorporando novos módulos como reembolso, folha de pagamentos, relatórios gerenciais ou integrações com sistemas de cotação de passagens aéreas, onde aplicar a arquitetura utilizada nos casos da loja virtual e da automação do processo de contratos de *leasing* pode

aumentar o tempo de desenvolvimento, fazendo a empresa perder dinheiro e tempo para atender sua demanda. Por outro lado não aplicando padrões arquiteturais adequados pode dificultar a expansão futura do software. Mesmo sendo um sistema pequeno é muito comum empresas terem alguns destes, sendo significativo o efeito cumulativo de arquiteturas inapropriadas.

Nos exemplos descritos temos três cenários diferentes cada um com suas necessidades e na escolha de um padrão arquitetural não há solução para atender todos os casos. Sendo necessário analisar a peculiaridade de cada aplicação e mesmo após selecionar um padrão terá que modificá-lo para se enquadrar as necessidades do projeto.[4]

2.1.1.1 Sistemas Complexos

Para Sommerville (2011) sistemas complexos são compostos por componentes de diferentes tipos que se relacionam para atingir um objetivo, estes componentes estão fortemente ligados, onde é necessário o funcionamento correto de todos.

O autor cita que os sistemas complexos são geralmente hierárquicos e englobam outros sistemas. Como por exemplo, o sistema de comando e controle da polícia que utiliza um sistema de geolocalização para obter os locais de ocorrências, estes são chamados de subsistemas, que podem operar sozinhos.

Ainda conforme o autor, sistemas que possuem software são segmentados em duas categorias, sistemas técnicos baseados em computador e sistemas sociotécnicos. Os sistemas técnicos baseados em computador incluem software e hardware, mas não processos e procedimentos, pessoas o utilizam para um objetivo específico, porém o sistema não possui o conhecimento deste objetivo, como por exemplo, telefone, televisores, jogos de computadores ou editores de texto.

Os sistemas sociotécnicos são descritos pelo autor como sistemas corporativos que tem como objetivo atender uma meta de negócio e incluem sistemas técnicos e pessoas para alcançar o seu propósito, tendo os processos operacionais e os operadores como parte do sistema. Por fazerem parte de um ambiente organizacional sofrem influência por parte da cultura e política da empresa, as mudanças de processos, de trabalhos ou organizacionais podem afetar os requisitos, o projeto e a operação do sistema. [2]

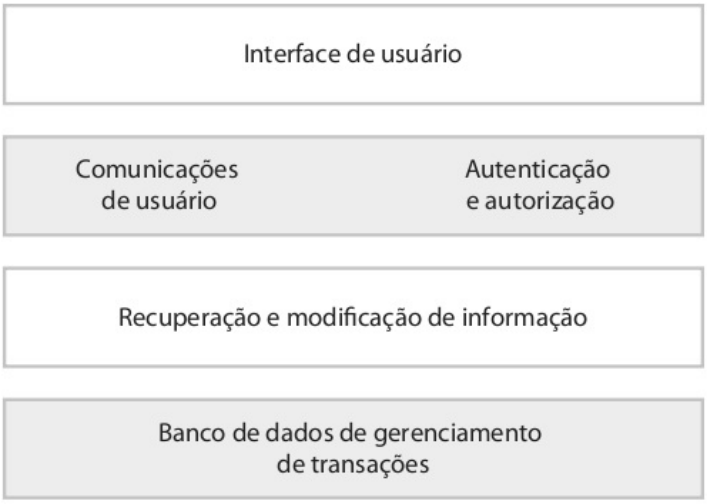
2.1.1.2 Sistemas de informação

Sommerville (2011) define como sistemas de informação, os sistemas que interagem com bancos de dados permitindo acesso controlado a informações, como por exemplo, catálogo de bibliotecas ou registros de pacientes em um hospital.

Sistemas de informação comumente são baseados na Inter-

net, a figura 1 exibe um modelo geral de sistemas de informação, onde a camada inferior é o banco de dados do sistema, a camada de comunicação com usuário é responsável pela entrada e saída dos dados da camada de interface com usuário, a camada de recuperação de informação é responsável por acessar e atualizar a fonte de dados conforme a lógica específica da aplicação e a camada mais superior é a de interface do usuário. [2]

Figura 1 – *Arquitetura de sistema de informação em camadas*



Fonte: Sommerville, 2011 [2]

2.1.1.3 Sistemas Distribuídos

Sistema distribuído é definido por Sommerville (2011) como um sistema que utiliza diversos computadores, mas é apresentado ao cliente como um único sistema coerente, diferente de sistemas centralizados que executam todos os componentes em um único computador. Estes sistemas tem como vantagens o compartilha-

mento de recursos como impressoras ou arquivos, são sistemas abertos que utilizam protocolos padrões que podem ser combinados com softwares ou equipamentos de fornecedores, permitem o processamento paralelo em diferentes computadores e possuem escalabilidade podendo adicionar novos recursos e toleram falhas e defeitos em alguns pontos do sistema, a não ser que seja na rede. [2]

2.2 Arquitetura de Software

Segundo Pressman (2011) a definição de arquitetura de software pode ser dada como as estruturas do sistema, os componentes de software, e como estes componentes interagem entre eles e as suas propriedades visíveis exteriormente. Sendo uma representação não operacional permite ao engenheiro de software analisar a eficácia diante dos requisitos do sistema, considerar alternativas arquitetônicas e também reduzir os riscos referentes à construção do software, onde a complexidade do componente varia conforme a necessidade.

Ainda segundo o autor, a arquitetura de software traz benefícios como auxiliar na comunicação entre todos os interessados no desenvolvimento do projeto, permite antecipar e prever problemas em etapas futuras da engenharia de software, tomadas de decisões nas fases iniciais do projeto e também exibir um modelo

de como o software está estruturado e de como seus componentes interagem. [7]

2.2.1 Estilos Arquiteturais

Para Pressman (2011) estilos arquitetônicos são *templates* para o desenvolvimento do software, pode-se traçar um paralelo de estilos arquitetônicos de software com os aplicados na construção civil quando definido um estilo pelo arquiteto para a construção de uma casa, onde ao se mencionar o estilo é possível ter ideia de como será sua planta. Na construção da casa a escolha do estilo auxilia nas decisões futuras como materiais de construção, dimensões finais e características personalizadas.[7]

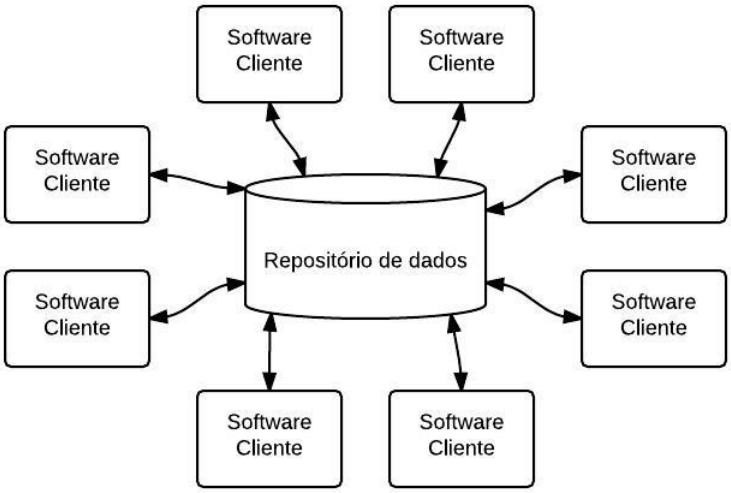
Para Sommerville (2011) o estilo arquitetural descreve como o sistema está organizado, por exemplo, utilizando o estilo cliente-servidor ou arquitetura em camadas. A escolha de estrutura mais adequada é fundamental para o cumprimento dos requisitos do sistema. [2]

2.2.1.1 Arquitetura de Repositório

Conforme define Sommerville (2011) o estilo de arquitetura de repositório centraliza o gerenciamento dos dados em um repositório central, onde todos os componentes têm acesso e toda comunicação entre componentes é realizada através do repositório.

Para o autor este estilo é indicado para sistemas com foco nos dados, onde a inclusão de novas informações dispara ações em outros componentes. Como mostra a figura 2 os componentes são independentes e qualquer alteração realizada em um propaga-se para os demais. Também outra vantagem deste estilo é o gerenciamento dos dados, por todos estarem em um único lugar, mas em contrapartida qualquer falha no repositório afeta todos os componentes, distribuí-lo em diversos computadores pode ser complexo e é necessário um ponto de atenção na redundância e na inconsistência dos dados. [2]

Figura 2 – *Estilo arquitetural de Repositório*



Fonte: Sommerville, 2011 [2]

2.2.1.2 Arquitetura Cliente-Servidor

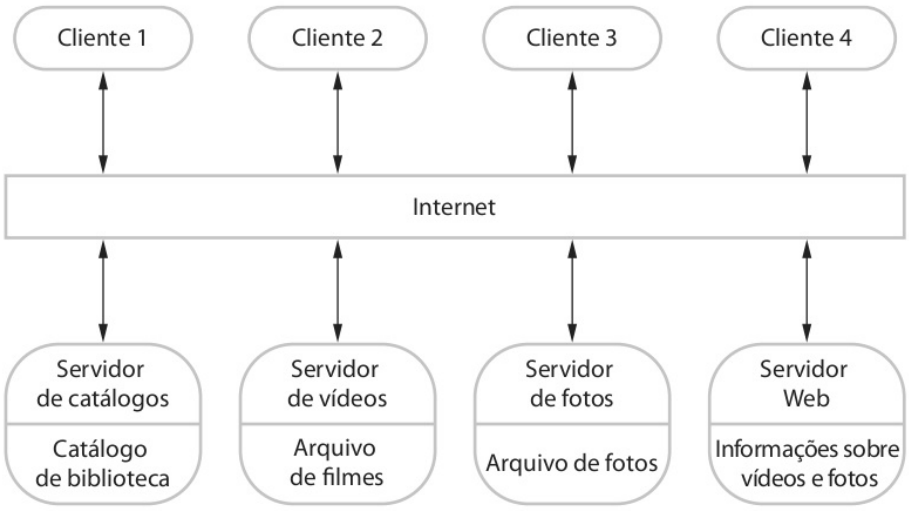
Para Sommerville (2011) no estilo cliente-servidor as funcionalidades são disponibilizadas em serviços alocados nos servidores que os clientes consomem. Os principais componentes são os servidores que oferecem os serviços, os clientes que consomem o serviço ofertado e uma rede que permite a comunicação entre clientes e servidores, conforme descreve a figura 3.

Este estilo é indicado quando se tem diversos locais de acesso a uma fonte de dados ou quando há carga variável em um sistema, por ser uma arquitetura que suporta sistemas distribuídos e também permite alocar diversos servidores pela rede para atender a demanda. Por outro lado os serviços e servidores são um ponto único suscetível a falhas e ataques, é influenciado pelo desempenho da rede utilizada na comunicação e o gerenciamento dos servidores de diversos fornecedores pode ser outra desvantagem.[2]

2.2.1.3 Arquitetura de Duto e Filtro

Segundo Sommerville (2011) no estilo arquitetural de duto e filtro todo processamento de dados é realizado por um componente de processamento (filtro), responsável pela transformação dos dados, onde os dados fluem como em um duto, entre os componentes realizando o processamento. Este estilo é recomendado para sistemas de processamento de dados em lotes ou transações, onde as

Figura 3 – *Estilo arquitetural Cliente-Servidor*



Fonte: Sommerville, 2011 [2]

entradas são processadas em etapas separadas para gerar saídas relacionadas.

Para o autor este estilo arquitetural tem como vantagem o estilo de *workflow* que é comum em processos de negócios, pode ser implementado sequencialmente ou concorrente e o reúso da transformação é de fácil entendimento. Mas as desvantagens são que todos os componentes analisam suas entradas e geram saídas que devem estar no padrão para a entrada de outro componente, o que pode impossibilitar o reúso de outros componentes com funcionalidades semelhantes que utilizam estruturas incompatíveis de dados. [2]

2.3 Padrões Arquiteturais

Conforme define Fowler (2006) os padrões auxiliam na resolução de problemas recorrentes dando soluções que possam ser utilizadas diversas vezes atendendo a especificidade de cada ocasião.[4]

Para Pressman (2011) padrões arquiteturais são definições estruturais que ao serem aplicadas dão a visão de como o software foi arquitetado sem entrar em detalhes de implementação.[7]

Como exemplo de arquitetura de software pode-se citar o padrão arquitetural MVC - Modelo Vista Controlador, muito difundido para interface com usuário. Onde o Modelo tem objetos que fazem parte do domínio, a Vista é a interface de apresentação do modelo para o usuário e o Controlador fica responsável por receber as informações do usuário, manipulá-las no Modelo e atualizar corretamente a Vista. Com suas camadas separadas este padrão permite a menor dependência entre elas e o desenvolvimento distinto do modelo facilitando a criação de diversas apresentações posteriormente. Este padrão arquitetural é muito utilizado em projetos Web. [4]

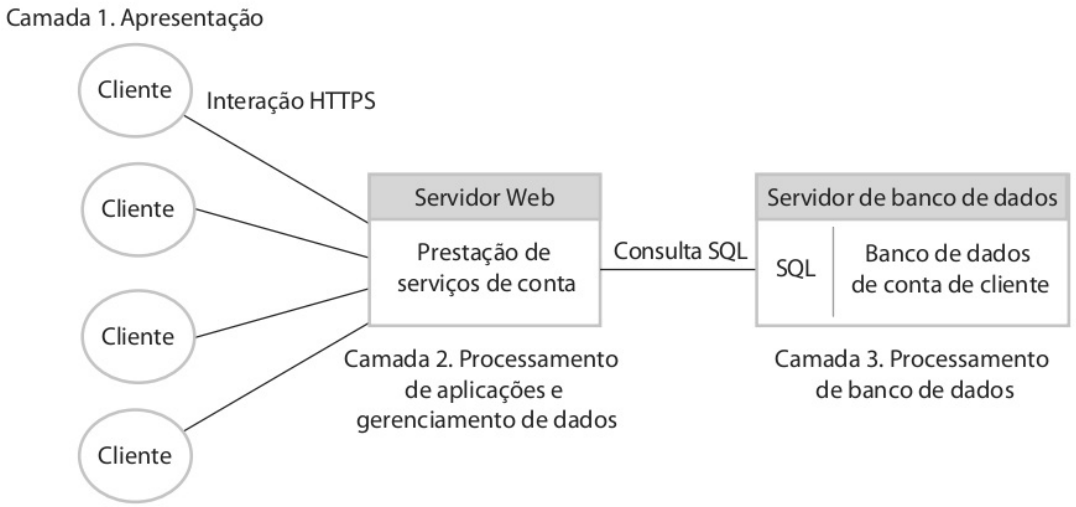
2.3.1 Cliente-Servidor multicamadas

Conforme descreve Sommerville (2011) este padrão arquitetural mantêm separadas as diferentes camadas do sistema, apre-

sentação, gerenciamento dos dados, processamento da aplicação e banco de dados. Permitindo assim a execução das camadas em diferentes processadores. Indicado para grandes aplicações com muitos usuários ou aplicações com dados voláteis e com integração de diversas fontes de dados. [2]

Na figura 4 o autor descreve um sistema de *internet banking* separado em três camadas, o banco de dados que fornece as informações, o servidor web que fornece os serviços da aplicação como transferências e consultas e o cliente que utiliza um computador com navegador de internet para acesso a aplicação. Este modelo permite adicionar servidores conforme a demanda de processamento ou também adicionando camadas, como por exemplo, recuperar dados de fontes diferentes.

Figura 4 – *Arquitetura de três camadas para um sistema de Internet banking*



Fonte: Sommerville, 2011 [2]

Fowler (2006) descreve este padrão com três camadas segmentadas em apresentação, domínio e fonte de dados, onde a camada de apresentação é responsável pela exibição e a interação entre usuário e software, com o objetivo principal de traduzir as informações inseridas pelos usuários em comandos para as camadas de domínio e de dados. Na camada de lógica de domínio, também conhecida como lógica de negócio, é onde todas as regras de negócio são aplicadas, executando validações e cálculos necessários de acordo com a entrada e a saída das outras camadas. Já a camada de dados na grande maioria das aplicações fica responsável pelo armazenamento dos dados persistentes, mas também pode fazer a comunicação com outros sistemas, troca de mensagens ou transações.

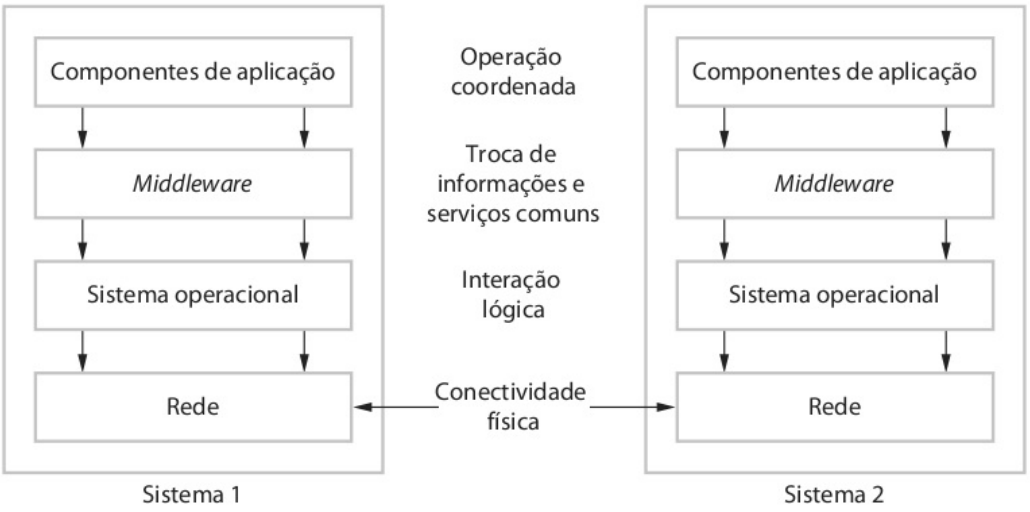
Neste padrão, Fowler (2006), indica que as camadas de lógica de domínio e fonte de dados não devem depender da camada de apresentação, permitindo diversas interfaces a usuários ou outros softwares sem a manipulação das camadas abaixo. Na divisão de camadas a complexidade deve ser analisada para uma melhor organização, separando-as em sub-rotinas, classes ou até pacotes diferentes, de acordo com o aumento de complexidade. [4]

2.3.2 Middlewares

Para Sommerville (2011) *middlewares* são softwares que gerenciam os componentes de um sistema distribuído. Estes sistemas podem ser desenvolvidos em diversas linguagens, ter protocolos de comunicação distintos e possuem o *middleware* como mediador para garantir a troca de dados e a comunicação. A figura 5 mostra o *middleware* entre os componentes do sistema.

O mesmo autor define dois tipos de *middlewares*, sendo os que coordenam a interação e a transparência entre os componentes do sistema, onde um componente não precisa saber a localização física do outro. O outro tipo é de *middlewares* que permitem reutilização por diversos componentes. [2]

Figura 5 – *O middleware em um sistema distribuído*

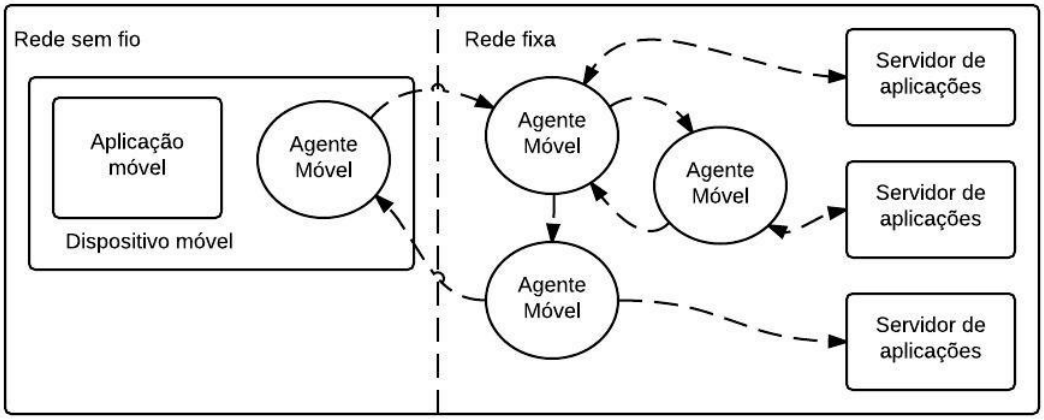


Fonte: Sommerville, 2011 [2]

2.3.2.1 Agentes Móveis

Para Spyrou, Samaras, Pitoura e Evripidou (2004) os agentes móveis são *middlewares* que contêm seus próprios dados e estados de execução, localizado entre o cliente móvel e o servidor estático pode realizar uma tarefa específica ou diversas, conforme a necessidade do cliente móvel, a figura 6 ilustra esse modelo. Após acionado o agente móvel age de forma independente do cliente solicitante, podendo se transportar para outro servidor, acionar novos agentes e retornar o resultado para o cliente ou outro servidor. [8]

Figura 6 – *Modelo de agentes móveis*



Fonte: Adaptado de Spyrou, 2004 [8]

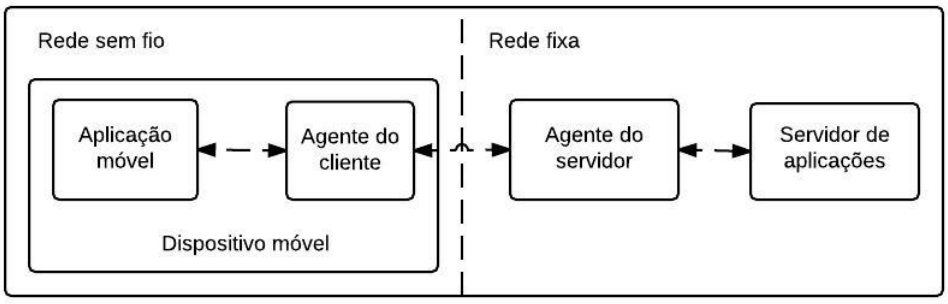
A tecnologia de agentes móveis é indicada para redes sem fio tirando a carga de processamento das limitações dos dispositivos móveis e transferindo para uma rede fixa, também migrando o agente entre os servidores para acompanhar o cliente. Utiliza-se

das coleções de dados para comunicação entre as aplicações móveis e os servidores estáticos.[8]

2.3.2.2 Client/Intercept/Server (C/I/S)

O modelo C/I/S possui um agente do lado do cliente, na rede sem fio com quem a aplicação móvel se comunica e outro agente no servidor ou *middleware* na rede fixa, onde pode responder para vários clientes e é responsável por se conectar ao banco de dados e todo processamento de regras de negócio retornando o resultado ao agente posicionado no cliente. O agente do cliente responde somente a aplicação móvel, não precisando se conectar ao banco e trabalhando em conjunto com o agente do servidor para interceptar e controlar a troca de mensagens com objetivo de reduzir a transmissão de dados pela rede sem fio e aperfeiçoar o processamento. O padrão é exemplificado na figura 7.

Figura 7 – *Modelo Client/Intercept/Server*



Fonte: Adaptado de Spyrou, 2004 [8]

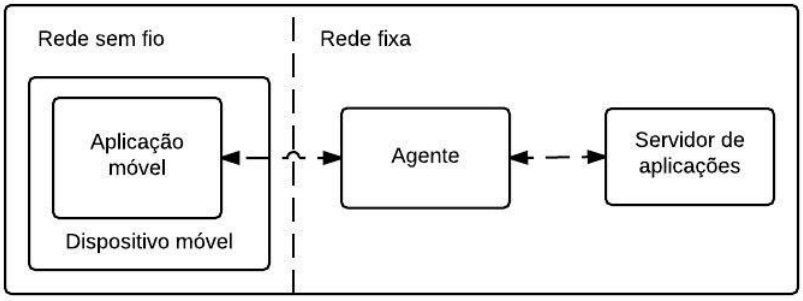
Com o agente no dispositivo móvel pode-se aplicar técnicas para armazenar informações do lado do cliente para acesso mais rápido ou também enfileirar as chamadas para o agente externo em caso de perda de conexão sem fio para realizá-las quando a comunicação for reestabelecida.[8][1]

2.3.2.3 Client/Agent/Server (C/A/S)

O modelo C/A/S é uma extensão do padrão três camadas no qual acrescenta um agente entre a aplicação cliente e a fonte de dados, onde toda transmissão de dados passa por ele. Este agente pode agir de diferentes formas e executar diversas funções, uma maneira é recebendo e retornando todas as requisições do cliente móvel. Outra forma é atendendo a uma necessidade específica, de forma que somente determinadas requisições sejam realizadas pelo agente, como por exemplo, chamadas a uma aplicação ou banco de dados. Neste padrão o agente fica responsável pela comunicação com a fonte de dados ou aplicação responsável. A figura 8 ilustra esse modelo.

Esta abordagem permite adicionar etapas de segurança ao agente e aperfeiçoar a transmissão de dados da rede fixa para o cliente móvel, mas não no sentido oposto. Como desvantagem o padrão C/A/S não atende em momentos sem conexão da rede móvel. [8][1]

Figura 8 *– Modelo Client/Agent/Server*



Fonte: Adaptado de Spyrou, 2004 [8]

2.4 Decisões de projeto de arquitetura

Segundo Sommerville (2011) o projeto de arquitetura é o resultado de um conjunto de decisões baseados no tipo de projeto, nas experiências do arquiteto de sistemas e nos requisitos funcionais e não funcionais, tendo como saída no final deste processo criativo a organização do sistema.

As decisões arquiteturais tomadas durante o processo de projeto de arquitetura afetam diretamente o desenvolvimento do sistema e levam em consideração os seguintes pontos:

- Pode-se utilizar uma arquitetura genérica?
- Como será a distribuição do sistema pelos núcleos ou processadores?
- Quais estilos ou padrões podem ser utilizados?

– Qual a abordagem fundamental para estruturar o sistema?

– Como os componentes serão segmentados em subcomponentes?

– Como serão controlados os componentes?

– Qual a melhor arquitetura para atender os requisitos não funcionais?

– Como o projeto de arquitetura será avaliado?

– Como documentar a arquitetura adotada?

Ainda segundo o autor a arquitetura escolhida e os requisitos não funcionais estão fortemente relacionados e de acordo com a criticidade dos requisitos não funcionais são baseadas as decisões para a definição da arquitetura do sistema. Os requisitos não funcionais definidos pelo autor são desempenho, proteção, segurança, disponibilidade e manutenção.

Se o desempenho for um requisito importante para o sistema, uma arquitetura projetada com poucos componentes auxilia diminuindo quantidade de comunicações entre eles para realização de uma tarefa, o que pode gerar menor granularidade e componentes maiores. Centralizar a implantação dos componentes em um único computador também é indicado, gerando maior desempenho comparado a sistemas distribuídos por diversos nós da rede.

Para os sistemas com maior foco em proteção o autor define que uma arquitetura em camadas com forte validação de proteção nas primeiras camadas e os com componentes mais críticos nas camadas mais internas auxilia neste requisito.

Em casos que a segurança é um requisito importante todas as operações devem ser centralizadas em um único componente, diminuindo o custo e problemas com a validação de segurança.

Para atender o requisito não funcional de disponibilidade o autor sugere componentes redundantes permitindo a manutenção ou substituição sem parar o sistema.

Se a manutenção for um requisito crítico deve-se utilizar uma arquitetura de baixa granularidade, facilitando a rápida alteração, evitar estruturas de dados compartilhadas e separar os produtores e consumidores de dados.

De acordo com a criticidade dos requisitos algumas decisões são conflitantes e uma solução para este impasse é a utilização de arquiteturas diferentes em diferentes componentes. Para o autor a solução para a dificuldade de avaliação do projeto de arquitetura é verificar o quão aderente estão os requisitos funcionais e não funcionais. [2]

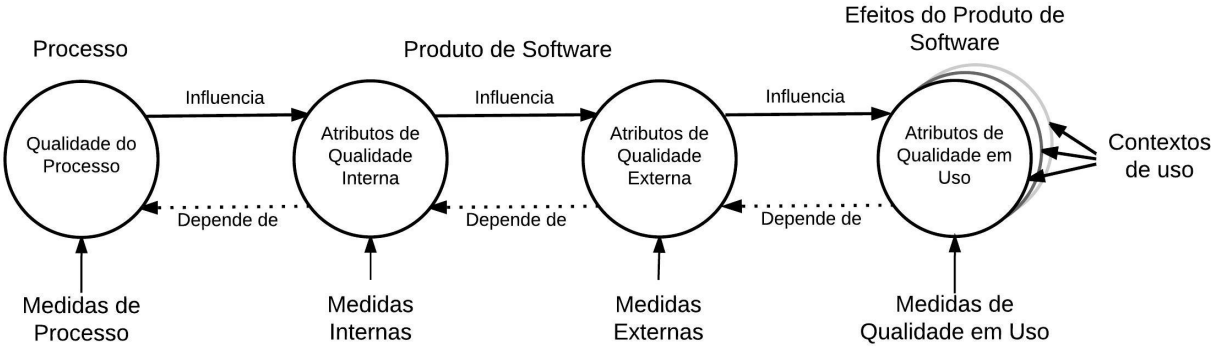
2.5 Requisitos de Qualidade de software - ISO 9126

A ABNT (Associação Brasileira de Normas Técnicas) define a ISO 9126 (2003), que em 2011 foi substituída pela ISO 25010, com objetivo de criar um modelo de qualidade do produto de software, este modelo é dividido em duas partes, qualidade interna e externa e qualidade de uso. Sendo a qualidade interna e externa segmentada em seis características que são subdivididas em subcaracterísticas. A qualidade de uso é divida em quatro características e para o usuário é o resultado das categorias de qualidade interna e externas aplicadas no software.

As características e o modelo definido permitem avaliar todo tipo de software, podendo utilizá-lo como base para os requisitos de qualidade e também comparar, especificar e avaliar o software por diferentes perspectivas dos interessados como desenvolvedores, adquirentes, pessoas da garantia de qualidade e responsáveis pela avaliação e especificação do produto.

Para a ABNT (2003) a melhoria do processo influência na melhoria da qualidade do produto de software que por sua vez melhora a qualidade em uso. Como mostra a figura 9, a qualidade interna do produto é pré-requisito para atender a qualidade externa do produto que também é pré-requisito para cumprir a qualidade em uso. [9]

Figura 9 – *Qualidade no ciclo de vida*

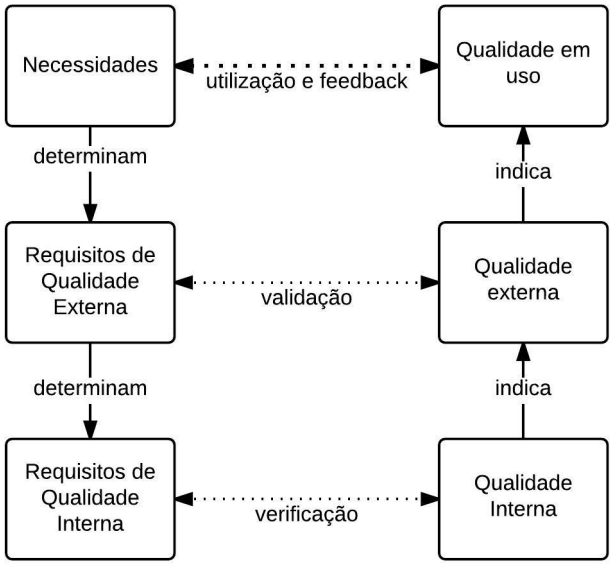


Fonte: Associação Brasileira de Normas Técnicas, 2003 [9]

Ainda segundo o mesmo autor a qualidade interna é definida como o conjunto de características do produto do ponto de vista interno, avaliada de acordo com os requisitos de qualidade interna, podendo ser aperfeiçoada durante a implementação do código, revisão ou testes. A qualidade externa é descrita como a totalidade de características do produto do ponto de vista externo, sendo medido durante a execução do produto em ambiente controlado com dados simulados com foco em corrigir a maioria dos erros. A qualidade em uso é definida como a qualidade do produto de software do ponto de vista do usuário quando executado no ambiente e no contexto especificado, medindo o quanto o software atende as necessidades do cliente. A figura 10 demonstra a relação dos requisitos e da qualidade do produto no ciclo de vida do software.

O autor divide o modelo de qualidade interna e externa

Figura 10 – *Qualidade no ciclo de vida do software*

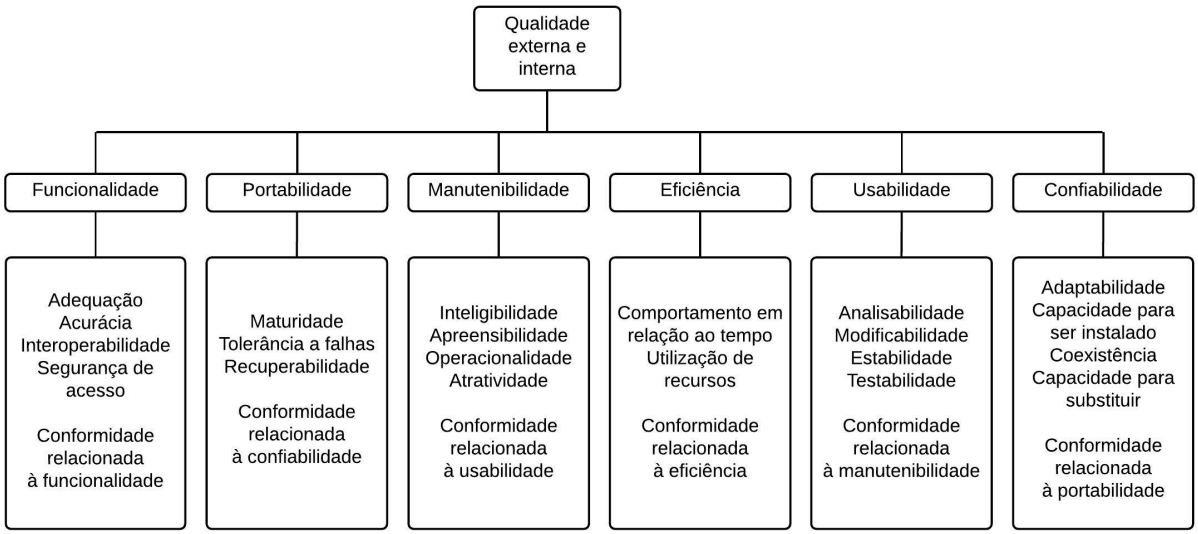


Fonte: Associação Brasileira de Normas Técnicas, 2003 [9]

em seis características: funcionalidade, confiabilidade, usabilidade, eficiência, manutenibilidade e portabilidade. Estas características por sua vez são divididas em subcaracterísticas conforme exibe a figura 11.

A figura 12 descreve o modelo de qualidade para qualidade em uso, dividindo-o em quatro características: eficácia, produtividade, segurança e satisfação. A qualidade em uso representa a qualidade do produto do ponto de vista do usuário e é medida com base na resposta do uso em seu ambiente e não por testes dos componentes do software. Também está diretamente relacionada à qualidade externa que por sua vez está ligada a qualidade interna do produto de software. [9]

Figura 11 – *Modelo de qualidade para qualidade interna e externa*



Fonte: Associação Brasileira de Normas Técnicas, 2003 [9]

Figura 12 – *Modelo de qualidade para qualidade em uso*

Fonte: Associação Brasileira de Normas Técnicas, 2003 [9]

2.6 Considerações do capítulo

Este capítulo descreveu aplicações corporativas, seus diferentes tipos, arquitetura de software, seus estilos e padrões arquiteturais e os requisitos de qualidade de software definidos pela ABNT

(2003). [9]

Com base nestes conhecimentos o próximo capítulo propõe uma arquitetura de software para atender a comunicação entre dispositivos móveis e sistemas da área de saúde.

Capítulo 3

Padrão arquitetural

Este capítulo apresenta a proposta de arquitetura de software para atender os requisitos funcionais e não funcionais de um Sistema de Registro Eletrônico em Saúde (S-RES).

3.1 Informática em Saúde

De acordo com a SBIS (Sociedade Brasileira de Informática em Saúde) nas últimas décadas houve uma grande evolução da tecnologia na saúde, um caminho sem volta, na informatização de processos antes controlados por papel que agora são armazenados em registros eletrônicos. As características específicas da área da saúde a tornam única, com ênfase na privacidade, confidencialidade, segurança e integridade das informações dos pacientes assistidos. [5]

Para os autores Cavalcante e Pinheiro (2011) os sistemas de informação em saúde apoiam a gestão estratégica na área da saúde, auxiliando a organização administrativa e clínica nas consultas, na coleta, no armazenamento e no processamento das informações do paciente e também no diagnóstico, prescrição de medicamentos e

todos os cuidados que envolvem o paciente. [10]

Segundo a SBIS o crescimento da utilização da tecnologia da informação na saúde é creditado à evolução tecnológica e a falta de capacidade de gerenciar todo conhecimento médico e as informações sobre os pacientes em processos utilizando o papel. Os processos de acesso à informação e de auxílio na tomada de decisão exercem um papel central na medicina moderna. [11]

3.1.1 Certificação para Sistemas de Registro Eletrônico em Saúde

Para a SBIS o crescimento da utilização de informática na área de saúde vem crescendo de forma irreversível e trazendo diversas vantagens, com isso para garantir a legalidade de sistemas que capturam, armazenam, processam, imprimam e transmitam dados do atendimento em saúde, em conjunto com o CFM (Conselho Federal de Medicina) a SBIS elaborou um manual de certificação para sistemas de registro eletrônico em saúde (S-RES) com requisitos de segurança, estrutura, conteúdo e funcionalidades.

A SBIS define o S-RES como um sistema que captura, armazena, processa, exibe, imprime e transmite de forma segura, completa e integra informações em saúde. A certificação segmenta os S-RES nas categorias básica ou ambulatorial. Sendo a categoria básica o sistema focado em assistência de indivíduos de forma básica e genérica, como por exemplo, automação de consultórios

clínicos. São definidos como ambulatorial o sistema focado em assistência ambulatorial como a parte ambulatorial de sistemas hospitalares ou sistemas integrados de informação em saúde.

A certificação prevê requisitos de segurança para o S-RES, estes requisitos são segmentados em duas categorias NGS1 (Nível de Garantia de Segurança 1) e NGS2 (Nível de Garantia de Segurança 2). Onde o NGS1 atende a S-RES que não pretendem eliminar a impressão de registros de saúde e o NGS2 foca em S-RES que viabilizam a eliminação do papel no armazenamento dos registros em saúde. O NGS2 engloba todos os requisitos do NGS1 da mesma forma que a categoria ambulatorial inclui a básica. [5]

Conforme definido pela SBIS a lista de requisitos que está detalhada no anexo A é composta por:

- Requisitos do Nível de Garantia de Segurança 1 (NGS1):
  - NGS1.01 - Controle de versão do software
  - NGS1.02 - Identificação e autenticação de pessoas
  - NGS1.03 - Controle de sessão de usuário
  - NGS1.04 - Autorização e controle de acesso de pessoas
  - NGS1.05 - Disponibilidade do RES
  - NGS1.06 - Componentes distribuídos
  - NGS1.07 - Segurança de Dados

    - NGS1.08 - Auditoria
    - NGS1.09 - Documentação
    - NGS1.10 - Tempo
    - NGS1.11 - Notificação de Ocorrências
    - NGS1.12 - Privacidade
    - NGS1.13 - Certificado Digital
    - NGS1.14 - Autenticação de usuário utilizando certificado digital
- Requisitos do Nível de Garantia de Segurança 2 (NGS2)
    - NGS2.02 - Assinatura Digital
    - NGS2.04 - Digitalização de Documentos
    - NGS2.05 - Carimbo de tempo
    - NGS2.06 - Certificado de atributo
    - NGS2.07 - Impressão de Registro Assinado Digitalmente
- Requisitos de Estrutura e Conteúdo
    - ESTR.01 - Estrutura do RES
    - ESTR.02 - Dados estruturados
    - ESTR.03 - Dados Administrativos
    - ESTR.04 - Dados clínicos
    - ESTR.05 - Tipos de dados

  - ESTR.07 - Dados contextuais
  - ESTR.08 - Associações
  - ESTR.09 - Representação de conceitos
  - ESTR.10 - Representação de texto
- Requisitos de Funcionalidades
  - FUNC.01 - Suporte aos processos de atenção
  - FUNC.02 - Problemas / condições de saúde e outras questões
  - FUNC.03 - Raciocínio Clínico
  - FUNC.04 - Suporte à decisão, protocolos clínicos e alertas
  - FUNC.05 - Gerenciamento de status
  - FUNC.06 - Prescrição e processamento de exames, investigações e solicitações
  - FUNC.07 - Assistência integral
  - FUNC.08 - Garantia de qualidade
  - FUNC.09 - Captura de dados
  - FUNC.11 - Apresentação dos dados
  - FUNC.12 - Escalabilidade e performance
  - FUNC.13 - Protocolos de mensagens
  - FUNC.14 - Troca de registros
  - FUNC.16 - Consentimento
  - FUNC.17 - Médico-legal

– FUNC.18 - Atores

– FUNC.19 - Competência e governança clínica

– FUNC.20 - Fé Pública

– FUNC.21 - Preservação de contexto

– FUNC.23 - Controle de versão

– FUNC.24 - Ética

– FUNC.25 - Direitos do paciente

– FUNC.27 - Evolução

– FUNC.28 - Acesso

A segurança é um dos principais requisitos de um S-RES, garantindo que somente pessoas autorizadas tenham acesso às informações sigilosas, permitindo a privacidade necessária dos pacientes assistidos.

Visando atender estes requisitos de segurança propostos pela ISO 9126-1 detalhados no capítulo 2.5 e os requisitos propostos pela SBIS descritos no capítulo 3.1.1, será proposta uma arquitetura de software para atender a autenticação e autorização de usuários no S-RES.

3.2 Sistema de Registro Eletrônico em Saúde

O sistema de registro eletrônico em saúde (S-RES) é definido pela SBIS como um sistema com objetivo de capturar, armazenar, manipular, exibir e compartilhar informações sobre a saúde dos pacientes de uma forma eletrônica garantindo a segurança e a integridade da informação. O S-RES pode ser composto por outros componentes, como sistemas gerenciadores de banco de dados (SGBD), sistema de gerenciamento de diretórios, usuários e papeis, por exemplo, Active Directory ou LDAP (Lightweight Directory Access Protocol), para auxiliar com o objetivo principal. [5]

Os usuários do S-RES são profissionais da área da saúde que dão assistência a pacientes como, por exemplo, médicos, enfermeiros, nutricionistas, fisioterapeutas, técnicos de enfermagem e outros profissionais que utilizam o sistema como ferramenta de trabalho auxiliando nos processos de hospitais e clínicas ambulatoriais documentando e garantindo a autenticidade das informações preenchidas por estes profissionais.

3.2.1 Requisitos funcionais

O foco da arquitetura proposta é permitir a utilização do S-RES através de dispositivos móveis, de acordo com os seguintes

requisitos funcionais:

- RF01 - Registrar e apresentar eventos, ocorrências ou episódios ocorridos no cuidado da saúde com paciente
- RF02 - Registrar dados clínicos e histórico de saúde do paciente
- RF03 - Gerenciar profissionais de saúde e suas autorizações no sistema
- RF04 - Apresentar dados clínicos, histórico de saúde e todas as atividades de cuidado do paciente de forma cronológica
- RF05 - Apresentar alertas e avisos sobre alergias, infecções ou dados clínicos relevantes para o profissional de saúde
- RF06 - Garantir o preenchimento de informações obrigatórias dos formulários através de regras de validação
- RF07 - Permitir a prescrição de exames, cuidados e medicamentos por profissionais da saúde
- RF08 - Apresentar os exames e respectivos resultados realizados pelo paciente
- RF09 - Registrar e apresentar a evolução do estado clínico do paciente
- RF10 - Registrar e apresentar procedimentos a serem seguidos pelos profissionais da saúde definidos pela instituição de saúde

- RF11 - Apresentar um sumário clínico do paciente de acordo com a necessidade do profissional
- RF12 - Permitir a comunicação com outros sistemas através de protocolos adotados por ambas as partes, como TISS ou HL7
- RF13 - Garantir a rastreabilidade das informações cadastradas e alteradas com data e profissional autor
- RF14 - Apresentar a lista de pacientes cadastrados
- RF15 - Registrar e apresentar todos os atendimentos realizados ao paciente

3.2.2 Requisitos não funcionais

Os requisitos não funcionais são baseados nos requisitos definidos no NGS1 e Escalabilidade e performance (FUNC.12) do manual de certificação da SBIS, com os seguintes requisitos:

- NGS1.02.01 - Identificação e autenticação de pessoa
- NGS1.02.02 - Método de autenticação de pessoa
- NGS1.02.03 - Proteção dos parâmetros de autenticação
- NGS1.02.04 - Segurança de senhas
- NGS1.02.05 - Controle de tentativas de login

– NGS1.02.06 - Identidade única da pessoa

– NGS1.02.08 - Informações na autenticação

– NGS1.03.01 - Bloqueio ou encerramento por inatividade

– NGS1.03.02 - Segurança contra roubo de sessão de usuário

– NGS1.04.01 - Impedir acesso por pessoas não autorizadas

– NGS1.04.02 - Mecanismo de controle de acesso ao RES

– NGS1.04.05 - Configuração de controle de acesso

– NGS1.04.06 - Concessão de autorizações

– NGS1.06.04 - Segurança da comunicação entre componentes

– NGS1.07.03 - Impedir exclusão e alteração

– NGS1.07.04 - Verificação de integridade dos dados

– NGS1.07.10 - Validação de dados de entrada

– NGS1.12.07 - Restrições para transmissão e exportação de RES

– FUNC.12.01 - Eficiência de processamento

3.2.3 Definição do escopo

Conforme a descrição apresentada sobre S-RES e seus requisitos funcionais e não funcionais propõem-se delimitar o escopo com os seguintes requisitos funcionais:

– RF08 - Apresentar os exames e respectivos resultados realizados pelo paciente

– RF09 - Registrar e apresentar a evolução do estado clínico do paciente

– RF14 - Apresentar a lista de pacientes cadastrados

– RF15 - Registrar e apresentar todos atendimentos realizados ao paciente

– RF16 - Visualizar e registrar informações utilizando um dispositivo móvel

Para alcançar o objetivo proposto os requisitos não funcionais atendidos serão:

– NGS1.02.01 - Identificação e autenticação de pessoa

– NGS1.02.02 - Método de autenticação de pessoa

– NGS1.02.03 - Proteção dos parâmetros de autenticação

– NGS1.02.04 - Segurança de senhas

– NGS1.02.05 - Controle de tentativas de login

– NGS1.02.06 - Identidade única da pessoa

– NGS1.07.10 - Validação de dados de entrada

– FUNC.12.01 - Eficiência de processamento

Este escopo delimitado de requisitos tem como objetivo servir como base para o projeto arquitetural proposto que caso implementado permitirá um profissional de saúde realizar autenticação no sistema, consultar os pacientes, consultar todos os atendimentos realizados ao paciente, consultar os exames e resultados, registrar e visualizar a evolução clínica destes pacientes em uma instituição de saúde utilizando um dispositivo móvel.

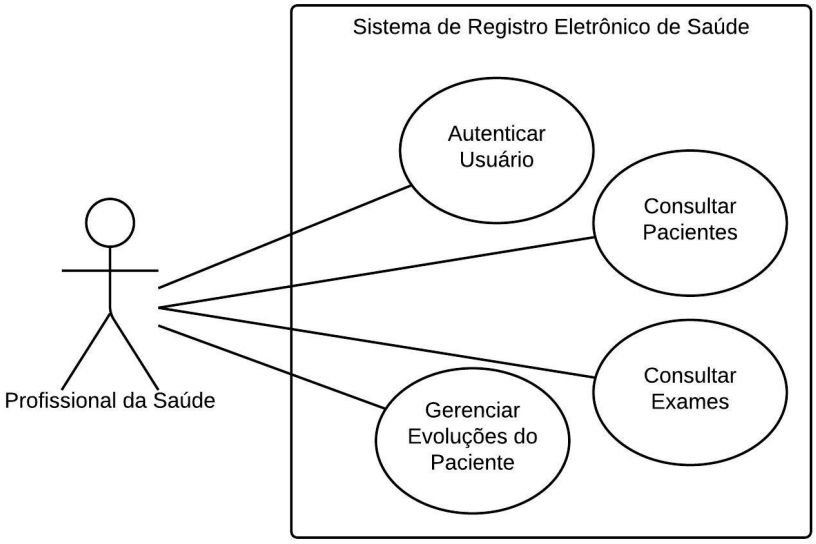
3.3 Projeto Arquitetural

Com base nas arquiteturas, estilos e padrões arquiteturais analisados e no escopo definido propõe-se um projeto arquitetural com as funcionalidades de autenticar o usuário, consultar pacientes, seus atendimentos, exames e gerenciar sua evolução clínica conforme descreve a figura 13.

Para alcançar o objetivo proposto serão utilizados os padrões arquiteturais cliente-servidor com multicamadas e agentes móveis em conjunto para um sistema utilizado em dispositivos móveis. A figura 14 exibe este projeto arquitetural.

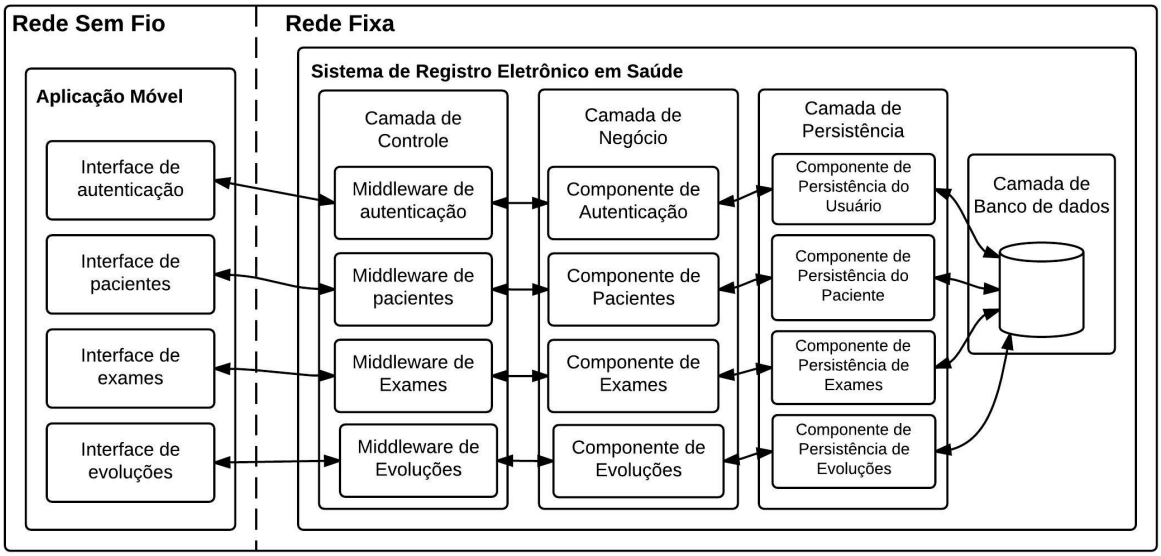
A camada de interface é responsável por capturar os dados fornecidos pelo usuário e enviá-los a camada de controle, ao respectivo *middleware*, após uma validação dos dados fornecidos, como por exemplo, preenchimento de campos obrigatórios de um

Figura 13 – *Diagrama de caso de uso*



Fonte: Elaborado pelo autor

Figura 14 – *Modelo do projeto arquitetural*



Fonte: Elaborado pelo autor

formulário e ao final do processamento apresentar a resposta ao usuário. A camada de interface é executada no dispositivo móvel através de um navegador de internet que interpreta HTML (*Hyper-Text Markup Language*) e JavaScript para manipulação e exibição das informações para os usuários e a validação dos dados fornecidos é executada utilizando JavaScript. Toda comunicação entre as camadas de interface e controle é realizada através do protocolo de comunicação HTTPS (*Hyper Text Transfer Protocol Secure*) onde os dados transmitidos são criptografados e a estrutura de dados utilizada na troca de mensagens será o JSON (JavaScript Object Notation).

As camadas de controle, negócio e persistência serão desenvolvidas utilizando a linguagem de programação orientada a objetos C#, auxiliando no tempo de desenvolvimento e com subcomponentes já nativos da linguagem como conversão para estrutura de dados JSON ou componentes de comunicação com banco de dados Microsoft SQL Server também nativa.

Os *middlewares* na camada de controle são responsáveis por intermediar a comunicação entre as camadas de interface e a camada de negócios, mas também por controlar as quantidades de tentativas de acesso, validar as informações de entrada recebidas pela camada de interface no dispositivo móvel e retornar o resultado da solicitado para interface após o processamento da camada de

negócios. Desta maneira, isolando e restringindo o acesso a camada de negócio, onde estão as regras de negócio e assim aumentando a segurança dos componentes de maior criticidade em camadas internas.

Os componentes da camada de negócio, após receber os dados da camada de controle, são responsáveis pelas validações, processamentos de acordo com as regras de negócio, solicitar e enviar dados para camada de persistência, processar o retorno destas informações e responder a camada de controle com as informações para exibição na interface. Nesta camada, cada componente possui suas responsabilidades de acordo com os requisitos funcionais e não funcionais, onde no componente de autenticação as responsabilidades são criptografar os dados de senha, verificar autenticidade da pessoa solicitante através de usuário único e senha, garantir a periodicidade da troca de senha e garantir o não acesso de pessoas não autorizadas, como por exemplo, usuários inativos, não cadastrados ou com informações erradas.

O componente de evoluções do paciente é responsável por validar a integridade dos dados recebidos e encaminhar ao componente de persistência de evoluções para armazená-los ou também para consultá-los caso solicitado pelo usuário. Nos componentes de exames e pacientes seguem o mesmo caminho solicitando dados a camada de persistência de acordo com os filtros escolhidos pelo

usuário e processa essas informações antes de retornar a camada de controle.

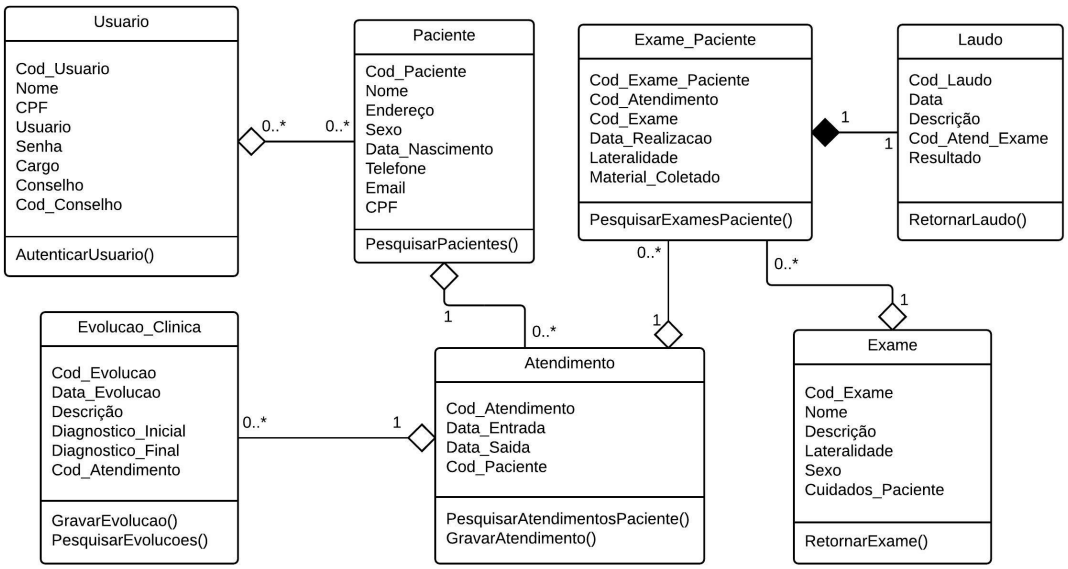
Os componentes da camada de persistência são responsáveis por recuperar e enviar as informações na camada de banco de dados e retornar a camada de negócio conforme as informações recebidas. A comunicação com o banco de dados é realizada utilizando o driver nativo do C# para o banco de dados Microsoft SQL Server.

Na camada de banco de dados está a responsabilidade de armazenar todas as informações do sistema utilizando um SGBD (Sistema Gerenciador de Banco de Dados) Microsoft SQL Server. O banco de dados mesmo sendo uma parte do sistema pode ser distribuído em um ou diversos computadores, conforme a necessidade de escalabilidade e desempenho desejado para o S-RES.

Baseado no escopo definido e projeto arquitetural proposto a figura 15 descreve as entidades e o relacionamento entre elas.

Cada usuário do sistema pode atender diversos pacientes e o paciente pode ser assistido por diversos usuários, estes pacientes podem ser atendidos diversas vezes na mesma instituição de saúde, onde cada atendimento tem sua data de início e fim e possuí exames e evoluções de pacientes atrelados. O Exame possui uma entidade onde armazena informações como nome, descrição, em quais os lados do corpo e em quais sexos podem ser realizados, se necessário, para evitar duplicidade de informações em cada exame

Figura 15 – *Diagrama de classes*



Fonte: Elaborado pelo autor

realizado pelo paciente. A entidade de laudos está fortemente ligada ao exame realizado pelo paciente, armazenando o resultado e descrições após conclusão da análise do material coletado.

3.3.1 Decisões arquiteturais

Para auxiliar nas decisões tomadas referente ao projeto arquitetural será utilizado o questionário apresentado no capítulo 2.4 proposto por Sommerville (2011):

a. Pode-se utilizar uma arquitetura genérica?

Para atender os requisitos não funcionais é necessária a adaptação dos padrões arquiteturais cliente-servidor multicamadas em conjunto com *middlewares* e não utilizar somente uma arquitetura

genérica.

b. Como será a distribuição do sistema pelos núcleos ou processadores?

A camada de interface com o usuário será executada no dispositivo móvel do próprio usuário, já o sistema com as camadas de controle, negócio e persistência será hospedado em um ou diversos servidores, onde uma ferramenta de controle de carga pode direcionar as requisições para os servidores com menor utilização. Também é possível hospedar a camada de banco de dados em um único servidor ou em diversos servidores distribuídos com ferramentas de replicação disponibilizadas pelo Microsoft SQL Server para manter a integridade dos dados armazenados. Distribuir o sistema e o SGBD em diversos servidores permite aumentar a escalabilidade e o desempenho do sistema, esta decisão pode ser tomada de acordo com a qualidade de uso percebida na fase de testes ou após a implantação.

c. Quais estilos ou padrões podem ser utilizados?

Adotou-se o padrão arquitetural cliente-servidor multicamadas onde o sistema recebe requisições de clientes em diferentes locais através da rede sem fio, o que permite distribuir o servidor em diversos computadores e o cliente entende o servidor como um único sistema coeso independente da quantidade de computadores que o hospede. Cada camada do sistema possui sua responsabili-

dade, facilitando a manutenção, onde alterações de menor impacto serão realizadas somente em uma camada, por exemplo, uma mudança de interface pode não interferir na camada de negócio. O projeto arquitetural também se baseou no padrão arquitetural de agentes móveis, bem difundido para utilização com dispositivos móveis. Onde há diversos *middlewares* cada um responsável por um grupo de operações diferentes que recebem a requisição do cliente e após o processamento retornam os dados de resposta.

d. Qual a abordagem fundamental para estruturar o sistema?

Atender os requisitos funcionais e não funcionais do escopo definido de um S-RES, que é um sistema de informação da área da saúde com diversas particularidades e necessidades.

e. Como os componentes serão segmentados em subcomponentes?

O componente que centralizar uma quantidade muito grande de operações sem o mesmo objetivo será segmentado em subcomponentes agrupando as operações semelhantes em um único local.

f. Como serão controlados os componentes?

Contendo um conjunto de operações bem definidas o controle do componente será feito pelo componente solicitante, como por exemplo, a camada de interface aguardando o resultado do

processamento de uma requisição enviada ao *middleware*.

g. Qual a melhor arquitetura para atender os requisitos não funcionais?

A arquitetura em camadas é proposta para atender os requisitos não funcionais mantendo os componentes com regras de negócio nas camadas mais internas, assim provendo maior segurança. E, ao possibilitar segmentar as responsabilidades e o papel de cada camada auxilia nos testes, na manutenção e na administração do sistema. Esta arquitetura também permite distribuir as camadas em diferentes computadores com foco na escalabilidade e desempenho do sistema.

3.4 Considerações do capítulo

Este capítulo descreveu um S-RES, sua importância na área da saúde e seus requisitos funcionais e não funcionais, baseado nessa definição e nos assuntos abordados no capítulo anterior delimitou-se um escopo para propor um projeto arquitetural que atendesse os requisitos funcionais e não funcionais.

Capítulo 4

Análise do projeto arquitetural

De acordo com Sommerville (2011) a arquitetura escolhida e os requisitos não funcionais devem estar fortemente relacionados e de acordo com a criticidade dos requisitos não funcionais são baseadas as decisões para a definição da arquitetura do sistema. Neste sentido, e considerando que os requisitos não funcionais estão relacionados com as características de qualidades do software descritas pela norma ISO 9126-1, para análise do projeto arquitetural proposto serão utilizadas as características de qualidade interna, propostas pela norma: funcionalidade e eficiência e suas respectivas subcaracterísticas segurança de acesso e comportamento em relação ao tempo.

A tabela 1 relaciona os requisitos não funcionais de acordo com o escopo definido para o sistema S-RES com as subcaracterísticas de Segurança de acesso e Comportamento em relação ao tempo definidos pela ISO 9126-1.

Com a adoção do padrão arquitetural cliente-servidor multicamadas as camadas são bem definidas e com suas funções específicas, sem se preocupar com a responsabilidade das demais camadas auxiliando no desenvolvimento, testes e manutenção. Com

Tabela 1 *– Relacionamento dos requisitos não funcionais do S-RES e as características de qualidade da ISO 9126-1*

Requisitos não funcionais	ISO 9126-1	
	Funcionalidade	Eficiência
	Segurança de acesso	Comportamento em relação ao tempo
NGS1.02.01 - Identificação e autenticação de pessoa	X	
NGS1.02.02 - Método de autenticação de pessoas	X	
NGS1.02.03 - Proteção dos parâmetros de autenticação	X	
NGS1.02.04 - Segurança de senhas	X	
NGS1.02.05 - Controle de tentativas de login	X	
NGS1.02.06 - Identidade única da pessoa	X	
NGS1.07.10 - Validação de dados de entrada	X	
FUNC.12.01 - Eficiência de processamento		X

Fonte: Elaborado pelo autor

o padrão arquitetural adotado é possível atender os requisitos não funcionais de Identificação e autenticação de pessoa, Método de autenticação de pessoa, Proteção dos parâmetros de autenticação, Segurança de senhas, Controle de tentativas de login, Identidade única da pessoa e Validação de dados. Como também os respectivos requisitos do modelo de qualidade associados a ISO 9126-1.

Conforme descreve Sommerville (2011), ao manter as regras de negócio com maior necessidade de segurança na camada de negócio, que fica mais interna no sistema, há o aumento da segurança. Ao agrupar as operações semelhantes no mesmo componente auxilia na manutenção e diminui a quantidade de comu-

nicações realizadas entre os componentes o que traz vantagens para o desempenho e a validação. Conforme o projeto de arquitetura proposto para o S-RES a tabela 2 relaciona os requisitos do sistema S-RES com as camadas responsáveis.

Tabela 2 *– Relacionamento requisitos SBIS com as camadas responsáveis*

Requisitos do S-RES	Camada Responsável
RF08 - Apresentar os exames e respectivos resultados realizados pelo paciente	Todas
RF09 - Registrar e apresentar a evolução do estado clínico do paciente	Todas
RF14 - Apresentar a lista de pacientes cadastrados	Todas
RF15 - Registrar e apresentar todos os atendimentos realizados ao paciente	Todas
RF16 - Visualizar e registrar informações utilizando um dispositivo móvel	Todas
NGS1.02.01 - Identificação e autenticação de pessoa	Negócio
NGS1.02.02 - Método de autenticação de pessoas	Negócio
NGS1.02.03 - Proteção dos parâmetros de autenticação	Todas
NGS1.02.04 - Segurança de senhas	Negócio
NGS1.02.05 - Controle de tentativas de login	Controle
NGS1.02.06 - Identidade única da pessoa	Negócio
NGS1.07.10 - Validação de dados de entrada	Interface e Controle
FUNC.12.01 - Eficiência de processamento	Todas

Fonte: Elaborado pelo autor

Todos os requisitos funcionais são vinculados a todas as camadas por conta da interação com todos os componentes do sistema. As consultas realizadas necessitam da camada de interface para fazer a requisição, que passará pela camada de controle para redirecionar para a camada de negócios correta, que solicitará a camada de persistência, que chegará ao banco de dados, responsável por armazenar as informações, retornará os dados e fará o caminho inverso, onde a camada de negócios poderá aplicar regras de negócio específicas e a camada de interface processará os dados e

exibirá de forma amigável ao usuário.

No registro das informações no sistema S-RES a interface é responsável por exibir o formulário, fazer validações dos dados inseridos, como também na camada de controle serão realizadas mais validações, as regras de negócio serão aplicadas na camada de negócio, em seguida as informações passam pela camada de persistência que se comunica com o banco de dados para armazenar as informações inseridas, já validadas e processadas. Após armazenamento dos dados o caminho inverso é feito para sinalizar ao usuário a conclusão da requisição.

A maior parte dos requisitos não funcionais está centralizada na camada de negócios, que também é responsável pelas regras de negócios dos requisitos funcionais. Os requisitos de identificação e autenticação de pessoa, método de autenticação de pessoas, segurança de senhas e identidade única da pessoa são mantidos na camada de negócio para garantir maior segurança em uma camada mais interna do sistema e centralizando em um único componente aumenta a manutenção e testes das funcionalidades relacionadas à autenticação.

Para atender o requisito não funcional de eficiência de processamento o projeto arquitetural permite distribuir as algumas camadas em diferentes servidores. O SGBD pode ser hospedado em diversos servidores conforme a necessidade de desempenho e es-

calabilidade, o próprio SGBD possui ferramentas de replicação dos dados para garantir a consistência da informação independente da instância de banco de dados acessada. O software também pode ser distribuído em diversos servidores, porém necessitará do auxilio de um software que realize o balanceamento da carga, onde o cliente faz requisições para o sistema e o software redirecionará a requisição para os servidores conforme a carga e a quantidade de servidores, porém o cliente entende o sistema de forma coesa e única.

As validações dos dados de entrada são realizadas nas primeiras camadas, interface e controle, desta maneira não são passadas informações inválidas para as camadas de negócio, persistência e banco de dados, assim despendendo tempo e processamento para retornar a inconsistência ao usuário e garantindo que as camadas internas não se preocupem com esta responsabilidade.

A camada de controle é responsável por controlar a quantidade de tentativas de login, também evitando gastar processamento e tempo passando para as demais camadas uma requisição que já excedeu o limite de tentativas.

4.1 Considerações do capítulo

Este capítulo analisou o projeto arquitetural proposto para um S-RES, descrevendo suas vantagens e responsabilidades distribuídas pelas camadas da arquitetura.

Capítulo 5

Considerações Finais

5.1 Contribuições do trabalho

A utilização de dispositivos móveis está em crescimento e com isso surgiram novas necessidades e desafios para as empresas e desenvolvedores. Este trabalho visou descrever um padrão arquitetural para aplicações da área da saúde que utilize um dispositivo móvel como interface para o cliente, facilitando suas atividades diárias e por consequência trazendo vantagens para a empresa.

Este trabalho descreveu a importância da escolha de estilos e padrões arquiteturais e quais as consequências da escolha destes modelos. Na maioria das situações não se pode utilizar uma arquitetura genérica, sendo necessário adequar um ou mais padrões para atender o objetivo proposto. As decisões tomadas na escolha do padrão arquitetural geram consequências sobre todas as etapas seguintes do desenvolvimento, testes, implantação e manutenção do produto de software e para auxiliar no projeto arquitetural do S-RES foi utilizado um questionário proposto por Sommerville (2011), que ajuda a levantar pontos chaves da escolha

do padrão arquitetural.

As decisões tomadas para o projeto arquitetural estão fortemente ligadas aos requisitos não funcionais e a criticidade de cada um, pois ao atender algum plenamente pode ser conflitante atingir o resultado esperado em outro, sendo necessária mudanças arquiteturais ou a definição de prioridades entre os requisitos não funcionais.

Os padrões arquiteturais propostos auxiliaram na superação dos desafios encontrados ao se trabalhar com dispositivos móveis, como a falta de capacidade de armazenamento e processamento, a intermitência da rede sem fio e o acesso a fontes de dados externas. A adoção de agentes móveis permite a comunicação com o S-RES através da rede sem fio assim transferindo somente as informações necessárias para o processamento e o acesso aos dados na rede fixa, mantendo a interface responsável por receber e validar os dados de entrada e apresentar a informação retornada ao final do processamento do servidor.

O padrão arquitetural cliente-servidor multicamadas permitiu que as camadas adotadas no projeto arquitetural tivessem seus papéis e responsabilidades definidos e delimitados, desta forma a implementação de comunicação com outros sistemas ou a utilização de interface em computadores ou dispositivos diferentes necessitará de uma adaptação das camadas de interface e controle, mas pre-

servando as camadas de negócio, persistência e banco de dados, economizando tempo de implementação e mantendo as regras de negócio centralizadas em um único local.

5.2 Trabalhos Futuros

A disseminação de aplicações corporativas que tenham os dispositivos móveis de interface com o cliente está em crescimento nos últimos anos com toda evolução tecnológica dos *smartphones*, neste sentido e utilizando este trabalho como base pode-se evoluir o projeto arquitetural proposto para outras áreas de negócio, diferentes da saúde.

A área da saúde também está em constante evolução tecnológica e os dispositivos móveis são grandes aliados nesta tarefa, para trabalhos futuros sugere-se evoluir o projeto arquitetural proposto para atender todos os requisitos funcionais e não funcionais de um Sistema de Registro Eletrônico em Saúde, que atenda diferentes instituições de saúde e por consequência melhorando o processo de trabalho das mesmas.

Referências

1 RAHAMAN, A.; BAUER, M. A comparison of software architectures for data-oriented mobile applications. *45th Hawaii International Conference on System Sciences*, 2013.

2 SOMMERVILLE, I. *Engenharia de Software*. 9ª. ed. [S.l.]: Pearson Prentice Hall, 2011. ISBN 978-85-7936-108-1.

3 GIESSMANN, A.; STANOEVSKA-SLABEVA, K.; VISSER, B. de. Mobile enterprise applications - current state and future directions. *45th Hawaii International Conference on System Sciences*, p. 1363–1372, 2012.

4 FOWLER, M. *Padrões de arquitetura de aplicações corporativas*. [S.l.]: Bookman, 2006.

5 Sociedade Brasileira de Informática em Saúde. *Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES)*. 2013. Disponível em: <http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2013_v4-1.pdf>.

6 ARAUJO, E. C. D. *Padrões e conceitos de Aplicações Corporativas*. 2013. Disponível em: <http://www.devmedia.com.br/padroes-e-conceitos-de-aplicacoes-corporativas/27569>.

7 PRESSMAN, R. S. *Software engineering: a practitioner's approach*. 7th. ed. [S.l.]: McGraw-Hill, 2011. ISBN 0-07-365578-3.

8 SPYROU, C. et al. Mobile agents for wireless computing: The convergence of wireless computational models with mobile-agent

technologies. *Mobile Networks and Applications Volume 9, Issue 5, October 2004*, 2004. ISSN 1572-8153.

9 Associação Brasileira de Normas Técnicas. NBR ISO/IEC 9126-1: Engenharia de software - Qualidade de Produto. Parte 1: Modelo de qualidade. 2003.

10 CAVALCANTE, R. B.; PINHEIRO, M. M. K. Política nacional de informação e informática em saúde: avanços e limites atuais. 2011. ISSN 2236-417X. Disponível em: <http://periodicos.ufpb.br/ojs2/index.php/pgc/article/view/10487/6893>

11 Sociedade Brasileira de Informática em Saúde. *O que é Informática em Saúde?* Disponível em: <http://www.sbis.org.br/site/site.dll/view?pagina=12>.

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

NGS1.01 - Controle de versão do software

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

NGS1.02 - Identificação e autenticação de pessoas

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

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

NGS1.02.04	Segurança de senhas	Condição: Utilização de autenticação baseada no método de usuário e senha. Utilizar os seguintes controles de segurança: • Qualidade da senha: deve ser verificada a qualidade da senha no momento de sua definição pelo usuário, obrigando a utilização de, no mínimo, 8 caracteres dos quais, no mínimo, 1 caractere deve ser alfabético e 1 numérico; • Periodicidade de troca de senhas: deve ser obrigatória a troca de senhas pelos usuários, em um período máximo configurável (vide ESTR.02.11) que não exceda a 6 meses. • Os processos de troca de senha devem exigir que a nova senha seja diferente da imediatamente anterior. • Quando da geração de senha que não seja definida pelo próprio usuário, tal processo deve impedir sua visualização por terceiros. • Recomenda-se a implementação de técnicas de SALT para a codificação da senha.	M	M
NGS1.02.05	Controle de tentativas de login	Possuir mecanismos para bloquear a conta do usuário após um número máximo configurável (vide ESTR.02.11) de tentativas inválidas de login que não exceda a 10 tentativas.	M	M
NGS1.02.06	Identidade única da pessoa	Toda pessoa usuária do S-RES deve possuir um identificador único. Campos de identificação unívoca devem ser validados para garantir tal unicidade. Para isso, no momento da inclusão ou edição, o sistema deve verificar a existência de duplicidade, comparando os identificadores unívocos deste usuário (ex: RG, CPF, número de identificação profissional, etc) com a base de usuários já existentes. Nota: Caso o S-RES opere na modalidade "S-RESaaS" (S-RES as a Service), a unicidade do identificador da pessoa deve ser por organização.	M	M
NGS1.02.07	Autenticação para operações sensíveis	Toda pessoa usuária deve ser novamente autenticada no momento da realização de operações sensíveis, tais como registro de dados clínicos, troca de senha, delegação de poder, etc.	R	R
NGS1.02.08	Informações na autenticação	Assim que completada uma autenticação de sucesso, o sistema deve exibir à pessoa usuária as seguintes informações: • data e hora da última autenticação com sucesso; • data e hora das tentativas de autenticação sem sucesso depois da última autenticação com sucesso.	M	M

NGS1.03 - Controle de sessão de usuário

ID	Título	Requisito	Local	Remoto
NGS1.03.01	Bloqueio ou encerramento por inatividade	A sessão de usuário deve ser bloqueada ou encerrada após período de inatividade. O período máximo de inatividade deve ser configurável (vide ESTR.02.11) no sistema. Não deve ser possível para o usuário do sistema desativar ou desabilitar tais controles. Nota: No caso de encerramento da sessão, recomenda-se que os dados inseridos e não salvos sejam preservados para reutilização no acesso seguinte.	M	M
NGS1.03.02	Segurança contra roubo de sessão de usuário	A sessão de comunicação remota deve possuir controles de segurança a fim de não permitir o roubo da sessão do usuário. Não deve ser permitido ao usuário desabilitar tais controles. Nota 1: O S-RES não deve ser suscetível a ataques de *replay e covert-channel.* Nota 2: O roubo de sessão pode ser possível inclusive em sessões protegidas (ex. SSL/TLS). Por exemplo, se o controle de sessão for realizado através de *cookie* na URL, em determinadas situações, a URL da sessão de um usuário pode ser obtida e utilizada por outro usuário, personificando o usuário anterior.	X	M

NGS1.04 - Autorização e controle de acesso de pessoas

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

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

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

NGS1.04.08	Acesso ao RES pelo paciente	Garantir que o paciente possa ter acesso a todas as suas informações pessoais e clínicas armazenadas no S-RES. Caso o S-RES não permita acesso direto do próprio paciente, deve existir um papel de usuário que permita realizar esta atividade em nome do paciente. Estas informações poderão ser geradas em formato eletrônico ou impresso. O sistema deverá disponibilizar uma interface para impressão de declaração do usuário (vide FUNC.25.02) de que está recebendo suas informações.	M	M
NGS1.04.10	Gerenciamento de grupos	Permitir o gerenciamento (criação, inativação e modificação) de grupos de usuários, de forma a possibilitar o controle de acesso a dados conforme os grupos aos quais o usuário pertence. Um usuário poderá pertencer a um ou mais grupos.	R	R

NGS1.05 - Disponibilidade do RES

ID	Título	Requisito	Local	Remoto
NGS1.05.01	Cópia de Segurança	O S-RES deve gerar cópia de segurança atendendo aos seguintes requisitos: • exportar os atributos de segurança e metadados em conjunto com os dados; • garantir, na restauração de uma cópia de segurança, que os atributos de segurança e suas associações sejam automaticamente recuperados, sem a intervenção do administrador; • assegurar que somente o usuário com papel de operador de backup possa exportar e restaurar uma cópia de segurança, garantindo que este usuário não tenha acesso direto às informações.	M	M
NGS1.05.02	Integridade na recuperação de dados	Possuir controle que garanta a verificação da integridade das informações na geração e na restauração da cópia de segurança, gerando um alerta caso ocorra alguma falha.	M	M
NGS1.05.03	Alerta de limiar de ocupação	O S-RES deve gerar alerta quando o espaço para armazenamento de registros atingir um limiar de ocupação a fim de possibilitar aos operadores a realização de medidas preventivas.	M	M

NGS1.06 - Componentes distribuídos

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

NGS1.06.04	Segurança da comunicação entre componentes	Em S-RES composto por diversos componentes distribuídos (localizados em computadores diferentes), a comunicação entre tais componentes (como, por exemplo, com o banco de dados) deve oferecer os seguintes serviços de segurança: autenticação de parceiro (ambas as partes), integridade dos dados e confidencialidade dos dados. A segurança pode ser aplicada ao canal de comunicação ou às mensagens trocadas.	X	M
NGS1.06.05	Controle de acesso entre componentes	Em S-RES composto por diversos componentes distribuídos (localizados em computadores diferentes), na comunicação entre tais componentes (como, por exemplo, com o banco de dados), o acesso ao componente deve ser restrito somente aos parceiros (componentes) previamente autorizados.	X	M
NGS1.06.06	Comunicação entre S-RES	Condição: haver troca de dados direta entre S-RES distintos. A comunicação entre S-RES deve oferecer os seguintes serviços de segurança: autenticação de parceiro (ambas as partes) utilizando certificados digitais, integridade dos dados e confidencialidade dos dados.	M	M
NGS1.06.07	Confirmação de entrega	Condição: haver troca de dados direta automática entre sistemas (não via interface). A troca de dados entre S-RES deve possuir controles de confirmação de entrega/recebimento dos dados. Nota: Como exemplo podemos citar o TISS.	M	M
NGS1.06.08	Integridade e origem de componentes dinâmicos	Caso o S-RES utilize componentes que exijam download para sua execução (ex.: ActiveX, Applet, aplicações para tablet, etc), estes devem possuir controle de integridade e possibilidade de verificação da origem (ex.: pelo uso de assinatura digital do componente).	M	M
NGS1.06.09	Método de autenticação de parceiro de comunicação	Deve ser utilizado o método de chaves assimétricas com certificado digital para autenticação de parceiro de comunicação.	R	R

NGS1.07 - Segurança de Dados

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

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

NGS1.08 – Auditoria

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

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

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

NGS1.09 - Documentação

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

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

NGS1.10 - Tempo

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

NGS1.11 – Notificação de Ocorrências

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

NGS1.12 – Privacidade

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

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

NGS1.13 – Certificado Digital

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

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

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

NGS1.14 – Autenticação de usuário utilizando certificado digital

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

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

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

NGS2.02 – Assinatura Digital

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

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

NGS2.02.06	Propósito da assinatura	Incluir, em toda assinatura digital realizada, o propósito da assinatura (atributo *commitment-type-indication*), ou seja, o tipo de comprometimento que o signatário assume no momento de firmar a assinatura digital. O S-RES deve incluir o atributo de propósito de assinatura (atributo *commitment-type-indication)*. O propósito da assinatura deve ser requisitado ao usuário antes da aplicação da assinatura ou ser pré-definido naquela situação. Neste último caso, o S-RES deve informar ao usuário o tipo de propósito que será incluído na assinatura: prova de aprovação ou prova de criação. Quando a assinatura representa o compromisso do signatário com o conteúdo assinado, deve ser utilizado o propósito "prova de aprovação" (*proof of approval*) . [RFC 5126]	R
NGS2.02.07	Visualização das informações a serem assinadas	Permitir a visualização da informação a ser assinada antes da sua assinatura.	M
NGS2.02.08	Homologação ICP-Brasil	Os componentes de um S-RES que utilizam certificação digital para assinatura digital devem estar homologados pela ICP-Brasil.	R
NGS2.02.09	Exportação de registros assinados	Na exportação de registros assinados, utilizar o formato AD-RC (Assinatura Digital com Referências Completas) ou AD-RT (Assinatura Digital com Referências de Tempo), incluindo todos os objetos necessários à validação (certificados dos signatários, cadeias de certificação, dados de revogação, certificados de atributos, etc).	M
NGS2.02.11	Resultado da verificação da assinatura digital	O sistema deve, a qualquer tempo, prover meios para validação e exibição do estado de validade de um documento assinado digitalmente. O resultado da verificação de uma assinatura digital deve retornar um dos seguintes estados: • Válida: assinatura valida; • Inválida: assinatura inválida; • Indeterminada: quando não é possível determinar se a assinatura está válida ou inválida, geralmente devido a falta de objetos críticos (ex: certificado, objeto de revogação, carimbo de tempo, certificado da cadeia, atributos obrigatórios, etc). Exceto para o estado válido, a causa deverá ser indicada.	M
NGS2.02.12	Validação com objeto de revogação ideal	Revalidar o registro assinado com o objeto de revogação obtido após a próxima publicação ("next update") do estado de revogação do certificado pela AC. Caso essa validação indique que a assinatura foi realizada com um certificado revogado: • uma mensagem imediata deve ser enviada aos responsáveis da instituição e do profissional cujo certificado foi revogado; • o registro deve ser colocado na lista de registros pendentes de assinatura.	R

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

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

NGS2.04 – Digitalização de Documentos

Requisitos aplicáveis somente para S-RES da categoria GED.

ID	Título	Requisito	Presença
NGS2.04.01	Assinatura digital do sistema de GED	Todo documento digitalizado deve ser assinado pelo componente de digitalização com certificado digital especificado no NGS2.04.08, com o propósito de garantia de integridade e de indicação de que a imagem assinada foi originada em um processo de digitalização. Este propósito deve ser estabelecido incluindo o atributo assinado "commitment-type-indication" com o propósito genérico "id-cti-ets-proofOfDelivery", enquanto não seja definido um propósito mais específico.	M
NGS2.04.02	Assinatura digital do operador	O operador de digitalização deve assinar digitalmente o documento digitalizado, com certificado ICP-Brasil de acordo com NGS2.01.05, com o propósito de conferência, garantindo a verificação do enquadramento e a qualidade da imagem digitalizada em comparação à original, refazendo o processo de digitalização em casos de imperfeições. Este propósito deve ser estabelecido incluindo o atributo assinado "commitment-type-indication" com o propósito genérico "id-cti-ets-proofOfReceipt", enquanto não seja definido um propósito mais específico. Essa assinatura deve ser aposta como uma contra-assinatura da assinatura do sistema de GED.	M
NGS2.04.03	Assinatura digital do responsável	O responsável deve assinar digitalmente o documento digitalizado, com certificado ICP-Brasil de acordo com NGS2.01.05, com o propósito de criação, garantindo a autenticidade da imagem digitalizada em comparação à original. Este propósito deve ser estabelecido incluindo o atributo assinado "commitment-type-indication" com o propósito genérico "id-cti-ets-proofOfCreation", enquanto não seja definido um propósito mais específico. Essa assinatura deve ser aposta como uma contra-assinatura da assinatura do sistema de GED.	M
NGS2.04.06	Termo de conduta para digitalização	Permitir ao usuário a realização de operações de digitalização somente após a assinatura digital do "Termo de conduta para digitalização" que deve conter requisitos sobre confidencialidade das informações e sobre a responsabilidade do processo.	M
NGS2.04.07	Homologação ICP-Brasil	Os componentes de um S-RES que utilizam certificação digital para autenticação e assinatura digital devem ser homologados pela ICP-Brasil.	R

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

NGS2.05 - Carimbo de tempo

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

NGS2.06 - Certificado de atributo

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

NGS2.07 – Impressão de Registro Assinado Digitalmente

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

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

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

8.4. Requisitos de Estrutura e Conteúdo

ESTR.01 - Estrutura do RES

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

ESTR.02 - Dados estruturados

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

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

ESTR.03 - Dados Administrativos

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

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

ESTR.04 - Dados clínicos

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

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

ESTR.05 - Tipos de dados

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

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

ESTR.07 - Dados contextuais

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

ESTR.08 - Associações

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

ESTR.09 - Representação de conceitos

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

ESTR.10 - Representação de texto

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

8.5. Requisitos de Funcionalidades

FUNC.01 - Suporte aos processos de atenção

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

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

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

FUNC.03 - Raciocínio Clínico

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

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

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

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

FUNC.05 – Gerenciamento de status

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

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

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

FUNC.07 - Assistência integral

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

FUNC.08 - Garantia de qualidade

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

FUNC.09 - Captura de dados

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

FUNC.11 - Apresentação dos dados

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

FUNC.12 - Escalabilidade e performance

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

FUNC.13 - Protocolos de mensagens

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

FUNC.14 - Troca de registros

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

FUNC.16 - Consentimento

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

FUNC.17 - Médico-legal

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

FUNC.18 - Atores

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

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

FUNC.19 - Competência e governança clínica

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

FUNC.20 – Fé Pública

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

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

FUNC.21 - Preservação de contexto

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

FUNC.23 - Controle de versão

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

FUNC.24 - Ética

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

FUNC.25 - Direitos do paciente

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

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

FUNC.27 - Evolução

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

FUNC.28 - Acesso

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