Guia para Validação de Sistemas Computadorizados

Guia nº 33/2020 – versão 1

ANVISA

Agência Nacional de Vigilância Sanitária - Anvisa

2020

Guia para Validação de Sistemas Computadorizados

VIGENTE A PARTIR DE 14/04/2020

Início do período de contribuições: 14/04/2020
Fim do período de contribuições: 12/08/2020

Este Guia expressa o entendimento da Anvisa sobre as melhores práticas com relação a procedimentos, rotinas e métodos considerados adequados ao cumprimento de requisitos técnicos ou administrativos exigidos pelos marcos legislativo e regulatório da Agência.[1]

Trata-se de instrumento regulatório não normativo, de caráter recomendatório e não vinculante, sendo, portanto, possível o uso de abordagens alternativas às proposições aqui dispostas, desde que compatíveis com os requisitos relacionados ao caso concreto. A inobservância ao conteúdo deste documento não caracteriza infração sanitária, nem constitui motivo para indeferimento de petições, desde que atendidos os requisitos exigidos pela legislação.

As recomendações contidas neste Guia produzem efeitos a partir da data de sua publicação no Portal da Anvisa ficam sujeitas ao recebimento de sugestões da sociedade por meio de formulário eletrônico, disponível em https://pesquisa.anvisa.gov.br/index.php/33174?lang=pt-BR.

As contribuições[2] recebidas serão avaliadas e poderão subsidiar a revisão do Guia e a consequente publicação de uma nova versão do documento. Independentemente da decisão da área, será publicada análise geral das contribuições e racional que justifique a revisão ou não do Guia.

[1] Portaria nº 1.741, de 12 de dezembro de 2018, que dispõe sobre as diretrizes e os procedimentos para melhoria da qualidade regulatória na Agência Nacional de Vigilância Sanitária (Anvisa).

[2] A fim de garantir maior transparência ao processo de elaboração dos instrumentos regulatórios editados pela Anvisa, esclarecemos que os nomes dos responsáveis pelas contribuições (pessoas físicas e jurídicas) são considerados informações públicas e serão disponibilizados de forma irrestrita nos relatórios e outros documentos gerados a partir dos resultados deste Guia. Já o e-mail e o CPF dos participantes, considerados informações sigilosas, terão seu acesso restrito aos agentes públicos legalmente autorizados e às pessoas a que se referem tais informações, conforme preconiza o artigo 31, §1º, inciso I da Lei nº 12.527, de 18 de novembro de 2011. Outras informações que venham a ser consideradas sigilosas pelos participantes poderão ser apensadas em campo específico no formulário eletrônico.

SUMÁRIO

1. ESCOPO

O objetivo deste guia é a proposição de diretrizes que ajudem na obtenção, por parte do setor regulado, de sistemas computadorizados corretamente instalados e validados e que atendam aos requisitos regulatórios.

Este Guia é aplicável aos sistemas computadorizados utilizados nas áreas, equipamentos e demais atividades relevantes às Boas Práticas de Fabricação de Insumos e Medicamentos. A proposta é internalizar o documento GAMP 5 de modo a facilitar a compreensão do leitor acerca das diretrizes propostas por aquele guia internacional.

Fazem parte do escopo deste Guia os sistemas computadorizados categorias 3, 4 e 5, as *interfaces* entre sistemas e planilhas.

Estão abrangidos os sistemas acima mencionados, instalados em arquitetura *stand-alone* ou rede, podendo esta rede ser instalada de modo local, nacional ou global.

Este guia substitui o guia homônimo publicado por esta Agência em abril de 2010.

2. INTRODUÇÃO

Se a empresa regulada decidir pela utilização deste Guia é recomendado que sua implantação seja efetuada em sua totalidade (no que for aplicável) e não parcialmente, pois todas as atividades descritas neste documento são necessárias conjuntamente para a realização de uma sequência adequada de aquisição, validação, operacionalização e finalmente aposentadoria do sistema computadorizado, especialmente para sistemas mais complexos.

3. BASE LEGAL

- Resolução – RDC nº 69 de 08 de dezembro de 2014 – que dispõe sobre as Boas Práticas de Fabricação de Insumos Farmacêuticos Ativos;
- Resolução – RDC nº 301, de 21 de agosto de 2019 – que dispõe sobre as Diretrizes Gerais de Boas Práticas de Fabricação de Medicamentos;
- Instrução Normativa – IN nº 43, de 21 de agosto de 2019 – que dispõe sobre as Boas Práticas de Fabricação complementares aos sistemas computadorizados utilizados na fabricação de Medicamentos;
- Instrução Normativa – IN nº 47, de 21 de agosto de 2019 – que dispõe sobre as Boas Práticas de Fabricação complementares às atividades de qualificação e validação

4. CONCEITOS, TERMOS E DEFINIÇÕES

4.1 CONCEITOS-CHAVE

4.1.1 Entendimento do Processo e do Produto

O entendimento do processo a ser automatizado/informatizado (ex.: gerenciamento de materiais; gerenciamento de documento; gerenciamento de registros analíticos etc.) é fundamental na definição dos

requisitos do sistema. O entendimento do processo e do produto é a base para a tomada de decisões com base em ciência e risco de modo a assegurar que o sistema é adequado ao uso pretendido.

Os esforços para assegurar a adequação ao uso pretendido devem se concentrar naqueles aspectos que são críticos para a segurança do paciente, qualidade do produto e integridade dos dados. Estes aspectos críticos devem ser identificados, especificados e verificados.

Para alguns sistemas utilizados na fabricação, os requisitos de processo dependem de um completo entendimento das características do produto. Para estes sistemas, a identificação dos Atributos Críticos de Qualidade (ACQ) e dos Parâmetros Críticos de Processo associados permitem que os requisitos de controle de processos sejam definidos.

A especificação dos requisitos deve focar nos aspectos críticos. A extensão e os detalhes da especificação do requisito devem ser comensurados com o risco associado, a complexidade e a inovação do sistema.

O entendimento incompleto do processo dificulta o atendimento efetivo e eficiente do benefício do sistema computadorizado ao negócio.

4.1.2 Abordagem do Ciclo de Vida dentro do Sistema de Gerenciamento da Qualidade (SGQ)

Implica na realização de atividades de modo sistemático desde a concepção até a aposentadoria do sistema, permitindo um gerenciamento e uma abordagem consistente para todos os sistemas.

À medida que é adquirido um conhecimento maior do sistema durante a sua utilização, o Sistema de Gerenciamento da Qualidade (SGQ) deve permitir a melhoria contínua do processo e do sistema, baseada em revisões periódicas e avaliações dos dados operacionais e de desempenho e em análises das causas-raiz de falhas ocorridas. Melhorias identificadas e ações corretivas tomadas devem seguir gerenciamento de mudanças.

Uma abordagem apropriada de ciclo de vida permite a garantia da qualidade e da adequação ao uso pretendido do sistema, além da obtenção e manutenção do atendimento aos requisitos regulatórios.

4.1.3 Atividades Escalonáveis do Ciclo de Vida

As atividades do ciclo de vida devem ser escalonadas de acordo com:

- O impacto do sistema na segurança do paciente, na qualidade do produto e na integridade de dados (avaliação de risco);
- A complexidade do sistema e sua inovação (arquitetura e categorização dos componentes do sistema);
- O resultado da avaliação do fornecedor (capabilidade);
- O impacto do sistema nos negócios (também pode motivar o escalonamento).

A estratégia de escalonamento deve ser claramente definida em um plano e seguir políticas e procedimentos estabelecidos e aprovados.

4.1.4 Gestão de Risco de Qualidade Baseada em Ciência

O gerenciamento do risco à qualidade é um processo sistemático para avaliação, controle, comunicação e revisão dos riscos. A sua aplicação permite que esforços sejam concentrados nos aspectos críticos de um sistema computadorizado de uma maneira controlada e justificada.

O gerenciamento do risco à qualidade deve ser baseado em um entendimento claro do processo e do impacto potencial à segurança do paciente, à qualidade do produto e à integridade dos dados. Para os sistemas que controlam ou monitoram os Parâmetros Críticos de Processo, estes devem ser rastreáveis aos Atributos Críticos de Qualidade e às submissões regulatórias dos sistemas de fabricação.

Técnicas quantitativas e qualitativas podem ser utilizadas para identificar e gerenciar riscos. Controles e medidas de mitigação são desenvolvidos para reduzir riscos a um nível aceitável. Os controles implantados devem ser monitorados durante a operação cotidiana para assegurar efetividade contínua.

4.1.5 Aproveitamento do Envolvimento do Fornecedor

As empresas do setor regulado devem buscar maximizar o envolvimento do fornecedor por todo o ciclo de vida do sistema, caso este possua avaliação satisfatória, com o propósito de se utilizar o seu conhecimento, experiência e sua documentação.

O fornecedor pode auxiliar na determinação dos requisitos do usuário, nas avaliações de risco, na criação das especificações funcionais e outras, na configuração do sistema, na realização dos testes, no suporte e na manutenção do sistema.

O planejamento deve determinar como utilizar a documentação do fornecedor, incluindo a documentação de testes, para evitar desperdício de esforços e duplicidade. A justificativa para a utilização desta documentação deve ser baseada na sua avaliação satisfatória do fornecedor, que pode incluir a realização de auditorias *in loco*.

Essa documentação deve ser avaliada quanto a sua adequabilidade, exatidão e abrangência e ficar disponível durante o ciclo de vida do sistema.

4.2 TERMOS-CHAVE

4.2.1 Atendimento às BPx

Atendimento a todos os requisitos regulatórios farmacêuticos e associados à ciência da vida.

4.2.2 Dono do Processo (*Process Owner*)

O dono do processo é o responsável por assegurar que o sistema computadorizado e sua operação estejam conformes e adequados para o uso pretendido de acordo com procedimentos operacionais padrão (POP) por todo o seu ciclo de vida. É o indivíduo responsável pelo processo de negócio ou processos gerenciados. Esta pessoa pode ser o chefe da unidade ou departamento que utiliza o sistema, mas a responsabilidade deve ser baseada principalmente em conhecimento específico do processo ao invés da posição na organização.

4.2.3 Dono do Sistema (*System Owner*)

É o indivíduo responsável pela disponibilidade, suporte e manutenção de um sistema computadorizado, bem como a segurança dos dados mantidos neste sistema. Geralmente é o chefe do departamento responsável pelo suporte e manutenção do sistema, sendo que o papel deve ser baseado em conhecimento específico do sistema

ao invés da posição na organização. O dono do sistema é o responsável por assegurar que o sistema tenha suporte e manutenção de acordo com procedimentos aplicáveis.

NOTA: A responsabilidade pelo controle de acesso ao sistema deve ser acordada entre o dono do processo e o dono do sistema. Em algumas situações o dono do processo pode ser também o dono do sistema.

A propriedade dos dados mantidos no sistema deve ser definida e normalmente pertence ao dono do processo.

4.2.4 Especialista no Assunto (*Subject Matter Expert*)

É o indivíduo com conhecimento profundo em uma área ou campo específico (cromatografia, gerenciamento de materiais, processo de fabricação etc.). As responsabilidades do especialista incluem planejamento e a definição da estratégia de verificação, definição dos critérios de aceitação, seleção dos métodos apropriados, execução dos testes de verificação e revisão dos resultados obtidos nos testes.

4.2.5 Regulamentos BPx

Os requisitos internacionais farmacêuticos, tais como aqueles estabelecidos pela ANVISA, FDA, Diretivas Europeias, regulações Japonesas e outras legislações nacionais aplicáveis ou regulações internas das próprias empresas.

Os regulamentos BPX incluem, mas não são limitados à: BPF; BPC; BPL; BPD; Boas Práticas de Qualidade; Boas Práticas de Farmacovigilância e Regulações de Produtos Médicos.

4.2.6 Sistema de Gerenciamento da Qualidade

Sistema de gerenciamento para direcionar e controlar uma organização com respeito à qualidade.

4.2.7 Sistema Computadorizado

Um sistema computadorizado consiste em: *hardware*, *software* e nos componentes de rede, juntamente com as funções controladas e documentação associada. A figura 1 apresenta uma representação esquemática de um sistema computadorizado.

4.2.8 Sistema Computadorizado Atendendo às BPx

Sistemas computadorizados sujeitos aos regulamentos BPx. A companhia regulada deve assegurar que tais sistemas atendam às regulações apropriadas.

4.2.9 Validação de Sistemas Computadorizados

Obtenção e manutenção do atendimento às regulações aplicáveis de BPx e sua adequação ao uso pretendido por meio do uso de:

- Adoção de princípios, abordagens e atividades do ciclo de vida dentro da estrutura dos planos e relatórios de validação;
- A aplicação de controles operacionais apropriados por todo o ciclo de vida do sistema.

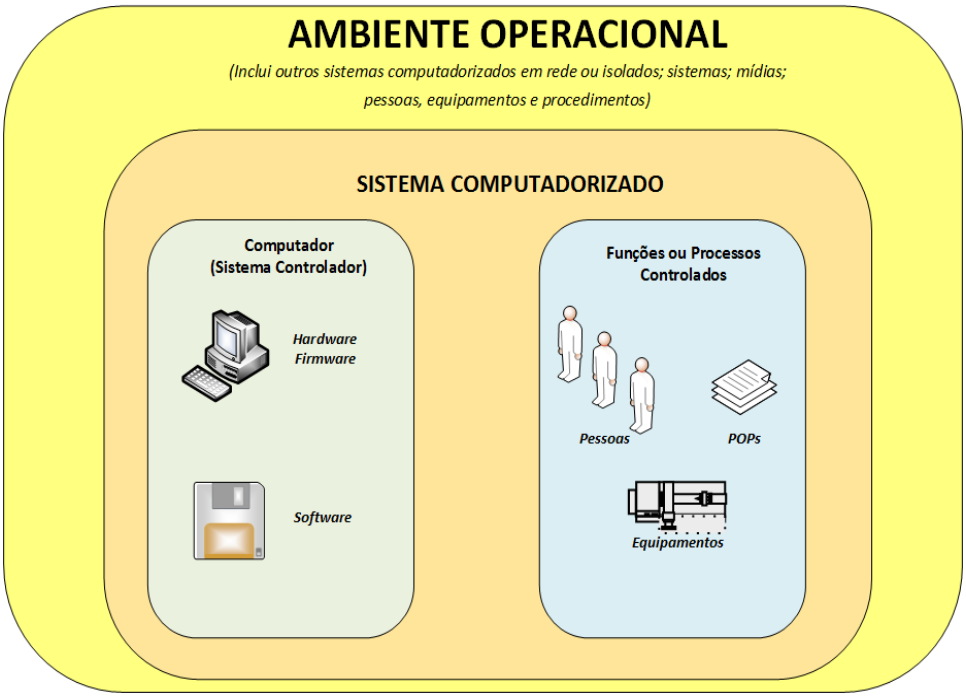

Figura 1. Sistema Computadorizado.

Fonte: PIC/S Good Practices for Computerised Systems in Regulated "GxP" Environments (PI 011).

5. ABORDAGEM DO CICLO DE VIDA

5.1 INTRODUÇÃO

O atendimento aos requisitos regulatórios e a adequação ao uso pretendido podem ser obtidos adotando-se uma abordagem de ciclo de vida seguindo as Boas Práticas.

Uma abordagem de ciclo de vida implica em definir e realizar atividades de modo sistemático a partir da concepção, entendimento dos requisitos desde o desenvolvimento, liberação e uso operacional, até a aposentadoria do sistema.

Nesta seção do guia são apresentados: o ciclo de vida do sistema computadorizado, uma abordagem geral para especificação e verificação e uma estrutura para a validação de um sistema computadorizado.

Uma parte importante da implantação da abordagem do ciclo de vida para os sistemas computadorizados é a definição, por parte da empresa regulada, dos funcionários que irão exercer os papéis de Dono do Processo, Dono do Sistema e de Especialista no Assunto, para cada um dos sistemas instalados na empresa.

O entendimento e a qualificação dos funcionários escolhidos das/nas respectivas funções são a pedra fundamental para que todos os sistemas computadorizados sejam adequadamente escolhidos, validados, operacionalizados e aposentados, atendendo às BPF pertinentes e às demandas regulatórias.

5.2 CICLO DE VIDA DE SISTEMAS COMPUTADORIZADOS

O ciclo de vida de um sistema computadorizado abrange todas as atividades desde o conceito inicial até a aposentadoria.

O ciclo de vida de qualquer sistema consiste em quatro fases:

- Conceito
- Projeto
- Operação
- Aposentadoria

Um inventário de sistemas computadorizados deve ser mantido. Uma avaliação do impacto nas BPx deve ser realizada no início da fase de projeto para determinar se um sistema é regulado pelas BPX, e em caso positivo, que regulações específicas são aplicáveis. Isto deve ser realizado como parte da avaliação de risco inicial do sistema. Para sistemas similares, pode ser apropriado basear a avaliação BPx nos resultados de uma avaliação anterior, contanto que empresa regulada tenha um procedimento estabelecido para tal atividade.

5.2.1 Conceito

Durante a fase de conceito, a companhia regulada considera a oportunidade de automatizar um ou mais processos com base em necessidades e benefícios ao negócio. Normalmente nesta fase os requisitos iniciais são desenvolvidos e soluções potenciais são consideradas. A partir de um entendimento inicial do escopo, dos custos e benefícios, uma decisão é tomada sobre o andamento da fase de projeto. É a etapa na qual a empresa toma a decisão de mudar uma atividade realizada de modo manual por um sistema computadorizado.

5.2.2 Projeto

A fase de projeto envolve o planejamento, a avaliação e seleção do fornecedor, os vários níveis de especificação, a configuração (ou codificação para as aplicações customizadas) e verificação que leva à aceitação e liberação para operação. O gerenciamento de risco é aplicado para se identificar os riscos e para removê-los ou reduzi-los a um nível aceitável.

Esta fase abrange as atividades de definição dos requisitos do usuário, com base na decisão tomada na fase de conceito, seguida da avaliação e seleção do fornecedor para aquisição do sistema, com consequente instalação e validação do sistema computadorizado pela empresa regulada. **Em resumo, nesta etapa são realizadas as atividades de aquisição e validação do sistema computadorizado.**

5.2.3 Operação

Esta normalmente é a fase mais longa e é gerenciada pelo uso de procedimentos operacionais definidos e atualizados por pessoas que foram adequadamente treinadas, instruídas e experientes. **Esta fase equivale na prática ao tempo de utilização do sistema computadorizado validado pela empresa regulada**. A manutenção do controle (incluindo segurança), da adequação do uso pretendido e do atendimento às BPx são aspectos-chave. O gerenciamento das mudanças de diferentes impactos, escopo e complexidade é uma atividade importante durante esta fase.

5.2.3 Aposentadoria

É a fase final do ciclo de vida do sistema computadorizado. **Como o próprio nome diz: o sistema é aposentado.** Envolve decisões sobre retenção, migração ou destruição dos dados e o gerenciamento destes processos.

Os fornecedores de produtos e serviços devem ser envolvidos, quando apropriado, por todo o ciclo de vida. Pode ser apropriado delegar muitas das atividades descritas para os fornecedores, se a sua avaliação for satisfatória e houver medidas de controle. As fases do ciclo de vida são mostradas na figura 2.

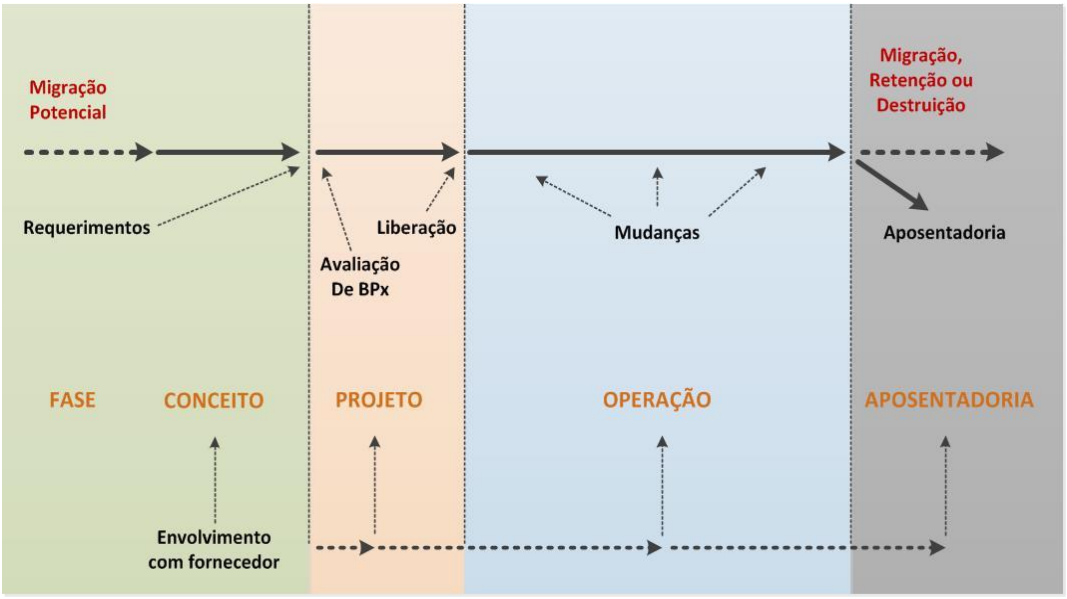

Figura 2. As Fases do Ciclo de Vida.
Fonte: GAMP5

5.3 ESTRUTURA DE VALIDAÇÃO DE SISTEMAS COMPUTADORIZADOS

5.3.1 Introdução

Deve existir uma estrutura para a validação de sistemas computadorizados que assegure a obtenção e manutenção de atendimento às BPX por todo o ciclo de vida do sistema computadorizado.

Esta estrutura é baseada em planos e relatórios específicos por sistema e a aplicação de controles operacionais apropriados. Planos e relatórios de validação provêm uma abordagem consistente e disciplinada para atendimento dos requisitos regulatórios. Tais documentos são valiosos para preparação para/e durante as inspeções regulatórias.

O Sistema de Gerenciamento do Risco à Qualidade da empresa regulada tem o papel de efetivamente e eficientemente cobrir a grande variedade de sistemas existentes.

Se o sistema computadorizado for parte de um processo ou sistema de fabricação mais amplo, principalmente em um ambiente integrado de Qualidade por Projeto (QbD), a validação do sistema realizado de forma específica e em separado pode não ser necessária. Este ambiente requer entendimento completo tanto do processo quanto do produto e que os parâmetros críticos de processo possam ser, com exatidão e confiabilidade, previstos e controlados dentro do espaço do projeto. Neste caso, a adequação do sistema computadorizado ao uso pretendido dentro do processo, pode ser adequadamente demonstrada pela

documentação da engenharia ou atividades do projeto juntamente com a subsequente validação de processo ou contínua verificação da qualidade do processo ou sistema no geral. Os mesmos princípios se aplicam à adoção da Tecnologia Analítica de Processo (PAT).

5.3.2 Terminologia

A terminologia específica utilizada para descrever as atividades do ciclo de vida varia de empresa para empresa e de tipo sistema para outro. Há várias razões para isto acontecer:

- As empresas reguladas utilizam abordagens diferentes;
- Há diferença de ênfase em BLP, BPC, BPF e dispositivos médicos;
- Há diferenças nos requisitos das diversas agências regulatórias;
- São seguidos diferentes padrões, locais e internacionais;
- Há diferentes tipos de sistemas computadorizados (TI, fabricação, laboratórios);
- Fornecedores utilizam diferentes modelos e abordagens de desenvolvimento.

Este Guia, em harmonia com o documento GAMP 5, pretende ser flexível e não tem o propósito de prescrever um conjunto único de termos, excluindo outros.

A tabela 1 apresenta o relacionamento entre a terminologia tradicional para Qualificação e as atividades descritas neste Guia.

Os termos utilizados para descrever a etapa de verificação dos sistemas são os que possuem maior diversidade. Esta seção descreve como a terminologia tradicionalmente utilizada para qualificação se relaciona com as atividades descritas neste Guia.

Qualquer que seja a terminologia utilizada pela empresa, o requerimento que se sobrepõe a tudo é que a empresa regulada possa demonstrar que o sistema está conforme e é adequado para o uso pretendido.

O uso da terminologia de qualificação em relação a sistemas computadorizados e o relacionamento entre QO e QD particularmente, varia de empresa para empresa.

Sendo que cabe às empresas decidir sobre a estratégia de verificação que irá utilizar.

Tabela 1. Relacionamento entre a Terminologia Tradicional para Qualificação e as Atividades Descritas neste Guia.

Termo tradicional	Descrição	Atividade de Verificação – Guia
Qualificação de Projeto (QP/DQ)	Verificação documentada de que o projeto proposto para as instalações, sistemas e equipamentos é adequado para o propósito pretendido	Revisão de Projeto
Qualificação de Instalação (QI/IQ)	Verificação documentada de que o sistema foi instalado de acordo com especificações escritas é pré-aprovadas.	Verificação, teste ou outra verificação para demonstrar que as atividades de instalação e configuração do *hardware* e do *software* foram realizadas corretamente
Qualificação Operacional (QO/OQ)	Verificação documentada de que o sistema opera de acordo com especificações escritas é pré-aprovadas e em toda a faixa operacional especificada.	Realização de testes ou outra verificação do sistema contra especificações para demonstrar correta operação da funcionalidade que apoia o processo de negócio específico por toda a especificações escritas é pré-aprovadas
Qualificação de Desempenho (QD/PQ)	Verificação documentada de que o sistema é capaz de desempenhar as atividades dos processos conforme esperado, de acordo com especificações escritas é pré-aprovadas, dentro do escopo do processo do negócio e ambiente operacional.	Realização de testes ou outra verificação do sistema para demonstrar adequação ao uso pretendido e para permitir a aceitação do sistema a partir dos requisitos especificados

6. GERENCIAMENTO DO RISCO À QUALIDADE

6.1 INTRODUÇÃO

O gerenciamento do risco à qualidade consiste em um processo sistemático para avaliação, controle, comunicação e revisão dos riscos. É um processo iterativo utilizado durante todo o ciclo de vida do sistema computadorizado, desde sua concepção até aposentadoria. A figura 3 apresenta graficamente este conceito.

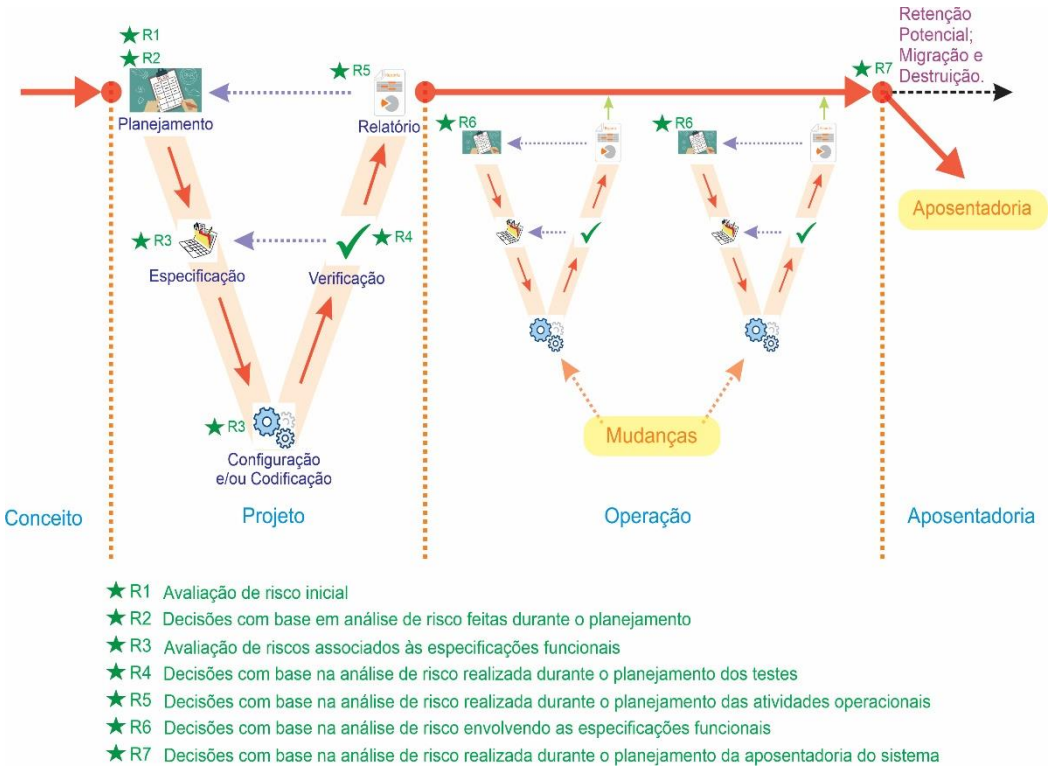

Figura 3. Uma Abordagem Baseada em Risco para Sistemas Computadorizados Compatíveis com as BPx.
Fonte: GAMP5

6.2 GERENCIAMENTO DO RISCO À QUALIDADE COM BASE CIENTÍFICA

A determinação dos riscos inerentes a um sistema computadorizado requer entendimento dos seguintes pontos:

- O impacto do sistema computadorizado na segurança do paciente, na qualidade do produto e na integridade dos dados;
- Os processos de negócios suportados pelo sistema;
- Os Atributos Críticos de Qualidades (CQA) para os sistemas que monitoram ou controlam os Parâmetros Críticos de Processo (CPPs);
- Os requisitos dos usuários;
- Os requisitos regulatórios;
- A abordagem do projeto (contratos, métodos, cronogramas);
- Componentes do sistema e arquitetura;
- Funções do sistema;
- Capabilidade do fornecedor.

A empresa deve também considerar outros riscos aplicáveis tais como segurança, saúde e meio-ambiente.

6.3 PROCESSO DE GERENCIAMENTO DO RISCO À QUALIDADE

Há um guia internacional disponível (ICH Q9) que trata sobre o gerenciamento do risco à qualidade dentro da indústria farmacêutica.

Ele define os dois princípios primários do gerenciamento do risco à qualidade, a saber:

- A avaliação do risco à qualidade deve ser baseada no conhecimento científico e ser interligado à proteção do paciente;
- O nível de esforço, a formalidade e a documentação do processo de gerenciamento do risco à qualidade deve ser comensurado com o nível do risco.

No contexto dos sistemas computadorizados, o conhecimento científico tem por base as especificações do sistema e o processo de negócio que o sistema suporta.

O processo para gerenciamento do risco à qualidade envolve a execução de 05 (cinco) etapas:

1. Execução da avaliação de risco inicial e determinação do impacto do sistema;
2. Identificação das funções que tenham impacto na segurança do paciente, na qualidade do produto e na integridade dos dados;
3. Execução das avaliações de risco funcionais e identificação dos controles necessários;
4. Implantação e verificação dos controles apropriados;
5. Revisão dos riscos e monitoramento dos controles implantados.

Estas etapas são detalhadas a seguir.

6.3.1 Etapa 1 – Avaliação do Risco Inicial

Deve ser realizada uma análise de risco inicial com base no entendimento dos processos e avaliações dos riscos do negócio, nos requisitos do usuário, nos requisitos regulatórios e áreas funcionais conhecidas.

Os resultados desta avaliação de risco inicial devem incluir a decisão sobre se o sistema é regulado pelas BPx (avaliação de BPx). Também deve ser incluída uma avaliação geral do impacto do sistema.

Com base nesta avaliação de risco inicial e do impacto do sistema pode não ser necessário realizar as etapas subsequentes se o risco já estiver em um nível aceitável.

O esforço necessário, a formalização e a documentação das etapas subsequentes devem ser determinadas com base no nível de risco e o impacto do sistema nas BPx.

6.3.2 Etapa 2 – Identificação das Funções

As funções que tenham impacto na segurança do paciente, na qualidade do produto na integridade dos dados devem ser identificadas pela construção da informação reunida na etapa 1, referindo-se às especificações relevantes e levando-se em conta a abordagem do projeto, a arquitetura do sistema e a categorização dos componentes do sistema.

6.3.3 Etapa 3 – Avaliação dos Riscos Funcionais

As funções identificadas na etapa 2 devem ser avaliadas considerando-se os possíveis perigos e como os potenciais danos advindos destes perigos podem ser controlados.

Pode ser necessário executar uma avaliação mais detalhada que posteriormente analise a severidade do dano, a probabilidade de ocorrência e a probabilidade de detecção.

O julgamento, sobre a realização ou não uma avaliação detalhada de funções específicas, deve ser realizado caso a caso e o critério pode variar. Os critérios a serem levados em consideração são:

- A criticidade dos processos suportados;
- O impacto específico das funções dentro do processo;
- A natureza do sistema (complexidade e inovação).

Controles apropriados devem ser identificados com base na avaliação realizada. Há uma gama de opções disponível para se efetuar o requerido controle dependendo do risco identificado. Os controles incluem, dentre outros:

- Modificação do projeto do processo;
- Modificação do projeto do sistema;
- Aplicação de procedimentos externos;
- Aumento dos detalhes ou formalidade das especificações;
- Aumentando o número e o nível dos detalhes das revisões de projeto;
- Aumentando a extensão ou o rigor das atividades de verificação.

Onde for possível é preferível que a eliminação do risco seja efetuada no nível de projeto.

6.3.4 Implantação e Verificação dos Controles

As medidas de controle identificados na etapa 3 devem ser implantadas e verificadas para assegurar que elas foram implantadas com sucesso. Os controles devem ser rastreáveis aos riscos relevantes identificados.

A atividade de verificação deve demonstrar que os controles são efetivos na execução da redução do risco requerida.

6.3.5 Revisão dos Riscos e Monitoramento dos Controles

Durante a execução da revisão periódica dos sistemas, ou em outras oportunidades definidas, a empresa deve rever os riscos. A verificação deve evidenciar se os controles ainda são efetivos e ações corretivas devem ser efetuadas se forem encontradas deficiências.

A empresa também deve considerar os seguintes pontos:

- Se os perigos anteriormente não identificados estão presentes;
- Se os perigos anteriormente identificados não são mais aplicáveis;
- Se o risco estimado associado a um perigo não é mais aceitável;
- Se a avaliação original está atualmente invalidada (ex.: após mudanças nas regulações aplicáveis ou mudanças na utilização do sistema).

Quando for necessário, os resultados da avaliação devem retroalimentar o processo de gerenciamento de risco. Se houver um potencial de que o risco residual ou sua aceitabilidade tenha mudado, o impacto sobre as medidas de controle de risco previamente implantadas tem de ser considerado e o resultado desta avaliação devidamente documentada.

A frequência e a extensão de qualquer revisão periódica devem ter como base o nível de risco associado.

7. CATEGORIZAÇÃO DE *SOFTWARE* E *HARDWARE*

7.1 INTRODUÇÃO

Esta seção descreve como os componentes *software* e *hardware* podem ser analisados e categorizados. Estas categorias de *software* e *hardware* podem então ser utilizadas juntamente com a Avaliação de Risco e Avaliação do Fornecedor para estabelecer uma estratégia de ciclo de vida adequada.

As categorias 3 a 5 não possuem fronteiras absolutas e que as atividades recomendadas para uma dada categoria podem ser adequadas para um sistema ou componente que pertença à outra categoria.

7.2 UTILIZAÇÃO DAS CATEGORIAS DO GAMP

Geralmente há um aumento do risco de falhas e defeitos quando se faz uma progressão de um conjunto *software-hardware* padrão para um conjunto *software-hardware* customizado. O aumento do risco vem da combinação de uma maior complexidade e menor experiência do usuário. A categorização pode ser parte de uma abordagem efetiva de gerenciamento do risco à qualidade quando acoplada com avaliação de risco e avaliação do fornecedor.

A maioria dos sistemas possui componentes de complexidade variável, tais como um sistema operacional, componentes não configurados, e componentes configurados ou customizados. O esforço deve ser concentrado na seguinte proporção: Customizado > Configurado > Não-Configurado > Infraestrutura. A categorização pode ajudar a concentrar o esforço onde o risco é maior.

Há dois modos principais de ser utilizar as categorias:

- Avaliação do sistema de modo holístico;
- Avaliação detalhada por componente.

Na avaliação holística, a categoria do componente principal pode ser utilizada para ajudar a definir a abordagem para avaliação do fornecedor ou seleção dos resultados a serem entregues no ciclo de vida. A combinação da categorização com a avaliação do impacto do sistema pode ajudar a decidir se uma auditoria no fornecedor é necessária.

Na avaliação individualizada, a categorização é útil quando aplicada em conjunto com outras ferramentas de gerenciamento de risco e com consideração da complexidade e tamanho do sistema. A maioria dos sistemas computadorizados é formada por múltiplos componentes e a categorização de tais componentes podem ser utilizadas para a definição das atividades específicas do ciclo de vida.

Por exemplo, um sistema de gerenciamento cromatográfico (CDS) que possui um *software* de controle e de dados instalado no computador e que roda em um sistema operacional e um banco de dados e mais subsistemas com *firmware* instalado, tais como controladores de bomba, auto injetores e fornos de colunas. Neste contexto, estes últimos componentes são muito menos complexos do que o *software* de dados e controle, sendo assim razoável que seja gasto mais esforço na aplicação instalada no computador do que nos subsistemas.

Um Controlador Lógico Programável (PLC) ou outro controlador pode ser parte integrada de um equipamento de processo e a verificação da operação correta faz parte da verificação geral do equipamento integrado. Em tais casos, análise detalhada das categorias dos componentes individuais pode não ser necessária.

7.3 CATEGORIAS DE *SOFTWARE*

7.3.1 Categoria 1 – *Software* de Infraestrutura

Elementos de infraestrutura se interligam para formar um ambiente integrado para rodar e dar suporte a aplicações e serviços.

Há dois tipos de *software* nesta categoria:

1. ***Softwares* de Camada (*Layered Software*) Comercialmente Disponíveis ou Estabelecidos** – Aplicações são desenvolvidas para rodar sob o controle deste tipo de *software*. Este tipo de *software* inclui: sistemas operacionais, gerenciadores de banco de dados, ferramentas de programação estatística, e pacotes de planilhas (mas não aplicações desenvolvidas utilizando-se estes pacotes).
2. **Ferramentas de *Software* de Infraestrutura** – Este tipo inclui ferramentas tais como: *software* de monitoramento de rede; ferramentas de agendamento de tarefas em lote; *software* de segurança; antivírus e ferramentas de gerenciamento da configuração. Avaliação de risco deve ser realizada, contudo, nas ferramentas com alto impacto potencial, tais como, gerenciamento de senha ou de segurança para se determinar se controles adicionais são apropriados.

> Os *softwares* de camada não são sujeitos a verificação funcional específica, embora as suas características sejam testadas funcionalmente e desafiadas indiretamente durante a realização de testes na aplicação. As identidades e os números das versões do *software* de camada e do sistema operacional devem ser documentados e verificados durante a instalação.
>
> As ferramentas e os *softwares* de infraestrutura geralmente são altamente confiáveis e significativamente removidos de qualquer aspecto de risco ao paciente. Todos os *softwares* de infraestrutura devem ser controlados e gerenciados.

7.3.2 Categoria 3 – Produtos Não-Configurados

Esta categoria inclui os produtos de prateleira utilizados para o processo de negócio. Abrange tanto os sistemas que não podem ser configurados para atender aos processos de negócios quanto os sistemas que são configuráveis, mas que somente a configuração *default* é utilizada. Em ambos os casos, a configuração para rodar no ambiente do usuário provável (ex.: ajuste de impressora). Julgamento com base no risco e complexidade deve determinar se os sistemas utilizados com a configuração *default* podem ser considerados Categoria 3 ou 4.

Uma abordagem simplificada para o ciclo de vida pode ser aplicada a esta categoria. Avaliação do fornecedor pode não ser necessária. A necessidade e extensão da avaliação do fornecedor devem ser baseadas no risco. Requisitos do usuário são necessários e devem ter como foco os aspectos-chave de utilização. As especificações funcionais e de projeto não são necessárias, embora haja a necessidade de existir especificação suficiente (normalmente no ERU/URS) para permitir a realização de testes. A verificação consiste basicamente em uma fase de testes única.

Todas as mudanças devem ser controladas, incluindo os pacotes de "*patches*" fornecidos pelo fornecedor. Procedimentos Operacionais Padrão devem ser estabelecidos para uso e gerenciamento do sistema e planos de treinamento devem ser implantados.

Gerenciamento da configuração deve ser aplicado. Para sistemas onde a configuração *default* é utilizada, o gerenciamento da configuração demonstra que a opção "*default*" esteja selecionada corretamente.

7.3.3 Categoria 4 – Produtos Configurados

Softwares configuráveis fornecem *interfaces* e funções padrão que permitem a configuração de processos de negócio específico para o usuário. Isto envolve normalmente a configuração de módulos de *software* predefinidos.

Muito do risco associado com o *software* depende do quão bem o sistema é configurado para atender as necessidades do usuário. Pode haver um aumento do risco associado ao novo *software* e atualizações maiores.

É preciso haver documento de requisitos do usuário (ERU/URS) detalhado para esta categoria de *software*. A abordagem para avaliação do fornecedor e do produto configurável deve ser baseada no risco e deve ser documentada.

O documento de Especificação Funcional pode não ser de propriedade do usuário/empresa regulada, mas deve haver documentação suficiente para assegurara rastreabilidade das especificações funcionais e seus respectivos testes.

A abordagem utilizada pela empresa regulada deve abranger as camadas de *software* envolvidas e suas respectivas categorias. A abordagem deve refletir o resultado da avaliação do fornecedor, o risco às BPF, tamanho e complexidade do sistema. Ela deve definir as estratégias para mitigação de quaisquer fraquezas identificadas durante o processo de avaliação do fornecedor.

7.3.4 Categoria 5 – Aplicações Customizadas

Estes sistemas e subsistemas são desenvolvidos para atender a necessidades específicas da empresa regulada. O risco inerente ao *software* customizado é alto. A abordagem de ciclo de vida e as decisões acerca do sistema devem levar em consideração este risco alto, porque não existe experiência do usuário ou informação sobre confiabilidade do sistema.

A abordagem utilizada para avaliação do fornecedor deve ser baseada no risco e documentada. Uma auditoria no fornecedor é necessária para confirmar que existe um adequado Sistema Gerenciamento da Qualidade para controlar o desenvolvimento e suporte contínuo para a aplicação. Na ausência de um Sistema Gerenciamento da Qualidade adequado, os fornecedores devem se adequar para pode proporcionar uma base apropriada para o gerenciamento do desenvolvimento e suporte da aplicação.

A abordagem utilizada pela empresa regulada deve abranger as camadas de *software* envolvidas e suas respectivas categorias. A abordagem deve refletir o resultado da avaliação do fornecedor, o risco às BPF, tamanho e complexidade do sistema. Ela deve definir as estratégias para mitigação de quaisquer fraquezas identificados durante o processo de avaliação do fornecedor.

7.3.5 Exemplos Típicos e Abordagens

Tabela 2. Categorias de *Software*, Descrição e Abordagem Típica para o Ciclo de Vida.

Categoria	Descrição	Exemplos Típicos	Abordagem Típica
Software de Infraestrutura (1)	• *Software* de Camada (isto é, sobre os quais aplicações são construídas) • *Software* utilizados para gerenciar o ambiente operacional	• Sistemas operacionais • Mecanismos de bancos de dados • Middleware • Linguagens de programação • Pacotes estatísticos • Planilhas • Ferramentas de monitoramento de rede • Ferramentas de agendamento • Ferramentas de controle de versão	• Registro do número da versão e verificação da correta instalação • Vide *GAMP Good Practice Guide: IT Infraestructure Control and Compliance*
Software Não-Configurado (3)	Parâmetros em tempo de execução podem ser inseridos e armazenados, mas o *software* não pode ser configurado para se adequar aos processos de negócio	• Aplicações com base em *firmware* • *Softwares* do tipo COTS • Instrumentos de Laboratório (Vide *GAMP Good Practice Guide: Validation of Laboratory Computerized Systems*)	• Ciclo de vida abreviado • Abordagem para avaliação do fornecedor com base no risco • Registro do número da versão e verificação da correta instalação • Testes com base no risco contra os requisitos, tendo por base a sua utilização (para sistemas simples a calibração pode ser a substituta dos testes) • Existência de procedimentos para a manutenção do atendimento e adequação ao uso

Tabela 2: Categorias de *Software*, Descrição e Abordagem Típica para o Ciclo de Vida (continuação).

Categoria	Descrição	Exemplos Típicos	Abordagem Típica
Software Configurado (4)	*Softwares*, geralmente mais complexos, que podem ser configurados pelo usuário para atender as suas necessidades especificas. O código do *software* não é alterado.	• LIMS • Sistemas de aquisição de dados • SCADA • ERU • MRPII • DCS • CDS • EDMS • BMS • Planilhas • HMI (*Human Machine Interfaces*) simples **NOTA**: Exemplos específicos de tipos de sistemas acima podem conter elementos customizados substanciais.	• Abordagem de ciclo de vida • Abordagem para avaliação do fornecedor com base no risco • Demonstração de que o fornecedor possui um Sistema de Gerenciamento da Qualidade • Alguma documentação do ciclo de vida mantida pelo fornecedor (ex.: Especificações de Projeto) • Registro do número da versão e verificação da correta instalação

			• Realização de testes com base no risco para demonstrar que a aplicação funciona conforme projetada, em um ambiente de teste • Realização de testes com base no risco para demonstrar que a aplicação funciona conforme projetada, em um ambiente de produção • Existência de procedimentos para a manutenção do atendimento e adequação ao uso e gerenciamento dos dados
Softwares customizados (5)	*Software* customizado projetado e codificado para atender a um processo de negócio.	Varia, mas inclui: • Aplicações de TI desenvolvidas internamente e externamente • Aplicações para controle de processo desenvolvidas internamente e externamente • Lógica de escada personalizada • *Firmware* personalizado • Planilhas (macro)	Mesma abordagem utilizada para a Categoria 4, mais: • Uma avaliação de fornecedor mais rigorosa, com possível auditoria deste • Posse da documentação de todo o ciclo de vida do sistema (Especificações Funcionais, Especificações de Projeto, testes estruturais etc.) • Revisão do Projeto e do Código Fonte

7.4 CATEGORIAS DE *HARDWARE*

7.4.1 *Hardware* Categoria 1 – Componentes-Padrão de *Hardware*

A maioria dos *hardwares* utilizados por empresas reguladas pertencem a esta categoria.

Os componentes do *hardware* padrão devem ser documentados incluindo detalhes acerca do fornecedor ou fabricante e número de versão. A correta instalação e conexões dos componentes devem ser verificadas. O modelo, o número de versão e se disponível e o número de série do *hardware* pré-montado devem ser registrados. *Hardwares* pré-montados não tem de ser desmontados. Em tais casos os detalhes do *hardware* podem ser adquiridos a partir da folha de dados do *hardware* ou outra especificação do material. Gerenciamento da configuração e controle de mudanças são aplicáveis.

7.4.2 *Hardware* Categoria 2 – Componentes Customizados Embutidos de *Hardware*

São aplicáveis além dos requisitos descritos no item acima, os descritos neste item. Itens customizados de *hardware* devem possuir uma Especificação de Projeto (EP/DS) e serem sujeitos a testes de aceitação. A abordagem para avaliação do fornecedor deve baseada no risco e documentada. Na maioria dos casos uma Auditoria no Fornecedor deve ser realizada para desenvolvimento de hardware customizado. Sistemas montados utilizando-se *hardware* customizado de diferentes fontes requerem verificação para confirmar a compatibilidade dos componentes de *hardware* interconectados. Qualquer configuração de *hardware* deve ser

definida na documentação de projeto e verificada. Gerenciamento da configuração e controle de mudanças são aplicáveis.

8. LISTA DE INVENTÁRIO

As empresas reguladas devem manter um inventário de seus sistemas computadorizados.

O inventário deve apresentar informação resumida sobre cada sistema, descrevendo: nome do sistema; equipamento ou aplicação associado(a); impacto/criticidade; categoria; propriedade (setor, dono do sistema, dono do processo); versão atual; fornecedor; data e situação de validação.

Equipamentos automatizados podem ser listados separadamente e duplicação deve ser evitada.

O inventário deve abranger o nível dos sistemas que dão suporte aos processos do negócio e não itens individuais de *hardware* (componentes) que devem ser cobertos por procedimentos locais do setor de tecnologia de informação.

Este inventário pode ser utilizado para o planejamento das revisões periódicas.

9. VALIDAÇÃO DE SISTEMAS COMPUTADORIZADOS

9.1 INTRODUÇÃO

Será apresentada uma estratégia para a realização da validação de sistema computadorizado, desde a definição dos requisitos do usuário, seleção do sistema, execução e aprovação do relatório de validação.

Esta estratégia é aplicável aos sistemas pertencentes à categoria 3, 4 e 5, que são a grande maioria dos sistemas computadorizados existentes nas indústrias farmoquímicas e farmacêuticas.

Nesta seção também serão descritos os processos auxiliares de gerenciamento de risco, mudança e de configuração, revisão do projeto, rastreabilidade e gerenciamento de documentação.

Serão utilizadas neste guia terminologias que são comumente utilizadas pelas indústrias farmoquímicas e farmacêuticas, a saber: Políticas de Validação, Plano Mestre de Validação e Plano de Validação.

A empresa regulada deve incluir a validação de sistemas computadorizados em sua política de validação e/ou Plano Mestre de Validação. Estes documentos devem expressar a abordagem geral corporativa ou da planta da empresa para a atividade de validação dos sistemas computadorizados e para manutenção da sua situação de validado.

É recomendado que seja preparado um Plano de Validação para cada sistema computadorizado que tenha relevância nas BPF, com foco nos aspectos relacionados à qualidade do paciente, à qualidade do produto e à integridade dos dados.

Para equipamentos automatizados de fabricação, a validação do sistema computadorizado em separado deve ser evitada. A especificação e a verificação do sistema computadorizado devem fazer parte de uma abordagem integrada de engenharia para assegurar o atendimento e adequação ao uso pretendido do equipamento automatizado dentro de um todo.

A figura 4 mostra as etapas envolvidas na validação dos sistemas que formam parte do ciclo de vida do sistema computadorizado, desde a definição de requisitos do usuário, passando pela aquisição e validação do sistema computadorizado e execução dos processos auxiliares pertinentes.

Estas etapas são igualmente aplicáveis à fase de projeto e às subsequentes mudanças ocorridas durante a fase operacional do sistema.

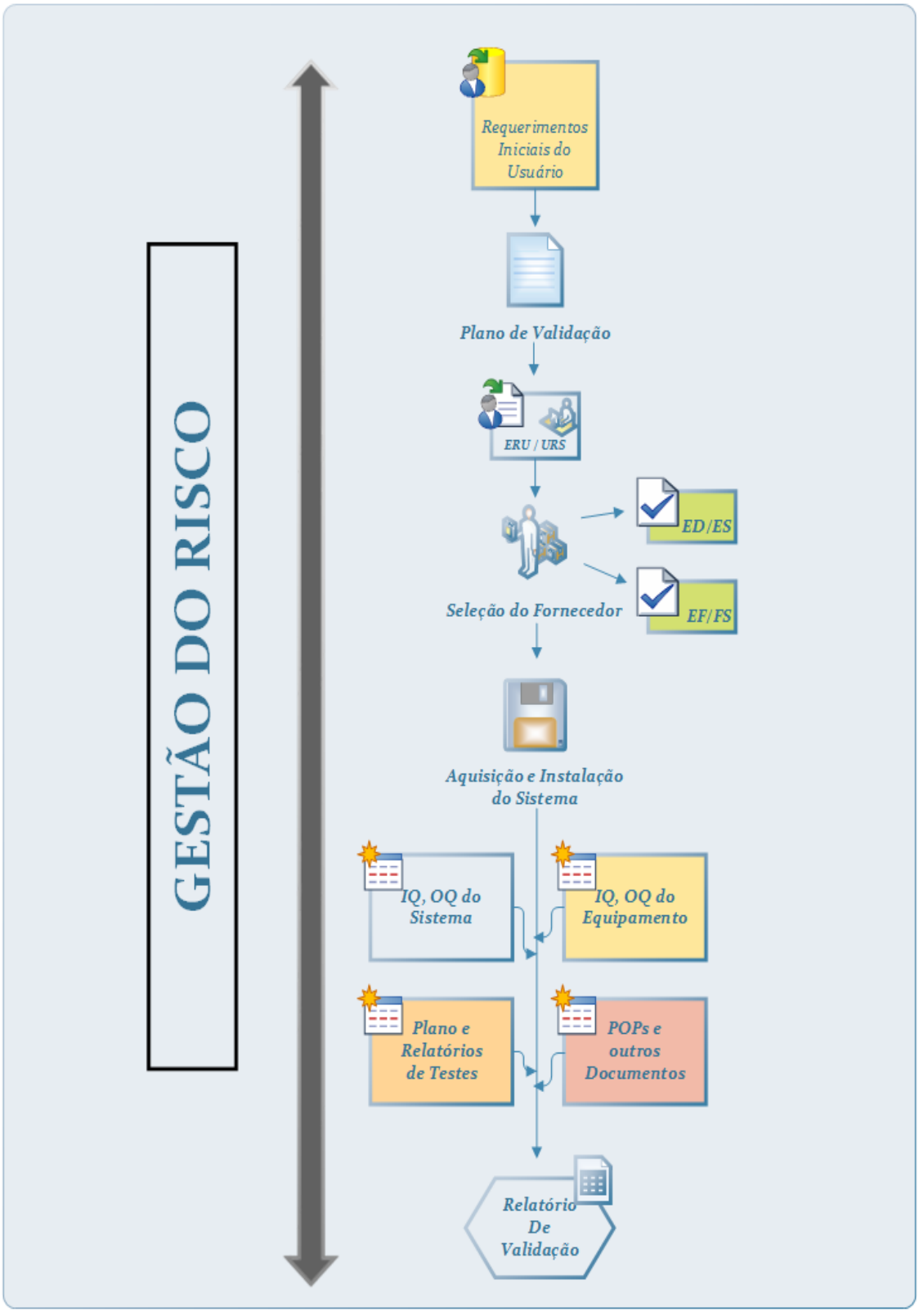

Figura 4. Fluxo do Processo de Validação de Sistemas (Categorias 3, 4 e 5).

9.2 PLANO DE VALIDAÇÃO

9.2.1 Introdução

É no plano de validação onde descreve-se o projeto, identificam-se as ações a serem realizadas para uma validação bem-sucedida e definem-se claramente os critérios de aceitação para a liberação do sistema.

Deve definir:

- Quais atividades são necessárias;
- Como as atividades serão realizadas e quem são os responsáveis;
- Quais são os resultados esperados;
- Quais são os critérios de aceitação;
- Como a situação de conformidade será mantida durante a vida útil do sistema.

O planejamento deve começar o mais rápido possível, idealmente durante o desenvolvimento do documento descrevendo as especificações dos requisitos dos usuários (ERU/URS).

Um plano similar ou genérico pode ser gerado para sistemas similares, mas que adequadamente reflita as características de cada sistema.

Com relação aos papeis e responsabilidades, o plano de validação é de responsabilidade do Dono do Processo. Podendo ser delegada para o Gerente de Projeto, se for o caso, podendo ser envolvido também o Dono do Sistema.

9.2.2 Conteúdo do Plano

9.2.2.1 Introdução e Escopo

Deverá conter:

- O escopo do sistema;
- Os objetivos do processo de validação;
- Revisão, manutenção ou atualização do próprio plano.

9.2.2.2 Visão Geral do Sistema

A descrição geral do sistema deverá conter:

- Propósito do negócio e uso pretendido para o sistema;
- Uma descrição em alto nível do sistema;
- Uma visão geral da arquitetura do sistema;
- Diagramas do sistema.

9.2.2.3 Estrutura Organizacional

Os papeis e responsabilidade devem ser descritos, tais como:

- Gerente do Projeto;

✓ Planejamento e gerenciamento do projeto;

✓ Controle das atividades do projeto, recursos e custos;

✓ Monitoramento do progresso dos trabalhos e iniciação de CAPA;

✓ Assegurar que os problemas e objetivos do projeto sejam resolvidos e atendidos;

✓ Gerenciar os desvios de qualidade envolvendo o sistema:

✓ Responder ao patrocinador ou à alta gerência;

✓ Assegurar a conformidade do sistema em conjunto com a Unidade da Qualidade.

- Unidade da Qualidade;

✓ Assegurar a conformidade do sistema aos requisitos regulatórios, de qualidade e às políticas da empresa;

✓ Prover suporte para a revisão e aprovação dos resultados gerados pelo trabalho de validação;

✓ Avaliação e aprovação do fechamento dos desvios da qualidade;

✓ Aprovação da liberação do sistema para uso.

- Dono do Processo e/ou Dono do Sistema

✓ Implantação e gerenciamento do sistema pela comunidade de usuários do sistema;

✓ Aprovação de cada etapa/fase do processo de validação.

Os especialistas no assunto (SME) são aqueles indivíduos com *expertise* específica e responsabilidade em uma área particular ou campo, como por exemplo, análise cromatográficas, unidade da qualidade, engenharia, automação, desenvolvimento etc.

As responsabilidades destes especialistas podem incluir: planejamento e definição das estratégias de verificação do sistema; execução de revisões; definição dos critérios de aceitação; seleção de testes de métodos apropriados; execução de testes de verificação e revisão dos resultados.

9.2.2.4 Gerenciamento do Risco à Qualidade

A abordagem utilizada para o gerenciamento do risco à qualidade deve ser descrita.

Uma avaliação de risco deve ser realizada com base no entendimento dos processos do negócio, requisitos do usuário, requisitos regulatórios e áreas funcionais conhecidas. Os resultados obtidos devem incluir uma decisão sobre se o sistema é relevante às BPF e uma avaliação geral sobre o impacto do sistema.

Sistemas complexos, tais como os sistemas do tipo ERP, podem possuir algumas funcionalidades que são relevantes às BPF e outras que não são. Em tais casos, o método utilizado para tomar tal decisão deve ser descrito e deverá considerar os seguintes pontos:

- Os requisitos para decidir sobre os níveis de impacto nas BPx;
- Os procedimentos para executar a avaliação;
- A situação atual do processo, reconhecendo-se que esta avaliação pode ser repetida e atualizada.

Quaisquer procedimentos ou padrões específicos utilizados para realizar o gerenciamento do risco à qualidade devem ser definidos.

9.2.2.5 Estratégia de Validação

A estratégia a ser utilizada para a validação do sistema deve ser descrita, com base nas seguintes considerações:

- Avaliação de risco;
- Avaliação dos componentes do sistema e sua arquitetura;
- Avaliação do fornecedor.

As conclusões-chave de qualquer avaliação realizada devem ser formalizadas.

Quaisquer procedimentos ou padrões específicos utilizados devem ser definidos.

A estratégia de validação deve incluir:

- O modelo de ciclo de vida;
- As categorias de *hardware* e *software* do sistema;
- As requisitos e resultados necessários para cada etapa do projeto;
- Os critérios de aceitação para cada etapa;
- Abordagem utilizada para assegurar a rastreabilidade dos dados e documentos;
- Abordagem utilizada para a revisão do projeto.

9.2.2.6 Resultados Esperados

Os resultados a serem produzidos devem ser listados, incluindo a responsabilidade pela produção (de documentos, testes, resultados), revisão e aprovação.

9.2.2.7 Critérios de Aceitação

Os critérios de aceitação geral para o sistema, tal como a bem-sucedida execução de uma etapa definida do projeto, devem ser descritos.

9.2.2.8 Controle de Mudanças

Os requisitos para o controle de mudanças do projeto devem ser definidos, incluindo referência aos procedimentos relevantes.

A etapa na qual o controle de mudança operacional será aplicado deve ser definida.

9.2.2.9 Procedimentos Operacionais Padrão

Os procedimentos operacionais padrão (POP) que serão criados ou atualizados como resultado da implantação do sistema devem ser definidos e as responsabilidades pela sua elaboração, revisão e aprovação definidas.

9.2.2.10 Processos Auxiliares

Detalhes dos processos auxiliares devem ser definidos ou referenciados, incluindo, mas não limitados a:

- Treinamento;
- Gerenciamento da documentação;

- Gerenciamento da configuração;
- Manutenção da sua situação de validado.

9.2.2.11 Glossário

Devem ser incluídas as definições de quaisquer termos e abreviações que possam ser pouco conhecidos.

9.3 DOCUMENTO CONTENDO AS ESPECIFICAÇÕES DOS REQUISITOS DO USUÁRIO (ERU/URS)

9.3.1 Introdução

O documento Especificações dos Requisitos do Usuário (ERU/URS) define os requisitos para um sistema computadorizado ou um componente do sistema.

A extensão e o detalhamento deste documento devem ser comensurados com o risco, a inovação e a complexidade do sistema e deve ser suficiente para dar suporte às subsequentes atividades de análises de risco, especificação, configuração/projeto e verificação, se necessário.

Para sistema de baixo risco e comercialmente disponível, pode ser apropriado incluir este documento na documentação de compra do sistema, enquanto para uma aplicação complexa e customizada podem ser necessários vários níveis de especificação.

O documento de ERU/URS é de responsabilidade da empresa regulada, mas pode ser escrita por uma empresa terceirizada ou pelo fornecedor do sistema.

O documento Especificações dos Requisitos do Usuário (ERU/URS) define com clareza e precisão o que a empresa regulada deseja que o sistema faça. Ele é impulsionado pelas necessidades do processo do negócio.

Para os sistemas de categoria 4 e 5 os requisitos devem ser desenvolvidos com independência em relação às soluções disponíveis no mercado.

Para os sistemas de categoria 3, particularmente, pode haver número limitado de fornecedores ou mesmo um fornecedor preferido para determinado tipo de sistema, que justifique a utilização de soluções disponíveis no mercado.

Os requisitos devem abranger os seguintes pontos, podendo abranger outros que não estejam listados:

- Operacionais;
- Funcionais;
- Dados;
- Técnicos;
- *Interface*;
- Ambientais;
- Desempenho;
- Disponibilidade;
- Segurança;
- Manutenção;
- Regulatórios;
- Migração de quaisquer dados eletrônicos;

- Restrições a serem observadas;
- Ciclo de vida.

Os requisitos devem abordar regulações BPx aplicáveis e dar destaque aos aspectos que são críticos para a segurança do paciente, a qualidade do produto e a integridade dos dados. O documento de ERU não deve incluir requisitos do tipo “atende à 21CFR Part 11” ou “atende à legislação da Anvisa” e sim definir que funcionalidade o sistema deve possuir para gerenciar o risco à segurança do paciente, à qualidade do produto e à integridade dos dados.

Os requisitos devem possuir as seguintes características:

- Suficiente e adequados (Específicos; Mensuráveis, Atingíveis; Realísticos; Testáveis);
- Específicos o suficiente para a realização de testes e verificações (Inequívocos; Claros; Precisos; Completos);
- Capaz de auxiliar a rastreabilidade ao longo da cadeia requerimento → configuração/projeto → teste;
- Prover a base para a realização formal de testes e ser utilizada para a seleção do fornecedor;
- Priorizados com ênfase na identificação dos requisitos mandatórios. Podendo ser utilizada a abordagem de três níveis de prioridade, descrita abaixo:
  - ✓ Mandatório (alta);
  - ✓ Benéfico (média);
  - ✓ Bom ter (baixa).
- Identificado de forma unívoca, com versão controlada e manutenção de seu controle;Capaz de ser utilizado como meio de comunicação e gerenciamento dos requisitos críticos ao longo do ciclo de vida do sistema ao invés de ser apenas um exercício;
- Prover o fornecedor do sistema com a declaração definitiva dos requisitos mandatórios e desejáveis.

A propriedade dos requisitos pertence à a empresa regulada. As necessidades operacionais do negócio e quaisquer problemas associados jamais poderão ser completamente entendidas e capturadas sem a efetiva participação dos usuários do sistema. Os requisitos documentados formam a base para a aceitação do sistema pelos usuários.

9.3.2 Conteúdo do Documento de ERU/URS

9.3.2.1 Introdução

O item introdução deve prover informação sobre:

- Quem produziu o documento, sob que autoridade e para que propósito;
- A situação contratual do documento (se aplicável), como por exemplo se desenvolvimento customizado ou terceirizado;
- Relacionamento ou dependência com outros documentos.

9.3.2.2 Visão Geral

Deve ser fornecida uma visão geral do sistema, explicando porque o sistema é necessário e o que é requerido do sistema. Os seguintes pontos devem ser considerados:

- Contextualização: descreve o objetivo geral do sistema no contexto atual e a situação desejada;

- Escopo:
  - ✓ A inserção do sistema na visão de longo prazo da empresa;
  - ✓ Limites e fronteiras do sistema: que parte do processo de negócio está sendo automatizada;
  - ✓ Objetivos-chave e benefícios;
  - ✓ Requisitos de BPx aplicáveis;
  - ✓ Outras regulações aplicáveis.

9.3.2.3 Requisitos Operacionais

Os requisitos operacionais incluem:

- **Funções** – são os requisitos funcionais que habilitam o sistema a executar o processo de negócio que está sendo automatizado, tais como:
  - ✓ Cálculos, incluindo todos os algoritmos críticos;
  - ✓ Segurança contra danos;
  - ✓ Segurança incluindo controle de acesso;
  - ✓ Trilhas de auditoria;
  - ✓ Utilização de assinaturas eletrônicas;
  - ✓ Saídas (ex.: relatórios);
  - ✓ Mensagens de erro inequívocas.

- **Dados** – requisitos relacionados ao manuseio de dados, considerando-se o seu impacto na segurança do paciente, na qualidade do produto e na integridade dos dados, abrangendo os seguintes pontos:
  - ✓ Definição dos registros eletrônicos;
  - ✓ Definição dos tipos de dados, incluindo a identificação das características, formatação, parâmetros críticos, intervalo e formato de datas válidos, limites e exatidão e assim por diante;
  - ✓ Onde e como os dados serão gravados (ex.: bancos de dados relacionais, arquivos criptografados etc.)
  - ✓ Campos necessários;
  - ✓ Migração de dados (importação e exportação);
  - ✓ Entrada de dados e subsequente edição;
  - ✓ Backup e recuperação;
  - ✓ Requisitos para arquivamento;
  - ✓ Segurança dos dados e integridade.

- **Requisitos Técnicos** – Abrange os seguintes pontos:
  - ✓ Mudanças na operação do sistema (inicialização, parada, teste, falhas);
  - ✓ Recuperação em caso de desastre;
  - ✓ Desempenho e requisitos de tempo. Devem ser quantitativos e inequívocos;
  - ✓ Ação necessária em caso de ocorrência de falhas;
  - ✓ Requisitos de capacidade;
  - ✓ Requisitos de velocidade de acesso para leitura e gravação de dados;
  - ✓ Requisitos de hardware (ex.: tela touch-screen, tipo de teclado; tipo de mouse e mouse pad; tipo e número de processadores físicos, placa de rede);
  - ✓ Portabilidade e acesso remoto;

✓ Eficiência (velocidades de carregamento das telas e do sistema, atualização de telas e geração de relatórios);
✓ Tipo e versão da plataforma em que o sistema irá funcionar (Windows, Unix, Linux etc.);
✓ Tipos e versões dos protocolos utilizados;
✓ Configurabilidade.

- ***Interfaces*** – devem ser definidas (se aplicável), abrangendo os seguintes pontos:

✓ Interface(s) com o usuário – definidas em termos de níveis de acesso (operador, administrador, gerente do sistema) ou funções quando apropriado;
✓ Interface(s) com outros sistemas;
✓ Interface(s) com equipamentos, tais como sensores ou atuadores. Isto pode incluir listas de I/O (entrada e saída) para sistemas utilizados para controle de processos;
✓ Forma de entrada e saída de dados pelos usuários (ex.: teclado, leitor de código de barras, impressoras etc.).

- **Ambiente** – envolve o ambiente no qual o sistema irá funcionar, abrangendo os seguintes pontos:

✓ Layout – layout físico da planta ou outro local de trabalho que pode ter impacto no sistema, tais como links à distância (acesso remoto) ou limitações de espaço;
✓ Condições físicas (ex.: temperatura; umidade; interferência externa; proteção contra radiofrequência, eletromagnético e/ou interferência de UV; poeira, alta vibração);
✓ Requisitos físicos;
✓ Requisitos de potência/energia (ex.: voltagem; amperagem; filtragem; frequência; proteção de aterramento; fornecimento de energia elétrica ininterrupto/UPS);
✓ Quaisquer requisitos físicos ou lógicos.

9.3.2.4 Restrições

Devem ser identificadas e documentadas quaisquer restrições nas especificações ou na operação do sistema, abrangendo os seguintes pontos:

- Compatibilidade, levando-se em conta quaisquer sistemas ou *hardware* existentes que compartilharão os mesmos recursos ou terão *interfaces* para troca de informação (ex.: envio e recebimento de receitas de produção e de valores de parâmetros do processo etc.);
- Disponibilidade de acesso (ex.: local, intranet e internet);
- Requisitos de confiabilidade;
- Período máximo permitido para manutenção ou outro tempo de inatividade;
- Obrigações legais;
- Métodos de trabalho;
- Níveis de habilidade e conhecimento do usuário;
- Capabilidade e flexibilidade de expansão;
- Melhorias possíveis;
- Tempo de vida esperado;
- Suporte a longo prazo.

9.3.2.5 Ciclo de Vida

Devem ser identificados e documentados quaisquer requisitos que possam impactar o desenvolvimento do ciclo de vida no fornecedor e quaisquer atividades de verificação subsequente.

Os seguintes pontos devem ser abrangidos:

- Requisitos de desenvolvimento (ex.: padrões mínimos a serem atendidos pela metodologia do fornecedor);
- Procedimentos para gerenciamento do projeto e garantia da qualidade;
- Métodos de projeto mandatórios;
- Requisitos de testes especiais;
- Dados de teste;
- Teste de carregamento;
- Simulações necessárias;
- Teste de Aceitação de fábrica (FAT);
- De que forma os itens a serem entregues devem ser fornecidos (ex.: formato e mídia);
- Documentação a ser entregue pelo fornecedor (ex.: especificações funcionais; especificações de testes; requisitos mínimos de *hardware* e *software*; especificações de projeto; guias ou manuais de manutenção e do usuário);
- Dados a serem preparados ou convertidos;
- Ferramentas de testes, manutenção, gerenciamento de dados e acessos;
- Cursos de treinamento;
- Instalações para arquivamento;
- Suporte e manutenção necessários após aceitação.

9.3.2.6 Glossário

Definições de quaisquer termos pouco conhecidos devem ser fornecidas.

9.3.2.7 Aprovações

Os aprovadores devem ser definidos. No mínimo, um dos aprovadores deve ser o dono do processo. Outros aprovadores poderiam ser o dono do sistema e a unidade da qualidade.

Uma vez aprovado o documento de ERU, quaisquer alterações devem ser realizadas por meio do controle de mudanças.

9.3.3 Tópicos Fora do Escopo

Esta seção é destinada a sistemas com níveis múltiplos de especificação e verificação e pode não ser aplicável a sistemas da categoria 3, de baixo risco e comercialmente disponível.

Os seguintes itens não devem ser incluídos na ERU/URS:

- Configuração do sistema/detalhes de projeto;
- Detalhes de implementação;

- Prazos do projeto;
- Custos;
- Detalhes organizacionais do projeto.

O item configuração do sistema/detalhes do projeto é uma parte da solução de como os requisitos serão atendidos, sendo definidos nas especificações subsequentes. Os detalhes de implementação também são totalmente dependentes da solução, não fazendo parte desta etapa.

9.3.4 Captura dos Requisitos

Para os sistemas de categoria 4 e 5, frequentemente é mais difícil e consome bastante tempo a preparação do documento de ERU/URS. O desenvolvimento deste documento é uma das tarefas mais importantes que a empresa regulada empreenderá dentro do projeto de implementação de um sistema computadorizado.

É imprescindível que o processo a ser automatizado seja devidamente mapeado antes de se definir a ERP/URS. Desta forma é importante detalhar o processo passo a passo, definindo as informações de entrada e de saída. Esta atividade deverá ser feita por equipe multidisciplinar, envolvendo inclusive o nível operacional.

Abaixo segue uma lista dos diversos modos que podem ser utilizados pela empresa regulada para a captura e refinamento dos requisitos do usuário:

- Discussões e entrevistas;
- Observação (entendimento do processo como um todo);
- Oficinas de trabalho - equipe multidisciplinar;
- Entendimento das armadilhas que podem ocorrer durante a definição dos requisitos.

9.4 SELEÇÃO DE FORNECEDOR DE SISTEMAS COMPUTADORIZADOS

9.4.1 Introdução

Após a construção do documento contendo os requisitos do usuário (ERU/URS), a empresa regulada irá selecionar o fornecedor do sistema computadorizado que atenda aos requisitos estabelecidos e descritos previamente.

As empresas reguladas devem executar avaliação formal de cada fornecedor de sistemas computadorizados relevantes às BPF e de seus serviços relacionados. Esta avaliação deve ser baseada na criticidade do sistema/serviço a ser provido.

Deverá existir uma justificativa formal para a não realização da avaliação de fornecedores de sistemas/serviços relevantes às BPF.

9.4.2 Tipos de Avaliação

Existem três opções para a realização de avaliação de um fornecedor de sistema/serviço:

- Avaliação básica baseada em informação disponível;
- Auditoria utilizando um questionário;
- Auditoria com visita no fornecedor realizada por um especialista, auditor ou time de auditoria.

Normalmente, uma auditoria básica é o suficiente para sistemas de baixo impacto, já para os sistemas de alto impacto pode ser necessário realizar uma avaliação mais profunda.

Auditoria por meio da utilização de questionário pode ser adequada para fornecedores de produtos e serviços padrão e configuráveis.

9.4.3 Processo de Avaliação

As etapas principais para a avaliação do fornecedor são as seguintes:

1. Tomada da decisão com base no risco, da rota mais apropriada para execução da avaliação;
2. Execução da avaliação básica, se for suficiente, ou da avaliação por meio de questionário ou da avalição por meio da visita ao fornecedor, dependendo da decisão tomada acima;
3. Relatório da avaliação;
4. Determinação das ações corretivas e de acompanhamento, que pode envolver uma visita de acompanhamento na empresa do fornecedor;
5. Aprovação ou rejeição do fornecedor.

Se o fornecedor for aprovado, ele deve ser periodicamente reavaliado pela empresa regulada, de acordo com a frequência definida em procedimento operacional padrão.

9.5 DOCUMENTO CONTENDO AS ESPECIFICAÇÕES FUNCIONAIS (EF/FS)

9.5.1 Introdução

As especificações funcionais (EF/FS) definem o sistema que atende as necessidades do usuário, descritas nas especificações dos requisitos dos usuários (ERU/URS).

Para alguns sistemas, como aqueles comercialmente disponíveis e de baixo risco, pertencentes à categoria 3, uma abordagem simples consistindo em um nível simples de especificação e verificação é apropriada e um documento contendo as especificações funcionais não é necessário.

Um documento de Especificações Funcionais define o que o sistema deve fazer e que funções e instalações serão fornecidas. Ele fornece uma lista de objetivos de projeto para o sistema. Os testes formais serão baseados nas especificações funcionais.

O documento contendo as especificações funcionais é produzido pelo fornecedor e deve ser revisado e aprovado pela empresa regulada. É frequentemente considerado um documento contratual.

As seguintes diretrizes devem ser seguidas durante a produção da especificação:

- Todas as restrições de projeto (ex.: as limitações externamente definidas que um sistema deve atender, tais como plataforma de *hardware*/*software*, velocidade, potência, teste, condições ambientais e operacionais) devem ser explicitamente documentadas;
- Ambiguidade, duplicação e contradição devem ser evitadas;
- Convenções consistentes de nomenclatura devem ser adotadas;
- Cada função e instalação descrita devem ser testáveis;
- *Interfaces* internas e externas devem ser claramente definidas;
- As especificações funcionais devem ser claras o suficiente para permitir que o projeto prossiga sem haver necessidade frequente de consulta ao autor destas especificações
    - ✓ Tanto os usuários quanto os programadores devem entender as especificações funcionais;

✓ O uso de diagramas e gráficos é recomendado quando apropriado.

As especificações funcionais devem ser preparadas e organizadas de modo que permita a rastreabilidade por todo o ciclo de vida, desde os requisitos individuais até os testes associados.

9.5.2 Conteúdo do Documento de EF/FS

Abaixo segue a lista de tópicos que podem fazer parte do documento de EF/FS, não se pretendendo ser prescritiva nem exaustiva.

9.5.2.1 Introdução

As seguintes informações devem ser fornecidas:

- Propriedade do documento;
- Quem produziu o documento, sob que autoridade e para que propósito;
- A situação contratual do documento (se aplicável);
- Relacionamento com outros documentos (ex.: ERU/URS).

9.5.2.2 Visão Geral

Deve cobrir os seguintes tópicos, quando apropriado:

- Escopo e objetivos;
- Referência aos regulamentos de BPF relevantes;
- Impacto na segurança do paciente, qualidade do produto e integridade dos dados;
- Descrição em alto nível (realizar uma subdivisão em componentes primários do sistema);
- As principais *interfaces* entre o sistema e outros sistemas e/ou o ambiente;
- Premissas/restrições;
- Não conformidades em relação às especificações dos requisitos dos usuários, devendo ser documentadas e justificadas.

9.5.2.3 Funções

A descrição em alto nível deve ser dividida ao nível das funções individuais.

Os seguintes aspectos devem ser abordados, quando apropriado:

- O objetivo da função e os detalhes de sua utilização, incluindo *interface* com outras partes do sistema. Entradas, saídas, cálculos críticos, algoritmos e o impacto em outras funções e/ou sistemas e /ou ambiente devem ser destacadas;
- Desempenho: resposta, dimensionamento, processamento centralizado ou distribuído e taxa de transferência – Estes pontos devem se quantitativos e inequívocos;
- Segurança e proteção – Ação em caso do *software* ou *hardware* selecionado falhar; auto verificação; verificação de valor de entrada; redundância; restrições de acesso; tempos fora de ar e recuperação de dados;
- Funções que são configuráveis e quaisquer limites para configuração;
- Rastreabilidade aos requisitos específicos do ERU/URS;

- Condições de falhas, ações de falhas, arquivos de registros e diagnósticos.

9.5.2.4 Dados

Os seguintes aspectos devem ser abordados, quando apropriado:

- Definição – os dados devem ser definidos de um modo hierárquico, com os objetos complexos sendo construídos de objetos mais simples (ex.: arquivos de registros). Os parâmetros críticos devem ser destacados;
- Acesso;
- Intervalo permitido para os valores de entrada e de saída;
- Campos necessários;
- Verificação da validação dos dados;
- Relacionamento dos dados;
- Capacidade de armazenamento de dados, tempo de retenção e detalhes sobre arquivamento dos dados;
- Integridade e proteção dos dados;
- Migração dos dados (importação e exportação).

9.5.2.5 *Interfaces*

As *interfaces* entre sistemas devem ser descritas, definindo como os sistemas e os subsistemas interagem, o que elas provêm e o que elas necessitam. Para sistemas regulados pelas BPx, a proteção das *interfaces* é importante. Os seguintes pontos devem ser abordados quando apropriado:

- *Interfaces* com os usuários. Isto deve ser definido em papéis (perfil de acesso), tais como, operador, administrador, gerente do sistema etc. Tópicos a serem considerados: tipos de periféricos; formato geral de telas e relatórios; tratamento e relatórios de erros e segurança. Modo(s) de entrada do usuário deve(m) ser definido(s), tais como, teclado e *mouse*, *touchscreen*; caligrafia via caneta;
- *Interfaces* com equipamentos, tais como sensores e equipamento da planta;
- *Interfaces* com outros sistemas. Isto deve cobrir a natureza e tempo de interação e os métodos e regras que governam a interação entre os sistemas. Se houver alguma restrição de *middleware*, isto deve ser registrado.

Os seguintes tópicos devem ser considerados para qualquer tipo de *interface*:

- Dados transmitidos e recebidos;
- Tipo de dados, formato, intervalos e significado dos valores;
- Tempo;
- Taxas de transferência de dados;
- Protocolos de comunicação: iniciação e ordem de execução;
- Quaisquer compartilhamentos de dados, criação, duplicação, uso, armazenagem ou destruição;
- Mecanismos para iniciação e interrupção;
- Comunicação por meio de parâmetros, áreas de dados comuns ou mensagens;
- Acesso direto aos dados internos;
- Tratamento de erros, recuperação e relatório;
- Acesso e segurança.

9.5.2.6 Atributos Não-Funcionais

O modo como o sistema irá atender aos requisitos não-funcionais devem ser descritos. Os seguintes itens devem ser abordados quando apropriado:

- Disponibilidade (confiabilidade, redundância, verificação de erro, operação em *stand-by*);
- Manutenção (possibilidades de expansão e aprimoramento; capacidade extra; mudanças prováveis no ambiente e vida útil).

9.5.2.7 Ambiente

Quaisquer requisitos especiais lógicos ou físicos, tais como encriptação ou proteção física (acesso controlado), devem ser avaliados.

9.5.2.8 Glossário

Definições de quaisquer termos pouco conhecidos devem ser fornecidas.

9.5.2.9 Apêndices

Quando apropriado, por exemplo, para pequenos sistemas, apêndices devem ser fornecidos para definição das especificações de *hardware* e *software*.

9.6 DOCUMENTO CONTENDO A CONFIGURAÇÃO E O PROJETO

9.6.1 Introdução

Esta seção aborda sobre como definir a configuração necessária dos componentes do sistema e do projeto do sistema.

Dependendo do tipo de sistema (configurável ou customizado), as especificações de configuração e de projeto fornecem uma expansão técnica detalhada das especificações funcionais. Definem os recursos e flexibilidade do sistema, as propriedades e as suas especificações. As informações geradas formam a base para subsequente atividade de gerenciamento da configuração.

Não há necessidade de preparação de documentos separados para definição da configuração e do projeto. Uma hierarquia de especificações pode ser necessária para sistemas maiores e mais complexos, já para sistemas menores mais simples ou considerados de baixo risco as especificações podem ser combinadas.

9.6.2 Visão Geral

9.6.2.1 Configuração

Para produtos configuráveis devem ser preparadas especificações de configuração que compõem o sistema para que este atenda aos requisitos do usuário. Isto inclui a definição de todas as configurações e parâmetros.

Estas especificações de configuração são produzidas pelo fornecedor do sistema e revisadas e aprovadas pela empresa regulada.

É possível manter este conjunto de especificações de configuração em sistemas que possuem gerenciamento de configuração robusto (*audit trails* detalhados e completos). Tal abordagem deve ser bem documentada.

9.6.2.2 Projeto (*Design*)

Para aplicações customizadas deve ser preparado um documento contendo o projeto do *hardware* e do *software.* Assim pode ser necessário preparar um documento contendo as especificações de configuração.

O projeto de *hardware* define os componentes de *hardware* que compõem o sistema, como por exemplo, arquitetura do componente ou do sistema, ou *interfaces*.

O projeto de *software* possui dois níveis. No nível mais alto ele define os módulos do *software* (subsistemas) que irão formar o *software* de sistema completo, as *interfaces* entre estes módulos e as interfaces entre outros sistemas externos. No nível mais baixo, o projeto de *software* descreve a operação dos *softwares* de módulos individuais. Estas especificações devem ser inequívocas, claras e precisas.

As especificações de projeto são produzidas pelo fornecedor do sistema e revisadas e aprovadas pela empresa regulada.

A empresa regulada deverá possuir uma abordagem unificada para a realização da especificação e verificação da infraestrutura que suporta os seus projetos de sistemas e tal atividade não deverá ser repetida para cada sistema.

9.6.3 Considerações Gerais

A utilização de tabelas e diagramas para ilustrar as Especificações de Configuração e de Projeto é altamente recomendado. Tabelas padronizadas podem ajudar a assegurar que todos os parâmetros e configurações foram definidos. Diagramas podem ajudar dentro do projeto de *software* a esclarecer e explicar o fluxo de dados, o controle lógico, as estruturas de dados e as *interfaces*. Diagramas no projeto de *hardware* podem ajudar a entender sobre a arquitetura e a conectividade.

Configuração e Projeto devem cobrir tanto os aspectos de *hardware* quanto de *software*. Dependendo do risco, tamanho e complexidade do sistema estes pontos podem ser cobertos por uma especificação simples ou podem demandar uma hierarquia de especificações abrangendo *hardware* e *software* separadamente. Cada especificação deve ser referenciada de modo individual e ser rastreável à especificação de alto nível associada.

Todas as especificações devem ser estruturadas de modo a apoiar a rastreabilidade por todo o ciclo de vida a partir do requerimento individual até o teste associado a este requerimento.

9.6.4 Conteúdo do Documento

As seções descritas abaixo não pretendem ser prescritivos nem exaustivos. O nível de seu detalhamento depende do risco, da complexidade e da inovação do sistema. Podem fazer parte de um documento simples ou de uma hierarquia de documentos**.**

9.6.4.1 Introdução

Deve conter os seguintes itens:

- Propriedade do documento contendo a configuração e o projeto;
- Quem produziu o documento, sob que autoridade e para que propósito;

- A situação contratual do documento (Se aplicável);
- O relacionamento com outros documentos (ERU/URS; EF/FS; outras especificações de configuração e de projeto etc.).

9.6.4.2 Visão Geral

Esta seção deve descrever brevemente a configuração e/ou projeto. Dependendo da complexidade do sistema, isto pode cobrir o sistema completo, o *hardware* e/ou *software*. Esta seção pode ser ilustrada utilizando-se diagramas.

9.6.4.3 Configuração

A configuração necessária dos componentes deve ser fornecida, incluindo, mas não limitada a:

- Configurações, ou parâmetros de configuração, necessários;
- Razão para configuração, com referência à especificação de controle;
- Ferramentas ou métodos que serão utilizados para definir as opções necessárias de configuração;
- Dependências ou impactos de/em outros módulos ou sistemas
- Itens de infraestrutura tais como sistemas operacionais ou software em camadas;
- Segurança das configurações.

Para sistemas pequenos pode ser possível incorporar estas informações dentro do documento de Especificações Funcionais.

9.6.4.4 Projeto do *Hardware*

9.6.4.4.1 O Sistema Computadorizado

A arquitetura geral do *hardware* necessário deve ser definida. Em um alto nível isto pode ser ilustrado por diagrama de blocos, apresentando tanto as funções das partes quanto seus relacionamentos funcionais. Os seguintes itens devem ser cobertos, quando apropriado:

- Sistema do computador principal – Deve descrever os componentes primários de *hardware* do sistema computadorizado principal, tais como, unidade de processamento central (CPU), memória, tipo de *bus*; exatidão do relógio etc.;
- Armazenagem – Descrever todos os dispositivos de memória propostos com suas respectivas capacidades máximas de armazenagem, tais como, *hard disk*; *CD writer*, fitas etc.;
- Periféricos – Deve descrever os dispositivos periféricos necessários, incluindo quaisquer requisitos específicos para sua instalação;
- Interconexões/redes – Deve descrever todas interconexões dos componentes de *hardware* e quaisquer conexões com outros equipamentos, dispositivos e sistemas computadorizados. Esta descrição pode conter os seguintes itens: especificações dos cabos; especificações dos conectores; requisitos de blindagem; redes ou outras conexões externas etc.;
- Configuração;
- Sistemas embutidos (dentro do equipamento de processo) – Deve incluir os seguintes elementos: diagramas de *layout* para detalhamento do painel de controle e arranjos internos e xternos; diagramas de

localização para indicar onde os sensores e outros dispositivos estão instalados no equipamento; diagramas da fiação elétrica e desenhos da tubulação/processo e diagrama de instrumentação (P&ID);

- Referência aos padrões/normas relevantes.

9.6.4.4.2 Entradas e Saída

Os formatos das entradas e saídas devem, quando necessários serem especificados. Estes podem incluir os sinais digitais e/ou analógicos.

Para os equipamentos externos os seguintes elementos devem ser considerados:

- Exatidão;
- Isolamento;
- Faixa de corrente e voltagem;
- Tipos e número de cartões de *interface*;
- Tempo.

9.6.4.4.3 Ambiente

O ambiente operacional para o *hardware* deve ser definido. Os seguintes tópicos devem ser considerados:

- Temperatura;
- Umidade;
- Interferência externa;
- Segurança física;
- Blindagem contra interferência de radiofrequência, eletromagnética e/ou UV;
- Proteção contra danos físicos tais como poeira ou vibração.

9.6.4.4.4 Fornecimento de Energia

Os requisitos para fornecimento de energia para o *hardware* configurado devem ser descritos. Os seguintes elementos devem ser considerados:

- Filtragem;
- Carregamento;
- Aterramento;
- Estabilidade;
- Fontes de alimentação ininterruptas (UPS);
- Consumo de energia e/ou emissão de calor para calcular a capacidade necessária de ar condicionado ou de sistema de aquecimento, ventilação e ar condicionado (HVAC).

9.6.4.5 Projeto do *Software*

O *software* deve ser projetado de acordo com padrões reconhecidos para desenvolvimento de *software*, quando apropriado.

Especificações de projeto de *software* são requeridos para aplicações customizadas. Estas especificações não são requeridas para sistemas configuráveis, pois neste caso o projeto de *software* é revisado ou avaliado como parte da avaliação do fornecedor do sistema computadorizado.

9.6.4.5.1 Descrição do *Software*

Os módulos que formarão o sistema computadorizado devem ser descritos, declarando-se brevemente o propósito de cada módulo. Uma lista discriminando todas as *interfaces* existentes entre os módulos e quaisquer *interfaces* com sistemas externos deve ser apresentada. Um diagrama do sistema é recomendado.

9.6.4.5.2 Dados do Sistema

Os dados do sistema e os objetos de dados relevantes devem ser definidos. Os dados devem ser caracterizados de um modo hierárquico, sendo os objetos complexos construídos a partir de objetos mais simples.

Os objetos podem incluir os seguintes itens:

- Bancos de dados e coleções de arquivos;
- Arquivos;
- Registros.

Uma descrição dos objetos de dados inclui, dentre outros:

- Tipos de dados (inteiros, números de pontos flutuantes, caracteres, booleanos, cadeia de caracteres (*string)*, objetos (imagens e documentos), etc.);
- Formato de dados (alfanumérico ou numérico, comprimento do campo, datas, etc.);
- Precisão dos dados;
- Exatidão de dados.

Cada arquivo e estrutura de dados deve ser unicamente identificado. A utilização de métodos de descrição de formatos de dados tais como “Modelo de Relacionamento de Entidade” ou similar pode ser considerado.

É aceitável que os dados de sistemas sejam definidos separadamente como em um dicionário. Se isto for feito deste modo, esta abordagem deve ser claramente explicada e documentada.

9.6.4.5.3 Descrição do Módulo

Para cada módulo, os seguintes pontos devem ser abrangidos:

- Operação do módulo: a descrição pode tomar a forma de um pseudocódigo ou fluxograma;
- *Interfaces* com outros módulos: este ponto pode referenciar ao diagrama do sistema, se houver um;
- Tratamento de erros e verificação de dados;
- Mapeamento de dados de cada módulo;
- Dados do módulo do *software*.

Para cada subprograma do módulo do *software*, os seguintes pontos devem ser cobertos:

- Operação do subprograma: a descrição pode tomar a forma de um pseudocódigo;
- As etapas envolvidas em cada processo a ser executado e as entradas e saídas de cada etapa;
- Parâmetros: cada parâmetro deve ser identificado como um dos exemplos abaixo:
  - ✓ Parâmetro de entrada;
  - ✓ Parâmetro de saída;
  - ✓ Parâmetro de entrada e de saída.
- Algoritmos;
- Deve ser identificado como cada parâmetro passa no teste, ou por valor ou por referência;
- Quaisquer efeitos colaterais do subprograma;
- Tipo de linguagem, incluindo a versão do "core" e da plataforma;
- Referência a quaisquer padrões de programação;
- Descrição ou exemplos de todas as telas de exibição;
- Dados dos subprogramas.
- Descrição ou exemplos de todos os relatórios implementados, seu significado e manipulação e quando foram gerados.

O nível de detalhe pode ser fornecido em especificações separadas.

9.6.4.6 Glossário

Definições de quaisquer termos pouco conhecidos devem ser fornecidas.

9.7 PLANO DE TESTES PARA SISTEMAS COMPUTADORIZADOS

9.7.1 Introdução

A realização dos testes no sistema atende aos seguintes objetivos:

- Identificação de defeitos que podem ser corrigidos ou removidos antes de sua utilização;
- Prevenção de falhas que podem afetar a segurança do paciente, a qualidade do produto ou a integridade dos dados;
- Provimento de evidência documentada que o sistema executa as suas funções como foi especificado;
- Demonstração de que o sistema atende aos requisitos pretendidos;
- Provimento de confiança de que o sistema é adequado para o uso pretendido;
- Provimento da base para aceitação do usuário;
- Atendimento de um requisito regulatório chave, quando apropriado.

9.7.2 Papéis e Responsabilidades

A empresa regulada deve definir os papeis e responsabilidades relacionadas à execução dos testes no sistema.

Estes papeis e responsabilidades podem incluir:

- Usuário – responsável pelo sistema em questão e pela aprovação dos documentos de teste;
- Especialista no Assunto (SME) – pode atuar como gerente de teste, executor, revisor ou autorizador;

- Gerente de teste – planejamento dos testes e redação dos planos de testes;
- Analista de teste – responsável por desenvolvimento dos casos de testes e roteiros de testes;
- Executor de teste – este papel deve ser o mais independente possível. Não deve ser o autor do *software* ou dos roteiros de testes, se possível;
- Revisor de teste – responsável por revisar os casos de testes, os roteiros de testes e os resultados de testes – não deve ser a mesma pessoa que realizou os testes;
- Unidade da Qualidade – papel definido pelas BPF;
- Fornecedor – pode atuar como planejador de testes, executor, revisor ou autorizador de alguns dos testes.

9.7.3 Estratégias de Testes

9.7.3.1 Introdução

A estratégia de testes, também conhecida como plano de testes, deve definir uma abordagem adequada para a realização de testes em um sistema computadorizado específico.

A estratégia de testes é baseada nos seguintes pontos:

- Resultados das avaliações de risco;
- Um entendimento dos componentes do sistema (categorias GAMP), da complexidade e inovação do sistema;
- Resultados das avalições do fornecedor, se aplicável.

A estratégia de testes varia de acordo com a categoria do sistema, variando de um sistema simples da categoria 3 até um sistema complexo da categoria 5. A estratégia de testes deve ser revisada e aprovada pelo Especialista no Assunto.

A estratégia de testes deve definir:

- Que tipo de testes são necessários;
- O número e o propósito das especificações de teste;
- A utilização da documentação existente do fornecedor de acordo com a avaliação realizada no fornecedor;
- As fases de testes:
  - ✓ Localização e duração de cada fase de testes;
  - ✓ Recursos necessários para cada fase de testes;
  - ✓ Responsabilidades por cada fase de testes.
- A abordagem utilizada para prover evidências da realização dos testes (ex.: impressões);
- Procedimentos para gerenciamento das falhas nos testes;
- Formato da documentação de testes;
- A utilização de métricas de testes;
- Utilização de testemunha visual da realização dos testes.

9.7.3.2 Documentação dos Testes

A figura 5 abaixo apresenta uma estrutura típica para a documentação de testes.

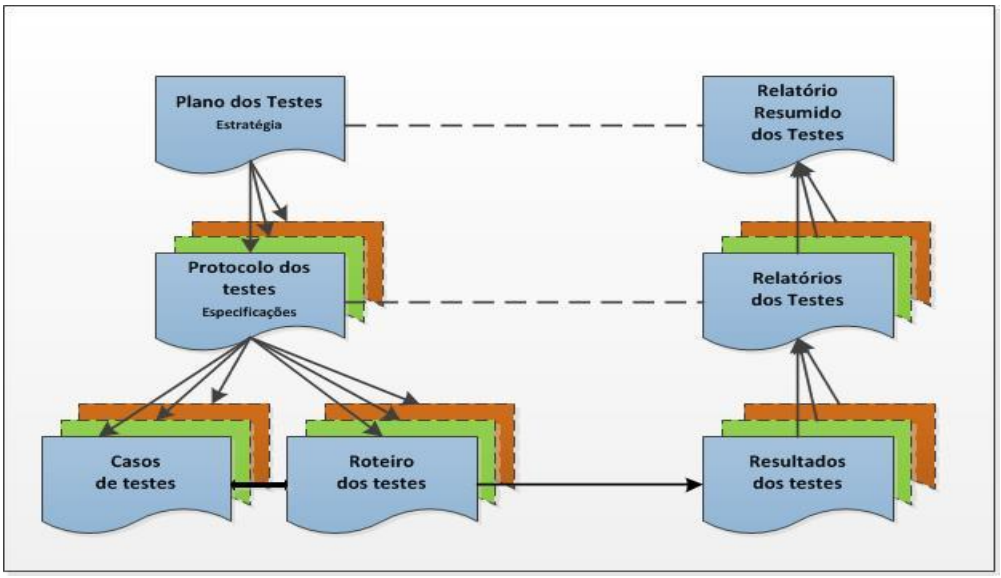

Figura 5. Estrutura Típica para Documentação dos Testes.
Fonte: GAMP5

A utilização de *templates* para realizar a documentação dos testes, tais como, especificações de testes, registros dos resultados de testes e relatório de testes, ajuda na consistência, facilita a revisão e evita erros nos documentos.

Nesta seção é descrito cada tipo de documento apresentado na figura 5.

9.7.3.2.1 Estratégia de Testes

Descrito no item 9.7.3.1.

9.7.3.2.2 Especificações de Testes

São um conjunto de roteiros de testes que são adequados para um propósito específico de uma fase específica de um projeto.

As especificações de teste devem cobrir, os seguintes pontos, quando aplicável:

- Introdução;
- Quem produziu o documento, sob que autoridade e para que propósito;
- A situação contratual do documento definido;
- Relacionamento a outros documentos;
- Escopo – deve declarar onde a especificação de teste se encaixa na estratégia geral de testes;
- Os roteiros/casos de testes a serem executados;
- Versão do *software* ou configuração em teste;
- Propósito;
- Recursos;
- Pessoal necessário para realização de cada teste ou grupo de testes;
- Métodos utilizados;
- Qualquer agrupamento ou ordenamento lógico dos testes;
- Pré-requisitos;
- Ambiente;

- Ferramentas, incluindo as ferramentas automatizadas de testes;
- Referência às especificações;
- Documentação necessária;
- Revisões e aprovações necessárias.

9.7.3.2.3 Casos/Roteiros de Testes

Os casos de testes/roteiros devem conter os detalhes dos testes. O roteiro de teste deve ser descrito em detalhe suficiente para permitir a repetição consistente do teste.

Cada roteiro de teste deve, quando possível, incluir os seguintes pontos:

- Referência de teste única;
- Referência cruzada para controle da especificação;
- Título do teste;
- Descrição do teste, incluindo o objetivo do teste;
- Etapas do teste – uma descrição passo-a-passo das ações a serem executadas pelos executores, juntamente com os resultados esperados;
- Critérios de aceitação – Resultado(s) esperados que deve(m) ser atendidos para que o parâmetro específico desafiado seja considerado aprovado ou tenha passado no teste;
- Etapas pré-testes – incluindo quaisquer pré-requisitos de testes ou preparação;
- Dados a serem registrados – descrição dos dados a serem coletados e registrados;
- Ações pós-testes – seção opcional que detalha as ações necessárias para retornar o sistema ao estado original.

9.7.3.2.4 Resultados de Testes

Os resultados dos testes devem estar disponíveis para subsequente revisão e inspeção. A informação a ser retida deve incluir os testes que passaram, os que falharam, os registros de falhas nos testes, os relatórios de testes e qualquer documentação de evidência de realização dos testes tais como impressões, notas e fotos.

9.7.3.2.5 Relatório de Testes e Relatório Resumido de Testes

Os relatórios de testes devem conter:

- Introdução;
- Escopo dos testes;
- Organização dos testes;
- Quem realizou e quem revisou os testes;
- Resumo dos resultados dos testes de uma forma tabular;
- Resumo das falhas nos testes;
- Conclusões;
- Para projetos grandes ou complexos que possuem múltiplos relatórios de testes as conclusões gerais podem ser documentadas em um relatório resumo de testes.

9.7.3.3 Componentes da Estratégia de Testes

Os seguintes pontos devem ser levados em conta no desenvolvimento da estratégia de testes:

- Políticas e procedimentos da empresa;
- Resultados das avaliações de risco;
- Resultados da avaliação de fornecedor;
- Categorias de sistemas do GAMP;
- Outros documentos, tais como: especificações dos requisitos; avaliação de risco inicial; especificação funcional; especificação de configuração; documentos de projeto; resultados de outras atividades realizadas nos diferentes estágios do desenvolvimento do *software* e matriz de rastreabilidade.

9.7.3.4 Tipos de Testes

Existem basicamente dois tipos de atividades de testes:

- Testes de Caixa Branca (*White Box Testing*) – também conhecidos como testes baseados no código ou testes estruturais, onde os testes são identificados com base no código-fonte, no conhecimento das especificações detalhadas do projeto e outros documentos do desenvolvimento;
- Testes de Caixa Preta (*Black Box Testing*) – testes realizados com base nas especificações funcionais, desta forma conhecidos como testes funcionais.

Os testes de caixa preta podem ser suficientes contanto que a avaliação do fornecedor tenha encontrado evidência adequada da realização dos testes de caixa branca.

Tipos específicos de testes devem ser considerados, dependendo da complexidade e inovação do sistema, do risco associado e da avaliação do fornecedor do sistema a ser testado, incluindo:

- Testes de Caso Normal (Caso Positivo ou Testes de Capabilidade) – desafios da habilidade do sistema para executar o que ele deveria executar, incluindo desencadeamento de mensagens de erro e de alarme, de acordo com as especificações;
- Testes de Casos Inválidos (Caso Negativo ou de Resistência) – desafios à habilidade do sistema em não fazer o que não deveria fazer, de acordo com as especificações;
- Testes de Repetibilidade – desafios à habilidade do sistema de fazer repetidamente o que deveria fazer ou continuamente, se associado a algoritmos de controle em tempo real;
- Teste de Desempenho – desafios à habilidade do sistema em fazer o que deveria fazer o mais rápido e efetivamente possível, de acordo com as especificações;
- Teste de Volume/Carga - desafios à habilidade do sistema em gerenciar altas cargas como deveria fazer. Testes de volume/carga são necessários quando os recursos do sistema são críticos;
- Teste de Regressão - desafios à habilidade do sistema para:

1. Manter as funcionalidades após ser modificado de acordo com requisitos especificados;
2. Assegurar que os módulos do *software* não envolvidos nas modificações não sejam afetados adversamente.

- Testes de Estrutura/Caminho - desafios à estrutura interna do programa para desafiar as rotinas/algoritmos, valores das variáveis, valores de retorno das funções etc.

Os testes devem desafiar o sistema. Assim, por exemplo, se o sistema for concebido ou pretendido para registrar os valores dos parâmetros monitorados ou controlados em um banco de dados a uma frequência estabelecida (ex.: a cada segundo, minuto, etc.), essa condição ou pior caso deve ser testada de forma a assegurar que os dados gerados durante a rotina serão gravados corretamente.

9.7.3.5 Ambientes de Testes

A estratégia de teste deve considerar e definir os ambientes necessários para a realização dos testes. Para sistemas típicos da categoria 3 haverá somente um ambiente. Para sistemas mais complexos, a realização dos testes pode ocorrer em diferentes ambientes durante a fase de projeto, que podem incluir:

- Ambiente de desenvolvimento, onde ocorre a produção do protótipo ou a programação;
- Ambiente de teste, onde os testes formalmente são executados;
- Ambiente operacional onde o sistema está instalado em seu ambiente-alvo.

Os testes formais, à medida do possível, devem ser executados em ambiente operacional. Para tal, os registros devem ser claramente distintos dos registros de produção ou os registros de testes podem ser arquivados antes do início da operação. Os testes também poderão ser executados em um ambiente de teste separado ou nos dois ambientes.

Os documentos de testes devem especificar que ambiente irá ser utilizado. Ao ser utilizado um ambiente de teste, a estratégia de teste escolhida deve justificar a equivalência dos resultados dos testes aos resultados que seriam obtidos no ambiente operacional.

Testes formais devem ser executados somente em ambientes sob gerenciamento da configuração.

9.7.3.6 Testes de Aceitação

Testes de aceitação são aqueles específicos realizados para atender algumas necessidades contratuais. Estes testes usualmente formam parte de um pré-definido grupo de testes funcionais realizados para demonstrar a adequação do sistema ao uso pretendido e atendimento aos requisitos do usuário. Em tais situações, deve-se aproveitar resultados dos testes já realizados, evitando assim duplicações de testes.

A aceitação pode ser realizada em duas etapas, Aceitação na Fábrica (*Factory*) ou da Planta (*Site*), a saber:

- Testes de Aceitação na Fábrica (*Factory Acceptance Tests* – FAT) – são executados nas instalações do fornecedor antes de sua entrega, para mostrar que o sistema está funcionando bem o suficiente para ser instalado e testado nas instalações do usuário;
- Testes de Aceitação na Planta (*Site Acceptance Tests* – SAT) - são executados nas instalações da empresa regulada para mostrar que o sistema está funcionando no seu ambiente operacional e que sua *interface* com outros sistemas e periféricos e está funcionando corretamente.

Esta abordagem é frequentemente utilizada para equipamentos automatizados e sistemas de controle.

O ambiente para a realização do teste de aceitação (teste ou operacional) deve ser definido.

9.7.4 Execução dos Testes

Todos os testes são executados de acordo com especificações e roteiros pré-definidos e aprovados e mantidos sob controle de versão.

9.7.4.1 Pré-requisitos

Os seguintes requisitos gerais devem ser atendidos antes de se iniciar a execução formal dos testes:

- Deve existir um gerenciamento de configuração formal antes de se iniciar a execução formal dos testes. Todos os itens a serem testados (*Firmware/software/hardware*) que estão dentro do escopo da fase de testes específica, devem ser considerados como linha de base e estar sob controle de mudanças antes da execução dos testes;
- Toda a documentação necessária deve estar disponível como descrita nas especificações de testes;
- Todos os pré-requisitos devem estar disponíveis;
- Se houver necessidade de calibração de algum equipamento, isto deve ser efetuado e documentado. O equipamento de calibração deve ser certificado, rastreável a padrões nacionais e referenciado de acordo com os procedimentos dos clientes;
- Todo o pessoal responsável pela execução dos testes, incluindo os usuários finais, deve ser treinado nos procedimentos de teste e deve ser capaz de demonstrar confiança suficiente para operação do sistema em teste. O treinamento deve ser documentado.
- Todos os colaboradores envolvidos devem estar treinados nas Boas Práticas de Documentação.

9.7.4.2 Execução

Os testes devem ser executados da seguinte forma:

- De acordo com uma especificação pré-definida e pré-aprovada.
- Cada teste deve ser executado de acordo com o roteiro de teste e os resultados devem ser registrados;
- Cada teste deve ser executado por uma pessoa adequadamente treinada, inclusive nas Boas Práticas de Documentação;
- Os resultados dos testes devem ser documentados diretamente no momento de sua execução e devem ser mantidos;
- Todos os resultados de testes devem ser registrados imediatamente e com exatidão;
- A identidade do executor do teste deve ser registrada;
- Os registros de testes feitos manualmente devem ser legíveis. Anotações de forma abreviadas devem ser evitadas e valores reais devem ser registrados sempre que possível;
- O executor do teste deve decidir se o critério de aceitação é atendido e se o teste passou ou não. O roteiro de teste deve declarar se o teste PASSOU ou FALHOU;
- No caso de uma FALHA no teste, o executor deve decidir se continua a execução dos testes, aborta os testes ou se refere ao item 9.7.4.4 (Revisão de Testes), de acordo com procedimentos de testes aprovados. Todos os testes que falharem devem ser registrados;
- Os procedimentos de testes devem ser flexíveis o suficiente para permitir ao executor do teste poder decidir se continua a realizar o teste quando encontrar situações tais como quando constatado que o sistema funciona corretamente, mas o roteiro de teste está incorreto;
- Todos os testes que falharem devem ser rastreáveis durante a correção até o fechamento final. As correções dos testes falhos podem requerer testes de regressão para se verificar que as correções não introduziram novos problemas em outros módulos ou rotinas do sistema.

A execução dos testes deve ser auditada periodicamente, por amostragem, pela Unidade da Qualidade da empresa regulada.

9.7.4.3 Documentação-Suporte dos Testes

Documentação, tais como impressões, impressões de telas, anotações, fotos etc., são necessárias para dar suporte aos resultados dos testes.

Sistemas mais complexos necessitam documentação-suporte mais extensiva e completa do que sistemas mais simples.

Documentação-suporte desnecessária, que não adiciona qualquer valor aos resultados dos testes deve ser evitada.

9.7.4.4 Revisão dos Testes

Após a conclusão da execução dos testes os resultados devem ser revistos para verificar:

- Que todos os testes foram cobertos;
- A legibilidade, exatidão e completude dos testes;
- Que todos os documentos relevantes foram incluídos e que a documentação está completa e corretamente preenchida;
- Que os critérios de aceitação foram cumpridos;
- Que todos os registros de testes falhos foram incluídos;
- Conformidade com os procedimentos.

Alternativamente o executor dos testes pode solicitar uma revisão dos testes quando ocorrer uma falha, de modo a se decidir quais ações serão tomadas e quais serão as próximas etapas.

As revisões devem ser realizadas e documentadas por uma pessoa diferente do executor do teste, tal como um revisor de teste ou um grupo, ou o especialista no assunto.

Em caso de falhas nos testes, o revisor dos testes deve decidir que ação irá tomar e que tipo de reteste será executado, se necessário. Estas decisões devem ser documentadas.

Falhas nos testes podem resultar de:

- Erro no modo como o roteiro foi escrito. Ação corretiva: atualização, seguida da aprovação do roteiro de testes corrigido e considerar a necessidade da realização de reteste;
- Erro no modo como o requisito foi definido. Ação corretiva: atualização do requisito, com possível execução de reteste e explanação no relatório de teste;
- Erro no modo como o teste foi executado pelo testador. Ação corretiva: repetição do teste;
- Erro do sistema. Ação corretiva: aplicação de um controle de mudança e repetição do teste.

9.7.5 Atividades de Testes Realizadas pelo Fornecedor

Há diferentes modelos de desenvolvimento de *software*, incluindo:

- Cascata;
- Espiral;
- Prototipagem;
- Modelo em V.

Qualquer que seja o modelo utilizado, o fornecedor deve definir a implantação do modelo, incluindo os controles de qualidade necessários e descrever o modo utilizado para demonstrar que o sistema computadorizado é adequado para o uso pretendido.

As estratégias de testes devem ser estabelecidas, implantadas e documentadas adequadamente.

A configuração do *hardware* e do *software* utilizada nos testes deve ser documentada. Isto inclui: sistemas subjacentes tais como sistema operacional, banco de dados e rede; *hardware* para redes; servidores e clientes, quando apropriado.

9.7.5.1 Testes Realizados Durante o Desenvolvimento

Testes internos realizados pelo fornecedor devem ser executados de acordo com especificações de testes definidas e aprovadas. Tipos de testes mais comumente executados são:

- Teste de aceitação para o *hardware* e *software* adquiridos – *hardware* e *software* comprados devem ser sujeitos a testes de aceitação antes de serem utilizados para o desenvolvimento do sistema;
- Testes dos módulos/unidades – testes individuais nos componentes do *software*, garantindo prontidão para a posterior inserção em um sistema integrado;
- Testes de Integração e do Sistema – testes dos componentes integrados do sistema, subsistemas e do sistema completo.

9.7.5.2 Testes Contratuais

As atividades de execução de testes e verificação devem ser definidas para propósito de negócios, entre o fornecedor do sistema computadorizado e a empresa regulada.

9.7.6 Testes Automatizados

Ferramentas automatizadas de execução de testes de verificação podem ser utilizadas para melhorar a efetividade e a eficiência da execução dos testes. Podem ser utilizadas tanto para a execução dos testes de caixa preta quanto dos testes de caixa branca.

Qualquer utilização destas ferramentas deve ser definida na estratégia de testes.

Estas ferramentas devem ser utilizadas de acordo com instruções e manuais definidos e mantidos sob Gerenciamento da Configuração. Normalmente pertencem à categoria 1 do GAMP.

É importante que sejam definidas as responsabilidades com relação aos seguintes aspectos:

- Propriedade (Quem é o dono), administração e manutenção da ferramenta de teste;
- Manutenção dos dados dos testes;
- Manutenção dos documentos de testes (incluindo especificações de testes, roteiros de teste e resultados dos testes);
- Instruções e manuais de uso.

Preferencialmente, estas ferramentas de testes deveriam possuir os recursos de assinaturas eletrônicas e registros eletrônicos que atendam aos requerimentos regulatórios.

9.7.6.1 Exemplos de Ferramentas de Execução de Testes Automatizados

Abaixo seguem alguns exemplos de ferramentas para execução automatizada (depuração de código fonte e ferramentas de testes) de testes do código fonte:

- *Drivers* de testes automatizados (execução automática dos testes);
- Geradores de dados de testes;
- Simuladores de ambientes;
- Analisadores estáticos;
- Executores dinâmicos;
- Executores simbólicos;
- *Drivers* de volume/carga.

9.7.6.2 Documentação dos Testes Automatizados

Os roteiros de testes automatizados devem ser controlados de acordo com procedimentos aprovados.

Os registros (*logs*) gerados pelo computador resultantes da execução dos roteiros automatizados de testes são normalmente gerados automaticamente a partir da execução dos roteiros.

O cabeçalho do registro (*log*) deve prover a seguinte informação:

- Identificação do registro;
- Data e hora da execução;
- Nome e versão do roteiro de teste;
- Identidade do executor do teste e o nome do ambiente de teste.

O registro não pode ser editado ou apagado. Eles devem ser arquivos do tipo “somente leitura” (*read-only*), devendo ser mantidos para revisões ou auditorias futuras.

A documentação de testes automatizados deve ser mantida no mínimo pelo mesmo período que os registros de testes realizados em papel.

A utilização e o gerenciamento da documentação de testes automatizados devem ser aprovados previamente pela Unidade da Qualidade como parte do desenvolvimento da estratégia de testes.

9.7.7 Testes Aplicados às Diferentes Categorias de Sistemas

Esta seção apresenta as considerações práticas para o planejamento dos testes a serem realizados nos sistemas pertencentes às categorias 3, 4 e 5.

Para aqueles sistemas computadorizados em cuja composição faz parte um equipamento gerenciado por uma aplicação (*software*), há a necessidade de se realizar também a qualificação destes equipamentos, cuja metodologia é descrita em guias internacionais e legislações específicas e não é escopo deste guia.

As atividades de IQ e OQ de *hardware*/*software* muitas vezes são realizadas pela empresa fornecedora do software, mas tais atividades devem ter participação ativa na realização e aprovação por parte da empresa regulada.

9.7.7.1 Aspectos Aplicáveis a Todas as Categorias de Sistemas

9.7.7.1.1 Testes de Instalação de *Hardware/Software* (IQ)

Muitas empresas denominam esta atividade de Qualificação de Instalação (IQ). O propósito é verificar e documentar que os componentes do sistema estão instalados de acordo com as especificações, documentação do fornecedor e requisitos locais e globais.

Deve ser evidenciada que a documentação junto com a sistema está completa e que os requisitos de instalação e de uso local e global estão de acordo as especificações.

Os testes de instalação fornecem uma linha de base de configuração para as subsequentes atividades de verificação e validação, permitindo verificar os métodos de instalação, as

ferramentas de testes e/ou roteiros utilizados. Isto compõe a base para o gerenciamento da configuração do sistema instalado.

Os testes de instalação devem verificar se os seguintes documentos estão disponíveis, quando apropriado:

- Guias técnicos e do usuário;
- Procedimentos operacionais padrão;
- Cronogramas de treinamento;
- Acordos de Nível de Serviço;
- Procedimentos de segurança;
- Livros de registro;
- Inventário do *hardware;*
- Lista de instrumentos;
- Folhas de especificações;
- Certificados e procedimentos de calibração;
- Diagramas de tubulação/processo e instrumentação (P&ID);
- Lista de equipamentos e folhas de especificações;
- Inventário do *software* (incluindo procedimento de instalação, lista de *software* do sistema, lista de *softwares* de aplicação, lista de dados, configurações iniciais de dados para inicialização);
- Código-fonte do programa (categoria 5);
- Programa de manutenção preventiva;
- Lista de peças de reposição críticas.

9.7.7.1.2 Testes de Operações de *Hardware/Software* (OQ)

Abaixo segue uma lista geral, aplicável a todos os sistemas. Deve ser utilizada para ajudar na verificação do sistema instalado:

- Teste de queda de energia (prevenção contra perda de dados críticos ou perda da ação de controle; facilidade de reinicialização do controle);
- Acesso ao sistema e recursos de sistema;
- Trilhas de auditoria e registro de ações críticas, incluídas interações manuais;
- Recursos de entrada manual de dados e validação da entrada;
- Recursos de assinatura eletrônica;
- Mensagens de erro e de alarme;
- Cálculos críticos;

- Transações críticas;
- Transferência de dados críticos para outros pacotes ou sistemas para posterior processamento;
- *Interfaces* e transferência de dados;
- *Backup* e restauração;
- Arquivamento e recuperação de dados;
- Habilidade em lidar com cargas de alto volume, particularmente se o sistema for acessado por muitos usuários ou necessitar registrar muitos valores dos parâmetros controlados/monitorados ao mesmo tempo, como parte de uma aplicação em rede, por exemplo.

9.7.7.2 Atividades de Testes para um Produto Não-Configurado

Estes sistemas computadorizados são aqueles denominados de sistemas de "prateleira" (*Off-the-shelf*), significando que não são configurados para um processo específico de negócio ou são utilizados com a sua configuração padrão (*default*). São classificados como categoria 3 do GAMP.

A empresa regulada pode decidir por fazer uma avaliação do fornecedor para verificar a qualidade do produto, dependendo do risco. Baseado no resultado satisfatório desta avaliação e dos riscos envolvidos, uma abordagem simples consistindo em um nível apenas de especificação e verificação pode ser aplicada.

Os testes devem ter como foco os seguintes pontos:

- Aqueles relacionados à instalação do sistema, descritos no item 9.7.7.1.1;
- Testes dos Requisitos do Usuário que demonstrem a adequação ao uso pretendido, podendo incluir a realização de testes de funcionalidade do sistema em comparação aos requisitos pré-estabelecidos, dependendo do risco envolvido;
- Os Testes dos Requisitos do Usuário devem também incluir a entrega e aceitação da documentação completa enviada pelo fornecedor, incluindo especificações, manuais e desenhos, se ainda não realizados;
- Quaisquer testes posteriores ou mais rigorosos em função das avaliações de risco e do fornecedor;
- Quaisquer outros aspectos relevantes listados no item 9.7.7.1.2.

9.7.7.3 Atividades de Testes para um Produto Configurado

Um produto configurado envolve a configuração de um *software* comercialmente disponível que roda em componentes padrão de *hardware*. Estes sistemas que são configurados para um processo de negócio específico são classificados como categoria 4 do GAMP.

Em tal situação, baseado no resultado satisfatório da avaliação do fornecedor e nos riscos envolvidos, a estratégia de testes utilizando a abordagem de três níveis (configuração, funcionalidade e requisitos) é a recomendada. A quantidade de documentos de testes necessários para cobrir estes três níveis dependerá da complexidade e do impacto do sistema.

Os testes devem ter como foco os seguintes pontos:

- Aqueles relacionados à instalação do sistema, descritos acima no item 9.7.7.1.1;
- Testes de Configuração – para cada Especificação de Configuração deve existir uma Especificação de Teste de Configuração associada. Os testes devem verificar se o sistema foi
instalado de acordo com as especificações. Os testes podem ser realizados por meio de inspeção ou verificação da documentação do fornecedor;

- Testes Funcionais – funcionalidade que dá suporte ao específico processo de negócio. Nesta atividade a documentação do fornecedor pode ser aproveitada. Tipos possíveis de testes funcionais: caso normal (positivo); caso inválido (negativo); repetibilidade; desempenho; volume/carga; regressão; testes estruturais;
- Testes dos Requisitos do Usuário que demonstrem a adequação ao uso pretendido, podendo incluir a realização de testes de funcionalidade do sistema em comparação aos requisitos pré-estabelecidos, dependendo do risco envolvido;
- Os testes de requisitos devem também incluir a entrega e aceitação da documentação completa enviada pelo fornecedor, incluindo especificações, manuais e desenhos, se ainda não realizados;
- Quaisquer testes posteriores ou mais rigorosos realizados como resultado das avaliações de risco e do fornecedor;
- Quaisquer outros aspectos relevantes listados no item 9.7.7.1.2.

9.7.7.4 Atividades de Testes para uma Aplicação Customizada

Alguns sistemas computadorizados são desenvolvidos para atender requisitos específicos do usuário, quando não existem soluções comercialmente disponíveis. Os *softwares* desenvolvidos para tais sistemas são classificados como categoria 5 do GAMP.

Em tais casos e baseados na avaliação satisfatória do fornecedor e dos riscos envolvidos, uma abordagem de testes baseada nos quatro níveis (projeto do módulo (unidade); integração; funcionalidade e requisitos) é aplicável.

A quantidade de documentos de testes necessários para cobrir estes quatro níveis dependerá da complexidade e impacto do sistema.

Os testes devem ter como foco os seguintes pontos:

- Aqueles relacionados à instalação do sistema, descritos no item 9.7.7.1.1;
- Revisão do novo código, requerida como resultado da avaliação de risco;
- Testes dos módulos de *software* para verificar se estão de acordo com as suas especificações de projeto – para cada Especificação de Projeto de Módulo de *Software*, uma Especificação de Teste de Módulo de *Software* associada deve ser produzida. Os testes de módulo de *software* a serem executados devem assegurar que o módulo de software atende às especificações;
- Testes de integração de software para testar se os módulos funcionam corretamente quando operando em conjunto – a Especificação de Testes de Integração de Software define aqueles testes que demonstram que todos os módulos de software se comunicam entre si corretamente e que o sistema de software atende à especificação de projeto. Uma Especificação de Teste de Integração de Software deve ser produzida quando mais de um módulo de software compor o sistema final;
- Teste de configuração (se aplicável) – para cada Especificação de Configuração, uma Especificação de Teste de Configuração associada deve ser produzida. Os testes devem verificar se o sistema foi configurado de acordo com a especificação. Os testes podem tomar a forma de inspeções ou verificação da documentação do fornecedor;
- Testes Funcionais – funcionalidade que suporta o processo específico de negócio com base nas avaliações de risco e do fornecedor (Esta é uma área na qual a documentação do fornecedor pode ser aproveitada);
- Testes dos Requisitos (URS) - demonstrar que o sistema é adequado para o uso pretendido; isto pode incluir a realização de testes da funcionalidade do sistema contra os requisitos pré-definidos, com base no risco;

- Os testes dos requisitos devem também incluir a entrega e aceitação de toda a documentação do fornecedor, incluindo especificações, manuais e desenhos, se ainda foi realizada esta atividade;
- Quaisquer testes posteriores ou mais rigorosos realizados como resultado das avaliações de risco e do fornecedor;
- Quaisquer outros aspectos relevantes listados no item 9.7.7.1.2.

9.7.8 Relatório de Testes

Deve ser gerado relatório de teste que resuma as atividades realizadas e os resultados obtidos e que contenha as conclusões finais.

A aprovação do relatório de testes constitui a liberação formal do sistema para execução das etapas subsequentes do ciclo de vida.

Os relatórios de testes devem atender os requisitos das especificações de teste correspondentes ou no caso de um relatório de resumo de testes, deve atender com os requisitos da estratégia de teste.

9.8 ATIVIDADES COMPLEMENTARES

9.8.1 Descrição do Sistema

9.8.1.1 Introdução

Esta seção busca atender um requisito regulatório recorrente:

“Deve existir uma descrição atualizada e detalhada do sistema, contendo os princípios, objetivos, itens de segurança, alcance do sistema e suas principais características de uso, e a *interface* com outros sistemas e procedimentos.”

A necessidade de uma descrição do sistema pode ser coberta por uma ou mais especificações existentes ou outros documentos ou um documento separado pode ser produzido.

O principal uso de tal documento é ajudar novos usuários e reguladores a entender o que o sistema faz e como tal é escrito em uma linguagem não técnica até onde for possível.

9.8.1.2 Considerações Gerais

A Descrição do Sistema deve ser mantida por toda a vida útil do sistema.

Para sistemas complexos que são utilizados por diversos departamentos ou plantas/sítios (ex.: ERU) um documento separado pode ser o mais adequado. Para sistemas mais simples é prática comum incluir a descrição do sistema em uma outra especificação ou outro documento.

Uma descrição completa do sistema, que atenda às expectativas regulatórias, deve ser estabelecida antes do sistema ser liberado para uso operacional.

A descrição do sistema deve ser sujeita a controle de mudanças e revisão periódica.

9.8.1.3 Conteúdo do Documento

A descrição deve cobrir somente as características principais do sistema. Informação detalhada sobre tópicos específicos deve ser incluída em outras especificações e não repetidas.

9.8.1.3.1 Introdução

Esta parte deve explicar o contexto do sistema dentro do processo de negócio e da empresa regulada em geral. Isto deve ser considerado a partir das seguintes perspectivas:

- Departamental;
- Dentro da planta/sítio;
- Dentro da divisão;
- Do ponto de vista global.

9.8.1.3.2 Funcionalidade do Sistema Principal

Esta parte contempla a descrição das funções-chave do sistema, tanto em relação às BPx quanto às não BPx, sendo que muitas delas podem ser críticas para o negócio.

As funções podem ser agrupadas para manter a descrição em alto nível. A utilização de diagramas é encorajada para explicar relacionamentos entre funções-chave.

9.8.1.3.4 Ambiente Computacional

Esta parte deve ser coberta por um diagrama de alto nível apresentando a arquitetura que dá suporte ao sistema, abrangendo, quando apropriado:

- A infraestrutura que dá suporte ao sistema (ex.: configurações do servidor, arranjos de armazenagem etc.);
- *Interfaces* para os usuários;
- *Interfaces* para equipamentos;
- *Interfaces* para outros sistemas;
- *Interfaces* fora da empresa;
- O fluxo de dados por meio das *interfaces;*
- Características de segurança tais como *firewalls.*

9.8.1.3.5 Componentes do Sistema

Uma indicação dos componentes principais de *hardware* e de *software* devem ser fornecidos. Deve incluir informação acerca dos servidores e equipamentos de armazenagem, bem como os sistemas operacionais, tipos de banco de dados e aplicações. Deve fazer referência a qualquer documentação de configuração relevante para o sistema. Um inventário detalhado de todos os componentes do sistema não é necessário neste documento.

9.8.1.3.6 *Interfaces* do Sistema

Esta parte deve contemplar uma visão geral das *interfaces*-chave para outros sistemas e equipamentos, assim como o fluxo de dados entre os sistemas envolvidos.

9.8.1.3.7 Controle de Acesso

Esta parte deve contemplar uma visão geral das características de controle de acesso ao sistema, tanto físico (se relevante) quanto lógico.

9.8.1.3.8 Controles de Segurança

Esta parte deve contemplar uma visão geral dos controles de segurança estabelecidos, tanto físicos quanto lógicos. Estes devem incluir o *software* para proteção dos dados e registros, como, por exemplo, antivírus e anti-*malware*.

9.8.1.3.9 Registros e Assinaturas eletrônicos

Deve ser incluída uma descrição dos tipos de registros eletrônicos criados e gerenciados pelo sistema e os tipos de assinaturas eletrônicas utilizadas, se for relevante.

9.8.1.3.10 Glossários

Definições de quaisquer termos que não sejam familiares devem ser fornecidas.

9.8.2 Gerenciamento da Configuração e de Mudança

Processos para gerenciamento da configuração devem ser estabelecidos de modo que o sistema computadorizado e todos seus componentes possam ser identificados e definidos a qualquer momento.

Devem ser estabelecidos também procedimentos para o gerenciamento de mudanças. O ponto ou fase na qual o gerenciamento de mudanças foi introduzido deve ser definido. Este gerenciamento deve ser aplicado tanto para a fase de projeto quanto para a fase operacional.

Qualquer envolvimento do fornecedor nestes gerenciamentos deve ser definido e acordado.

9.8.3 Revisão de Projeto

Em etapas adequadas do ciclo de vida, revisões de projeto planejadas e sistemáticas das especificações do projeto e desenvolvimento devem ser realizadas. Esta revisão do projeto deve avaliar os resultados a serem obtidos para assegurar que eles satisfaçam os requisitos especificados. Ações corretivas devem ser definidas e desenvolvidas.

O rigor da execução da revisão de projeto e a extensão da documentação deve ser baseada em risco, complexidade e inovação.

9.8.4 Gerenciamento da Documentação

O gerenciamento da documentação inclui preparação, revisão, aprovação, emissão, mudança, retirada e arquivamento.

9.8.5 Matriz de Rastreabilidade

Rastreabilidade é um processo para que:

- Os requisitos sejam endereçados e rastreáveis às respectivas especificações de projeto e funcionais.
- Os requisitos sejam rastreáveis às respectivas verificações.

Além de demonstrar cobertura do projeto e da verificação, a rastreabilidade ajuda na avaliação e no gerenciamento de mudanças.

A rastreabilidade deve focar nos aspectos críticos para a segurança do paciente, qualidade do produto e integridade dos dados e é conhecida como Matriz de Rastreabilidade dos Requisitos

Para produtos não-configurados, rastreabilidade entre os requisitos do usuário e a verificação realizada pode ser o suficiente.

Para produtos configurados, a coluna de especificação de desenho (*Design Specification* - DS) pode ser substituída por uma conexão com os itens de configuração, proporcionando rastreabilidade entre requisitos do usuário, configuração e verificação.

Para aplicações customizadas, a rastreabilidade deve ser apresentada desde o nível de especificação de projeto, passando pelas especificações funcionais até a verificação dos requisitos do usuário.

A figura 6 apresenta um exemplo de matriz de rastreabilidade, sendo que AR, significa Análise de Risco.

Requisito	Análise de riscos	Especificação Funcional	Especificação do Projeto	Teste
U1.1.1	AR1	F2.4.1	D2.5	T1.1
U1.1.2	AR2	F2.4.5	D2.4	T1.2
U1.2.1	AR3	F3.1	D1.1	T2.3.1
U1.2.2	AR4	F3.2	D1.2	T8.1
U1.2.3	AR5	F3.3	D.3.3	T8.2

Figura 6. Exemplo de Matriz de Rastreabilidade.
Fonte: GAMP5

9.9 RELATÓRIO DE VALIDAÇÃO

9.9.1 Introdução

Deve ser produzido um relatório de validação com foco nos aspectos relacionados à segurança do paciente, à qualidade do produto e à integridade dos dados. Ele deve resumir as atividades executadas, quaisquer desvios ocorridos em relação ao que foi planejado, as ações corretivas mais importantes e uma declaração acerca do atendimento do sistema ao uso pretendido.

O nível de detalhamento do relatório deve refletir o risco, a complexidade e a inovação do sistema

A estrutura do relatório deve refletir a estrutura do plano correspondente.

O relatório deve ser aprovado, pelo menos, pelo dono do processo e a pela Unidade da Qualidade. Pode também ser apropriado que outros aprovadores do plano correspondente também aprovem o relatório, tal como o dono do sistema.

É comum que se produza um relatório final. Podem existir, contudo outros relatórios (parcial ou de fases da validação) que alimentem este relatório final ou que seja criado depois para suplementá-lo.

9.9.2 Conteúdo do Relatório de Validação do Sistema Computadorizado

9.9.2.1 Introdução e Escopo

A introdução deve refletir o plano correspondente e ressaltar quais diferenças possam ter surgido desde que o plano foi emitido. Deve conter a seguinte informação:

- Propósito e escopo do relatório;
- Quem elaborou o relatório e sob que autoridade;
- Resumo da abordagem utilizada;
- Referência cruzada aos planos, procedimentos e políticas que nortearam o relatório.

9.9.2.2 Mudanças de Escopo

Pode ser necessário alterar a abordagem inicial. O relatório deve ressaltar e justificar tais alterações de escopo.

9.9.2.3 Avaliação do Fornecedor

As atividades de avaliação do fornecedor devem ser resumidas ou referenciadas a outros documentos-fonte, tais como um Relatório de Avaliação ou Auditoria do Fornecedor.

Se a documentação do fornecedor foi aproveitada/utilizada, deve haver uma discussão sobre as medidas tomadas para assegurar a sua adequação.

Informação já disponível em outros documentos não deve ser repetida.

Conteúdo de relatórios de auditoria no fornecedor não deve ser incluído no relatório de validação.

9.9.2.4 Resumo das Atividades

O resumo deve se referir à documentação existente e não deve haver duplicação de informação.

Esta seção pode incluir subseções relevantes à cada fase.

9.9.2.5 Resumo dos Resultados Obtidos

O relatório deve verificar que todos os resultados esperados no plano de validação correspondente foram obtidos e aprovados. Isto inclui a documentação de desenvolvimento do sistema e Procedimentos Operacionais Padrão (POP) necessários para o suporte operacional.

9.9.2.6 Resumo dos Desvios e Ações Corretivas

O relatório deve descrever quaisquer atividades e resultados que não atenderam às expectativas especificadas no plano e explicar o seu impacto e as respectivas ações corretivas. As ações corretivas mais importantes devem ser ressaltadas e os próximos passos adequados identificados ou referenciados.

9.9.2.7 Declaração da Adequação ao Uso Pretendido

Deve haver uma clara declaração sobre a situação do sistema e se ele é adequado para o uso pretendido, tendo em mente quaisquer desvios ou ações corretivas importantes.

9.9.2.8 Treinamento

O relatório deve verificar que o pessoal envolvido com os novos processos, equipamentos ou sistemas tenham sido treinados e que este treinamento foi documentado.

9.9.2.9 Manutenção do Atendimento e Adequação ao Uso Pretendido

O relatório deve delinear como a situação de atendimento do sistema será mantida. Isto pode ser eficientemente atingido referenciando-se as políticas e procedimentos relevantes. Vide os documentos descritos na Seção 11 deste Guia.

9.9.2.10 Glossário

Definições de quaisquer termos pouco conhecidos devem ser fornecidos.

9.9.2.11 Apêndices

Pode haver a necessidade da existência de apêndices, dependendo do propósito, tamanho e complexidade do relatório, o estilo corporativo da empresa regulada e suas políticas adotadas para a preparação de relatórios.

10.LISTA DE INVENTÁRIO

As empresas reguladas devem manter um inventário de sistemas computadorizados.

O inventário deve apresentar informação resumida sobre cada sistema, descrevendo: nome do sistema; equipamento ou aplicação associado(a); impacto/criticidade em relação às BPx; categoria do GAMP; propriedade (setor, dono do sistema, dono do processo); versão atual; fornecedor; situação de validação.

Equipamentos automatizados podem ser listados separadamente e duplicação deve ser evitada.

O inventário deve abranger o nível de sistemas que dão suporte aos processos do negócio e não itens individuais de *hardware* (componentes) que devem ser cobertos por procedimentos locais do setor de tecnologia de informação.

Este inventário pode ser utilizado para o planejamento das revisões periódicas.

11.FASE OPERACIONAL DE SISTEMAS COMPUTADORIZADOS

11.1 INTRODUÇÃO

Esta seção trata da fase do ciclo de vida do sistema subsequente a sua validação, na qual o sistema computadorizado validado é liberado para utilização pelo usuário final.

A fase operacional pode durar muitos anos e pode incluir mudança de *software*, *hardware*, processo de negócio e requisitos regulatórios. A integridade do sistema e de seus dados deve ser mantida por todo o período de sua utilização, incluindo quando for aposentado, e deve ser verificada quando for realizada sua revisão periódica.

À medida que se for adquirindo experiência com o sistema computadorizado, devem ser buscadas oportunidades de melhoria para o processo e sistema, com base na revisão periódica, na avaliação dos dados operacionais e de desempenho, nas análises das causas-raiz das falhas ocorridas. Informações obtidas dos processos de gerenciamento de incidentes e das CAPA's podem prover dados relevantes para a avaliação do sistema.

O gerenciamento de mudança deve prover um mecanismo para a adoção imediata de melhorias tecnicamente adequadas de acordo com as abordagens utilizadas para especificação, projeto e verificação descritos neste Guia. O rigor da abordagem, incluindo a extensão da documentação e da verificação deve ser baseada no risco e na complexidade da mudança.

A tabela 3 apresenta os procedimentos necessários para o bom andamento da fase operacional do sistema computadorizado.

Tabela 3. Procedimentos Operacionais Associados à Fase Operacional do Sistema.

Grupos de Processos	Procedimentos	Seção
Entrega	• Processo de Entrega	**11.2**
Gerenciamento de serviço e Desempenho de Desempenho	• Estabelecimento e Gerenciamento dos Serviços de Suporte	**11.3**
	• Monitoramento de Desempenho	**11.4**
Gerenciamento de Incidentes e CAPA	• Gerenciamento de Incidentes	**11.5**
	• CAPA	**11.6**
Gerenciamento de Mudanças	• Gerenciamento de Mudanças e da Configuração do Sistema	**11.7**
	• Atividades de Reparo	**11.8**
Auditorias e Revisão	• Revisão Periódica • Auditorias Internas	**11.9**
Gerenciamento da Continuidade	• *Backup* e Restauração	**11.10**
	• Continuidade do Negócio e Recuperação de Desastre	**11.11**
	• Gerenciamento da Segurança	**11.12**

Segurança e Administração do Sistema	• Administração do Sistema	**11.13**
Gerenciamento dos Registros	• Retenção, Arquivamento e Recuperação	**11.14**

11.2 ENTREGA DO SISTEMA

11.2.1 Introdução

Entrega do sistema é o processo de transferência da responsabilidade do sistema, do time de projeto ou um grupo de serviço para o usuário final. É um processo importante, pois a obtenção da conformidade e a adequação ao uso pretendido somente não são suficientes para assegurar uma transferência bem-sucedida para a fase operacional.

O processo de entrega normalmente envolve o time de projeto (grupo de desenvolvimento e/ou fornecedor), o dono do processo, o dono do sistema e a unidade da qualidade.

11.2.2 Requisitos-Chave

A empresa regulada deve ser capaz de demonstrar a aceitação formal do sistema após a realização de testes e transferência controlada para o ambiente operacional da rotina de trabalho. Esta atividade deve ser documentada.

11.2.3 Responsabilidades

O gerente de projeto é o responsável por preparar o sistema para a sua entrega. O dono do processo e o dono do sistema são responsáveis pela aceitação do sistema para uso operacional.

A responsabilidade pela conclusão de quaisquer ações excepcionais no momento da entrega deve ser acordada entre as partes.

Deve ser dada uma consideração acerca da definição de um período para monitoramento do sistema após a sua entrega e de uma estratégia de reversão/retorno no caso de ocorrência de um problema significativo durante o período de monitoramento.

11.2.4 Execução da Atividade de Entrega

A empresa deve definir o escopo, incluindo os itens de configuração, o período para ocorrência da entrega e os critérios de aceitação.

A seguir deve estabelecer um plano para realização da entrega, que pode ser um documento à parte ou ser parte do Plano de Validação. Uma lista de verificação pode ser utilizada para assegurar a aceitação e a transferência de responsabilidades.

O próximo passo é a execução das atividades para entregar o sistema para o grupo recebedor.

Deve ser estabelecido um acordo entre as partes para a conclusão (justificada) ou transferência de quaisquer questões abertas e atividades ou documentação incompletas do ambiente de projeto para o ambiente operacional. Para a entrega ser bem-sucedida não podem persistir desvios críticos.

Um relatório deve ser preparado, assinado pelo grupo transferidor e pelo grupo recebedor. Este documento pode ser parte do Relatório de Validação do sistema.

11.3 GERENCIAMENTO DO SERVIÇO DE SUPORTE

11.3.1 Introdução

As atividades de Estabelecimento e Gerenciamento dos Serviços de Suporte garantem que os serviços de suporte, sejam internos ou externos, sejam adequadamente especificados e gerenciados. Este processo é frequentemente gerenciado por meio da utilização dos Acordos de Nível de Serviço (*Service Level Agreement* – SLA).

O gerenciamento do serviço e monitoramento do desempenho do sistema são relacionados ao gerenciamento dos registros gerados para evidenciar a operação e o desempenho adequados do sistema. Adicionalmente, há interação potencial com o gerenciamento de incidentes, com CAPA's e com o gerenciamento de mudanças quando os resultados do serviço ou monitoramento indicam que há problemas que precisam ser corrigidos.

O suporte necessário para cada sistema e como este será provido, devem ser estabelecidos formalmente. O suporte pode ser provido por recursos internos e externos. Este processo deve assegurar que acordos para suporte, planos de manutenção e procedimentos operacionais padrão sejam estabelecidos.

Os Acordos de Nível de Serviço podem ser estabelecidos separadamente para sistemas individuais ou para cobrir grupos de sistemas similares (ex.: equipamentos em um único laboratório).

Pode ser útil haver um formato padrão para os Acordos de Nível de Serviço e as empresas reguladas, além de um procedimento operacional padrão para descrever como preparar um Acordo. Uma abordagem baseada em risco para definição do conteúdo e dos detalhes deve ser considerada.

Os Acordos de Nível de Serviço devem ser acordados, entendidos e aprovados, tanto pelo dono do sistema quanto pelo fornecedor do serviço. Estes acordos devem definir, sem ambiguidade, o sistema cujo serviço de suporte será prestado, devendo definir como o serviço será provido e as responsabilidades do prestador de serviço e do dono do sistema.

A qualificação do fornecedor do serviço deve ser assegurada e monitorada por meio de avaliações apropriadas, podendo inclusive haver auditorias no prestador do serviço.

11.3.2 Requisitos-Chave

Deve haver um acordo formal com os fornecedores, incluindo uma declaração nítida de responsabilidades. Neste contexto, subentende-se fornecedores, tanto os terceirizados externos quanto outros departamentos da empresa, pertencentes a outras estruturas gerenciais da empresa.

11.3.3 Responsabilidades

É de responsabilidade do dono do sistema assegurar que o suporte necessário seja identificado e que o Acordo de Nível de Serviço seja estabelecido, seguido, monitorado e relatado.

É de responsabilidade do dono do sistema assegurar que o fornecedor do serviço seja sujeito à avaliação de fornecedor adequada.

É de responsabilidade do fornecedor do serviço assegurar a competência do pessoal de suporte e que eles estejam adequadamente treinados e trabalhem conforme os procedimentos acordados e o Acordo de Nível de Serviço.

É de responsabilidade da organização que presta o serviço de suporte, identificada no Acordo de Nível de Serviço, executar os termos do Acordo.

11.3.4 Execução das Atividades

A atividade de gerenciamento de serviço de suporte envolve a realização das seguintes ações, nesta ordem:

- Primeiramente são identificadas as necessidades de suporte.
- A seguir é realizada a avaliação e a seleção do (s) fornecedor(es) do serviço de suporte.
- O próximo passo é o estabelecimento do Acordo de Nível de Serviço.
- A etapa posterior envolve o estabelecimento dos procedimentos operacionais padrão para suporte do sistema.
- A partir de então são monitorados a Qualidade e o Desempenho do sistema, por meio de auditorias ou verificações de desempenho.

Caso o contrato de suporte não atenda às expectativas este deve ser rescindido.

11.4 MONITORAMENTO DO DESEMPENHO DO SISTEMA

11.4.1 Introdução

O impacto da falha do sistema computadorizado vai variar dependendo da sua criticidade. Quando apropriado, o desempenho do sistema deve ser monitorado para que os problemas possam ser detectados de modo oportuno. Esta atividade permite ao usuário se antecipar à ocorrência das falhas, por meio da utilização de ferramentas e técnicas de monitoramento.

O monitoramento do desempenho faz parte de um programa de manutenção preventiva geral que tem por objetivo a aquisição de dados de desempenho que são úteis para o diagnóstico de problemas do sistema. O monitoramento pode indicar tendências que podem indicar problemas de desempenho e que podem ser utilizadas como parte das ações corretivas e preventivas (CAPA) para reduzir o tempo de inatividade da aplicação ou sistema.

Os Planos de Monitoramento de Desempenho são específicos por sistema. Porém, pode ser prático desenvolver um Procedimento Operacional Padrão sobre como preparar estes planos e desenvolver alguns parâmetros genéricos de monitoramento.

O nível de detalhamento do plano de monitoramento vai depender do risco associado, da complexidade e da inovação do sistema. Pode não ser necessário desenvolver planos de monitoramento para sistemas simples e de baixo risco, podendo isto ser coberto por algum outro documento.

Os Planos de Monitoramento de Desempenho podem ser integrados aos Acordos de Nível de Serviço discutidos na seção 11.3.1.

O monitoramento de desempenho pode ser um processo automático ou manual, ou mesmo a combinação de ambos.

Os registros de monitoramento de desempenho devem ser sujeitos à auditoria interna periódica.

11.4.2 Requisitos-Chave

A necessidade e a extensão das atividades de monitoramento devem ser baseadas no risco do sistema à segurança do paciente, à qualidade do produto e à integridade dos dados.

Os parâmetros de desempenho apropriados devem ser definidos com base nos riscos identificados.

11.4.3 Responsabilidades

É de responsabilidade do dono do sistema assegurar que o desempenho do sistema seja monitorado e que as ações apropriadas sejam tomadas quando necessário.

É de responsabilidade do dono do sistema informar ao dono do processo e à Unidade da Qualidade sobre quaisquer problemas de desempenho que possam causar impacto na segurança do paciente, na qualidade do produto e na integridade dos dados, devendo também invocar o Gerenciamento de Incidentes.

11.4.4 Execução das Atividades

A atividade de monitoramento do desempenho envolve a realização das seguintes ações, nesta ordem:

- Realizar a avaliação de risco;
- Definir o plano de monitoramento;
- Iniciar o monitoramento do desempenho do sistema, as atividades de controle de mudanças, o gerenciamento de incidentes e de manutenção;
- Realizar as revisões e avaliações periódicas como fonte de dados para a Revisão Periódica do sistema.

11.4.5 Parâmetros monitorados

Dependendo dos riscos às BPx das aplicações/sistemas instalados e o tipo do equipamento computadorizado envolvido, as seguintes condições devem ser verificadas com ferramentas adequadas, a intervalos apropriados:

- Servidores/estações de trabalho/PCs/sistemas de controle;
- Utilização da CPU;
- Utilização do cache;
- Tempo de resposta interativa;
- Número de transações por unidade de tempo;
- Tempo de espera médio do trabalho;
- Utilização da capacidade do disco;
- Carga I/O (Entrada/Saída);
- Mensagens de erro do sistema, incluindo falhas do sistema operacional e mensagens de aviso;
- Situação do *hardware*;
- Existência de trabalhos em lote críticos;

- Existência de processos críticos;
- Disponibilidade de filas de impressoras;
- Alarmes;
- Redes;
- Disponibilidade de componentes (servidor, roteador, etc.);
- Carga de rede (ex.: número de colisões);
- Transmissões;
- Aplicações;
- Monitoramento de mensagens de erro;
- Tempos de resposta;
- Número de usuários concorrentes;
- Disponibilidade geral do sistema para os usuários.

NOTA: Os parâmetros citados acima são apenas exemplos e não uma lista completa.

11.4.6 Mecanismos de Notificação

Dependendo do risco associado ao parâmetro monitorado, mecanismos tais como um ou mais descritos abaixo devem ser utilizados para notificar os principais interessados sobre as condições de exceção ocorridas:

- Mensagem no console do sistema;
- E-mail para o operador do sistema;
- E-mail para os prestadores de serviço externos;
- Listas ou registros impressos;
- Alarmes visuais ou sonoros.

11.4.7 Estrutura do Plano de Monitoramento

O plano de monitoramento deve cobrir as seguintes áreas:

- Parâmetros monitorados;
- Limites de alerta;
- Frequência de observação;
- Ferramenta de monitoramento;
- Mecanismo de notificação e pessoa/sistema a ser informado;
- Documentação dos resultados do monitoramento;
- Período de armazenagem/retenção dos resultados;

É recomendado utilizar um formato tabular para a documentação do plano.

11.4.8 Revisão do Plano de Monitoramento

Os seguintes itens devem ser verificados durante a revisão do plano de monitoramento:

- Se os parâmetros e componentes apropriados são monitorados;
- Se os riscos determinados na análise de risco são abordados adequadamente;

- Se os intervalos de tempo e os limites de alerta para os parâmetros monitorados são adequados;
- Se os métodos de notificação são utilizados e permitem um alerta oportuno;
- Se os resultados do monitoramento são retidos com segurança.

11.5 GERENCIAMENTO DE INCIDENTES

11.5.1 Introdução

O processo de gerenciamento de incidentes tem por objetivo categorizar os incidentes de modo a direcioná-los para uma resolução oportuna.

Deve haver um procedimento definindo como os problemas relacionados a *software*, *hardware* e procedimentos operacionais serão capturados, revisados, priorizados, desenrolados, dimensionados e concluídos.

O objetivo principal do Gerenciamento de Incidentes é assegurar que quaisquer desvios não planejados que possam ter impacto na segurança do paciente, na qualidade do produto ou na integridade dos dados possam ser resolvidos antes de causar danos.

O Gerenciamento de Incidentes deve ser desenhado para que o sistema/aplicação/serviço seja devolvido ao usuário o mais rápido possível. Este processo/procedimento normalmente é algo genérico e pode ser aplicado a todos os sistemas.

Os incidentes devem ser avaliados levando-se em consideração qualquer impacto na segurança do paciente, na qualidade do produto e na integridade dos dados. A Unidade da Qualidade deve ser consultada para auxiliar na definição dos critérios de aceitação a serem utilizados nesta avaliação e para auxiliar na avaliação do incidente.

11.5.2 Requisitos-Chave

O processo de gerenciamento de incidentes deve assegurar que eventos operacionais que não façam parte da operação padrão (ex.: desvios, problemas e erros) sejam identificados, avaliados, resolvidos e concluídos de um modo oportuno. Estas atividades devem ser documentadas.

11.5.3 Responsabilidades

É de responsabilidade do dono do processo assegurar que o processo de gerenciamento de incidentes e o procedimento estejam estabelecidos para dar suporte ao sistema.

É de responsabilidade do especialista no assunto (SME) avaliar os incidentes ocorridos e consultar a Unidade da Qualidade sobre aqueles que tenham impacto na segurança do paciente, na qualidade do produto ou na integridade dos dados e aplicar as devidas ações corretivas.

É de responsabilidade do dono do sistema assegurar que os incidentes sejam resolvidos e concluídos quando for aplicável.

É de responsabilidade da Unidade da Qualidade assegurar que os procedimentos associados ao gerenciamento de incidentes sejam seguidos e que as ações adequadas tenham sido realizadas e documentadas.

11.5.4 Execução das Atividades

As atividades de gerenciamento de incidentes envolvem a realização das seguintes ações:

- Identificar e registrar o incidente;
- Avaliar o incidente. O resultado desta avaliação pode ser uma das seguintes opções: não há necessidade de tomada de ação; tomada de ação de acordo com procedimento pré-estabelecido; encaminhar para competências superiores;
- Resolução do problema e preparação do relatório de incidente;
- Conclusão/fechamento do incidente.

11.6 AÇÕES CORRETIVAS E PREVENTIVAS (CAPA)

11.6.1 Introdução

As atividades CAPA envolvem o processo de investigação, entendimento e correção de discrepâncias com base na análise da causa raiz, de modo a evitar a sua recorrência.

No ambiente operacional as atividades CAPA relacionadas aos sistemas computadorizados devem fazer parte do sistema geral de atividades CAPA existente para as demais áreas. Quando os incidentes ocorrem, ou quando as oportunidades de redução das falhas do sistema são identificadas por outros meios, as ações corretivas e preventivas devem ser identificadas e processos devem ser estabelecidos para assegurar que as CAPA's sejam implantadas efetivamente.

O processo CAPA é fortemente associado com o processo de Gerenciamento de Incidentes e o processo de Reparo.

O processo CAPA normalmente é genérico, ou seja, um processo pode ser aplicado a todos os sistemas. A empresa regulada deve avaliar se manterá um registro de CAPA para todos os sistemas ou um registro para grupos de sistemas similares ou um registro para cada sistema.

Qualquer ação corretiva ou preventiva tomada para eliminar as causas de uma não conformidade real ou potencial deve possuir um grau de acordo com a magnitude dos problemas e proporcional aos riscos encontrados.

Os registros das CAPA's devem ser sujeitos a auditorias internas periódicas.

11.6.2 Requisitos-Chave

O processo CAPA deve cobrir:

- As ações corretivas de um problema identificado ou de um problema potencial;
- A determinação da causa raiz e tomada de ação corretiva para potencialmente evitar a recorrência de um problema similar;
- A ação preventiva para evitar a recorrência de um problema potencial similar, quando apropriado;
- Avaliação da eficácia das ações tomadas.

Deve ser estabelecido um procedimento para registrar e analisar os incidentes e permitir que a ação corretiva seja tomada. Estas atividades devem ser documentadas.

11.6.3 Responsabilidades

É responsabilidade do dono do processo assegurar que um processo CAPA seja implantado para o sistema computadorizado e que as responsabilidades sejam delegadas para o dono do sistema.

É responsabilidade da Unidade da Qualidade assegurar que os procedimentos CAPA sejam seguidos e ações apropriadas tenham sido tomadas e documentadas.

É responsabilidade do especialista no assunto (SME) assegurar que as ações corretivas e preventivas acordadas sejam realizadas e completadas.

11.6.4 Execução das Atividades

As atividades de CAPA envolvem a realização das seguintes ações:

1. Identificação e registro do problema;
2. Determinação da ação emergencial a ser tomada;
3. Determinação da provável causa raiz. Esta atividade pode começar a partir da imediata correção do problema. Normalmente envolve um time multidisciplinar;
4. Determinação da Ação Preventiva. Esta ação pode envolver Gerenciamento da Documentação, Gerenciamento de Mudança, Treinamento, Suporte e Administração;
5. Registro do resultado obtido. Deve ser escrita uma justificativa racional caso nenhuma ação seja tomada;
6. Avaliação do sucesso da Ação Corretiva e/ou Ação Preventiva realizada(s).

11.7 GERENCIAMENTO DAS MUDANÇAS E DA CONFIGURAÇÃO DO SISTEMA

11.7.1 Introdução

O gerenciamento de mudanças é uma atividade crítica e fundamental para a manutenção da conformidade dos sistemas e dos processos. Todas as mudanças propostas durante a fase operacional do sistema, sejam elas relacionadas a *software*, *hardware*, infraestrutura ou utilização do sistema, devem ser sujeitas a um processo formal de controle de mudanças. Este processo deve assegurar que a mudança proposta seja adequadamente revisada para avaliação do impacto e risco da sua implantação. O processo deve assegurar que as mudanças sejam adequadamente avaliadas, autorizadas, documentadas, testadas e aprovadas antes de sua implantação e devidamente concluídas.

Algumas atividades tais como substituições e tarefas administrativas do sistema devem ser cobertas por processos de reparo e de administração do sistema.

O gerenciamento de mudanças deve prover um mecanismo para uma pronta implantação de melhorias contínuas de processos e sistemas com base na revisão e avaliação periódica, nos dados operacionais e de desempenho e nas análises das causas raiz das falhas ocorridas.

O Gerenciamento da Configuração inclui aquelas atividades necessárias para definição precisa do sistema computadorizado a qualquer momento do seu ciclo de vida, desde a etapa inicial de desenvolvimento até a sua aposentadoria.

Um item de configuração é um componente do sistema que não é alterado como resultado de uma operação normal do sistema. Itens de configuração só podem ser alterados por meio de um processo de gerenciamento de mudanças. Devem existir procedimentos formais para identificar, definir e estabelecer os itens da configuração inicial e para controlar e registrar as modificações e liberações de itens de configuração, incluindo atualizações e pacotes.

O Gerenciamento da Configuração e o Gerenciamento de Mudanças são intimamente relacionados. Quando mudanças são propostas, ambas as atividades precisam ser tratadas em paralelo, particularmente durante a avaliação do impacto das mudanças.

Ambas atividades devem ser aplicadas ao escopo completo dos sistemas incluindo os componentes de *hardware* e *software* e a respectiva documentação e registros associados, particularmente aquelas com impacto em BPx.

11.7.2 Requisitos-Chave

O gerenciamento de mudanças deve continuar até a aposentadoria do sistema. Se os dados são mantidos depois do sistema aposentado, o gerenciamento destes dados deve estar sujeito ao controle de mudanças.

Todas as mudanças devem ser revisadas, avaliadas quanto ao risco e impacto, autorizadas, documentadas, testadas e aprovadas antes de sua implantação.

A configuração de *hardware* e *software* deve ser documentada durante todo o ciclo de vida do sistema. O nível de detalhamento deve ser suficiente para permitir que o sistema seja reconstruído em caso de perda total do sistema.

Os testes de verificação das mudanças devem ser proporcionais ao risco à segurança do paciente, à qualidade do produto e à integridade dos dados.

11.7.3 Responsabilidades

É responsabilidade do Dono do Processo assegurar que um sistema de gerenciamento de mudanças e de configuração esteja implantado.

É responsabilidade da Unidade da Qualidade assegurar que os procedimentos existentes para estas atividades sejam seguidos.

É responsabilidade de cada membro do time associado a cada mudança executar a sua parte no processo de modo correto.

11.7.4 Gerenciamento de Mudanças

Esta atividade segue as mesmas diretrizes seguidas por outras áreas relevantes às Boas Práticas de Fabricação.

Contudo, processos específicos ou variações do processo padrão podem ser necessários para os seguintes tipos de mudanças:

- Substituições por componentes similares;
- Mudanças na administração do sistema;
- Mudanças emergenciais;
- Mudanças temporárias;
- Mudanças globais.

Os dados de monitoramento de desempenho do sistema podem ocasionar uma proposta de mudança, podendo estes dados serem utilizados para apoiar a avaliação do risco e o impacto e na mudança proposta.

11.7.5 Gerenciamento da Configuração

O gerenciamento da configuração durante a fase operacional deve começar com a configuração denominada de linha de base (inicial) e os registros de gerenciamento de configuração associados. Estas informações devem fazer parte da etapa de entrega de sistema pelo time de validação para o ambiente operacional (rotina).

O Gerenciamento da Configuração consiste das seguintes atividades:

- Identificação da Configuração – O QUE deve ser mantido em controle;
- Controle da Configuração – COMO executar o controle;
- Situação da Configuração – COMO documentar o controle;
- Avaliação da Configuração – COMO verificar o controle.

Deve haver um procedimento operacional padrão envolvendo as atividades, responsabilidades, procedimentos e cronogramas relacionados ao gerenciamento da configuração durante a fase operacional do sistema.

O gerenciamento da configuração e os registros associados fazem parte essencial da atividade de recuperação de desastre, onde o sistema e seus componentes podem ser corretamente remontados e integrados para o reestabelecimento operacional do sistema computadorizado.

11.7.6 Identificação da Configuração

Os componentes dos sistemas sujeitos a gerenciamento de configuração devem ser claramente estabelecidos. O sistema deve ser desmembrado em itens de configuração, que devem ser identificados durante a etapa de definição das especificações e do desenvolvimento.

Um item de configuração é um componente do sistema que não se altera como resultado de uma operação normal do sistema. Itens de configuração devem ser modificados apenas pela aplicação do gerenciamento de mudanças. Exemplos de itens de configuração são: *software* de aplicação; *software* embutido, componentes de *hardware* e documentação do sistema.

A lista formalmente estabelecida dos itens de configuração e suas versões são denominadas de configuração de linha de base (*Configuration baseline*).

11.7.7 Controle da Configuração

Mudanças nos itens de configuração devem ser coordenadas e controladas. Isto inclui as seguintes atividades:

- Controle da versão;
- Controle da mudança;
- Armazenagem do item de configuração;
- Controle de entrega.

Um nome e número de versão únicos devem ser utilizados para identificar cada item de configuração.

O controle de mudanças deve ser aplicado para cada item de configuração. Mudanças de *hardware*, *software* e configuração devem ser realizadas por pessoas autorizadas e controles devem ser mantidos.

11.7.8 Situação da Configuração

Deve existir documentação demonstrando a situação e o histórico dos itens de configuração. Tal documentação deve incluir: detalhes das mudanças realizadas; números das últimas versões e identificadores de liberação. Isto evidencia que as especificações do sistema são revisadas, atualizadas e aprovadas.

Esta atividade pode ser executada de vários modos, incluindo por meio de um documento com versão controlada descrevendo a configuração de linha de base ou por meio de ferramentas automatizadas.

11.7.9 Avaliação da Configuração

Todas as atividades documentadas devem ser sujeitas a gerenciamento para assegurar que a situação do sistema é exata e atualizada e provê uma fonte para auditoria do gerenciamento de configuração do sistema.

A revisão periódica dos sistemas em operação deve incluir a verificação de que atual informação acerca da configuração do sistema esteja correta e exata.

11.7.19 Execução das Atividades

As atividades de gerenciamento de mudanças e de configuração envolvem a realização das seguintes ações, sendo que somente os itens 2, 4 e 6 estão relacionados ao gerenciamento da configuração, especificamente:

1. Proposta para mudança – registrar os detalhes para a motivação da mudança e preparar os requisitos do usuário para a mudança proposta;
2. Avaliação do impacto da alteração – identificação do impacto regulatórios e nos registros; identificação dos itens de configuração (componentes do sistema) afetados;
3. Decisão sobre a proposta – aceitar ou rejeitar;
4. Desenvolvimento do processo – Inclui: *software*, *hardware* e atualização da documentação;
5. Teste da mudança implantada;
6. Aprovação e implantação – Itens a serem considerados: treinamento; atualização de processos do negócio e comunicação;
7. Fechamento.

Os registros das atividades associadas ao gerenciamento de mudanças e de configuração devem ser sujeitos a auditorias internas periódicas.

11.8 ATIVIDADES DE REPARO DO SISTEMA

11.8.1 Introdução

O Reparo do Sistema é a atividade que consiste no gerenciamento de consertos ou substituição de componentes que apresentem falhas ou defeitos. O objeto de reparo pode ser até um item de configuração. É uma forma de controle de mudança na qual as especificações relevantes não são alteradas.

O conserto ou a substituição de componentes de sistemas computadorizados que apresentem falha ou defeito, geralmente relacionados a *hardware* ou infraestrutura, devem ser gerenciados de acordo com procedimento definido. Tais atividades devem ser autorizadas e implantadas somente dentro de um contexto de gerenciamento de controle de mudanças.

Muitas atividades de reparo são emergenciais e requerem rápida resolução. Portanto, o processo de gerenciamento de incidentes e de controle de mudanças deve ser estruturado de modo a permitir que tais atividades possam ocorrer sem demora ou sem haver aumento de risco à integridade operacional do sistema computadorizado.

O processo de reparo pode ser integrado ao processo de gerenciamento de mudança e de configuração, mas é possível ser utilizada uma rota mais simplificada.

Quando a falha (ou o reparo) puder impactar a segurança do paciente, a qualidade do produto ou a integridade dos dados, então um processo de gerenciamento de incidentes deve ser iniciado.

Os registros de reparos ou substituições devem ser sujeitos a auditorias internas periódicas e sua revisão deve formar parte do processo de gerenciamento de desempenho.

11.8.2 Requisitos-Chave

Os procedimentos a serem seguidos em caso de falha ou defeito do sistema devem ser estabelecidos, aprovados e verificados.

Quaisquer falhas e ações corretivas tomadas devem ser registradas.

Deve ser estabelecido um procedimento para registrar e analisar erros e permitir que ações corretivas sejam tomadas.

Estas atividades devem ser documentadas.

11.8.3 Responsabilidades

É de responsabilidade do dono do sistema identificar aqueles componentes que são elegíveis para reparo ou substituição. Informação relevante obtida na fase de projeto/validação pode ficar disponível antes e após a entrega do sistema, como por exemplo uma lista de peças sobressalentes para quando o sistema ser tornar operacional.

É de responsabilidade do dono do sistema assegurar que os procedimentos sejam seguidos.

É de responsabilidade do time que efetua o reparo (ou substituição) executar o procedimento de modo completo e exato, incluindo as atualizações dos registros quando necessário (ex.: livro de registro).

É de responsabilidade da Unidade da Qualidade assegurar que os procedimentos de reparo sejam seguidos e as ações apropriadas sejam tomadas e documentadas.

11.8.4 Execução das Atividades

As atividades de gerenciamento de incidentes envolvem a realização das seguintes ações:

1. Identificação da falha (podendo ser via gerenciamento de incidentes);
2. Avaliação do impacto – identificação do impacto nos processos e registros regulados; identificação dos itens de configuração (componentes do sistema) afetados; definição dos documentos e requisitos de testes;
3. Avaliação e determinação da ação a ser tomada – conserto ou substituição;

4. Realizar o conserto ou a substituição – incluindo *hardware* e atualização da documentação e dos livros de registros;
5. Verificação do reparo ou substituição;
6. Retorno ao uso – comunicação aos usuários.

Nota: Os itens 2 a 6 devem contemplar o gerenciamento da configuração.

11.9 REVISÃO PERIÓDICA

11.9.1 Introdução

As revisões periódicas são utilizadas durante todo a vida operacional do sistema computadorizado para verificar que este permanece compatível com os requisitos regulatórios, apto para o uso pretendido e atende as políticas e procedimentos da empresa. As revisões devem confirmar que, para os componentes do sistema, o suporte necessário e os processos de manutenção e controles regulatórios esperados (planos, procedimentos e registros) estão estabelecidos.

As revisões periódicas devem ser:

- Programadas a intervalos apropriados condizentes com impacto e a história operacional do sistema. Avaliações de risco devem ser utilizadas para se determinar se os sistemas estão no escopo e se a frequência para a realização da revisão periódica é adequada;
- Executadas de acordo com um procedimento pré-definido;
- Documentadas e com as ações corretivas rastreáveis.

O processo de revisão periódica deve ser genérico e aplicável a todos os sistemas.

Pode ser útil desenvolver listas de verificação (*checklists*) para realizar as revisões.

11.9.2 Requisitos-Chave

Um processo para definição do tempo e agendamento das revisões periódicas deve ser definido. Os períodos para revisão dos sistemas devem ser baseados no impacto do sistema, na sua complexidade e inovação. As decisões tomadas com base em risco devem ser documentadas.

Problemas encontrados durante a revisão devem ser documentados, juntamente com as ações corretivas tomadas. Devem ser avaliadas as implicações maiores relacionadas a estas ações corretivas.

As ações corretivas devem ser resolvidas e aprovadas.

11.9.3 Responsabilidades

É de responsabilidade do dono do processo assegurar que as revisões periódicas sejam conduzidas e que sejam dadas respostas apropriadas às conclusões da revisão.

É de responsabilidade da Garantia da Qualidade assegurar que as revisões periódicas sejam agendadas, executadas e documentadas.

A revisão deve ser conduzida por um ou mais pessoas dependendo do escopo da revisão. Participantes podem incluir: Unidade da Qualidade; o Especialista no Assunto; usuários; Tecnologia de Informação; Engenharia; Assuntos Regulatórios. As conclusões devem ser documentadas.

11.9.4 Cronograma para Revisão

Frequências para realização de revisões periódicas devem ser baseadas no impacto do sistema, na sua complexidade e inovação.

Métodos aceitáveis incluem:

- Por sistemas, sendo a frequência definida nos respectivos relatórios de validação do sistema;
- Baseado em revisões regulares e análise do inventário de sistemas;
- Baseado em eventos específicos, sejam planejados ou não;
- Baseado no número e na complexidade das solicitações de mudanças.

Qualquer que seja o método (ou combinação destes) escolhido, isto deve ser documentado e aprovado pela alta gerência da empresa regulada e os critérios para decisão e as responsabilidades devem ser claramente definidos.

11.9.5 Revisão de um Sistema

11.9.5.1 Preparação

Informações relevantes deverão estar disponíveis, para realização da revisão, tais como:

- Documentação do sistema, incluindo: planos, especificações, testes, relatórios, rastreabilidade, documentação de gerenciamento de risco, revisões de projeto, manuais do usuário, materiais de treinamento e registros;
- Procedimentos Operacionais Padrão de operação e de manutenção;
- Informação sobre o gerenciamento da configuração;
- Informação sobre gerenciamento de mudanças;
- Registros de incidentes;
- Informação sobre segurança e controle de acesso;
- Relatórios de quaisquer auditorias anteriores dos sistemas individuais;
- Relatório de Validação.

Os objetivos, o time e a agenda para a realização da revisão devem ser definidos. O time de revisão deve assegurar que o material de referência necessário e as pessoas estejam disponíveis e que o dono do processo esteja comprometido com os resultados da revisão.

11.9.5.2 Condução da Revisão

Problemas encontrados durante a revisão devem ser documentados, juntamente com as ações corretivas recomendadas. Dependendo do processo de gerenciamento criado pela empresa, uma auditoria de acompanhamento pode ser agendada.

Durante a definição da agenda para a revisão, os seguintes pontos devem ser considerados:

- A documentação deve estar completa, atualizada e correta, incluindo:
  - ✓ Especificação e verificação;
  - ✓ Operação e manutenção;
  - ✓ Lista de itens de configuração.
- Registros de quaisquer mudanças feitas no sistema;
- O nível de mudança realizada no sistema e a natureza da mudança;
- Ações excepcionais requeridas por um Relatório de Validação;
- Relatórios de auditorias anteriores e as respectivas ações tomadas;
- Quaisquer controles implementados para gerenciar riscos que estejam ainda em funcionamento efetivo;
- Evidência de operação instável ou não confiável;
- Mudanças no ambiente, processo ou requisitos do negócio, legislação ou melhores práticas aceitas;
- Procedimentos operacionais;
- Planejamento de Continuidade do negócio;
- Pessoal (incluindo qualificações, treinamento, experiência e continuidade);
- Segurança do sistema e controle de acesso;
- Manutenção do sistema e registros de incidentes;
- *Backups* de *software* e de dados.

11.9.6 Execução das Atividades

As atividades de revisão envolvem a realização das seguintes ações:

1. Definição da política e processo para estabelecimento do tempo e do agendamento das revisões periódicas – Pode ser específico por sistemas, definido nos respectivos Relatórios de Inspeção; definidos na Lista de Inventário de Sistemas Computadorizados, baseados gatilhos ou em eventos;
2. Preparação para a realização da revisão – A evidência pode incluir planos, registros de incidentes/mudanças, auditorias ou revisões anteriores;
3. Execução da revisão;
4. Documentação dos resultados da revisão;
5. Execução da Ação Corretiva, se aplicável.

11.10 *BACKUP* E RESTAURAÇÃO

11.10.1 Introdução

Backup é o processo de copiar os registros, dados e *software* para protegê-los contra perda de integridade ou disponibilidade do original. Restauração é a subsequente restauração de registros, dados ou *software* quando requisitado/necessário.

Backup e restauração não deve ser confundido com arquivamento e recuperação.

11.10.2 Requisitos-Chave

Procedimentos devem ser estabelecidos para descrever e discriminar os *backup's* de registros, dados e *software*, realizados na rotina, para um local de armazenagem seguro e adequadamente separado do local de armazenagem primário. A frequência da execução do procedimento de *backup* deve ser baseada em uma avaliação de risco.

Devem existir procedimentos escritos para assegurar a restauração e a manutenção dos registros e dados relevantes às BPF, no caso de ocorrência de falhas.

O procedimento de *backup*, instalações de armazenagem e mídia utilizada devem assegurar a integridade dos dados. Deve haver um registro do *backup* realizado, com referências à mídia utilizada para a armazenagem.

O meio de armazenamento utilizado deve ser documentado e justificado quanto a sua confiabilidade.

Os processos de *backup* devem ser verificados quando forem estabelecidos. Adicionalmente, deve haver procedimentos e planos para execução regular de teste da capacidade de execução de *backup* e restauração. Estas ações devem ser documentadas.

11.10.3 Responsabilidades

O dono do processo é o responsável pela:

- Definição dos dados que necessitem de *backup*, devendo incluir os dados relevantes às BPF;
- Definição da disponibilidade e requisitos de controle de acesso aos dados relevantes às BPF.

O dono do sistema é o responsável por:

- Assegurar que a organização do *backup* e da restauração do *software* para o sistema operacional esteja definida atendam às regulações aplicáveis, de acordo com as diretrizes da Garantia da Qualidade, quando aplicável;
- Assegurar o adequado desempenho do *backup* e da restauração do *software* e dos dados para o sistema operacional;
- Assegurar os controles de acesso apropriados.

11.10.4 Processo de *Backup* e Restauração

11.10.4.1 Mídia de *Backup*

O *backup* deve ser realizado em mídia adequada e esta deve ser utilizada de acordo com a recomendação dos fabricantes

Na seleção e utilização da mídia de armazenagem devem ser considerados os seguintes pontos:

- A expectativa média de sua vida útil;
- As condições ambientais aceitáveis para sua armazenagem;
- Requisitos para sua verificação, renovação e sobrescrição.

Orientações sobre armazenagem, transporte e manutenção dos vários tipos de mídias, magnéticas e óticas, utilizados na armazenagem de dados estão disponíveis, em geral, na documentação fornecida pelo fabricante do produto.

11.10.4.2 *Backup* do Sistema Operacional

Os *backups* de *software* são criados para assegurar que a última e correta versão do *software* esteja disponível e possa ser restaurada em curto espaço de tempo e sem erro, em caso de falha ou após alterações realizadas durante o desenvolvimento.

Todos os componentes de *software* necessários para o sistema operacional devem ser incluídos no escopo do *backup* para assegurar que todo o sistema possa ser restaurado.

O processo de *backup* do *software* deve ser definido e documentado. Este *backup* pode ocorrer:

- Após toda modificação do *software*, sendo que neste caso a realização do backup dos componentes modificados do software pode ser suficiente. Devendo ser esta atividade documentada como parte do controle de mudanças;
- A intervalos regulares (ex.: anualmente) como *backup* completo, com base no risco e na natureza do negócio.

As cópias de *backup* devem ser armazenadas em local seguro.

A mídia de *backup* deve ser fisicamente segura e protegida de fogo, água e outros perigos. O processo de armazenagem, padrões e acessos devem ser definidos e documentados.

Pelo menos duas gerações de cópias de *backup* devem ser armazenadas: a atual e a anterior à última alteração realizada. Com base no risco, pode ser aconselhável manter mais gerações para evitar a possibilidade de propagação de erros em todas as cópias de *backup* disponíveis.

Os seguintes dados devem ser claramente associados com a mídia de *backup*, seja no rótulo, seja em livro de registro, de modo seguramente rastreável:

- Data de criação;
- Designação do sistema;
- Designação do *software*;
- Versão e/ou *software*/*firmware* número de construção (*build number*), se aplicável;
- Número atual (geração e possível múltiplos *backups*);
- Razão para o *backup* do *software;*
- Data do *backup*;
- Identidade da pessoa que realizou o *backup*.

Backups do *software* devem ser realizados enquanto o sistema estiver em operação. Registros dos *backups* realizados devem ser mantidos. As instruções para realização de *backup* e restauração devem ser armazenadas de modo seguro juntamente com a mídia de *backup*.

Com base no risco e no processo de *backup*, as operações de *backup* devem ser revisadas periodicamente e a restauração do *backup* deve ser periodicamente executada para verificar se irá funcionar corretamente quando necessário.

11.10.4.3 *Backup* dos Dados

Dados eletrônicos relevantes às BPF devem ser mantidos de modo seguro pelo tempo de retenção definido. Enquanto os dados são frequentemente mantidos em disco rígido utilizando-se conceitos de redundância ou

discos espelhados, *backups* adicionais de dados relevantes às BPF formam uma parte-chave para se evitar a perda de dados em caso de falha do sistema. Os dados devem ser recuperáveis em curto espaço de tempo e sem erro e cópias mantidas remotamente para se evitar perda devido a alguma falha comum em um local (ex.: fogo). O tipo e a frequência de execução do *backup* devem ser baseados no risco.

Os dados devem ser periodicamente salvos na mídia de *backup*. O dono do sistema deve estabelecer e documentar a organização dos *backups* de dados, cobrindo os seguintes aspectos:

- Tipos de *backup* (completo ou incremental);
- Intervalo: diário, semanal, mensal, trimestral, anual ou não cíclico (retenção permanente);
- Número de gerações. O número de gerações define o número de *backups* identicamente realizados que são mantidos. Visto que as mídias de *backup* são frequentemente reutilizadas, após o número de gerações ser atingido, os *backups* subsequentes serão sobrescritos sobre o *backup* mais velho. Por exemplo: se o número de gerações definido for quatro, o quinto *backup* irá sobrescrever o primeiro, o sexto irá sobrescrever o segundo e assim por diante;
- Falha do *backup* – Ações a serem realizadas em caso de falha do *backup* devem ser estabelecidas, tais como a repetição do *backup* durante o dia. As ações executadas em caso de falhas devem ser documentadas (ex.: livro de registro) pela pessoa responsável pelo sistema computadorizado;
- Rotulagem da Mídia de *Backup*. Os seguintes itens devem constar no rótulo da mídia, ou registrado em livro de registros: designação do sistema; designação do *software*/dados; versão e/ou número de construção do *software/firmware* (se aplicável); data de criação; data do primeiro uso; número atual (gerações, possíveis múltiplos backups); data do *backup*; razão para o *backup* e identidade do operador;
- Duração de utilização. A mídia deve ser somente utilizada pelo tempo que tem garantia;
- O tipo de mídia utilizada deve ser documentado;
- Local de Armazenagem. Os locais de armazenagem devem ser seguros e adequadamente identificados e rastreáveis;
- Ferramentas de *Backup* de Dados e Procedimentos Correspondentes. Dados relevantes às BPF devem ser armazenados de forma adequada que permita sua restauração. A localização e o nome do procedimento de controle devem ser documentados. Os procedimentos devem cobrir a restauração, as atividades de verificação e reinicialização após falha do sistema;
- Revisão do *Backup* de dados. O dono do processo, ou pessoa delegada, é responsável por assegurar a bem-sucedida realização do *backup*. Falhas devem ser investigadas e mídias de armazenagem com defeitos potenciais devem ser descartadas e substituídas. As ações devem ser documentadas em livro de registros.

11.10.4.4 Restauração

Procedimentos escritos e testados devem ser utilizados para execução da restauração. Quando a restauração for realizada manualmente, isto deve ser registrado e assinado.

O dono do processo, ou pessoa delegada, deve autorizar a restauração de dados. Estas pessoas são os responsáveis por assegurar que o procedimento de restauração esteja em conformidade com as regulações de Boas Práticas.

Se a restauração for motivada por razões técnicas, o dono do processo e o dono do sistema devem fazer uma avaliação sobre o processo e os possíveis riscos. O método de restauração utilizado e o controle da operação de restauração devem ser documentados.

11.10.4.5 Integridade por Longo Período

As mídias de armazenagem eletrônicos se degradam com o passar do tempo, portanto, a reutilização da mídia deve ser realizada de acordo com as orientações do fabricante com relação à sua vida útil.

No caso improvável de que uma cópia de *backup* seja mantida por um período que se aproxima do fim de vida útil da mídia, a integridade dos *backups* contidos na mídia deve ser revisada de acordo com as especificações do fabricante. É preferível copiar os dados em uma mídia nova a revisar a mídia antiga.

Os procedimentos de *backup* e de restauração devem ser verificados periodicamente. A frequência deve ser baseada no risco. Esta verificação pode ser realizada por mídia, da restauração do *backup* para um sistema de teste e verificando-se a sua correta operação.

Uma abordagem comum e pragmática consiste em combinar a verificação do processo de *backup* com o teste de recuperação de desastre. A restauração do *backup* para o sistema rodando em produção, com o propósito de se realizar um teste, não é recomendável, pois um erro no procedimento pode resultar em perda de dados.

Os procedimentos de *backup* e restauração devem ser verificados durante a revisão periódica do sistema. As conclusões devem ser documentadas.

11.10.5 Execução das Atividades

As atividades de *backup* e restauração envolvem a realização das seguintes ações:

1. Avaliação de risco, levando-se em conta a probabilidade e risco de ocorrência de danos;
2. Definição da estratégia para a realização das operações de *backup*, abrangendo: frequência, local de armazenagem, tempos de respostas necessários, período de retenção e mídia de armazenagem;
3. Desenvolvimento dos procedimentos escritos de *backup* e de restauração, abrangendo: responsabilidades, treinamento e documentação;
4. Definição dos procedimentos e planos de testes para verificação das operações de *backup* e de restauração;
5. Execução dos testes, documentando os resultados e as ações tomadas;
6. Execução das operações de *backup* de acordo com procedimento estabelecido;
7. Monitoramento do sistema durante sua vida operacional.

11.11 PLANEJAMENTO PARA CONTINUIDADE DO NEGÓCIO/RECUPERAÇÃO DE DESASTRE

11.11.1 Introdução

O Planejamento para Continuidade do Negócio consiste em uma série de atividades e processos relacionados com a garantia de que a empresa regulada está totalmente preparada para responder efetivamente quando da ocorrência de falhas e perturbações.

Processos críticos para o negócio e sistemas que dão suporte a estes processos devem ser identificados e seus riscos associados devem ser avaliados. Planos devem ser estabelecidos e exercitados para assegurar a oportuna e efetiva retomada destes processos e dos sistemas críticos para o negócio.

O Plano para Continuidade do Negócio define como o negócio pode continuar a funcionar e como lidar com os dados após a ocorrência de falhas. Define as etapas necessárias para a restauração dos processos do negócio após a ocorrência de desastre e como os dados gerados durante a ocorrência deste evento devem ser

gerenciados. Também identifica os gatilhos para se invocar o Plano, os papéis, as responsabilidades e a comunicação necessária.

Uma das atividades realizadas durante a atuação do Plano para Continuidade do Negócio, envolve a criação de planos aprovados e treinados/exercitados para a recuperação de sistemas em caso de ocorrência de um desastre. Estes planos devem ser detalhados com relação às precauções a serem tomadas para minimizar os efeitos de um desastre, permitindo que a organização continue ou rapidamente retorne suas funções críticas. Deve haver um foco na prevenção de desastres, como por exemplo, com a provisão de redundância para os sistemas críticos.

11.11.2 Requisitos-Chave

A segurança do paciente, a qualidade do produto e a integridade dos dados não podem ser comprometidos por falhas ou quebra do sistema computadorizado.

A empresa regulada deve realizar planejamento para continuidade do negócio para ativamente proteger sua habilidade em fornecer seus produtos para o público e atender aos requisitos regulatórios.

O Plano para Continuidade do Negócio deve prover procedimentos ou processos alternativos para serem implementados de modo a substituir funcionalidade ausente de algum sistema e permitir a continuidade segura do negócio durante a falha.

Planos para Continuidade do Negócio devem incluir provisão para a realização de ensaios. Processos alternativos definidos pelo Plano para Continuidade do Negócio devem ser adequadamente documentados e o pessoal envolvido adequadamente treinados.

As empresas reguladas devem ser capazes de demonstrar que elas podem assegurar que os serviços críticos e processos podem continuar e que há uma retomada oportuna das funções essenciais do negócio.

Planos para Continuidade do Negócio e seus ensaios devem ser sujeitos a auditorias internas periódicas.

11.11.3 Responsabilidades

É de responsabilidade da alta gerência da empresa, incluindo os donos de processo, os donos de sistema e a Unidade da Qualidade, assegurar que Planos para Continuidade do Negócio apropriados estejam estabelecidos, testados periodicamente e uma vez iniciados, sejam seguidos, documentados e comunicados.

É de responsabilidade do dono do processo e do dono do sistema assegurar que planos de recuperação de desastre apropriados estejam estabelecidos para os sistemas de modo a dar suporte aos Planos para Continuidade do Negócio.

11.11.4 Execução das Atividades

As atividades de Planejamento para Continuidade do Negócio e Recuperação de Desastres envolvem a realização das seguintes ações:

1. Estabelecimento da necessidade do planejamento e do gerenciamento para continuidade do negócio, incluindo o Planejamento para Recuperação de Desastre, identificando-se os processos e serviços chave para o negócio. Obtenção do suporte da alta gerência;

2. Avaliação e análise de risco. Determinação dos eventos adversos e danos que podem adversamente afetar a organização. Avaliação da severidade de cada evento e a probabilidade de sua ocorrência;
3. Definição das estratégias para a Continuidade do Negócio. Seleção de estratégias alternativas para recuperação, ao mesmo tempo mantendo a habilidade da organização para executar suas funções críticas;
4. Desenvolvimento do Plano para Continuidade do Negócio. Identificação de papeis e responsabilidades, recursos organizacionais e dos gatilhos que podem provocar a utilização do Plano e sua escalação;
5. Implantação do Plano para Continuidade do Negócio;
6. Manutenção e Ensaio. Pré-planejamento e coordenação de ensaios, documentando-se e avaliando-se os resultados de cada ensaio, incorporando as lições aprendidas dentro do Plano para Continuidade do Negócio. Manutenção da atualidade do Plano e a sua capabilidade de acordo com a estratégia da empresa e dos requisitos regulatórios. Publicização dos resultados dos ensaios aos principais interessados.

11.12 GERENCIAMENTO DA SEGURANÇA DO SISTEMA

11.12.1 Introdução

O gerenciamento da segurança do sistema é o processo para assegurar a confiabilidade, integridade e disponibilidade dos sistemas, registros e processos da empresa regulada.

Um gerenciamento de segurança efetivo protege os sistemas computadorizados da empresa de modo a minimizar os impactos ao negócio causados por vulnerabilidades e incidentes de segurança.

11.12.2 Requisitos-Chave

Medidas devem ser implantadas para assegurar que os sistemas computadorizados das empresas reguladas e seus dados sejam adequados e protegidos contra perdas acidentais ou intencionais, danos ou mudanças não autorizadas.

Tais medidas devem garantir controle, integridade e disponibilidade contínuos e quando apropriado, a confidencialidade dos dados regulados.

Este processo deve incluir:

- Estabelecimento e manutenção de papéis e responsabilidades, políticas, padrões e procedimentos ligados à segurança;
- Execução periódica de monitoramento de segurança e testes, por exemplo, verificação manual do livro de acesso ao sistema, notificações automatizadas de bloqueios de acesso ao sistema, testes de *tokens* e assim por diante;
- Implementação de ações corretivas para fraquezas e incidentes de segurança identificados;
- Assegurar a existência de uma lista de pessoas autorizadas a acessar o sistema.

O desenho dos mecanismos físicos e técnicos de segurança deve ser avaliado e se necessário, testado.

Os registros associados à segurança do sistema devem ser sujeitos a auditorias internas periódicas.

11.12.3 Responsabilidades

A responsabilidade pela segurança do sistema, incluindo controle de acesso, deve ser acordada entre o dono do processo e o dono do sistema.

É de responsabilidade da Unidade da Qualidade assegurar que os procedimentos de segurança sejam seguidos.

O usuário do sistema computadorizado é o responsável pelo atendimento aos requisitos de segurança definidos durante a utilização do sistema computadorizado.

11.12.4 Princípios

As medidas para gerenciamento de segurança devem ser planejadas e implementadas com base nas seguintes considerações:

- Impacto do sistema – avaliação dos riscos associados ao sistema;
- Conscientização dos funcionários – treinamento dos usuários;
- Gerenciamento de incidentes – registros e ações tomadas para resolução dos incidentes;
- Política de segurança da informação - segurança física; segurança do acesso ao sistema; acesso por terceiros; sistemas de mensagens eletrônicas; recursos de rede compartilhados; acesso e utilização de internet; utilização de recursos de computação móveis; conectividade a sistemas computadorizados externos; políticas de antivírus e detecção de intrusão.

11.13 ADMINISTRAÇÃO DO SISTEMA

11.13.1 Introdução

A administração do sistema envolve a rotina de gerenciamento e suporte aos sistemas para assegurar que eles estejam operando eficientemente e efetivamente.

11.13.2 Requisitos-Chave

As tarefas de administração do sistema devem ser identificadas, documentadas e possuírem suporte de procedimentos de controle.

Os administradores dos sistemas devem ser treinados e ter sua competência evidenciada na execução das atividades. As tarefas de administração do sistema devem ser segregadas das atividades operacionais relacionadas ao sistema.

Quaisquer atividades relacionadas ao sistema que forem cobertas por procedimentos operacionais padrão precisam estar sujeitas ao gerenciamento de mudanças e de configuração.

As tarefas de administração de sistema devem ser sujeitas a auditorias internas periódicas.

11.13.3 Responsabilidades

O dono do processo tem a responsabilidade geral por assegurar que o sistema seja utilizado e mantido de modo correto por meio de procedimentos e instruções de trabalho detalhadas.

É de responsabilidade do dono do sistema assegurar que as tarefas delegadas ao administrador do sistema estejam claramente identificadas e documentadas. O dono do sistema e o administrador do sistema podem ser a mesma pessoa.

11.13.4 Execução das Atividades

As atividades de administração do sistema envolvem a realização das seguintes ações:

1. Estabelecimento das necessidades e escopo das atividades de administração do sistema computadorizado;
2. Estabelecimento do cronograma de suporte, para as atividades regulares (diário, semanal, mensal etc.);
3. Identificação das tarefas relacionadas à administração do sistema, que podem ser motivadas pelo processo de Gerenciamento de Incidentes;
4. Estabelecimento dos procedimentos operacionais padrão para a administração do sistema.

11.14 GERENCIAMENTO DE REGISTROS (RETENÇÃO, ARQUIVAMENTO E RECUPERAÇÃO)

11.14.1 Introdução

Políticas para retenção de registros devem ser estabelecidos, com base em um claro entendimento dos requisitos regulatórios, das políticas corporativas e dos guias existentes. Requisitos de arquivamento são relevantes para qualquer registro que necessita ser removido de sistemas operacionais antes do final de seu período de retenção definido.

Arquivamento é o processo de retirada de registros e dados do sistema computadorizado e colocá-los em um local ou sistema diferente, frequentemente protegendo-os contra mudanças posteriores. Pode ser também necessário reter em arquivo as aplicações que dão suporte aos registros e dados.

Os procedimentos para arquivamento e recuperação devem ser estabelecidos com base em um claro entendimento dos requisitos regulatórios.

Arquivamento e recuperação não devem ser confundidos com *backup* e restauração.

O arquivamento deve ser sujeito a auditorias periódicas internas.

11.14.2 Requisitos-Chave

Os registros e dados relevantes às BPF devem estar seguros por meio físico e eletrônico contra danos acidentais ou dolosos, por todo o período de retenção requerido.

Os papéis, responsabilidades e procedimentos para arquivamento e recuperação devem ser definidos, devendo haver procedimento operacional padrão que descreva a estratégia para arquivamento.

Registros e dados armazenados devem ser inicialmente e então periodicamente verificados quanto a sua acessibilidade, durabilidade, exatidão e completude, com base em uma análise de risco, levando-se em consideração o tipo de armazenagem, a mídia e o método de acesso.

Processos de arquivamento devem assegurar que o conteúdo seja preservado. Registros com aprovações requeridas pelos regulamentos de BPF devem assegurar que a validade da aprovação seja mantida por todo o período de arquivamento.

Agências regulatórias devem possuir acesso aos registros BPF durante uma inspeção, dentro de um determinado período. Cópias legíveis dos registros arquivados devem estar disponíveis quando solicitados.

11.14.3 Responsabilidades

É de responsabilidade do dono do processo assegurar que um processo/procedimento de arquivamento esteja estabelecido.

É de responsabilidade da Unidade da Qualidade assegurar que o processo/procedimento de arquivamento seja seguido.

A pessoa que realiza o arquivamento é o responsável por receber dos usuários os registros a serem arquivados, mantendo estes registros no estado em que foram recebidos e retornando-os no mesmo estado.

O dono do sistema é o responsável por manter ou atualizar os sistemas necessários para o acesso aos registros.

11.14.4 Arquivamento e Retenção

O procedimento de arquivamento deve prover controles para:

- Assegurar instalações de armazenagem seguras;
- Verificar e manter os registros arquivados por todo o período de retenção, isto é, para gerenciar o envelhecimento da mídia de armazenamento;
- Prover as capabilidades de indexação;
- Detectar o fim do período de retenção pretendido para registros especificados e notificar a gerência quando apropriado;
- Prover gerenciamento com a opção de extensão do período de retenção;
- Assegurar que quaisquer mudanças nos registros sejam executadas sob controle de mudanças;
- Destruir os registros com segurança quando for dada a devida autorização;
- Assegurar que a tecnologia para leitura dos registros arquivados permaneça disponível por todo o período de retenção.

Se o processo de arquivamento for computadorizado, o sistema deve ser validado. Este sistema de arquivamento automatizado de registros deve:

- Assegurar que os dados sejam protegidos por meio de *backup* a intervalos regulares. Os dados do *backup* devem ser armazenados pelo período de retenção, em um local seguro separado;
- Assegurar que o sistema e seu conteúdo estejam seguros;
- Permitir que seja feita verificação da acessibilidade, exatidão e completude dos registros, após a realização de mudanças relacionas a *hardware* e *software*;
- Ter a capacidade de manter rastreabilidade de mudanças nos registros;

- Assegurar que o sistema e seus conteúdos sejam seguros, mantendo preservado o seu significado;
- Considerar a disponibilidade contínua de dispositivos e *softwares* necessários para acessar os registros.

11.14.5 Recuperação

Os registros retidos devem ser prontamente recuperáveis para propósitos do negócio e regulatórios. O processo de recuperação deve ser documentado e deve ser dada consideração aos seguintes pontos:

- Deve haver autorização formal para acesso aos registros retidos;
- Deve haver capacidade de acesso *online* e *offline* aos dados eletrônicos, se aplicável;
- Deve haver capacidade de se obter cópias impressas e cópias eletrônicas legíveis dos dados eletronicamente armazenados;
- Deve haver meios para se recuperar qualquer registro requerido por regulação após a aposentadoria de um sistema regulado pelas BPF;
- Deve haver um exercício periódico de recuperação ou processo de verificação para conferir sua operação contínua.

11.14.6 Execução das Atividades

As atividades de Arquivamento e Recuperação envolvem a realização das seguintes ações:

1. Identificação dos registros e dados relevantes às BPF;
2. Definição da política de retenção destes registros e dados;
3. Definição da estratégia de arquivamento, abrangendo frequência, localização, tempo necessário de resposta, período de retenção, meio de retenção, responsabilidades, treinamento e documentação;
4. Implementação da estratégia de arquivamento;
5. Verificação das atividades de arquivamento, documentando resultados e ações tomadas;
6. Renovação ou regeneração dos resultados e dados arquivados;
7. Monitoramento da disponibilidade contínua dos resultados e dados arquivados;
8. Registro da destruição de acordo com a política de retenção, em caso de eventual aposentadoria do sistema.

12 MIGRAÇÃO DE DADOS

12.1 INTRODUÇÃO

Esta seção abrange os procedimentos relacionados ao planejamento, execução e verificação das atividades de migração de dados.

Não abrange a transferência de dados de um sistema para outro, dentro de um processo de negócio em andamento. Tal situação deve ser abordada por meio de atividades de especificação e verificação típicas.

A migração de dados é uma atividade que pode ocorrer frequentemente durante os ciclos de vida dos sistemas computadorizados utilizados por empresas reguladas.

Migração de dados é a atividade de transportar dados eletrônicos de um sistema para outro, ou simplesmente a transição de dados de um sistema para outro.

Alguns exemplos de migração de dados são:

- Uma atualização de uma versão em vigor de um banco de dados ou aplicação;
- Conversão de dados (ex.: de um banco de dados de um fornecedor para outro);
- Migração dentro do mesmo sistema (ex.: transporte de dados de uma aplicação de uma plataforma do servidor para outra);
- Migração de um sistema-origem para um sistema-alvo;
- Migração de múltiplos sistemas-origem para um sistema-alvo.

A complexidade e o risco envolvido no esforço de migração de dados podem aumentar significativamente se, regras forem utilizadas para a seleção de um subconjunto de dados do sistema-origem ou se dados forem transformados (ex.: conversão do tipo de dados; filtragem; limpeza; agregação; normalização) antes de serem inseridos no sistema-alvo. O objetivo final de qualquer migração de dados é o de se obter dados que permaneçam utilizáveis e retenham seu significado contextual. Controles de gerenciamento da qualidade devem existir para assegurar que os esforços de migração de dados sejam bem-sucedidos, compatíveis e repetíveis.

Cada atividade de migração de dados deve ser gerenciada por meio de plano e relatório.

12.2 GERENCIAMENTO DA QUALIDADE

12.2.1 Ciclo de Vida do Sistema

A migração de dados pode ocorrer muitas vezes durante o ciclo de vida de um sistema computadorizado, nas seguintes situações:

- Durante o desenvolvimento e implantação inicial do sistema;
- Durante as atualizações da aplicação;
- Durante a aposentadoria do sistema.

Como acontece com outras fases e atividades do ciclo de vida, as atividades de migração de dados serão mais consistentes e bem-sucedidas se o ciclo de vida contém procedimentos, ferramentas, *templates* e exemplos de migração de dados.

Um ciclo de vida completo deve prover orientação para todos os aspectos relacionados à migração de dados, incluindo:

- Papéis e responsabilidades;
- Requisitos de documentação;
- Controles de qualidade e conformidade;
- Atividades técnicas e de verificação;
- Gerenciamento de projeto.

Um procedimento operacional padrão é o melhor método para descrição e documentação do processo, incluindo os requisitos de qualidade e conformidade.

12.2.2 Gerenciamento de Risco

O ciclo de vida deve incluir um processo de gerenciamento de risco estabelecido, para avalição de riscos que são específicos para as atividades relacionadas aos sistemas computadorizados. Adicionalmente aos riscos normalmente encontrados em projetos tecnológicos, os seguintes itens devem ser avaliados quando se realiza a migração de dados regulados:

- O risco inerente à qualidade e conformidade associadas à migração dos dados, tais como: o impacto à segurança do paciente, qualidade do produto e integridade;
- O risco relacionado aos processos de negócio associados ao sistema computadorizado envolvido;
- O risco ao negócio devido ao sistema ficar indisponível ou os dados migrados não serem confiáveis;
- O nível de complexidade (ex.: múltiplas origens ou sistemas-alvo; múltiplas fases; muita transformação de dados);
- Risco tecnológico devido ao uso de sistemas ou ferramentas complexas ou de ponta.

12.2.3 Gerenciamento da Configuração e Controle de Mudanças

A migração de dados eletrônicos no ambiente regulado deve ser executada sob controle de mudança. Igualmente, todos os documentos e ferramentas utilizados no projeto de migração de dados devem ser controlados, utilizando-se o gerenciamento de configuração.

Durante a execução do projeto de migração, mudanças no sistema não relacionadas à migração devem ser proibidas. O motivo é que o sucesso do esforço de migração de dados depende de várias características dos sistemas (ex.: versões de *software*, esquemas de banco de dados) que devem permanecer inalteradas durante o projeto. Estas mudanças podem aumentar a complexidade da migração dos dados e o risco do projeto como um todo.

12.3 PONTOS IMPORTANTES

12.3.1 Adequação das Ferramentas de *Software* ao Uso Pretendido

A migração de dados normalmente envolve a utilização de ferramentas de *software* para automatizar algumas ou todas as atividades de extração, transformação, carregamento e verificação. Estas ferramentas tendem a pertencer à categoria 1 do GAMP – ferramentas de infraestrutura (ex.: migradores de banco de dados e verificadores, adquiridos de um fornecedor de *software*) ou à categoria 5 – aplicações customizadas (ex.: roteiros SQL, robôs de migração de dados, programas desenvolvidos internamente).

As ferramentas de infraestrutura devem ser adequadas para o uso pretendido. O rigor das atividades de especificação e verificação relacionadas devem ser proporcionais aos riscos associados. Dependendo do escopo, complexidade e customização das ferramentas de *software* utilizadas, os requisitos de validação podem variar desde a obtenção de evidência da realização de testes básicos até a preparação de especificações completas do *software* e sua verificação formal.

O Especialista no Assunto (SME) deve assegurar que as atividades adequadas do ciclo de vida e os objetivos a serem atingidos sejam identificados e executados.

A Unidade da Qualidade deve revisar e aprovar a documentação-chave, de acordo com os procedimentos da empresa.

Para as ferramentas de *software* que movem ou transformam dados, são três as principais áreas de risco:

1. Os dados serem movidos ou transformados incorretamente ou incompletamente;
2. Os dados já existentes no sistema-alvo serem prejudicados;
3. No caso de que sejam migrados apenas parte dos dados, os dados residuais do sistema-origem serem adversamente afetados pela remoção dos dados migrados.

É importante que seja desenvolvida e aprovada uma tabela de mapeamento de dados (i.e., campos do modelo de dados do sistema de origem mapeados para o modelo de dados do sistema de destino), quando se utiliza ferramentas de *software* para migração.

12.3.2 Verificação dos Dados

Os dados devem ser verificados sempre que forem movidos ou transformados. Há dois tipos gerais de verificação pós-migração dos dados: a verificação em ambiente de testes e a verificação em ambiente operacional.

Na verificação em ambiente de testes, um sistema-alvo teste é inicialmente preenchido com dados, então um teste de migração é executado e finalmente os dados no sistema-alvo são verificados para demonstrar que todos os dados migraram com sucesso e sem afetar adversamente os dados existentes. Esta verificação fornece evidência objetiva de que a ferramenta de *software* é adequada ao uso pretendido e fornece um nível de confiança sobre o processo de migração de um modo geral.

A intenção da verificação no ambiente operacional é a mesma: verificar o resultado do processo de migração tanto nos dados migrados quando nos dados existentes. A quantidade de dados envolvida, contudo, é normalmente muito maior e, portanto, mais difícil de ser verificar. Há duas abordagens gerais para solucionar este problema: amostragem de dados e ferramentas automatizadas de verificação de dados.

Na amostragem de dados, uma amostra estatística da população dos dados migrados e/ou existentes é verificada no sistema destino ou alvo. Padrões tais como ANSI/ASQ Z1.4 e ISO 2859, podem ser utilizados para se determinar o tamanho de amostra apropriado para verificar a conformidade da inteira população de dados no nível de confiança desejado.

As ferramentas de *software* automatizadas podem ser utilizadas para verificar 100% dos dados no sistema-alvo ou destino. Contudo, estas ferramentas apresentam um nível de risco mais alto e consequentemente a sua adequação deve ser rigorosamente determinada.

Uma parte importante da migração de dados é a confirmação de que todos os dados necessários foram migrados. Técnicas de verificação, tais como *checksum*, podem ser utilizadas para corroborar a transmissão completa dos dados.

Evidência objetiva da verificação dos dados deve ser gerada. Roteiros de verificação e folhas de dados, cópias de telas, registros de erros e relatórios em papel devem ser criados quando apropriado e factível.

12.3.3 Confiabilidade dos Dados de Origem

Se o sistema de origem é mantido em atendimento aos requisitos regulatórios, então a combinação dos controles do sistema de origem com os controles realizados durante o processo de migração deve prover garantia suficiente da exatidão e da integridade dos dados migrados.

Para documentar isto, o plano de migração de dados deve referenciar a apropriada documentação do sistema de origem.

Se a situação do sistema de origem é desconhecida, então há dois problemas: primeiro, a veracidade dos dados migrados do sistema de origem pode não ser confiável; e segundo, os dados migrados irão se misturar com os dados confiáveis já existentes no sistema destino controlado. Após a migração, os dados existentes confiáveis e os dados não confiáveis estarão misturados e de difícil distinção a não ser que sejam tomadas ações para identificar os dados migrados, tais como: diferenças nas datas de registro e anotações em campos definidos pelo usuário. Se isto não for possível, então as possíveis inconsistências de dados devem ser documentadas, explicando os controles existentes no sistema de origem e a justificativa do porquê os dados migrados devem ser confiáveis.

12.3.4 Usabilidade dos Dados Migrados no Sistema de Destino

Há três problemas principais a serem considerados, relacionados à usabilidade dos dados migrados para o sistema destino:

1. A funcionalidade do sistema destino não permite o desempenho de tarefas previamente executadas no sistema de origem;
2. Falta de completude dos dados migrados afeta a usabilidade dos dados;
3. Pode não ser suficiente migrar os dados. Migração separada dos metadados ou configuração do sistema destino pode ser necessária. Por exemplo, os dados de origem têm alguns direitos de acesso definido para eles, tais como grupos de usuários e direitos dos usuários. A migração dos dados pode não migrar estes metadados, que são normalmente separados dos dados. Contudo, estes grupos e direitos de usuários podem também ser necessários no sistema destino.

12.3.5 Trilhas de Auditorias (*Audit trails*)

Trilhas de auditorias podem ser problemáticas para o processo de migração de dados. Se o sistema destino possui uma trilha de auditoria, mas o sistema de origem não, deve ser criado um documento refletindo que a auditoria dos registros migrados começaram quando eles foram transferidos para o sistema destino. Se possível, estes registros devem ser distinguíveis dos registros que foram gerados no sistema destino.

Se ambos os sistemas possuem trilhas de auditorias e a migração for factível, a trilha de auditoria deve ser migrada juntamente com os dados auditados. Se for tecnicamente impossível migrar a trilha de auditoria ou fazer isto constituiria um risco muito grande, a trilha de auditoria original deve ser arquivada em um formato que possa ser recuperada ao longo do tempo.

Quando possível, uma trilha de auditoria criada pelo computador deve ser criada durante as atividades de movimentação e transformação associadas à migração dos dados, pois esta trilha de auditoria serve não apenas como uma ferramenta de verificação, mas também como um registro histórico das mudanças nos dados e deve ser arquivada em um formato que possa ser recuperada ao longo do tempo.

12.4 PLANO DE MIGRAÇÃO DE DADOS

Diferentes tipos de migração de dados requerem diferentes atividades e objetivos. Cada processo de migração de dados deve possuir um plano para migração de dados. Este plano serve como um roteiro de alto nível que orienta o time que realiza a migração a executá-la de modo adequado.

Este plano deve descrever todo o processo de migração, incluindo:

- Propósito e escopo do projeto de migração;
- Descrição do(s) sistema(s);
- Papéis e responsabilidades;
- Objetivos a serem atingidos;
- Estratégia para gerenciamento do risco;
- Estratégia para o gerenciamento da configuração, incluindo os ambientes de origem, estacionário e de destino;
- Visão geral e estratégia da ferramenta de *software* para assegurar a conformidade e adequação ao uso pretendido;
- Etapas de migração e atividades técnicas;
- Atividades de mapeamento e modelagem de dados;
- Regras de transformação;
- Estratégia de verificação de dados e critérios de aceitação;
- Plano de transição;
- Estratégia de reversão.

O plano para migração deve ser aprovado pelo dono do processo, dono do sistema, Unidade da Qualidade e Especialista no assunto, quando apropriado.

Podem ocorrer situações onde o plano de migração poderá ser utilizado mais de uma vez. Quando isto ocorrer, um relatório de migração de dados deve ser gerado.

12.5 RELATÓRIO DE MIGRAÇÃO DE DADOS

O relatório de migração de dados resume as atividades que foram conduzidas durante o processo de migração. Descreve quaisquer anomalias ou desvios ocorridos e lista os resultados das atividades de verificação, incluindo evidência objetiva, quando apropriado.

Pelo fato de o relatório ser utilizado para estabelecer a confiabilidade dos dados migrados, ele deve declarar claramente o resultado da atividade de migração.

O relatório de migração de dados deve ser aprovado pelo dono do processo, dono do sistema, Unidade da Qualidade e especialista no assunto, quando apropriado.

No caso em que a atividade de migração de dados for realizada como parte de um projeto de sistema computadorizado, tal como substituição ou atualização, o relatório pode ser registrado dentro da documentação do projeto e não precisa haver um documento separado.

13 APOSENTADORIA DE SISTEMAS COMPUTADORIZADOS

13.1 INTRODUÇAO

O processo de aposentadoria do sistema deve ser documentado por meio de um plano de aposentadoria, que geralmente recebe contribuições dos seguintes atores: dono do processo, Unidade da Qualidade, dono do sistema e Tecnologia da Informação.

Conteúdo do planejamento do processo pode incluir:

- Requisitos para destruição e retenção para os dados históricos ou registros;
- Identificação da configuração atual do *hardware* e *software*, bem como os sistemas que possuem interface, equipamentos ou instrumentos;
- Identificação de quaisquer sistemas externos que dependem dos dados ou registros do sistema.

A extensão e o rigor do planejamento dependem do impacto do sistema e dos riscos associados com a perda de dados.

O plano de aposentadoria do sistema deve ser aprovado pelo dono do processo e unidade da qualidade.

13.2 PLANO DE APOSENTADORIA DO SISTEMA

13.2.1 Introdução

A introdução deve incluir:

- Quem produziu o documento, sob que autoridade e para que propósito;
- Referência a políticas, procedimentos, padrões, guias e outros documentos.

13.2.2 Papéis e Responsabilidades

Os papéis e responsabilidades associados ao processo de aposentadoria devem ser documentados no plano, e devem abranger o dono do processo, a Unidade da Qualidade, o dono do sistema, o time de aposentadoria e seus membros e quaisquer outros atores que contribuírem para o processo.

13.2.3 Visão Geral e Implicações

Consideração deve ser dada ao efeito da aposentadoria do sistema em alguns aspectos, tais como:

- Estratégia – documentar o impacto na estratégia geral de tecnologia e iniciar quaisquer atualizações na documentação ou outras ações necessárias;
- Processo – descrever o impacto no suporte do processo de negócio após a aposentadoria;
- Tecnologia – o escopo e as fronteiras do sistema a ser aposentado devem ser determinados e documentados, bem como a justificativa para a aposentadoria. Identificar outros sistemas, instrumentos ou equipamento que possuam *interfaces* com o sistema que irá se aposentar. Dados ou fontes de informação podem estar localizados em vários sistemas. Identificar os componentes de infraestrutura (rede etc.) que precisarão ser desacoplados do sistema;
- Pessoal – descrever o impacto nos usuários do sistema.

13.2.4 Descrição do Processo de Negócio

O processo de negócio da pré-aposentadoria deve ser documentado e entendido na perspectiva do processo, do usuário e dos dados/registros. Isto ajuda a assegurar que todos os impactos sejam identificados e todos os ângulos de suporte e automação sejam traduzidos em um cenário pós-aposentadoria.

Este cenário futuro deve ser documentado e entendido, especialmente com relação as mudanças no processo de negócio e/ou usuário e a localização ou efeito nos dados/registros.

13.2.5 Abordagem para a Aposentadoria

A decisão sobre se o sistema será substituído deve ser documentada. Se o sistema for substituído, o planejamento da aposentadoria deve ser referenciado e sincronizado com o planejamento de implantação do sistema substituto. A abordagem para a desacoplagem da *interface*, desconexão da infraestrutura, finalização ou transição do suporte técnico e quaisquer suposições, exclusões, limitações ou dependências devem ser documentadas.

13.2.6 Migração, Arquivamento e Destruição de Dados e Registros

O plano deve identificar que dados devem ser migrados, arquivados ou destruídos e o processo de aprovação associado.

A abordagem para a migração de dados e para o arquivamento deve ser determinada com base no histórico de acesso aos dados, na necessidade de reprocessamento, no nível de risco do registro e na robustez da mídia utilizada. Devem ser estabelecidos controles para assegurar que os dados e registros permaneçam seguros, completos, exatos e que a relação assinatura/registro seja preservada, quando aplicável.

A abordagem deve levar em consideração os seguintes aspectos:

- Se os dados devem ser mantidos, devem possuir *backup* e serem armazenados, de acordo com cronogramas de retenção de dados e procedimentos da empresa;
- Antes dos dados serem movidos ou arquivados do sistema, os procedimentos apropriados de recuperação de dados devem estar disponíveis e testados;
- A mídia de dados arquivada deve ser armazenada e mantida, de acordo com as recomendações do fabricante e sob as condições ambientais necessárias;
- Se os dados e os registros forem migrados para um sistema substituto, a migração deve ser planejada, conduzida e verificada de modo a assegurar a integridade dos dados. Os procedimentos para migração devem ser testados ou confirmados antes dos dados serem completamente transferidos para fora do sistema;
- Os métodos a serem utilizados para migração/conversão e verificação dos registros de dados devem ser definidos. Isto pode incluir a realização de um trabalho piloto, antes da migração real dos dados ocorrer, ou uma operação temporária em paralelo de ambos sistemas (sistema novo e o sistema a ser aposentado);
- Se os dados vão ser migrados para o sistema substituto, a estratégia de testes para a verificação da migração deve ser definida. Se uma migração ou conversão automatizada for utilizada, a abordagem para assegurar sua adequação ao uso pretendido deve ser documentada.

13.2.7 Abordagem para Verificação

Deve ser identificada a documentação de verificação, necessária como parte do processo de aposentadoria do sistema.

13.2.8 Manutenção do Sistema e Descontinuação do Suporte

Devem ser planejadas as ações necessárias associadas à(s):

- Modificação ou término dos acordos internos ou externos de suporte;
- Operações, *backup* e restauração, recuperação de desastre e planos de continuidade do negócio;
- Segurança, suporte técnico e administração do usuário e programas de gerenciamento da configuração.

13.2.9 Gerenciamento da Mudança

Procedimentos formais de gerenciamento de mudança devem ser seguidos para a aposentadoria de um sistema computadorizado para assegurar que o processo de aposentadoria seja controlado e gerenciado.

As mudanças resultantes da aposentadoria do sistema devem ser abordadas, tais como as mudanças nos papeis de suporte (suporte técnico, super-usuários etc.) e o treinamento associado.

A abordagem para a comunicação do impacto da aposentadoria do sistema às pessoas envolvidas deve ser documentada.

13.2.10 Cronograma

O cronograma deve ser documentado e incluir as atividades individuais de aposentadoria e as respectivas responsabilidades, as datas de vencimento associadas e quaisquer outras tarefas, marcos críticos e pontos de verificação.

13.2.11 Execução da Aposentadoria

O momento da execução da aposentadoria deve ser cuidadosamente considerado.

Devem existir planos para continuidade dos negócios para o caso de ocorrer qualquer problema durante a aposentadoria ou trabalho de migração. Adicionalmente, um plano reserva é recomendado e deve incluir etapas detalhadas ou referências a procedimentos para configuração e reinstalação, a fim de tornar o sistema aposentado operacional novamente, se necessário.

13.2.12 Documentação e *Software* do Sistema

Documentação do sistema e do *software*, incluindo o código fonte (Categoria 5), tais como, documentação do ciclo de vida, documentação de validação, histórico de mudanças, procedimentos operacionais padrão relacionados ao sistema e outros documentos do sistema, devem ser definidos. A documentação a ser retida deve ter um dono responsável e um local seguro designado. Inventários afetados, procedimentos e outros documentos devem ser atualizados.

Decisões acerca da retenção do *software* e documentos específicos devem ser baseadas em seu potencial de uso futuro e em uma avaliação do risco associado a sua destruição.

13.3 RELATÓRIO DE APOSENTADORIA DO SISTEMA

Após a execução do plano de aposentadoria do sistema, um relatório resumido deve ser gerado para descrever a execução e os resultados obtidos. Se forem executadas atividades de testes ou verificação, os resultados destes testes devem ser resumidos e quaisquer desvios ocorridos devem ser discutidos juntamente com a sua resolução. Este relatório também pode relacionar toda a documentação relativa ao sistema aposentado.

14. VALIDAÇÃO DAS PLANILHAS

14.1 INTRODUÇÃO

Existem ferramentas disponíveis para a criação de uma ampla variedade de aplicações para o usuário final, incluindo análises estatísticas customizadas, bancos de dados local, filtragem, manipulação de dados e análise multivariada. Estas aplicações podem ser utilizadas para realização de atividades reguladas, porém estas aplicações tendem a ser as mais sub-documentadas dentro de um ambiente de BPF.

Este Guia dará ênfase nas planilhas por estas serem mais frequentemente utilizadas nas empresas para tratamento de alguns dados regulados pelas BPF.

O nível e o rigor da especificação e verificação (validação) utilizados nestas aplicações vão depender do risco envolvido, da sua complexidade e grau de inovação. As orientações aqui descritas são direcionadas às planilhas, mas os mesmos princípios podem ser utilizados para outros tipos de aplicações para o usuário final.

14.2 TIPOS DE APLICAÇÕES PARA USUÁRIO FINAL

14.2.1 Planilhas Descartáveis

São planilhas utilizadas do mesmo modo que uma calculadora, para realização de cálculos, sendo que não é mantida uma cópia eletrônica desta operação.

Esta atividade deve ser documentada do mesmo modo que o uso da calculadora seria realizado, ou seja, os valores e o resultados seriam registrados e assinados. Os resultados podem ser impressos, rotulados e assinados. Deve estar claro na folha de registros exatamente qual operação aritmética foi realizada. Isto pode ser facilitado pela impressão de uma cópia da planilha exibindo a fórmula de cálculo utilizada. Esta cópia se torna parte do registro BPF.

Os cálculos utilizados para processamento de dados de BPF devem ser verificados. Isto não significa que os algoritmos utilizados pelas funções nativas da planilha necessitam ser verificados quanto a sua exatidão, mas sim demonstrar que as fórmulas corretas estão sendo utilizadas. Ex.: (a + b) * c é diferente de a + (b * c), e este é um erro possível de ocorrer.

A verificação dos algoritmos pode ser realizada por meio da impressão da fórmula (*cell formulae*) ou por uma revisão feita por terceiros.

14.2.2 Planilhas Retidas como Documentos

Há planilhas que são utilizadas como um processador de texto e não como uma aplicação tradicional. A principal diferença é que a planilha pode ser utilizada tanto para registrar dados BPF quanto para manipulá-los. Dessa forma, se faz aconselhável gerenciá-las como documentos e não como aplicações. É extremamente difícil estabelecer que todas as cópias salvas posteriormente sejam as mesmas que as originais. Cálculos, portanto, devem ser verificados e detalhadamente explicados, quando existirem em um documento de texto. Isto inclui a evidência da fórmula utilizada, conforme descrito no item 14.2.1.

A não ser que a planilha seja adequadamente controlada, deve-se considerar a impressão em papel como o registro-mestre.

Há uma variedade de opções para se obter o controle adequado deste tipo de planilha:

- Utilização das opções internas de segurança da planilha, tais como células ou guias protegidas por senhas;
- Armazenagem da planilha em um diretório seguro;
- Gerenciamento da planilha em um sistema de gerenciamento eletrônico de documentos.

14.2.3 Planilhas Utilizadas como Banco de Dados

São aquelas planilhas utilizadas para gerenciar ou armazenar dados BPF eletronicamente. Os dados podem ser atualizados com frequência, o que pode causar dificuldades porque as planilhas não possuem os controles intrínsecos que possuem os bancos de dados relacionais, necessários para assegurar a integridade dos dados.

As planilhas geralmente possuem limitada ou nenhuma capabilidade para controlar a edição de dados ou para suportar trilhas de auditoria quando necessário. Ao se criar uma planilha, devem ser desenvolvidos controles externos para que sejam superadas estas deficiências.

Os usuários devem, portanto, estar plenamente conscientes das limitações e vulnerabilidades das planilhas quando propostas como alternativa a um aplicativo de banco de dados.

Devido às limitações das planilhas, deve-se utilizar bancos de dados relacionais ao invés de planilhas eletrônicas, visto que estas são limitadas quanto ao armazenamento e gerenciamento de dados podendo o arquivo se corromper quanto esta atingir determinados valores de dados.

Embora existam produtos comercialmente disponíveis destinados a fornecer recursos de trilha de auditoria para planilhas eletrônicas, como regra geral, o uso de planilhas eletrônicas nas quais as trilhas de auditoria sejam necessárias não devem ser utilizadas.

Softwares de planilha geralmente não são projetados para fornecer a funcionalidade de trilha de auditoria. Assim sendo, a utilização de um banco de dados com esta capacidade intrínseca é o preferível.

14.2.4 Aplicações do Tipo Template

Uma utilização muito comum de planilhas é o desenvolvimento de soluções do tipo *template*, onde os dados podem ser sujeitos à manipulação padrão e o resultado salvo como um documento único. Aplicações para a realização de análises estatísticas ou filtragem e manipulação de dados podem também pertencer a esta sub-categoria. Os *templates* podem ser utilizados por exemplo para a tabulação e processamento de dados de um estudo clínico ou, similarmente para tabulação e processamento de dado de resultados de testes de controle de qualidade antes da liberação do produto.

Ao desenvolver tais *templates*, usuários e desenvolvedores devem entender e documentar totalmente a manipulação necessária. Isto permite a confirmação clara das intenções de projeto contra os recursos do pacote padrão a serem estabelecidos e confirmados.

Os seguintes itens devem ser considerados:

- Cálculos devem ser verificados quanto a sua exatidão;
- O *template* vai rodar em uma estação de trabalho única ou disponibilizado para *download* de uma locação única? Se não, como se tem garantia de que todos os usuários utilizarão a versão correta? O controle da versão deve ser estabelecido, suportada por um processo de gerenciamento de mudança efetivo;

- Como o acesso à aplicação e aos campos de dados pelos usuários e pelo desenvolvedor serão controlados? Preferencialmente todas as células, excetuando-se aquelas utilizadas para a entrada de dados, devem ser bloqueadas e inacessíveis para o usuário;
- Como as funcionalidades irão ser configuradas? Existe um requisito para roteiro personalizado quando forem utilizados assistentes de aplicativos? Uma "macro" é um *software* customizado. Mesmo quando criado por captura de teclas, há um programa escrito em uma linguagem tal como a *Visual Basic for Applications*® (VBA) por trás de cada macro;
- Haverá mais de um módulo? Os testes de integração são apropriados nestes casos. Para planilhas isto pode envolver *links* diretos de células para outras planilhas. Estes *links* podem ser afetados por mudanças e deveriam ser abordados como parte do controle de mudanças.
- A entrada de dados será somente via teclado? Alimentações de dados externos necessitam de configuração e uma planilha pode não ser sofisticada o suficiente para lidar com entradas não usuais (ex.: uma cadeia de caracteres que seja muito longa poderá ser truncada e somente uma parte desta cadeia ser importada);
- A saída será salva em arquivo ou apenas impressa? Controles de registros eletrônicos podem ser necessários se o documento for retido eletronicamente.

14.2.5 Banco de Dados de Área de Trabalho

Bancos de Dados de Área de Trabalho são aqueles concebidos e instalados em uma estação de trabalho ou computador de uso de rotina. Estas soluções simples são destinadas para a armazenagem de pequenas quantidades de dados (ex.: MS Access).

O banco de dados de área de trabalho tanto de propriedade quanto o de código aberto oferece soluções superiores para o gerenciamento de grandes volumes de dados quando comparados às planilhas, mas eles ainda são geralmente significativamente menos seguros do que sistemas de gerenciamento de banco de dados mais sofisticados desenvolvidos para rodar em ambientes baseados em servidores dedicados e gerenciados pelo setor de TI através de DBA (ex.: Oracle®, MS SQL Server, etc.).

A utilização destes bancos menos seguros pode apresentar riscos significativos aos registros relevantes às BPF. É necessário haver controles externos para proteção destes registros.

14.3 ABORDAGEM COM BASE NO RISCO

As planilhas podem variar significativamente em risco e complexidade. Os seguintes pontos devem ser considerados para este tipo de aplicação de usuário final:

- Avalição de risco e medidas de controle de risco apropriadas para gerenciar os riscos identificados;
- A adoção da estratégia mais adequada para estabelecer as etapas de Especificação e Verificação da planilha, de forma que seja demonstrado que ela funcione do modo pretendido. Sendo que esta estratégia deve ser baseada em:
    - ✓ Impacto do sistema na segurança do paciente, qualidade do produto e integridade dos dados (avaliação de risco);
    - ✓ Complexidade e inovação do sistema (arquitetura e categorização dos componentes do sistema).

- Segurança apropriada para mitigar o risco de ocorrência de mudanças não autorizadas nos dados e na planilha;
- Gerenciamento da aplicação sobre controle de mudanças.

Políticas e procedimentos da empresa regulada devem definir a sua abordagem específica para a obtenção e manutenção do atendimento e adequação ao uso pretendido da planilha.

14.4 UTILIZAÇÃO DAS CATEGORIAS DO GAMP

O produto no qual a aplicação (Planilhas, *templates* etc.) for construída deve pertencer à Categoria 1. As categorias para as planilhas e outras aplicações para usuário final variam da Categoria 3 a 5.

A definição da categoria da planilha depende da sua complexidade e inovação. Deve ser observado que uma planilha que meramente faz uso do seu poder de edição tabular e não realiza cálculos deve ser considerada um documento.

Uma planilha que simplesmente utiliza suas funções originais (médias, desvios padrão) para realizar cálculos, não havendo configuração, apenas atuando como uma calculadora, pertence à Categoria 3.

Quando forem utilizadas as funções aritméticas da planilha, os cálculos devem ser completamente explicados. Isto inclui a verificação de que a fórmula utilizada foi utilizada adequadamente e que os resultados obtidos estejam corretos. Tal verificação pode ser documentada por meio da revisão e aprovação da planilha por uma segunda pessoa. Não é necessária verificação adicional, visto que não é necessário desafiar a exatidão dos cálculos.

Uma planilha do tipo *template* na qual o usuário insere um dado que automaticamente é enviado para outra célula onde são realizados cálculos específicos, pertence à Categoria 4, visto que o *template* é configurado pelo usuário antes de sua utilização.

Uma planilha que utiliza macros customizadas ou outras operações mais sofisticadas (ex.: edição de código-fonte) pertence à Categoria 5.

Para outras situações diferentes das mencionadas acima consultar as referências bibliográficas deste guia.

14.5 CONTROLES COM BASE NO RISCO

Os riscos às BPF devem ser avaliados. Os seguintes aspectos devem ser considerados:

- A integridade dos dados relacionados ao controle dos arquivos de dados, visto que a maioria das planilhas desenvolvidas processam dados;
- A complexidade da planilha, com base na suposição de que erros sistemáticos não detectados são mais prováveis de ocorrer em *software* não desenvolvido sob um rigoroso método de desenvolvimento e que planilhas mais complexas tem mais oportunidade de ocorrência de erros;
- O impacto potencial na segurança do paciente, qualidade do produto e integridade dos dados.

Com base nestas avaliações devem ser estabelecidos controles com foco em:

- Grau de verificação;
- Controle de segurança (tanto para o código da planilha quanto para os registros BPx que estão na planilha);

- Controle de mudanças;
- Controle da infraestrutura na qual a planilha é construída.

14.5.1 Grau de Verificação

A extensão e o rigor da verificação dependem do risco, da complexidade e da inovação da planilha.

Planilhas complexas e de alto risco necessitam de testes mais rigorosos. A quantidade de ramificações lógicas na planilha é um bom indicador da sua complexidade; se existirem muitas funções lógicas (IF, AND, OR, etc.) ou tabelas de pesquisa, a complexidade é maior. Embora sejam funções nativas, elas introduzem mais caminhos potenciais dentro da planilha e, portanto, mais ramificações que exigem uma estratégia de testes mais sofisticada.

Macros também aumentam a complexidade das planilhas, porque são efetivamente aplicações secundárias embutidas. Mesmo quando são criadas por meio de captura de teclas, há um programa com uma linguagem por trás da macro, embora as macros que simplesmente automatizam uma série de ações sejam menos preocupantes do que aquelas que contenham ramificações lógicas. As macros devem ser desafiadas por meio de testes de funcionalidade. Macros que incluam caminhos lógicos devem ser sujeitas a um maior rigor de verificação, com a devida atenção aos múltiplos caminhos lógicos.

14.5.2 Controle de Segurança

As considerações de segurança para as planilhas são semelhantes às existentes para as aplicações na rede ou servidor, tais como: acesso à planilha, acesso aos dados através da planilha e acesso aos dados ao nível do sistema operacional ou código da planilha. A segurança dentro do ambiente operacional deve ser adequada ao tipo de informação armazenada ou processada.

Para muitas planilhas, uma combinação de controles de infraestrutura (ex.: acesso restrito a diretórios) e controles disponível na planilha (ex.: senha de proteção para células da planilha) podem proporcionar alguma segurança contra mudanças não intencionais. Contudo, estes controles podem ser ineficientes para evitar que o criador da planilha faça mudanças fora do processo de controle de mudanças, particularmente no caso de a planilha estar localizada em uma estação de trabalho individual. Nestas situações o ideal é a colocação da planilha em ambiente de rede na qual os direitos de todos os usuários, incluindo o autor, sejam limitados, adicionando também um processo de *backup* regular programado.

Frequentemente, os dados são salvos dentro da própria planilha. A garantia da integridade destes dados requer o uso de controles muito rígidos, incluindo quaisquer controles necessários dos registros eletrônicos. Em casos onde a planilha for sujeita a algum tipo de edição, o controle adequado pode envolver o uso de um Sistema Eletrônico de Gerenciamento de Documento (EDMS). Como alternativa, podem ser mantidas cópias controladas em um formato que não possa ser alterado ou cópia impressa.

Os dados relevantes às BPF não podem ser salvos em um *drive* de disco local que não seja seguro e que não seja submetido à realização de cópias de segurança (*backup*) regularmente.

Se o grau de segurança da planilha não for adequado o suficiente para os dados nela gerenciados, a empresa regulada deve buscar uma aplicação que rode em um ambiente operacional mais robusto.

14.5.3 Controle de Mudança

Planilhas que processam dados relevantes às BPF devem ser sujeitas a controle de mudanças. O gerenciamento de versão é difícil no caso de planilhas. Em alguns casos, o gerenciamento da planilha dentro de um EDMS pode ser uma solução apropriada, visto que este sistema mantém uma trilha de auditoria das versões da planilha.

Uma outra solução é a utilização de ferramentas de biblioteca que são frequentemente utilizadas por desenvolvedores para gerenciar códigos. Estas ferramentas podem ser utilizadas para gerenciar qualquer tipo de arquivo, podem ser efetivas, relativamente fáceis de implementar e são menos caras que um sistema do tipo EDMS.

Como com qualquer processo de controle de mudança, mudanças na planilha devem ter um registro de mudança que inclua uma descrição da mudança e uma avaliação do impacto. Quando apropriado, os testes associados a esta função devem ser documentados.

15.5.4 Controle de Infraestrutura

Ambientes nos quais a planilha é instalada pertencem à Categoria 1 de *Software*. Estas ferramentas provêm ambiente de aplicação para planilhas, bancos de dados, roteiros ou roteiros que são desenvolvidos por usuários.

A instalação do ambiente deve ser verificada e o ambiente deve ser gerenciado quanto a mudanças e quanto a sua configuração.

14.6 ABORDAGENS PARA VALIDAÇÃO

A seguir são apresentadas 05 (cinco) diferentes aplicações para usuário final, dentre elas a planilha e um resumo breve das abordagens potenciais com base em considerações sobre o impacto nas BPF e na complexidade da aplicação. São exemplos ilustrativos e não são definitivos.

14.6.1 Tipo A – Planilhas Simples para Cálculos

Avaliação: alto impacto e baixa complexidade

Abordagem recomendada:

- Preparação do ERU(URS);
- Verificação documentada, realizada por uma terceira pessoa de que os cálculos são os corretos;
- Segurança para assegurar que é protegida contra mudança não autorizada;
- Segurança para assegurar que os usuários possam acessar somente as versões aprovadas;
- Armazenagem segura do documento eletrônico.

14.6.2 Tipo B – Planilha para Registro de Treinamento

Avaliação: baixo impacto e baixa complexidade.

Abordagem recomendada:

- Nenhuma funcionalidade específica necessita de especificação e verificação;

- Controles padrão para documentos eletrônicos contendo evidência para atendimento às BPF.

14.6.3 Tipo C – Banco de Dados de área De Trabalho

Avaliação: alto impacto e média complexidade

Abordagem recomendada:

- Abordagem típica de Categoria 4: plano de validação; ERU/URS; Especificação Projeto/Funcional (pode ser combinada); rastreabilidade; testes documentados, com critérios de aceitação pré-definidos; relatório de validação;
- Segurança para limitar acesso somente para pessoas autorizadas;
- Controle de mudanças.

14.6.4 Tipo D – Planilhas para Análises Estatísticas – Estudo Clínico

Avaliação: alto impacto e alta complexidade

Abordagem recomendada:

- Abordagem típica de Categoria 5: plano de validação; ERU/URS; Especificação Projeto/Funcional (pode ser combinada); rastreabilidade; testes documentados, com critérios de aceitação pré-definidos; relatório de validação;
- Segurança para limitar acesso somente para pessoas autorizadas;
- Controle de mudanças.

14.6.5 Tipo E – Planilhas para Análises Estatísticas – Estudo Clínico

Avaliação: baixo impacto e alta complexidade.

Abordagem recomendada:

- Verificação documentada, realizada por uma terceira pessoa de que os cálculos são os corretos;
- Controle de mudanças;
- Segurança para assegurar que é protegida contra mudança não autorizada;
- Segurança para assegurar que os usuários possam acessar somente as versões aprovados.

14.6.6 Tipo F – Bancos de dados de Área de Trabalho – Rastreabilidade de materiais produtivos

Exemplo de utilização deste tipo de *software*: disposição de rótulos impressos.

Avaliação: médio impacto e média complexidade.

Abordagem recomendada:

- Abordagem típica de Categoria 4: plano de validação; ERU/URS; Especificação Projeto/Funcional (pode ser combinada); rastreabilidade; testes documentados, com critérios de aceitação pré-definidos; relatório de validação;
- Segurança para limitar acesso somente para pessoas autorizadas;
- Controle de mudanças.

15 CONSIDERAÇÕES FINAIS

Para sistemas já instalados a empresa deverá decidir se o sistema é passível de ser validado ou não.

O primeiro passo a ser seguido deve ser a preparação do documento de ERU/URS partindo-se das orientações descritas neste Guia, de modo semelhante ao que seria feito para a aquisição de um sistema novo.

O passo seguinte é a avaliação deste sistema não validado utilizando-se o documento ERU/URS para decidir sobre se o sistema pode ser validado ou não. Deve ser avaliado ainda o impacto deste sistema não validado na integridade dos dados gerados; na qualidade do produto e na segurança do paciente.

Pode haver situações em que o sistema computadorizado avaliado, com as devidas mitigações, possa ser validado. Caso contrário, é necessária a troca do sistema.

16 GLOSSÁRIO E ACRÔNIMOS

Antivírus – *Software* utilizado para proteção dos computadores contra *malwares*. Também possui a utilidade de descontaminar um computador que estiver infectado com vírus, *worm* e códigos maliciosos. Esses programas precisam ser atualizados com frequência para garantir sua eficácia. Existem antivírus corporativos, que são mais completos e eficazes, dependendo do cenário, do que os antivírus gratuitos.

Aplicação– *Software* que faz uso de serviços de rede tais como transferência de arquivos, *login* remoto e correio eletrônico.

Backup – Rotina de segurança utilizada para a armazenagem, ou seja, uma cópia de dados ou configurações, normalmente em mídia removível, de toda ou parte das informações existentes nos discos rígidos ou na rede. É uma solução que pode ser adaptada, de acordo com as necessidades da empresa.

ERP (*Enterprise Resource Planning* ou "Planejamento dos recursos da empresa") – São *softwares* que integram todos os dados e processos de uma organização em um único sistema. Exemplos: Protheus, Focco, EMS, SAP, Sige Cloud, Conta Azul.

Firmware – Conjunto de instruções operacionais programadas diretamente no *hardware* de um equipamento eletrônico.

Hardware – Designação genérica de todo tipo de equipamento de informática, ou seja, é a parte física do computador. Exemplos: microcomputador, discos rígidos, memória, impressora, scanner, entre outros.

LAN (*Local Area Network* ou Rede da Área Local) – Trata-se de um conjunto de computadores que pertencem a uma mesma organização e que estão ligados entre eles numa pequena área geográfica por uma rede, frequentemente através de uma mesma tecnologia (a mais usada é a Ethernet).

Login – Identificação (nome de usuário) para acesso a um determinado computador ou sistema.

***Log* de dados** – É uma expressão utilizada para descrever o processo de registro de eventos relevantes em um sistema computacional.

***Malware* (*Malicious Software* ou *Software* Malicioso)** – É um software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não). Vírus de computador, *worms*, *trojan horses* (cavalos de tróia) e *spywares* são considerados malware.

MAN – Empresa que possui vários escritórios em uma mesma cidade e deseja que os computadores permaneçam interligados. Para isso existe a (*Metropolitan Area Network*), ou Rede Metropolitana, que conecta diversas Redes Locais dentro de algumas dezenas de quilômetros.

Oracle – É um SGBD (Sistema de Gestão de Banco de Dados) escrito em linguagem C e disponível em diversas plataformas materiais.

***Patch*[1]** – Pedaço de código-objeto inserido num programa executável como correção temporária de um erro.

***Patch*[2]** – Corrigir com *patch*[1]. Em programação consiste em reparar uma deficiência na funcionalidade de uma rotina ou programa existente, em geral, como resposta a uma necessidade imprevista ou a um conjunto de circunstâncias de operação. A correção por meio de *patches* constitui uma forma comum de adicionar uma característica ou uma função a um programa enquanto a próxima versão do *software* não é lançada.

PDF (*Portable Document Format*) – É um formato de arquivo criado pela empresa Adobe Systems para que qualquer documento seja visualizado, independente de qual tenha sido o programa que o originou.

RAM (*Random Access Memory* ou Memória de Acesso Aleatório) – É a memória disponível para uso das aplicações e processamentos. Seu conteúdo volátil é perdido sempre que o computador é desligado.

Rede– Genericamente um conjunto de computadores ligados que se comunicam entre si.

Recuperação de Desastre (DR) – Do inglês *Disaster Recovery*. Envolve um conjunto de políticas e procedimentos para permitir a recuperação ou continuação da infraestrutura de tecnologia e sistemas vitais na sequência de um desastre natural ou provocado pelo homem.

Redundância – É um termo amplo que representa a duplicação de componentes críticos, acrescentando confiabilidade ao sistema. Na tecnologia da informação a definição é aplicada mais frequentemente como a duplicação de dispositivos que são utilizados para *backup*.

Servidor – É basicamente, um computador mais potente do que o *desktop* comum. Ele foi desenvolvido especificamente para transmitir informações e fornecer produtos de *software* a outros computadores que estiverem conectados a ele por uma rede. Os servidores têm o *hardware* para gerenciar o funcionamento em rede *wireless* e por cabo ethernet, normalmente através de um roteador. Eles foram desenvolvidos para lidar com cargas de trabalho mais pesadas e com mais aplicativos, aproveitando a vantagem de um *hardware* específico para aumentar a produtividade e reduzir o tempo de inatividade.

SLA (*Service Level Agreement* ou "Acordo de Nível de Serviço") – Consiste em um contrato entre duas partes: a entidade que pretende fornecer o serviço e o cliente que deseja se beneficiar deste. Nele estão especificados, detalhadamente, todos os aspectos do tipo de serviço que será prestado, assim como os prazos contratuais, a qualidade do serviço e o preço a ser pago pelo trabalho.

Software – É um conjunto de códigos desenvolvido para executar funções específicas, normalmente para o usuário.

Template – É um modelo a ser seguido, com uma estrutura predefinida que facilita o desenvolvimento e criação do conteúdo a partir de algo construído.

Vírus – Denominação dada a pequenos programas desenvolvidos para causar danos em diversos níveis, podendo afetar a integridade de arquivos de dados (removendo partes ou arquivos por completo), prejudicando um computador em particular ou toda a rede de uma empresa.

WAN (*Wide Area Network*) – É o tipo de rede permite a interligação de redes locais, metropolitanas e equipamentos de rede, numa grande área geográfica (Exemplo: país, continente etc.).

Wireless – Tecnologia capaz de unir terminais eletrônicos, geralmente computadores, entre si devido às ondas de rádio ou infravermelho, sem necessidade de utilizar cabos de conexão entre eles. O uso da tecnologia *wireless* vai desde transceptores de rádio como *walkie-talkies* até satélites artificiais no espaço.

17 REFERÊNCIAS BIBLIOGRÁFICAS

17.1 REGULATÓRIAS

- Resolução – RDC nº 69 de 8 de dezembro de 2014;
- Resolução – RDC nº 301, de 21 de agosto de 2019;
- Instrução Normativa – IN nº 43, de 21 de agosto de 2019;
- Instrução Normativa – IN nº 47, de 21 de agosto de 2019.

17.2 TÉCNICAS

- GAMP 5 – A Risk-Based Approach to Compliant GxP Computerized Systems.
- PIC/S Guidance on Good Practices for Computerized Systems in Regulated "GxP" Environments (PI 011-3) – September 2007 (disponível no sítio http://www.picscheme.org).
- FDA Guidance for Industry Part 11, Electronic Records/Electronic Signatures – Scope and Application (August 2003).
- Dicionário Prático de Informática, Microsoft, 2000.

Agência Nacional de Vigilância Sanitária – Anvisa

SIA Trecho 5, Área Especial 57, Lote 200

CEP: 71205-050

Brasília – DF

www.anvisa.gov.br

www.twitter.com/anvisa_oficial

Anvisa Atende: 0800-642-9782

ouvidoria@anvisa.gov.br