Agência Nacional
de Vigilância Sanitária

Agência Nacional
de Vigilância Sanitária

GUIA DE VALIDAÇÃO DE SISTEMAS COMPUTADORIZADOS

Brasília, Abril de 2010

Colaboradores

Alessandra Tomazzini Bastos	ISPE- Brasil
Andre Tagliari	ISPE- Brasil
Camilo Mussi	ANVISA
Carlos César dos Santos	ANVISA
Edinaldo Fernando Ferreira	ISPE- Brasil
Ivan Amorim Sanchez	ISPE- Brasil
Jacqueline Condack Barcelos	ANVISA
Joselene Lima Ferreira Farias	ISPE- Brasil
Jozie Azevedo de Souza	ISPE- Brasil
Juan Sanchez Corriols	ISPE- Brasil
Kleber Costa	ISPE- Brasil
Lúcia Eichenberg Surita	ANVISA
Luiz Alberto dos Santos Lima	ISPE- Brasil
Marcia de Oliveira Fernandes	ANVISA
Mário Brenga Giampietro	ISPE- Brasil
Neriton Ribeiro de Souza	ANVISA
Rodrigo Alvarez	ISPE- Brasil
Rosimeire Pereira Alves da Cruz	ANVISA
Silvia Regina da Silva Martins	ISPE- Brasil
Svetlana Costa de Carvalho	ANVISA
Tatiana Ferreira Marques	ISPE- Brasil
Thais Mesquita de Couto Araújo	ANVISA

Índice

1. Introdução

Este guia foi elaborado para auxiliar no gerenciamento e validação de sistemas computadorizados que tenham impacto em BPx. A exatidão e a integridade dos registros de dados são essenciais para o ciclo de vida do produto, desde a área de pesquisa, passando por estudos pré-clínicos e clínicos, produção e controle de qualidade até a área de armazenamento e distribuição.

Este guia não deve ser adotado como regulamento, portanto, o seu cumprimento não é de caráter compulsório pelo setor regulado. Cada empresa deverá avaliar o conteúdo do guia e verificar sua aplicabilidade. A Vigilância Sanitária tampouco deverá exigir o cumprimento do conteúdo do guia por parte das empresas. A interpretação do conteúdo deste documento é de inteira responsabilidade das empresas que o utilizarem.

1.1 Objetivo

O objetivo do guia é descrever atividades e responsabilidades relacionadas à validação de sistemas computadorizados proporcionando a otimização das atividades envolvidas nesta atividade.

1.2 Abrangência

Este guia se aplica a sistemas computadorizados utilizados em empresas que executem atividades de fabricar insumos farmacêuticos e medicamentos observando o cumprimento do preconizado nas Boas Práticas de Fabricação e Boas Práticas de Laboratório. Este guia também pode ser aplicado a empresas distribuidoras de medicamentos e insumos farmacêuticos, no contexto das Boas Práticas de Distribuição.

A utilização de funções padrão dos sistemas é recomendável, uma vez que quanto maior o nível de customização, maiores serão os esforços de validação.

Nem todas as atividades definidas neste guia são aplicáveis a todos os tipos de sistemas computadorizados. A abordagem pode variar, de acordo com sua criticidade e complexidade. A decisão deve ser tomada pela empresa baseando-se no conhecimento dos riscos envolvidos na utilização de sistema computadorizados.

2. Avaliação de Criticidade dos Sistemas Computadorizados

A empresa deve possuir uma lista contendo todos os sistemas computadorizados instalados e suas respectivas avaliações de criticidade. A necessidade de validação deve ser estabelecida de acordo com os critérios abaixo.

Caso qualquer resposta às questões abaixo seja "SIM", o sistema deve ser validado por ter impacto em BPx.

- O sistema armazena dados que impliquem na rastreabilidade de produtos?
- O sistema gerencia:
  - ✓ a operação automatizada de equipamentos produtivos críticos ou de laboratórios individualmente (ex. compressoras, secadores de leito fluidizado, HPLC, dissolutores, etc.)?
  - ✓ a operação automatizada da geração de utilidades críticas (ex. água purificada, ar condicionado, ar puro, água para injetáveis, etc.)?
  - ✓ cadastramento de apresentações, dosagens, matérias primas, embalagens, potências, tamanho de lotes, etapas de produção, fórmulas mestras, etc.?
  - ✓ planejamento de Produção (ex. ordens de produção, números de lote, matérias primas, embalagens, etc.)?
  - ✓ processo de compras de materiais (ex. qualificação de fornecedores, controle de pedidos de fornecedores previamente qualificados, quantidades, potências, especificações, etc.)?
  - ✓ recebimento de materiais (ex. número de lotes, plano de amostragem, condições físicas, registro de avarias, etc.)?
  - ✓ armazenamento de materiais (ex. *status*, endereçamento, movimentações e transferências, recolhimentos, etc.)?
  - ✓ central de pesagem (ex. ordens de pesagem, potências, fracionamento, recipientes, balanças, etiquetas e lacres, resultados das pesagens, operadores, lotes de produtos, lotes de materiais, etc.)?
  - ✓ controle de produção (ex. ordens de fabricação, controles em processo, registros, operadores, materiais, números de lotes, equipamentos utilizados, sequências de utilização e operação, alarmes, amostras, etc.)?
  - ✓ serviço de atendimento ao cliente (ex. reclamações, ações, eventos adversos, etc.)?
  - ✓ documentação (ex. emissão, distribuição, revisão, controle de versões obsoletas, treinamento, etc.)?
  - ✓ sistemas de qualidade (ex. resultados fora de especificação, auto-inspeção, desvios, controle de mudanças, registros de resultados de análise de matéria prima, embalagem ou produtos, revisão periódica, etc.)?
  - ✓ programa de treinamento (ex. escopo, instrutores, listas de presença, certificados, etc.)?

- ✓ equipamentos (ex. plano e execução de manutenção, plano e execução de calibração, plano e execução de qualificação, etc.)?

3. Sistema Validável

3.1 Avaliação da Possibilidade de um Sistema ser Validado

A comprovação da qualidade e segurança de um sistema computadorizado não deve se restringir a realização de testes. Para confirmar o correto funcionamento de um *software,* e suas interações com o *hardware*, devem ser contemplados aspectos relacionados a infra-estrutura, segurança, manutenção de dados, dentre outros.

- **Sistemas novos:**

É necessária uma avaliação formal do sistema, de forma a assegurar a qualidade e garantir que o mesmo seja validável desde o seu desenvolvimento.

- **Sistemas legados:**

É necessária uma avaliação formal para identificar se o sistema é validável ou não. Caso não exista documentação necessária para comprovação da adesão às BPx, deverá ser verificada a viabilidade de desenvolvimento desta documentação.

Todo sistema que substituir **operações manuais** e que tenha sido classificado como relevante em relação às BPx deve atender, no mínimo, aos seguintes requisitos para ser considerado como validável:

- possuir documentação que descreva as necessidades do usuário em relação ao negócio – fornece informações dos requisitos do usuário para avaliação dos riscos;
- possuir Especificação Técnica/Funcional – fornece informações da funcionalidade do sistema para avaliação dos riscos atendendo aos requisitos do usuário;
- descrição do sistema;
- análise de riscos e avaliação de criticidade do sistema;
- avaliação documentada do histórico do sistema.

Todo sistema que substituir **registros manuais ou impressos** e que tenha sido classificado como relevante em relação às BPx deve atender, no mínimo, aos seguintes requisitos para ser considerado como validável:

- capacidade de armazenamento de dados críticos de operações ou controles com relevância em relação às BPx;
- controle para que entradas e modificações de dados sejam realizadas apenas por pessoas autorizadas (devem ser utilizadas medidas de segurança, tais como utilização de senhas, código pessoal, chaves ou acesso restrito aos terminais);
- capacidade de registrar tentativas de acesso por pessoas não autorizadas;
- capacidade de registrar os acessos autorizados, incluindo usuário, hora e data;

- manutenção dos registros de todas as entradas e alterações quando houver alteração de dados;
- possibilidade de impressão dos dados armazenados eletronicamente;
- inviolabilidade e proteção dos dados históricos, tanto de processo ou operações, quanto de rastreabilidade de modificações feitas pelo operador do sistema (por meios eletrônicos contra danos acidentais ou intencionais);
- possibilidade de realização de backup em intervalos regulares. Os dados de backup devem ser armazenados por um tempo definido e em local separado e seguro.

Se algum item acima não for atendido pelo sistema legado a ser validado, este deverá passar pelo processo de mitigação. Caso a mitigação ou *upgrade* não seja possível, a troca do sistema deve ser considerada.

As figuras 001 e 002 apresentam exemplos de fluxogramas pra validação de sistemas legados e sistemas novos, respectivamente.

Fluxograma de processo de validação de sistemas legados.

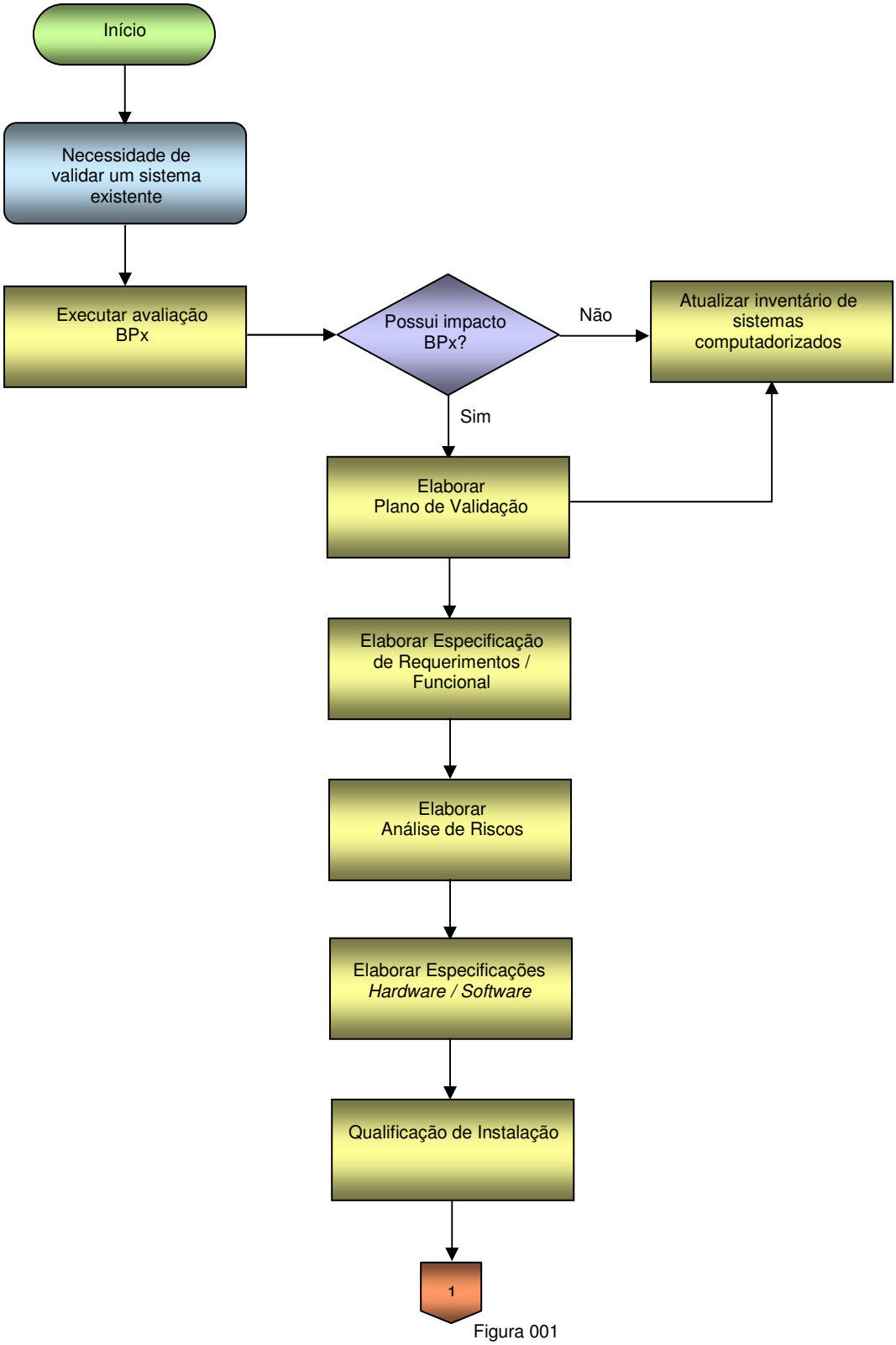

Figura 001

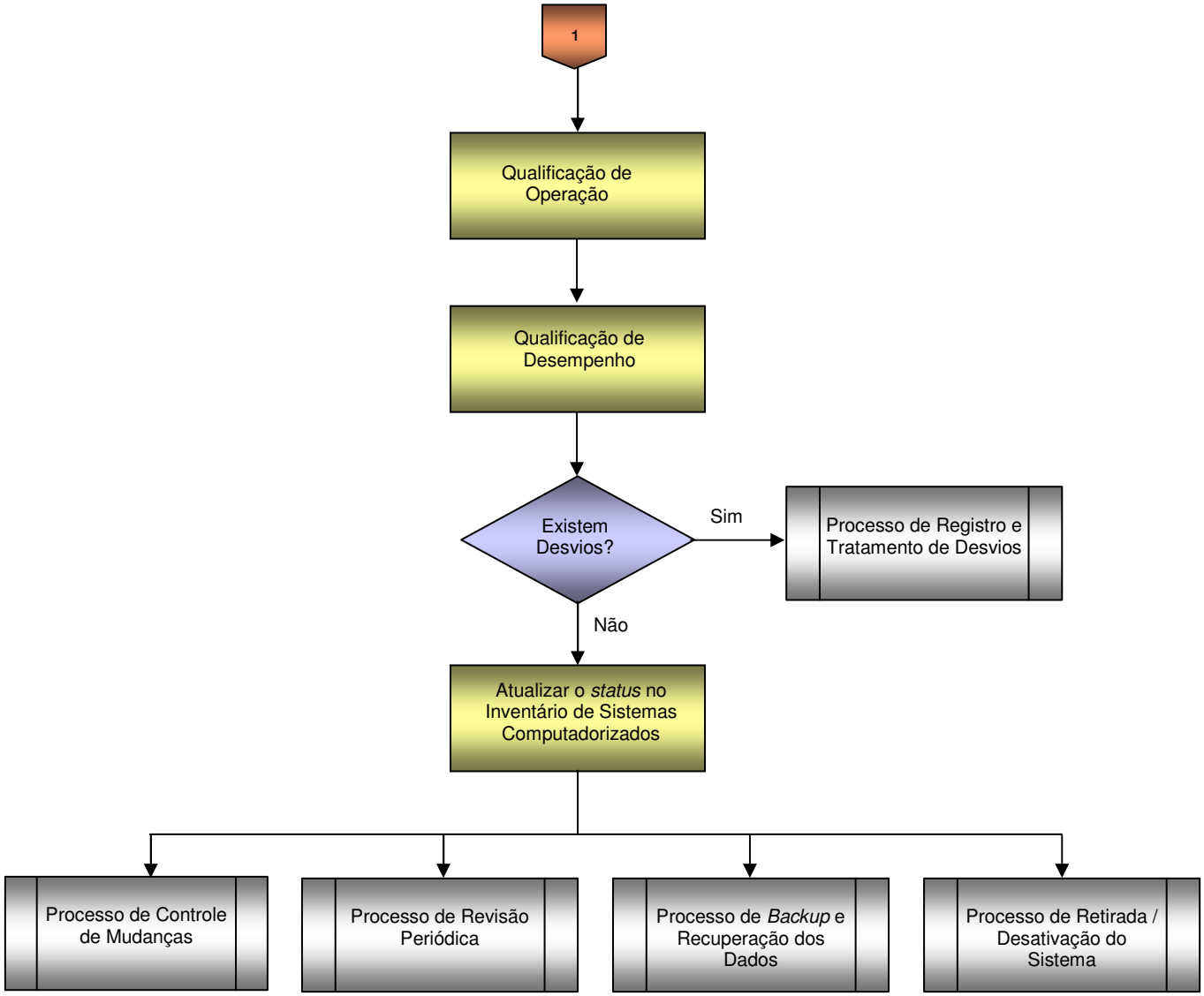

Figura 001 (cont.)

Figura 002: Fluxograma de processo de validação de sistemas novos.

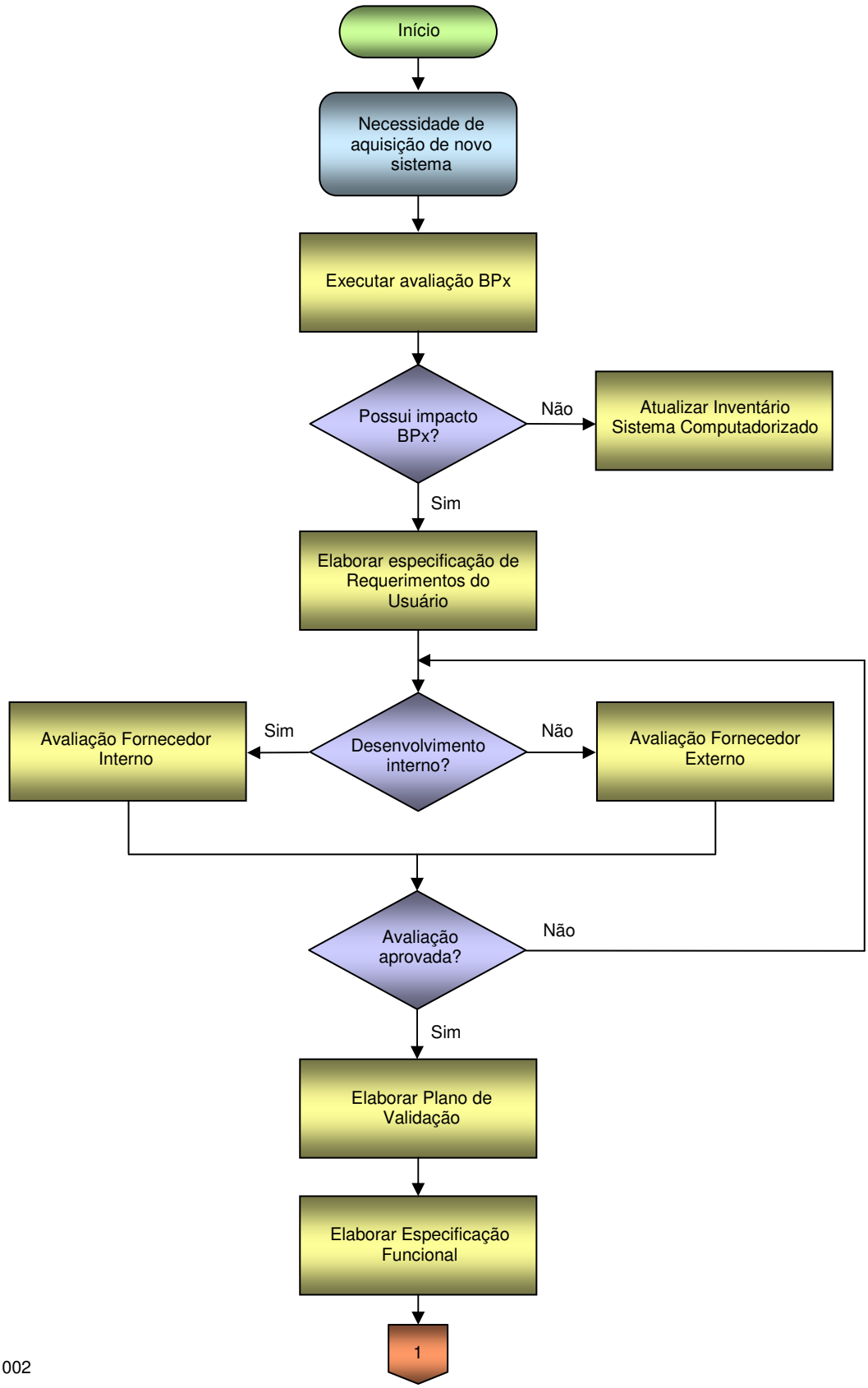

Figura 002

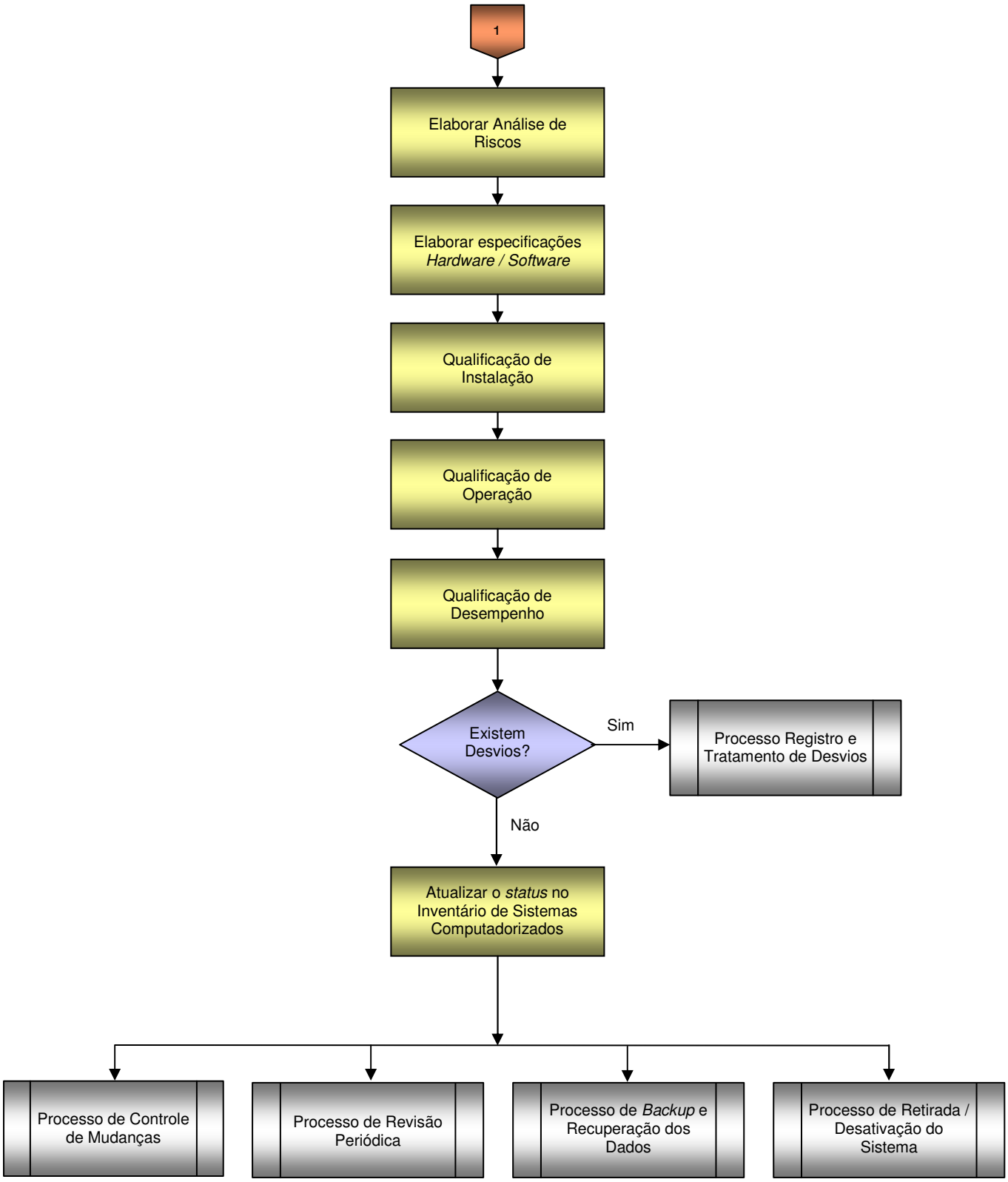

Figura 002 (cont.)

4. Ciclo de Vida

A abordagem do ciclo de vida detalha e define atividades de uma maneira sistemática desde concepção, atendimento aos requisitos, incluindo o desenvolvimento, liberação e uso, até sua retirada de operação (descontinuidade).

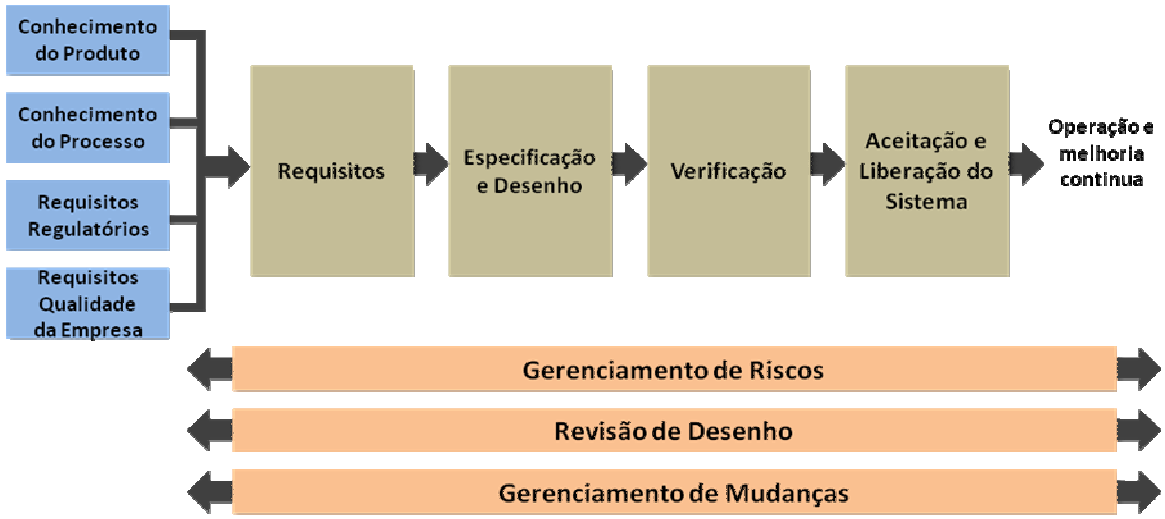

Figura 003

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

- conceito;
- projeto;
- operação;
- descontinuidade.

O ciclo de vida é ilutrado através da figura abaixo:

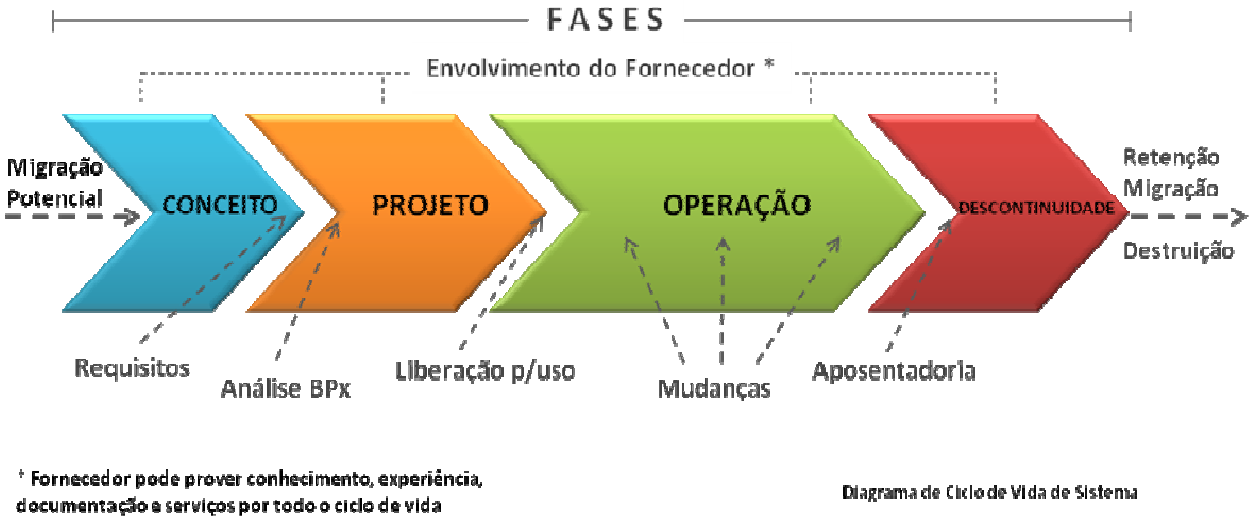

Figura 004

A fase de conceito pode ser utilizada para se rever, aprimorar e automatizar um ou mais processos, baseando-se nas necessidades e benefícios. Nesta fase, são desenvolvidos os requisitos iniciais e consideradas as potenciais soluções. A partir do entendimento do escopo, dos custos e benefícios, é tomada decisão quanto à continuidade do projeto.

A fase do projeto envolve planejamento, avaliação e seleção de fornecedor, bem como especificações, desenho, configuração, testes de aceitação e liberação para operação.

A fase de operação do sistema é a fase mais longa e deve ser gerenciada por procedimentos operacionais. Nesta fase é primordial o gerenciamento de mudanças e o controle da manutenção do estado de validado.

A fase final é a descontinuidade do sistema. Envolve decisão sobre retenção de dados, migração, destruição e o gerenciamento destes processos.

O gerenciamento de riscos deve ser aplicado em todas as fases para remover ou reduzir os riscos a um nível aceitável.

O ciclo de vida de sistemas computadorizados descrito nesta seção não deve ser confundido com a necessidade de se definir abordagem ou método para desenvolvimento de *software* pelo fornecedor.

A figura a seguir mostra a abordagem geral do ciclo de vida de sistemas computadorizados.

Figura 005

4.1 Fases do Ciclo de Vida

4.1.1 Conceito

As atividades desta fase dependem da estrutura organizacional. Cada empresa tem um processo distinto de gerenciamento de projetos. Geralmente, estas atividades estão fora do escopo de validação de sistemas, entretanto, quanto mais formalizada for esta fase, mais recursos apropriados existirão para suportar todas as fases do ciclo de vida do sistema.

4.1.2 Projeto

As fases do projeto são:

- planejamento;
- especificação, parametrização e configuração;
- verificação;
- relatório e liberação para uso.

As principais atividades de suporte são gerenciamento de riscos, gerenciamento da configuração e mudança, revisão do projeto e rastreabilidade.

A figura abaixo mostra como estes estágios de projeto e suas atividades de suporte são parte do ciclo de vida do sistema computadorizado. Possíveis mudanças poderão desencadear um novo ciclo de vida.

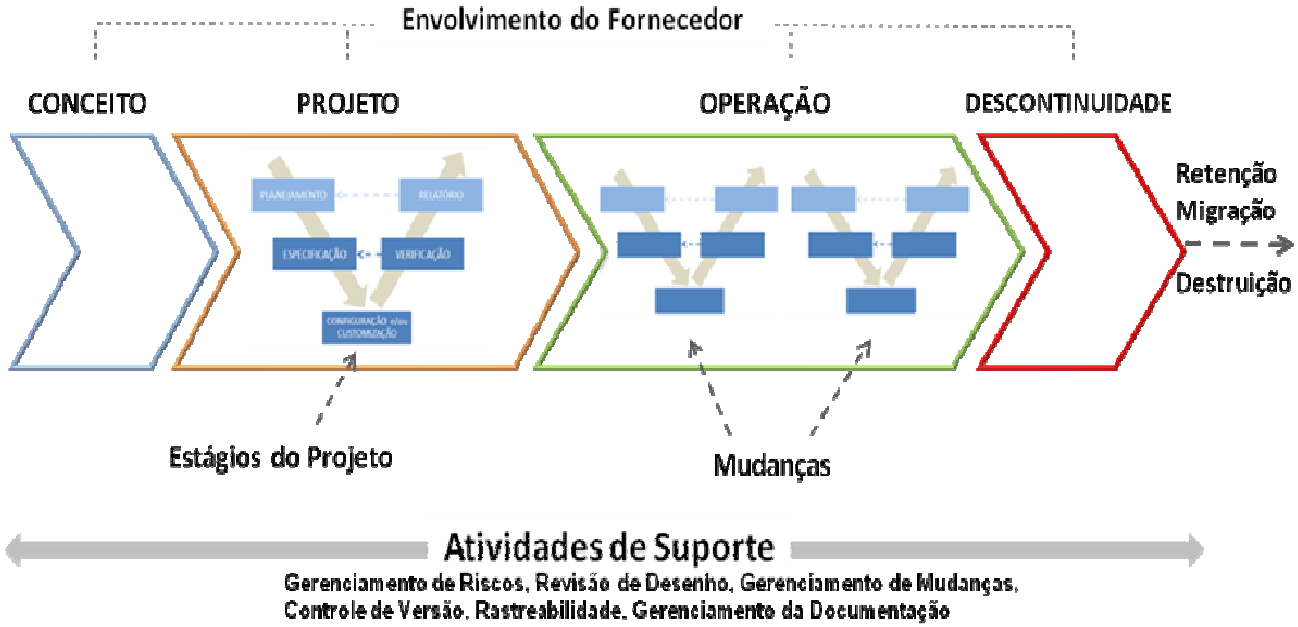

Figura 006

4.1.2.1 Planejamento

O planejamento deve abranger todas as atividades necessárias, responsabilidades, procedimentos e cronograma.

Durante as atividades de planejamento, deve ser considerada a avaliação de impacto em BPx. Em casos de utilização de documentação de fornecedor, a análise desta documentação deve ser prevista no planejamento. Toda documentação, independente da origem, deve estar disponível a qualquer momento.

Nesta fase é importante que os requisitos do usuário estejam claros e documentados.

A extensão e detalhamento dos requisitos e especificações devem ser suficientes para dar suporte ao gerenciamento de riscos, desenvolvimento e verificações do sistema.

A abordagem da fase de planejamento deve estar baseada no entendimento do processo e produto e requisitos regulatórios pertinentes.

4.1.2.2 Especificação, Configuração e Codificação

A função da especificação é permitir que o sistema seja desenvolvido, verificado e mantido.

A configuração deve estar em conformidade com um processo controlável e reprodutivo. Qualquer codificação de *software* deve ser desenvolvida em conformidade com padrões definidos. Os requisitos para as atividades de configuração e codificação dependem do tipo de sistema e do método de desenvolvimento adotado, porém, o gerenciamento da configuração é um aspecto fundamental para garantir o controle da configuração e codificação. Recomenda-se que a necessidade de revisão dos códigos seja incluída como parte do gerenciamento de riscos.

4.1.2.3 Verificação

Durante a etapa de verificação são realizados testes de desafio com o objetivo de verificar se as especificações foram atendidas. Esta fase pode envolver vários ciclos de revisão e testes dependendo do tipo de sistema, método de desenvolvimento utilizado e seu uso.

A extensão dos testes é proporcional aos riscos e complexidade do sistema. Existe uma gama de diferentes tipos de testes possíveis, incluindo:

- caso normal (positivo) – desafio das funções que o sistema deve executar de acordo com o especificado;
- caso inválido (negativo) – desafio das funções que o sistema não deve executar de acordo com o especificado;
- repetibilidade;
- desempenho;
- carga/migração de dados.

Os testes podem ser definidos em uma ou mais especificações de teste para abranger *hardware*, *software*, configuração e aceitação.

A estratégia para os testes deve definir os tipos, número e propósito. Ela deve ser revisada e aprovada por especialistas.

4.1.2.4 Relatório e Liberação Para Uso

O sistema deve ser aceito e liberado para uso em um ambiente operacional em conformidade com um processo controlado e documentado. A aceitação e liberação de um sistema com impacto em BPx requer a aprovação do dono do processo, dono do sistema e representante da unidade da qualidade.

No final do projeto, o relatório de validação do sistema computadorizado deve ser elaborado. Recomenda-se que o relatório contemple resumo das atividades realizadas, desvios encontrados, eventos inesperados, ações corretivas e a comprovação da conformidade aos requisitos especificados e ao uso pretendido para o sistema.

4.1.3 Atividades de Suporte

- Gerenciamento de riscos: um processo adequado de gerenciamento de riscos deve ser estabelecido.
- Gerenciamento de mudanças: um procedimento de gerenciamento de mudanças deve ser estabelecido tanto para a fase de projeto quanto para a fase operacional.
- Controle de versão de programa: um processo adequado de gerenciamento de codificação deve ser estabelecido para que o sistema e todos os seus componentes possam ser controlados.
- Revisão de Desenho ou Qualificação do Projeto: deve ser realizada na fase do projeto a fim de avaliar a aderência aos requisitos, especificações, riscos e testes. É recomendável que o resultado desta atividade gere uma Matriz de Rastreabilidade.
- Gerenciamento da documentação: inclui a elaboração, revisão, aprovação, emissão, mudança, descontinuidade e arquivamento.

4.1.4 Classificação de *Software*

A classificação de *software* pode ser usada juntamente com a avaliação de risco e avaliação do fornecedor para determinar uma estratégia adequada para o ciclo de vida. Geralmente os riscos de falhas ou defeitos aumentam com a customização do *software*. Neste contexto, a classificação pode ajudar a focar os esforços nos pontos onde os riscos são maiores.

Existem duas maneiras de usar a classificação:

- avaliação do sistema como um todo: a classificação do componente principal define a abordagem para a avaliação do fornecedor e definição do ciclo de vida.
- avaliação detalhada dos componentes: para sistemas contendo múltiplos componentes, dependendo da complexidade e do tamanho do sistema, cada nível de componente é classificado. A classificação de cada componente de *software* é utilizada para definir as atividades do ciclo de vida.

A classificação do *software* é composta por:

Classificação 1 - *Software* de Infraestrutura: constitui-se por elementos de infraestrutura ligados para formar um ambiente integrado para executar e suportar aplicações e serviços. Seguem abaixo alguns exemplos:

- sistemas operacionais;
- gerenciadores de banco de dados;
- linguagens de programação;
- programas estatísticos;
- softwares de monitoramento de rede;
- softwares de gerenciamento de segurança;
- antivírus;
- editores de texto e gerenciadores de planilhas.

Para esta classificação de *software* geralmente são realizados registros do número da versão, verificação da correta instalação conforme procedimentos de instalação aprovados.

Classificação 2 - Produtos Não Configurados: *software*s padrões que não podem ser alterados (*software*s de prateleira).

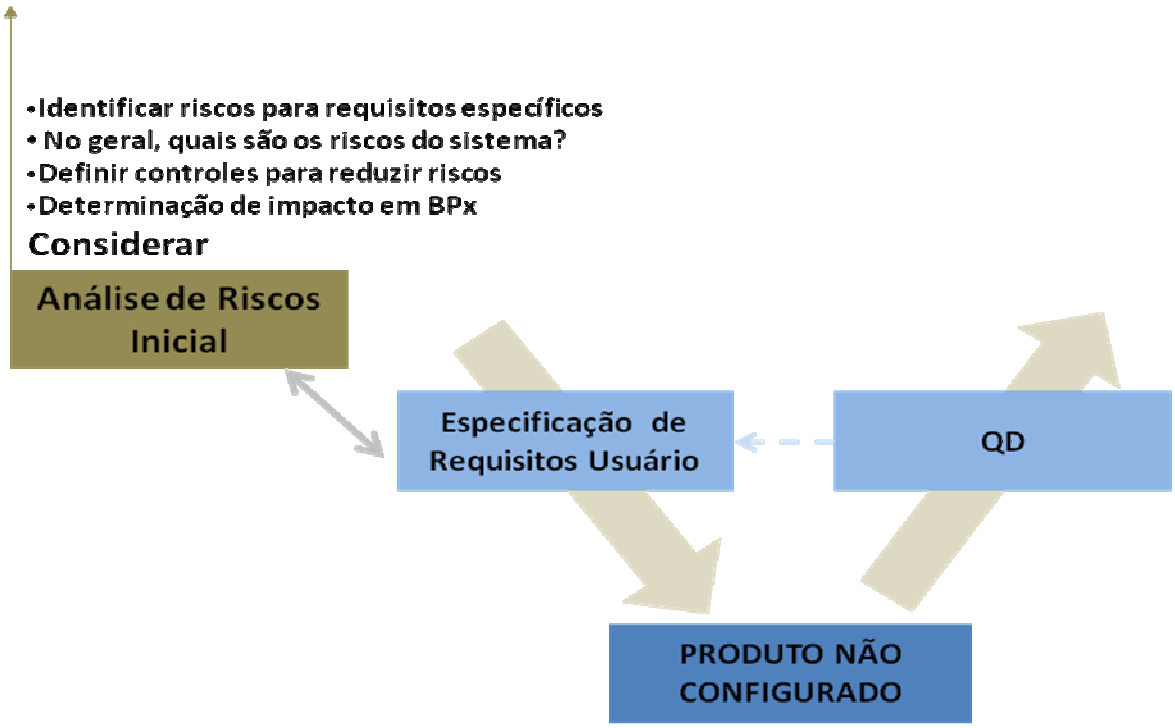

Figura 007

Para sistema com classificação 2, deve ser elaborado no mínimo o protocolo de testes e matriz de rastreabilidade com referência ao requisito do usuário.

Classificação 3 - Produtos Configuráveis ou Customizados: consiste por *software*s com funções que são configuráveis, desenvolvidos e/ou customizados para usos específicos. Esta classificação geralmente envolve a abordagem de ciclo de vida e avaliação de fornecedores.

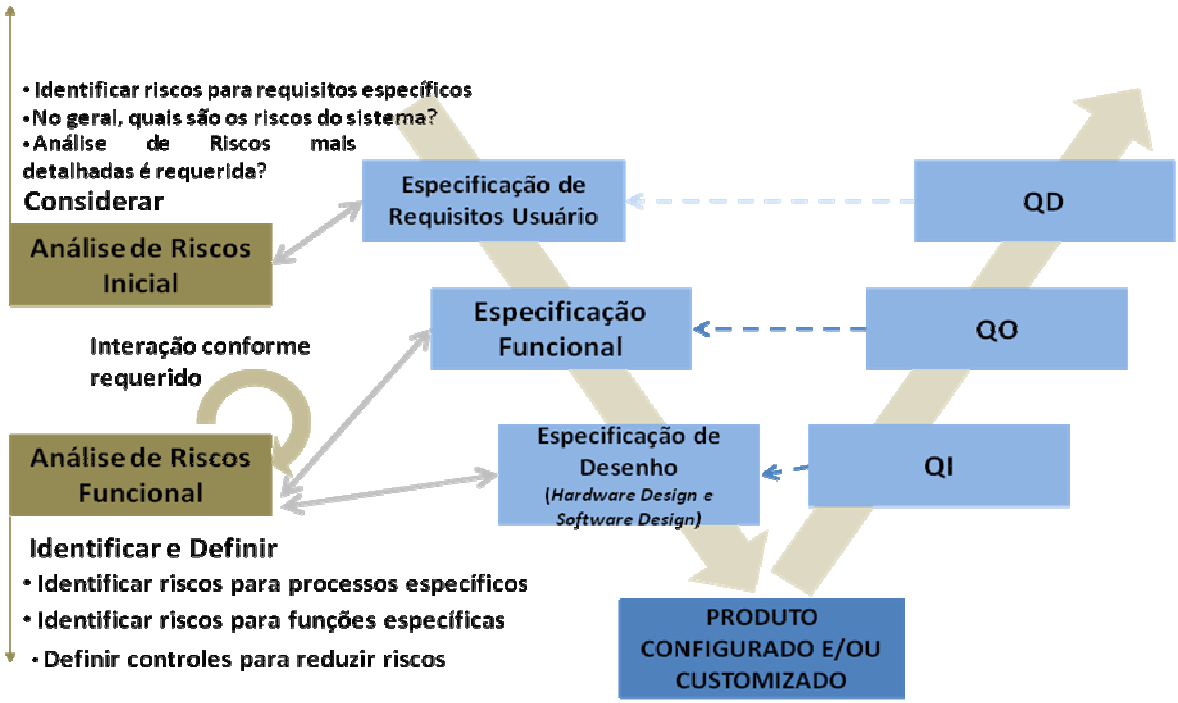

Figura 008

Para sistemas classificados como 3, deve ser elaborado, no mínimo:

- Requisito do Usuário;
- Análise de riscos;
- Plano de Validação;
- Especificação Funcional;
- Especificação Técnica (*Hardware* Design);
- *Software* Design;
- protocolos de testes (instalação, operação e desempenho);
- Matriz de Rastreabilidade;
- Relatório Final de Validação.

Recomenda-se que seja elaborado um Plano de Qualidade e Projeto pelo fornecedor anterior ao início da validação do sistema.

O Plano de Qualidade e Projeto é o documento que descreve o ciclo de vida do sistema, contém a forma de atendimento aos requisitos regulatórios do usuário pelo fornecedor do sistema. O documento pode incluir:

- escopo, limites e interfaces com outros sistemas;
- pré-requisitos para implementação do sistema;
- relação com outros documentos e normas;
- relação com os requisitos de validação do usuário;
- justificativa para o não atendimento aos requisitos do usuário (caso aplicável);
- relação com o Sistema de Qualidade do fornecedor;
- regulações BPx relevantes;
- impactos na qualidade do produto;
- classificação de *hardware* e *software*;
- ciclo de vida e suas fases;
- planejamento das atividades do ciclo de vida;
- planejamento das atividades de suporte;
- relatório de mudança durante o projeto;
- controle de versão de programa durante o projeto;
- gerenciamento da documentação;
- documentos a serem fornecidos e formato;
- subcontratados;
- equipe envolvida;
- relatórios de progresso.

4.1.5 Classificação de *Hardware*

4.1.5.1 Classificação 1 – Componentes de *Hardware* Padrões

Os componentes de *hardware* padrões são equipamentos ou parte de equipamentos que não são desenvolvidos exclusivamente para o sistema a ser validado. Neste caso, os componentes que constituem a arquitetura do sistema devem ser documentados. Os testes de qualificação de instalação do *hardware* devem comprovar seu desempenho, incluindo a conectividade com os demais componentes da arquitetura. O modelo, versão e número de série devem ser registrados. Os componentes de *hardware* padrões não devem ser desmontados para ter seus detalhes verificados ou registrados, evitando a perda de garantia. Os detalhes técnicos podem ser baseados em catálogos técnicos e manuais.

4.1.5.2 Classificação 2 - Componentes de *Hardware* Customizados

Os componentes de *hardware* customizados são equipamentos ou parte de equipamentos que são desenvolvidos exclusivamente para o sistema a ser validado. Itens customizados de *hardware* requerem especificação de desenho e testes de instalação. É recomendável realizar auditoria no fornecedor de forma a avaliar o desempenho no desenvolvimento. Conjuntos usando *hardware* customizado de diferentes fontes requerem verificação de conformidade para compatibilidade com outros componentes. Toda a configuração do *hardware* deve ser inclusa na documentação de desenho e qualificação de instalação.

4.2 Operação

Uma vez que o sistema tenha sido aceito e liberado é necessário manter a conformidade e a adequação ao uso. Isto é possível através de procedimentos para atualização de dados, treinamento, manutenção e gerenciamento.

Os procedimentos para manutenção do estado de validado estão detalhados no capítulo 16.

4.3 Descontinuidade

A descontinuidade do sistema abrange a retirada do sistema, disposição e migração dos dados necessários.

Os procedimentos para descontinuidade de sistemas estão descritas no capítulo 20.

5. Inventário de Sistemas Computadorizados

O objetivo de um Inventário de Sistemas Computadorizados é identificar todos os sistemas existentes na empresa. Durante o processo de levantamento dos sistemas, todas as áreas devem identificar se possuem ou não sistemas.

Deve ser identificada também a existência de planilhas eletrônicas que controlem informações relacionadas às BPx e as mesmas devem fazer parte do inventário. O inventário deve ser revisado periodicamente ou sempre que ocorra adição ou retirada de sistemas, incluindo aprovação formal.

O inventário de Sistemas Computadorizados deverá conter as seguintes informações:

- identificação, descrição e versão do sistema;
- identificação do dono do sistema;
- equipamento – identificar o equipamento que possua sistema computadorizado, por exemplo, compressora, estufa, HPLC, etc.;
- avaliação do impacto em BPx;
- estado do sistema (validado, não validado, etc.);
- número do relatório de validação, caso o sistema já tenha sido validado;
- interfaces com outros sistemas.

As seguintes informações devem ser disponibilizadas, quanto à infraestrutura:

- servidores e seus componentes (bancos de dados, sistemas operacionais, *backup* e recuperação, outros programas necessários ao funcionamento do sistema);
- estações de usuários;
- impressoras;
- comunicações entre plantas;
- componentes de rede;
- geradores e *No-Break*.

Desta forma, um sistema a ser validado, deverá estar no inventário, assim como seus componentes.

Com base no inventário deve-se proceder, através de uma análise de riscos, à priorização da validação dos sistemas que possuam impacto na qualidade dos produtos e ainda não tenham sido validados.

Através desta análise de riscos, deve-se estabelecer uma escala de valores de forma a priorizar a ordem em que os sistemas serão validados. Ou seja, quanto maior o impacto, mais alta a prioridade.

Pode-se identificar, inclusive, a necessidade de se validar diversos sistemas simultaneamente.

6. Plano Mestre de Validação

Recomenda-se que o Plano Mestre de Validação contenha a abordagem que será aplicada para a realização da validação de sistemas computadorizados. Esse Plano Mestre poderá ser geral ou específico para sistemas, dependendo da estrutura documental da empresa.

A elaboração do Plano Mestre deve contemplar, no mínimo, os itens descritos a seguir:

6.1 Objetivo

Descrição do objetivo da empresa, perante a validação de sistemas computadorizados, visando o que ela pretende alcançar com a sua implementação.

6.2 Escopo

Descrição de quais sistemas serão validados, de maneira que os projetos sejam referenciados e atrelados ao Plano Mestre de Validação.

6.3 Requerimentos para Revisão e Aprovação do Plano Mestre de Validação

Descrição das regras para revisão deste plano, quando necessário, visto que a empresa pode mudar o escopo com o decorrer do tempo, havendo assim a necessidade de uma revisão do plano. Recomenda-se que os proprietários/donos dos sistemas sejam envolvidos nesta etapa, tanto na criação quanto na revisão.

6.4 Política de Validação

Descrição da organização das políticas e/ou procedimentos referentes à validação de sistemas computadorizados. Para as empresas que tenham políticas corporativas, estas também devem contempladas na política de validação.

6.5 Estratégia de Validação

Descrição da estratégia de validação a ser seguida para novos sistemas e também para sistemas já existentes na empresa, contemplando sistemas automatizados com impacto em BPx (sistemas de informação, laboratório, automação, etc.).

Durante a qualificação de equipamentos que contenham sistemas computadorizados, os critérios e parâmetros envolvidos nas atividades de validação descritas neste guia devem ser considerados. Ambas as atividades podem ser feitas em conjunto ou serem tratadas separadamente.

6.6 Controle de Mudanças

Descrição do programa de controle de mudanças para assegurar que o estado validado dos sistemas seja mantido. É essencial assegurar que as mudanças nos sistemas não afetem o seu estado validado. Se uma mudança é feita em um sistema validado, uma avaliação do impacto deve ser feita, de forma a determinar a necessidade de revalidação ou quais são as atividades necessárias para manter o estado validado do mesmo.

Observação: Para a validação de sistemas, o termo revalidação não se aplica. O estado validado é mantido através do controle de mudanças e revisões periódicas.

6.7 Responsabilidades

O Plano Mestre de Validação deverá definir quais são os responsáveis por:

- definir as necessidades do negócio e uso pretendido do sistema;
- garantir a elaboração dos requisitos técnicos para o sistema;
- participar da análise de risco para avaliar se o sistema deve ou não ser validado;
- disponibilizar recursos para execução da validação;
- revisar / aprovar os documentos necessários para validar um sistema;
- garantir a manutenção do estado validado do sistema até este ser retirado de uso;
- garantir que os dados / registros sejam mantidos seguros durante o período de retenção;
- informar a área de validação sempre que um sistema for adquirido, desativado ou alterado para atualização do inventário de sistemas;
- gerenciar para que o sistema seja retirado de uso de acordo com procedimentos aprovados.
- gerenciar a estrutura de documentos para a validação de sistemas computadorizados em todo o seu ciclo de vida;
- disseminar as políticas de validação de sistema na empresa;
- informar os terceiros / prestadores de serviço / consultores quanto às diretrizes e/ou políticas da empresa para validação de sistemas;
- participar da definição dos requerimentos de validação de um sistema / projeto;
- participar da elaboração dos requisitos técnicos para o sistema;
- supervisionar a elaboração e execução de todos os documentos do ciclo de vida de validação do sistema;
- supervisionar processos de validação realizados por terceiros e assegurar que estejam em conformidade com políticas e procedimentos corporativos e locais da empresa;

- dar suporte após o encerramento do projeto de validação, avaliando, por exemplo, solicitações de mudanças de sistemas validados;
- manter o Plano Mestre de Validação e Inventário de Sistemas atualizados, de acordo com as informações fornecidas pelos donos dos sistemas.
- garantir o atendimento aos padrões de qualidade da empresa e regulamentos vigentes;
- informar os terceiros / prestadores de serviço / consultores quanto às diretrizes e/ou políticas da empresa para validação de sistemas, quando aplicável;
- realizar a aprovação final / liberação de um sistema validado;
- assegurar que todas as atividades de suporte à validação de sistemas (treinamento, qualificação de fornecedores, desvios, aspectos de BPx, controle de mudanças, entre outros) sejam cumpridas e monitoradas conforme procedimentos estabelecidos, visando à manutenção do estado validado dos sistemas.
- elaboração dos requisitos técnicos para o sistema;
- informar os terceiros / prestadores de serviço / consultores quanto às diretrizes e/ou políticas da empresa para validação de sistemas;
- elaborar / revisar os documentos técnicos gerados durante o projeto para assegurar que são compatíveis com a realidade / necessidade da empresa;
- participar / executar da qualificação de instalação;
- preparar infra-estrutura para execução dos testes (em ambiente de testes e/ou produtivo);
- manter a infra-estrutura de *hardware* e *software* dentro das condições ideais de operação e qualificação;
- seguir os procedimentos de controle de mudança, quando for necessário realizar quaisquer alterações nos sistemas computadorizados com impacto em BPx;
- Supervisão da atuação de terceiros/prestadores de serviço e consultores, quando aplicável;

6.8 Atividades de Validação

O Plano Mestre de Validação deve descrever as diretrizes para todas as atividades relacionadas à validação de sistemas computadorizados. No mínimo, os seguintes itens devem ser contemplados, de forma geral, apoiados por procedimentos operacionais padrões:

- avaliação de fornecedores de sistemas computadorizados;
- inventário de sistemas computadorizados;
- plano de validação;
- análise de riscos;
- classificação de hardware e software para definição de ciclo de vida de documentos e testes;
- matriz de rastreabilidade;
- qualificação de equipamentos, infraestrutura, etc.;
- calibração;
- relatórios de validação;
- manutenção do estado validado;
- descontinuação do sistema;
- treinamentos;
- gerenciamento de desvios;
- segurança e administração (diretrizes para plano de contingência, recuperação de desastre, *backup*, restauração, arquivamento, desempenho, instalação, antivírus e *firewall*).

7. Plano de Validação

O Plano de Validação é o documento que descreve qual abordagem será aplicada para a realização da validação de cada sistema computadorizado. Dependendo da estrutura de documentação da empresa o Plano de Validação pode ser o próprio PMV ou estar contido neste.

7.1 Estrutura do documento

Recomenda-se que a estrutura do documento contemple ao menos os seguintes itens:

- introdução e escopo;
- visão geral do sistema;
- estrutura organizacional;
- gerenciamento dos riscos;
- estratégia de validação
- relação dos documentos que compõe cada etapa da validação e o que se espera de cada etapa do processo de validação;
- critérios de aceitação;
- controle de mudanças e desvios;
- procedimentos operacionais padrões;
- processos de suporte (treinamentos, gerenciamento da documentação, gerenciamento da configuração, manutenção de estado validado);
- cronograma;
- glossário.

7.2 Requerimentos para Revisão e Aprovação do Plano de Validação

Descrição das regras para revisão deste plano, quando necessário, visto que a empresa pode alterar o sistema (ex. upgrade) e com isso haver a necessidade de uma revisão. Recomenda-se que os proprietários/donos do sistema sejam envolvidos nesta etapa, tanto na criação quanto na revisão.

7.3 Estratégia de Validação

A estratégia para o atendimento às BPx deve considerar os seguintes itens:

- avaliação de riscos;
- avaliação dos componentes e arquitetura do sistema;
- avaliação de fornecedor.
- as conclusões dos itens acima devem ser incluídas na estratégia.
- quaisquer procedimentos específicos ou padrões a serem seguidos devem ser definidos.

Recomenda-se que a estratégia de validação descreva, ao menos:

- categorização de software e hardware;
- o critério de aceitação para cada estágio;
- matriz de rastreabilidade;
- controles de mudança do projeto;
- tratamento de desvios.

7.4 Responsabilidades

A responsabilidade no planejamento da validação do sistema computadorizado, em um primeiro momento recai sobre o proprietário/dono do sistema, que pode delegar esta responsabilidade.

As responsabilidades devem ser descritas para cada uma das atividades a serem desenvolvidas ao longo do processo de validação.

Deverão ser definidas responsabilidades de aprovação para toda a documentação gerada ao longo de processo de validação.

8. Gerenciamento de Risco

8.1 Introdução

Este capítulo tem por objetivo introduzir o conceito básico para o gerenciamento de riscos durante todo o ciclo de vida dos sistemas computadorizados novos e existentes.

O gerenciamento de riscos é uma sistemática de processos para a avaliação, controle, comunicação e revisão de riscos. É um processo interativo e complexo utilizado durante todo o ciclo de vida do sistema computadorizado contemplando, inclusive, o seu processo de descontinuidade.

Basicamente, este gerenciamento está associado às metodologias de análise de riscos visando definir, identificar e eliminar as possíveis falhas, problemas ou riscos potenciais que estejam envolvidos nos processos relacionados aos sistemas computadorizados.

8.2 Responsabilidades

Em geral o gerenciamento de riscos é de responsabilidade da empresa como um todo, porém, estas responsabilidades podem ser delegadas a um comitê ou equipe interna. As responsabilidades fundamentais para esta atividade são basicamente as seguintes:

Responsabilidades	Descrição das atividades
Dono do Sistema	▪ Estabelecer uma equipe qualificada e fornecer recursos (pode ser estabelecido um gerente de projetos). ▪ Participar das análises de riscos, quando necessário. ▪ Realizar a aprovação da documentação.
Responsável por Validação de Sistemas / Especialistas	▪ Identificar e analisar criteriosamente os riscos relacionados à saúde do paciente, qualidade do produto e integridade dos dados. ▪ Desenvolver controles e medidas para o gerenciamento dos riscos.
Garantia da Qualidade	▪ Identificar, analisar e avaliar os riscos associados aos requisitos regulatórios. ▪ Realizar a verificação das políticas e procedimentos relacionados com o gerenciamento de riscos. ▪ Realizar a aprovação da documentação.
Fornecedor	▪ Disponibilizar, sempre que requeridas, todas as informações e documentos relacionados a um sistema computadorizado, contemplando inclusive a descrição do funcionamento e das possíveis falhas. ▪ Fornecer suporte e controle necessário para investigação dos desvios. ▪ Participar das análises de riscos, quando necessário.

8.3 Abordagem para o Gerenciamento de Risco

Este guia descreve uma abordagem recomendável para um gerenciamento de riscos com qualidade e confiabilidade. Desta forma, seguem abaixo dois pontos relevantes a serem considerados na qualidade de um gerenciamento de riscos:

- uma avaliação de riscos com qualidade deve basear-se nos conhecimentos científicos e na relação desses com a segurança do paciente;
- o nível de aplicação, qualidade e complexidade da documentação do gerenciamento de riscos deve ser compatível com o nível de riscos identificado.

8.4 Aplicação do Gerenciamento de Riscos nos Processos

Com o objetivo de aplicar um gerenciamento de risco com qualidade é necessário ter um profundo conhecimento dos processos envolvidos em um sistema computadorizado, considerando os potenciais impactos na segurança do paciente, qualidade do produto e integridade dos dados. Os seguintes aspectos devem ser considerados durante sua aplicação:

No contexto de sistemas computadorizados é recomendável basear-se no conhecimento das especificações do sistema e nos processos que os mesmos suportam ou com os quais interagem. Recomenda-se a utilização dos seguintes termos:

Dano: danos para a saúde, incluindo danos que podem ocorrer devido a uma perda de qualidade do produto ou de sua disponibilidade.

Perigo: fonte com potencial para provocar danos.

Risco: a combinação da probabilidade de ocorrência e a severidade do dano.

Severidade: medida das possíveis conseqüências do perigo.

8.4.1Quais são os perigos?

Para identificar os perigos de um sistema computadorizado é necessário ter discernimento e compreensão do que poderia dar errado no sistema, isto deve estar baseado no conhecimento dos especialistas e na experiência acerca dos processos e sua automação. Durante esta avaliação, devem ser consideradas as possíveis falhas do sistema e aquelas ocasionadas por uma ação incorreta dos usuários envolvidos.

8.4.2 Quais são os danos?

Os danos potenciais devem ser baseados na identificação dos perigos. Alguns exemplos de danos potenciais incluem:

- produção de medicamentos adulterados causada por falhas em um sistema computadorizado;
- falhas em instrumentos ou funções clínicas que conduzem a resultados e conclusões incorretas envolvidas nos estudos de pesquisas clínicas;
- falhas em sistemas computadorizados relacionados aos processos de produção, garantia e controle de qualidade, utilidades e quaisquer outros que sejam críticos.

8.4.3 Qual é o impacto?

Deve se avaliar o impacto na segurança do paciente, qualidade do produto e na integridade dos dados, visando estimar suas possíveis conseqüências.

8.4.4 Qual é a probabilidade da falha?

O entendimento da probabilidade de falhas em sistemas computadorizados auxilia na seleção de controles apropriados para o gerenciamento dos riscos identificados. Para alguns tipos de falhas como, por exemplo, falhas de sistema, pode existir certa dificuldade durante a atribuição deste valor, impossibilitando o cálculo apropriado da probabilidade em termos quantitativos durante uma avaliação de riscos.

8.4.5 Qual é a detectabilidade da falha?

O entendimento da detectabilidade de falhas em sistemas computadorizados auxilia na seleção de controles apropriados para o gerenciamento dos riscos identificados. Falhas podem ser detectadas automaticamente pelos sistemas computadorizados ou por métodos manuais.

8.4.6 Como será o Controle de Gerenciamento de Risco?

Um risco pode ser eliminado, totalmente reduzido ou reduzido a níveis aceitáveis através da aplicação de medidas de controle para a redução de sua probabilidade de ocorrência ou aumentando-se a sua detectabilidade. Esses controles podem ser automatizados, manuais ou uma combinação dessas duas formas.

8.5 Gerenciamento de Risco ao Longo da Vida Útil do Sistema

O fluxograma abaixo descreve basicamente cinco passos fundamentais e importantes para serem considerados durante a realização do gerenciamento de riscos:

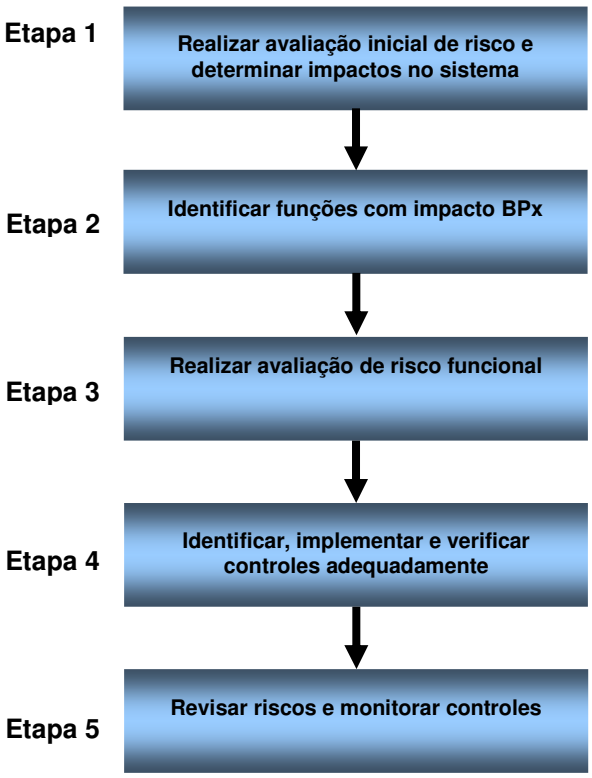

Figura 009

8.5.1 Etapa 1

A Etapa 1 é composta pela realização da avaliação inicial de riscos e determinação dos impactos do sistemas.

A avaliação inicial de riscos tem o objetivo de detectar se o sistema no geral tem impacto em BPx. Nesta fase, a avaliação não considera o detalhamento dos processos e particularidades de cada função. Os cenários de riscos são levantados de maneira genérica.

Exemplo para ERP: análise para a identificação dos módulos que possuem impacto em BPx.

Todas as avaliações iniciais podem contribuir para o projeto. Os pré-requisitos importantes para a realização desta atividade devem abranger:

- entendimento dos processos;
- definição dos limites de cada item envolvido com os processos;
- função principal do sistema computadorizado para suporte e apoio aos processos envolvidos;
- requerimentos claramente definidos (o desenvolvimento dos requerimentos pode ser alterado pela avaliação de riscos).

Os benefícios durante uma avaliação de risco inicial incluem:

- identificação antecipada dos pontos-chaves que requerem uma atenção durante as fases do projeto, incluindo atributos de qualidade e parâmetros críticos dos processos, quando aplicável;
- informações necessárias para o desenvolvimento, especificação e descrição do sistema;
- informações que auxiliam no desenvolvimento da estratégia para alcançar a conformidade e adequação às normas regulatórias.

Geralmente sistemas com impactos altos incluem:

- geração, manipulação ou controles de dados que visam suportar requisitos regulatórios, segurança e eficácia das operações envolvidas;
- parâmetros de controles críticos ou dados utilizados em qualquer fase, da fabricação;
- controles que visam fornecer dados para liberação do produto;
- controles de dados requeridos para o recolhimento de produtos;
- controle de eventos adversos e registros de reclamações;

8.5.2 Etapa 2

A Etapa 2 é composta pela identificação das funções ou processos que têm impacto em BPx para o sistema ou módulos que foram detectados na Etapa 1.

Para a definição dos processos é fundamental que seja realizado um levantamento ou mapeamento visando à identificação das principais funcionalidades e atividades críticas que estão envolvidas no sistema computadorizado.

Durante a definição dos processos é importante salientar que estes são muito mais do que um simples retrato da lógica de entradas e saídas entre usuários e funcionalidades. É uma atividade de análise e avaliação cujo resultado deve retratar claramente como ocorrem os trâmites internos no sistema/processo, quais são os seus pontos fracos, onde estão os riscos, como ocorrem os fluxos das informações, quais são as responsabilidades por cada etapa e, principalmente, quais são os resultados efetivos que constituem todos os processos relacionados ao sistema computadorizado. É recomendável a utilização de fluxogramas ou quaisquer outras ferramentas visuais.

Como princípio fundamental para um levantamento eficaz de riscos dos processos em um sistema computadorizado, é necessário entender as diferenças entre tarefas, atividades, funcionalidades, interfaces, sub-processos, processos e macro-processos (todos contemplando as diferentes áreas envolvidas).Após definição dos principais processos, o gerenciamento de riscos visa demonstrar a complexidade e dimensão de cada função critica relacionada a uma funcionalidade.

8.5.3 Etapa 3

A Etapa 3 é composta pela avaliação detalhada dos riscos das funcionalidades do sistema identificadas durante o mapeamento dos processos.

Os resultados da avaliação de impacto de cada funcionalidade podem influenciar na extensão e severidade das verificações a serem realizadas. Os testes podem focar as funcionalidades com impactos altos, minimizando esforços em processos de baixo risco.

Avaliações de riscos adicionais podem ser necessárias quando novos métodos ou requerimentos são solicitados durante o ciclo de vida.

8.5.4 Etapa 4

Esta etapa inclui a identificação, implementação e verificação dos controles para eliminação ou redução do risco.

Controles são basicamente medidas implementadas para reduzir um risco a um nível aceitável. Esses controles podem fazer parte de uma funcionalidade do sistema computadorizado, com procedimentos manuais em paralelo ou podem ser uma combinação e integração de ambos.

A seleção e utilização dos controles basicamente envolvem:

- eliminação dos riscos através de processos ou sistema redesenhados;
- redução dos riscos diminuindo a probabilidade de uma falha ocorrer;

- redução dos riscos através de implementação de outros processos que detectem a falha;
- redução dos riscos estabelecendo verificações ou métodos para identificação.

Atividades para minimização dos riscos envolvem:

- disponibilidade do sistema para uso;
- nível de freqüência de *backup* e restauração;
- plano de contingência;
- recuperação de desastre;
- segurança do sistema;
- controle de mudanças;
- revisões periódicas.

Controles adicionais podem ser incluídos posteriormente a avaliação dos riscos das funcionalidades. Recomenda-se realizar uma revisão da conclusão da avaliação de riscos, uma vez que estes novos controles podem resultar em processos e testes mais simplificados.

Exemplos de controles para redução de riscos:

Alguns controles de processos podem estar integrados a um sistema, tais como, alarmes, controle de acesso e/ou avisos de verificação. Alternativamente estes controles também podem estar disponíveis de forma independente em processos externos ao sistema, tais como, análises químicas, físicas ou verificação pelo usuário.

Controles Estratégicos
Inclusão de controles automáticos para os atributos de qualidade contemplados em sistemas computadorizados.
Implementação de procedimentos aos processos que contemplam possíveis falhas.
Inclusão de controles automáticos para sistemas computadorizados cujas avaliações identificaram a existência de: ▪ Verificação de dados no próprio sistema visando o controle e redução da probabilidade de entrada de dados incorretos; ▪ Meios que permitam identificar a entrada de dados pelo usuário aumentando a detecção de erros (Trilha de auditoria).
Utilização de métodos, ferramentas e componentes, parâmetros de limite e controle do ambiente operacional.
Aplicação de testes rigorosos comprovando que o sistema desempenha suas funcionalidades corretamente em condições de erros ou que possua condições de tratamento para os mesmos.
Aplicação e revisão de treinamento aos usuários envolvidos.

Se os controles selecionados não forem adequados para um nível de aceitação, amplas estratégias de controle podem ser consideradas e adotadas. Seguem abaixo alguns exemplos de abordagens mais amplas para o controle de riscos:

Modificação na Estratégia do Projeto
Estrutura e composição do projeto: A experiência e qualificação da equipe, o tipo de projeto, a organização, o nível de treinamento e a formação dos especialistas envolvidos. **Nível da documentação e revisão** Alterar a documentação aprovada incluindo ou retirando informações que refletem nos riscos já apontados.
Modificação nos Processos
Como os sistemas computadorizados são utilizados nos processos: Se o sistema computadorizado contempla ou induz a um determinado risco, considerar abordagens alternativas, modificando o processo. **Redesenho dos processos:** Alteração de processos orientando ou eliminando pontos-chaves de riscos.
Prevenção de Riscos
Os riscos são altos e uma nova forma de trabalho deve ser implementada.

8.5.5 Etapa 5

Esta etapa deve prever a revisão e o monitoramento dos controles adotados na Etapa 4, tarefa que pode ser realizada na revisão periódica para manutenção do estado validado ou durante a avaliação dos riscos desencadeada por um controle de mudanças.

A avaliação da criticidade da mudança deve incluir a extensão e verificação da documentação necessária, sempre se baseando nos riscos e na complexidade da mudança a ser realizada.

As avaliações de riscos relacionados ao planejamento de descontinuidade de um sistema computadorizado, geralmente inclui:

- abordagem dos dados e registros para retenção e migração;
- abordagem das verificações gerais contempladas no antigo sistema.

8.6 Metodologia para Análise de Riscos

A análise de riscos tem como propósito estabelecer uma maneira de combinação da severidade, probabilidade de ocorrência e detectabilidade de falhas, reduzindo estas a um nível aceitável. Severidade refere-se às possíveis conseqüências de um risco.

A metodologia apresentada neste documento fornece ferramentas simplificadas a serem utilizadas durante a elaboração de uma análise de riscos. Esta metodologia não é obrigatória, podendo ser utilizadas outras aplicáveis para este tipo de atividade.

Cada risco identificado em uma funcionalidade do sistema pode ser analisado considerando-se dois estágios importantes:

Severidade do impacto em BPx relacionado à probabilidade dessa falha ocorrer, determinando assim a classificação do risco.

A classificação do risco está ligada à determinação da probabilidade do risco ser detectado antes de ocorrer danos, determinando assim a prioridade de um risco.

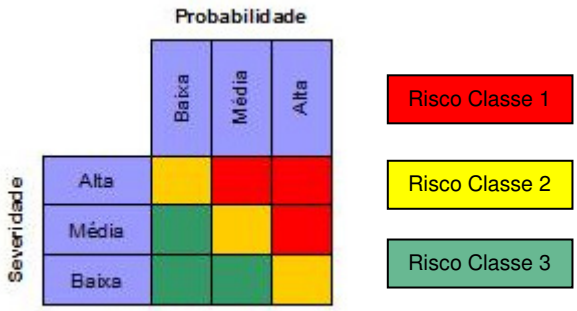

Figura 010 – Método para avaliar e classificar um risco

Severidade = Impacto na segurança do paciente, qualidade do produto e integridade dos dados (ou outro risco).

Probabilidade = Probabilidade da falha (risco) ocorrer.

Classe do Risco = Severidade x Probabilidade.

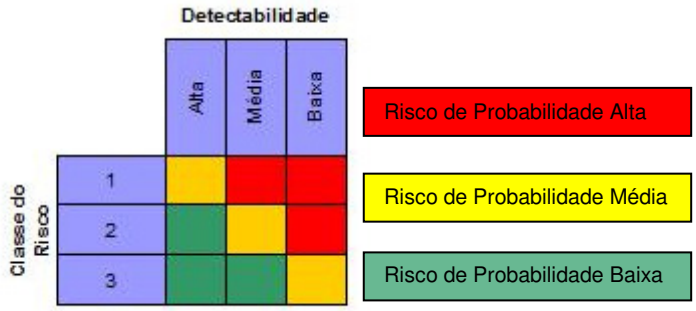

Figura 011 – Método para detectar e priorizar um risco

Detectabilidade = Probabilidade desta falha ser detectada antes do risco ocorrer.

Prioridade do Risco = Classe do Risco x Detectabilidade.

A prioridade do risco visa disponibilizar auxílio para focar a atenção em áreas regulamentadas da empresa, cujos processos estão mais expostos aos riscos. Isto pode ser considerado no relacionamento da tolerância do risco, que varia de empresa para empresa baseando-se na variedade dos processos e requisitos regulatórios aplicáveis.

A aplicação de uma metodologia eficaz depende da capacidade de definir com clareza os parâmetros estabelecidos para a classificação alto, médio e baixo de cada item a ser avaliado. Isso pode ser considerado especificamente no contexto de cada projeto do sistema.

8.7 Comunicação e Documentação do Risco

Conforme definido em diversas metodologias de análise de riscos, é fundamental a existência de uma comunicação e compartilhamento dos riscos, com os donos de sistemas, fornecedores e as demais áreas envolvidas nos processos avaliados. Os resultados obtidos visam determinar em conjunto a análise e eficácia das medidas de monitoramento e controle implementadas.

Esta comunicação e compartilhamento de riscos deve ser adotada durante todo o processo de gerenciamento dos riscos, principalmente quando envolve eventuais mudanças ou adaptações dos processos, posteriormente contribuindo para uma otimização e melhorias do mapeamento e gestão de processos.

A abordagem de gerenciamento de riscos somente será eficaz se as estratégias de controles forem devidamente colocadas em prática e monitoradas durante o ciclo de vida dos sistemas computadorizados, de forma a assegurar e garantir o atendimento e conformidade com os requisitos regulatórios. Conseqüentemente, como parte do processo de revisão periódica, os registros de riscos devem ser revisados e as estratégias de controle verificadas, assegurando que as mesmas permanecem implementadas e operando corretamente.

8.8 Visão geral do processo de análise de riscos

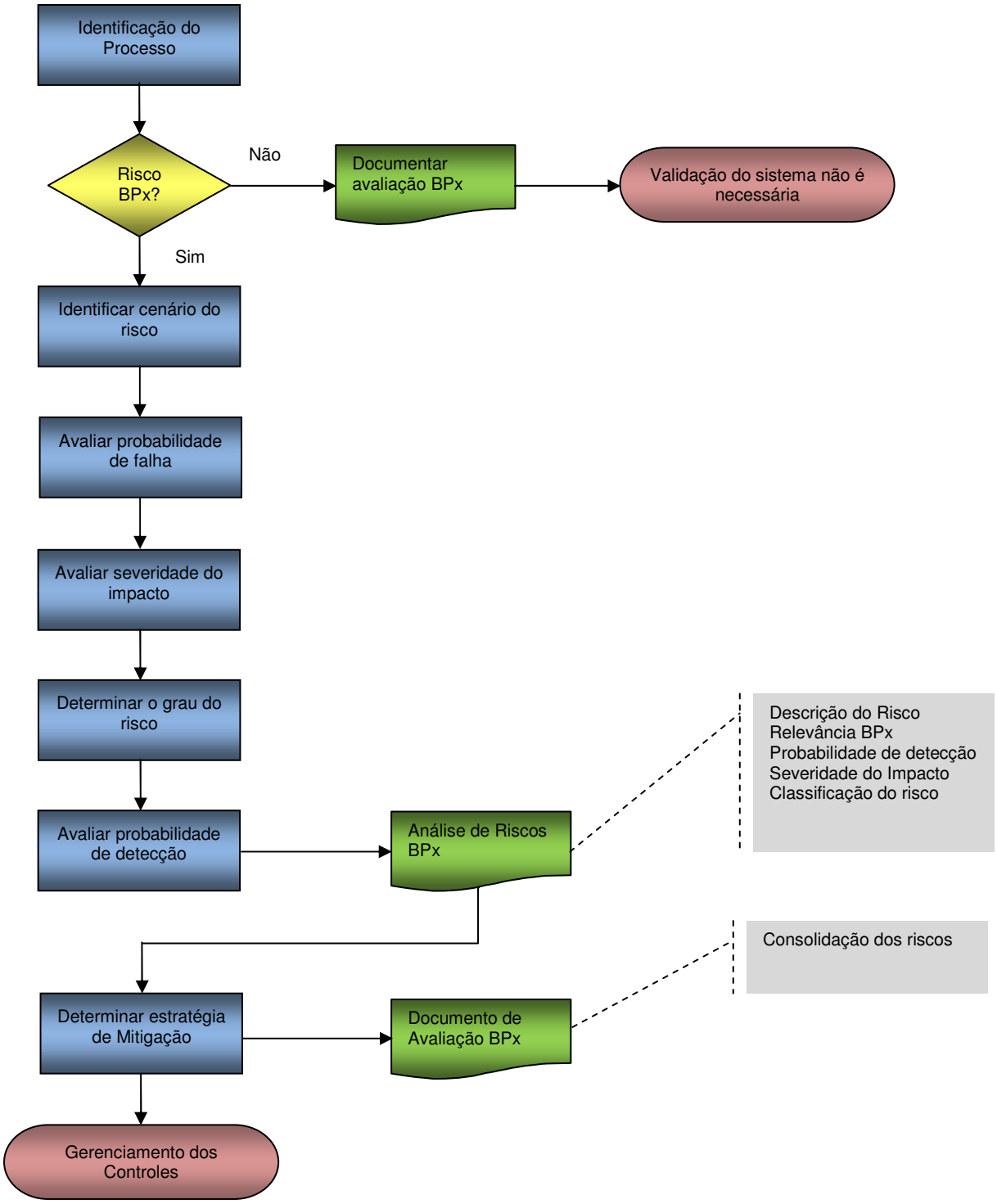

Figura 012

9. Especificação de Requisitos do Usuário (ERU)

A Especificação de Requisitos (ou Requerimentos) do Usuário define de forma clara e objetiva todos os requisitos necessários que um sistema computadorizado deve atender e pode ser utilizado como um documento contratual.

Geralmente é elaborado pelo usuário, porém pode ser elaborado em conjunto com o fornecedor, sendo revisado e aprovado pelos usuários envolvidos, incluindo a Garantia da Qualidade. Quando se trata de sistemas computadorizados já implementados na empresa (legados), este documento poderá ser elaborado no formato de uma Especificação Funcional de forma a integrar os requisitos dos usuários, conforme histórico de sua operação do sistema.

Durante a elaboração deste documento devem ser estabelecidas todas as necessidades da empresa em relação à instalação, operação e desempenho do sistema, inclusive equipamentos e utilidades que o suportam. Também devem ser consideradas todas as necessidades do usuário em termos de capacidade tecnológica, segurança dos dados e informações, requisitos de engenharia, interfaces, manutenção e atendimento às BPx.

A Especificação de Requisitos do Usuário, no contexto de ciclo de vida de sistemas computadorizados é uma etapa muito importante para o sucesso de um projeto de automação e/ou informatização, pois quando descrita de forma clara e precisa, contribui para a seleção de um fornecedor qualificado, para a elaboração de uma Especificação Funcional e análise de riscos detalhadas, possibilitando uma melhor avaliação do número de probabilidades de falhas, configuração do sistema, redução de custo do projeto, entre outros benefícios.

A ERU tem um papel muito importante para validação dos sistemas computadorizados, pois dependendo da estratégia e requisitos apontados neste documento, é possível mudar totalmente o custo e o escopo de um projeto. É recomendável que a elaboração deste documento seja realizada por uma equipe multidisciplinar para que todas as necessidades (por exemplo: *hardware*, *software*, infraestrutura, particularidades do projeto, etc.), sejam devidamente identificadas e descritas.

9.1 Conteúdo do Documento

Segue abaixo a relação dos principais itens que poderão ser considerados durante a elaboração de uma ERU:

9.1.1 Introdução

Esta seção deve conter as seguintes informações:

- descrição das responsabilidades;
- lista de referências cruzadas (relacionamento com outros documentos).

9.1.2 Objetivo e Escopo

Este item deve descrever de forma resumida o objetivo e escopo dos itens requeridos para um determinado projeto, orientando o fornecedor sobre o que o sistema deverá contemplar.

9.1.3 Considerações Gerais

Recomenda-se que esta seção contemple os seguintes itens:

- objetivos-chave;
- benefícios;
- funções principais e interfaces;
- requisitos BPx aplicáveis;
- outros requisitos aplicáveis;
- normas e guias a serem atendidas.

9.1.4 Mapeamento dos Processos

Este item descreve ou referencia o mapeamento de processos e/ou sub-processos relacionado ao sistema computadorizado a ser requerido ou implementado. Este item poderá ser elaborado através da descrição dos processos envolvidos ou através de fluxogramas que demonstrem uma visão geral de todas as atividades, processos, sub-processos, tomadas de decisão, resultados e interfaces do respectivo sistema.

O mapeamento de processos também se aplica a sistemas legados e pode ser elaborado separadamente à ERU.

9.1.5 Requisitos Funcionais

Este item deve descrever todas as funcionalidades requeridas no sistema pelos usuários. Cada requisito deve ter um único número de referência, para facilitar a rastreabilidade e a referência cruzada com outros documentos. Basicamente esta estrutura deve conter para cada item o número e a descrição do requisito.

Durante o levantamento dos requisitos funcionais, os seguintes parâmetros podem ser considerados:

- requisitos do usuário / requisitos funcionais;
- funcionalidades específicas derivadas de requisitos regulatórios (por exemplo: assinatura eletrônica e trilha de auditoria);
- funções de cálculos;
- requisitos da Interface com o usuário (por exemplo: layout, consultas, alarmes, relatórios, linguagem utilizada, etc.);
- interfaces com outros sistemas ou equipamentos;

- requisitos de hardware, sistemas operacionais e base de dados (por exemplo, no caso de sistema operacional, descrever a especificação mínima e versão);
- requisitos de desempenho (por exemplo: número de usuários, capacidade de armazenamento, tempo de resposta, etc.);
- requisitos de segurança de usuário incluindo níveis de acesso (por exemplo: usuário do sistema, administrador de dados, etc.);
- requisitos de acesso ao sistema; quando este for acessado à distância;
- requisitos de *backup* e restauração dos dados;
- requisitos para migração de dados;
- requisitos de ciclo de vida – lista de documentos;
- disponibilidade de recursos;
- outros requisitos técnicos.

9.1.6 Classificação dos Requisitos do Usuário

É recomendável realizar a classificação dos itens requeridos pelos usuários, pois este processo contribui para a identificação dos possíveis riscos às BPx que um sistema computadorizado pode possuir.

Seguem abaixo alguns dos principais itens a serem contemplados no processo de classificação dos requisitos do usuário:

Informativo: não é exatamente um requisito e sim uma informação que será dada aos fornecedores para auxiliá-los na elaboração de suas propostas comerciais;

Importante: requisito que obrigatoriamente será verificado durante o desenvolvimento do sistema/equipamento, mas que não será necessariamente avaliado durante o processo de validação do sistema, por não ter impacto em BPx;

Regulatório e/ou Mandatório: requisito que obrigatoriamente deverá ser considerado durante o desenvolvimento do sistema/equipamento e obrigatoriamente será avaliado durante o processo de validação do sistema por ter impacto em BPx;

Desejável: requisito que se deseja no desenvolvimento do sistema, porém o mesmo não obrigatoriamente poderá ser considerado pelo fornecedor, ou mesmo desconsiderado se acarretar custos demasiados ou dificuldade técnicas para atendê-lo.

9.1.7 Ambiente Físico

Esta seção irá definir o ambiente físico no qual o sistema deverá operar, podendo conter os seguintes tópicos:

- *layout: layout* físico das instalações ou outros locais de trabalho que possam ter impacto no sistema, como por exemplo, links para outros sistemas remotos ou limitação de espaço;
- condições físicas e ambientais (sujeira, poeira ou ambientes estéreis);
- condições atmosféricas: se o sistema irá trabalhar num ambiente com gases inflamáveis, soluções ácido-básicas, etc.;
- infraestrutura física: descrever a infraestrutura de redes, ambientes e as devidas especificações para atender aos requisitos.

9.1.8 Requisitos Não Operacionais

Esta seção deve contemplar, no mínimo, os requisitos não funcionais do sistema computadorizado:

- treinamentos;
- documentação exigida;
- manutenção do sistema;
- atualização de versões / correções de defeitos e/ou falhas.

10. Especificação Funcional

10.1 Introdução

A especificação funcional deve definir clara e completamente o que o sistema computadorizado faz e quais funções e instalações são fornecidas para atender as necessidades descritas nos Requisitos do Usuário. A especificação funcional tipicamente é produzida por um fornecedor, seja ele interno ou externo à empresa e deve ser revisada e aprovada pelo contratante, podendo ser considerado um documento contratual.

10.2 Requisitos Básicos

Recomenda-se que as seguintes informações sejam descritas na especificação funcional:

- detalhes dos aspectos funcionais e de dados do sistema que atenderão aos Requisitos do Usuário, em uma linguagem clara e compreensível para os usuários;
- todas as limitações do sistema, observando quaisquer divergências entre a funcionalidade fornecida pelo sistema com relação aos requisitos do usuário;
- todas as funções do sistema;
- descrição das interfaces internas e externas.

A Especificação Funcional deverá ser clara, para que em caso de consulta possa ser entendida, devendo ser preparada e organizada de uma maneira que permita rastreabilidade entre os requisitos do usuário e as funcionalidades.

10.3 Responsabilidades

Deve haver definição dos responsáveis por:

- elaborar o documento;
- revisar e aprovar o documento no que se refere à parte técnica, validação e requisitos regulatórios;

10.4 Conteúdo da Especificação Funcional

Esta seção propõe uma estrutura para elaboração deste documento.

10.4.1 Introdução

Esta seção poderá conter uma visão geral do sistema, descrevendo as funcionalidades e suas interfaces.

Nesta parte da documentação podem-se inserir referências às regulamentações relevantes, assim como, quaisquer divergências entre a funcionalidade fornecida pelo sistema e o respectivo requisito do usuário, caso existam.

10.4.2 Funções

Esta seção propõe conter as descrições constantes no Requisito do Usuário, devendo ser desdobradas para um nível de funções individuais. Poderá descrever as funções e instalações a serem fornecidas, juntas com modos específicos de operação.

Os seguintes aspectos geralmente são descritos:

- objetivo de cada função ou instalação, e os detalhes de seu uso, incluindo interface com outras partes do sistema. Entradas, saídas, cálculos críticos, lógicas de funcionamento, e impactos em outras funções e/ou outros sistemas e/ou o ambiente devem ser o foco;
- desempenho: resposta, tamanho, processamento centralizado ou distribuído;
- segurança: este tópico deve incluir ação em caso de falhas do software selecionado ou falhas no hardware, checagens automáticas, checagem de valores de entrada, redundância, restrições de acesso e recuperação de dados;
- funções que são parametrizáveis/configuráveis e seus limites;
- rastreabilidade para requerimentos específicos dos requisitos do usuário;
- condições de erro, ações para falhas, arquivos de eventos e diagnósticos;
- funções relativas à segurança do sistema.

10.4.3 Dados

Fluxograma e descrição dos dados de processo envolvidos no sistema;

- dados e parâmetros críticos;
- requisitos e configurações de acesso;
- faixas permitidas de valores para todas as entradas e saídas;
- campos requeridos;
- checagens de validação de dados;

- relacionamentos de dados;
- capacidades dos dados, tempo de retenção e detalhes do arquivamento deles;
- integridade dos dados e segurança;
- migração de dados, caso se aplique.

10.4.4 Interfaces

As interfaces do sistema devem ser descritas, definindo com quais os sistemas ou subsistemas interage, o que eles fornecem independentemente, e o que eles requerem. Para sistemas regulados pelas BPx, a segurança da interface é importante. Os seguintes assuntos devem ser descritos:

- interfaces com usuários: isto deve ser definido em termos de regras, por exemplo, operador, administrador, auxiliar, ou administrador do sistema - considerar tipos de periféricos, formato geral de telas e relatórios, manuseio de erros e relatórios de segurança;
- os modos para entrada do usuário também devem ser definidos, por exemplo, teclado e mouse, tela sensível ao toque, etc.;
- interface com o equipamento, tais como sensores e equipamento de planta;
- interface com outros sistemas: abrangendo o modo, métodos, tempo e regras de interação.

Os tópicos a serem considerados para quaisquer interfaces são listados a seguir:

- transmissão e recepção de dados;
- tipo do dado, formato, faixas e significado dos valores;
- temporização;
- valores de transferência de dados;
- protocolo de comunicação;
- qualquer compartilhamento de dados, criação, duplicação, uso, armazenagem ou destruição de dados;
- mecanismos para inicialização e interrupção;
- comunicação através de parâmetros, áreas de dados comuns ou mensagens;
- acesso direto para dados internos;
- manuseio de erros, restauração e relatórios;
- acesso e segurança.

10.4.5 Ambiente Operacional

Esta seção deve definir qualquer requerimento lógico ou físico no qual o sistema irá trabalhar, por exemplo: infraestrutura de comunicação (rede local, rede remota), condições ambientais (ambiente com pó, corrosivo), especificações de *hardware* (velocidade de processador, espaço em disco), espaço físico, utilidades, etc.

10.4.6 Restrições

Compatibilidade: considerar os sistemas já existentes e padrões que a empresa já trabalha;

Disponibilidade: definir os requisitos de confiabilidade, bem como períodos máximos admissíveis de parada de sistemas;

Procedimentos: considerar os requisitos regulatórios, impactos sobre o fluxo de trabalho atual, habilidades e qualificações atuais dos usuários.

10.4.7 Apêndices

Quando apropriado, por exemplo, em pequenos sistemas, os apêndices podem ser fornecidos para definir especificações de *hardware* e *software*.

11. Desenho de Software (Software Design)

11.1 Introdução

A especificação de desenho fornece detalhe técnico do sistema sendo uma expansão da especificação funcional. A especificação de desenho descreve como o sistema atenderá cada uma das funções definidas na especificação funcional.

De maneira geral especificações de desenho são produzidas pelo desenvolvedor do sistema.

11.2 Diretrizes gerais

O uso de diagramas e tabelas para ilustrar o sistema e configurações é altamente recomendável. Caso esses diagramas e tabelas sejam produzidos separadamente ou em outro documento, eles devem ser referenciados na especificação de desenho.

Diagramas podem ajudar no desenho do *software* para esclarecer e explicar o fluxo de dados, a lógica do sistema, a estrutura de dados e interfaces.

É aceitável a produção de mais de uma Especificação de Desenho para uma única Especificação Funcional. Neste caso, cada Especificação de Desenho deverá ser rastreável e referenciada na Especificação Funcional.

A especificação deve estar estruturada de forma que permita a rastreabilidade de requerimentos individuais.

11.3 Especificação de Desenho

É recomendável que todo o sistema computadorizado tenha uma especificação de desenho. Seu fornecimento à empresa dependerá do resultado de análise de riscos levando em conta sua complexidade e criticidade.

O documento de especificação pode conter as seguintes informações:

11.3.1 Descrição do Sistema

Os módulos ou as partes que compõem o sistema, quando aplicável, devem ser descritos individualmente de forma resumida. A lista de todas as interfaces entre os módulos e também as interfaces com sistemas externos deve ser incluída. Um diagrama de dados do sistema é recomendável.

11.3.2 Dados do sistema

Os dados e objetos do sistema devem ser definidos. Eles devem estar caracterizados de forma hierárquica sendo que esses objetos podem incluir:

- banco de dados;
- pacotes de arquivos;
- registros.

A descrição dos dados e objetos pode incluir:

- tipos de dados (inteiros, caracteres, booleanos, objetos, etc.);
- formato dos dados (alfanumérico, numérico, tamanho do dado, data, etc.).

11.3.3 Descrição dos módulos

Para cada módulo deve ser considerado:

- operação do módulo - a descrição pode estar em forma de linguagem de codificação ou de fluxograma;
- interfaces com outros módulos - pode ser referenciado no diagrama se existir;
- verificação de dados e tratamento de erros;
- mapeamento de dados para cada módulo.

Para cada função ou subprograma dentro do módulo pode ser considerado:

- descrição detalhada das funcionalidades;
- os passos envolvidos em cada programa e as entradas e saídas para cada passo;
- parâmetros, considerando a sua identificação como entrada ou saída ou os dois juntos;
- algoritmos;
- linguagem incluindo versão;
- referência para qualquer padrão de desenvolvimento adotado;
- descrição ou exemplos de todas as telas do sistema (isto pode ser uma referência para a documentação do usuário ou manual de operação);
- dados (conteúdo).

12. Especificação Técnica (Hardware Design)

A Especificação Técnica deve detalhar o desenho e os requisitos relacionados aos componentes de infraestrutura tecnológica na qual o sistema computadorizado será instalado para uso.

Este documento deve contemplar as especificações previstas e apropriadas para um sistema, contemplando todos os componentes e *software*s que compõem a infraestrutura.

A Especificação Técnica é baseada nos requisitos técnicos necessários para a instalação e configuração de um sistema computadorizado de forma a garantir sua integridade, segurança e desempenho em seu ambiente de teste e operacional.

Este documento deve ser referenciado nos demais documentos que envolvem o projeto de validação, conforme a estratégia e metodologia adotada pela empresa.

12.1 Conteúdo do Documento

Segue abaixo a relação dos principais itens que podem ser considerados durante a elaboração de uma Especificação Técnica:

12.1.1 Introdução

Este item deve descrever de forma resumida o objetivo e escopo dos itens técnicos utilizados ou necessários para o sistema, bem como a descrição das responsabilidades e a lista de referências cruzadas (relacionamento com outros documentos).

12.1.2 Requerimentos Técnicos

Este item deve descrever todos os requisitos técnicos, considerando *hardware* e *software,* para um determinado sistema computadorizado. Durante a avaliação e/ ou levantamento dos requerimentos técnicos os seguintes parâmetros podem ser considerados:

- requerimentos para configuração de funções e parâmetros (*set up*, especificações de controles, impactos, módulos, infraestrutura, etc.);
- descrição do hardware (considerando computadores, componentes, CPU, memórias, capacidade, etc.);
- especificações de cabeamento e conectores (internos e externos);
- diagramas elétricos, considerando sensores, instrumentação, alarmes, painel de controle, etc.;
- entradas/saídas de dados, considerando sinais analógicos e/ou digitais;
- temperatura e umidade do ambiente no qual os equipamentos estão instalados;
- interferências externas;
- segurança física.

12.2 Especificações de Hardware

Esta especificação deve prever descrição dos itens abaixo, quando aplicável, mas não limitados a:

12.2.1 Servidores

Descrever as características e configurações relacionadas ao servidor que comporta a instalação do sistema computadorizado, quando aplicável.

12.2.2 Arquitetura de Rede

A infraestrutura de rede deve ser devidamente documentada.

12.2.3 Estações de Trabalho

Os requisitos mínimos de *hardware* e *software* a serem contemplados em uma estação de trabalho (cliente) para o correto funcionamento e desempenho do sistema.

12.2.4 Hardware de Automação

Esta seção deve prever a descrição dos itens relacionados à automação, como por exemplo:

- desenhos técnicos, diagramas, esquemas elétricos, plantas, etc.;
- detalhar os componentes do hardware de automação e/ou controle como PLC, DCS e interfaces como IHM e supervisório, incluindo CPU, cartões de entradas e saídas, switches industriais, fontes, painéis, cartões de interface, etc.;
- detalhar elementos finais de atuação e instrumentação, tais como: sensores, válvulas, etc.;
- detalhar elementos de infraestrutura tais como: especificações de cabos, conectores, etc.;
- precisão e faixa (para instrumentação).

13. Testes de Qualificação (QI, QO e QD)

13.1 Protocolo de Qualificação de Instalação (QI)

Recomenda-se que o Protocolo de Qualificação de Instalação contemple a abordagem a ser aplicada para a realização desta etapa da validação do sistema computadorizado.

13.1.1 Objetivo

A Qualificação de Instalação (QI) visa verificar e documentar as condições de instalação do sistema e se este cumpre satisfatoriamente com os requisitos previamente aprovados na especificação técnica.

13.1.2 Alcance

Garantir a compatibilidade dos componentes técnicos com a especificação técnica:

- comprovar a sua instalação;
- controlar possíveis atualizações de componentes e versões do sistema;
- comprovar que toda a infraestrutura necessária à operação do sistema seja qualificada;

Comprovar, no mínimo, a existência de procedimentos aprovados para:

- backup e recuperação;
- controle de acesso ao sistema;
- controle de mudanças;
- desvios de qualidade;
- plano de contingência;
- controle de acesso à sala de servidores, quando aplicável.

13.1.3 Qualificação de infraestrutura

Existente: Quando a qualificação de infraestrutura for existente, esta deve ser referenciada no protocolo de QI e este deve contemplar a estratégia de instalação do sistema a ser qualificado.

Não-existente: Se não houver qualificação de infraestrutura anterior que englobe o sistema a ser qualificado, o protocolo de QI deve incluir tais componentes.

13.1.4 Descrição do Sistema

Descrição do objetivo, das atividades envolvidas e componentes do sistema a ser validado.

13.1.5 Procedimentos para a Execução dos Testes

Recomenda-se que os documentos que forneçam a base para elaboração do protocolo de testes sejam:

- Plano Mestre de Validação;
- Plano de Validação;
- Requisitos do Usuário;
- Especificação Técnica;
- Manuais do Sistema/Equipamentos.

13.1.6 Instruções Gerais

As verificações devem ser assinadas e datadas pelo executante e pelo conferente. Quando houver comprovação dos resultados do teste, é facultativa a assinatura do conferente.

Desvios, não-conformidades e/ou condições questionáveis detectados durante a execução da qualificação, devem ser registrados, investigados e controlados.

Todas as páginas adicionais devem ser anexadas e referenciadas no protocolo.

13.1.7 Conteúdo da Documentação

A verificação geral da documentação deve contemplar, no mínimo:

- controle da versão do protocolo;
- página contemplando assinatura dos revisores e aprovadores do protocolo;
- definição das responsabilidades para execução das atividades de qualificação.

13.1.8 Elaboração dos testes

Este item trata da descrição, clara e objetiva, da metodologia e estrutura adotada para a elaboração dos testes.

13.1.9 Preenchimento e execução dos testes

Descrição da forma de preenchimento e roteiro dos testes, recomendando-se que contenha:

- identificação do número do protocolo;
- identificação da versão do documento;
- data de emissão;
- referências dos número de documentos anexados aos testes (caso aplicável);
- número da página e total de páginas;

- resultado final de todos os passos do teste executado (aprovado/reprovado);
- cópia de tela, relatórios emitidos pelo sistema ou outra forma de comprovação de todos os resultados dos testes;
- registro de desvio, não-conformidade ou resultado inaceitável no próprio teste.

13.1.10 Controle de Mudanças

Descrição das ações a serem tomadas para execução de uma alteração ou correção do sistema validado durante ou após o término da Qualificação de Instalação.

13.1.11 Aprovação da Qualificação de Instalação

O encerramento da Qualificação de Instalação deve estar relacionado a uma conclusão que poderá ter a forma de relatório ou de um item do próprio protocolo.

13.1.12 Considerações Finais do Protocolo

Após a finalização da Qualificação de Instalação verificar se:

- todos os campos do protocolo foram preenchidos;
- os campos em branco foram inutilizados;
- todos os colaboradores envolvidos na Qualificação de Instalação foram registrados;
- todos os anexos do protocolo foram registrados;
- todos os desvios de qualidade foram registrados, e devidamente finalizados;
- os controles de mudanças originados no processo de Qualificação de Instalação foram registrados.

13.1.13 Manutenção do Estado Validado

Após a conclusão da Qualificação de Instalação, devem-se manter Planos e Procedimentos Operacionais de forma a assegurar que seja mantido o estado validado do sistema, garantindo a integridade dos dados e da documentação associada ao mesmo. Vide capítulo específico que trata o assunto.

13.2 Protocolo de Qualificação de Operação (QO)

Recomenda-se que o Protocolo de Qualificação de Operação contenha a abordagem utilizada para a realização desta etapa da validação do sistema computadorizado.

13.2.1 Objetivo

A Qualificação de Operação (QO) tem com objetivo referenciar, verificar e documentar as condições de operação do Sistema e se este cumpre satisfatoriamente com os requisitos pré-definidos para sua operação. Quando possível, o protocolo deve ser executado em ambiente de testes, sendo este cópia fiel do ambiente que será usado em produção.

13.2.2 Alcance

- Comprovar o atendimento à especificação funcional;
- Comprovar a existência de procedimentos aprovados para as funcionalidades com impacto em BPx, segurança e manutenção do sistema;
- Comprovar a compatibilidade de seus componentes com as funcionalidades a serem qualificadas;
- Possibilitar a verificação da capacidade tecnológica, para todas as funcionalidades a serem processadas (ex. confiabilidade, eficiência, rastreabilidade, registro de eventos, etc.);
- Possibilitar a verificação de conformidade com as normas de BPx e outras normas técnicas aplicáveis;
- Demonstrar que o sistema encontra-se funcionando corretamente através de desafios documentados com base na análise de riscos.

13.2.3 Descrição do Sistema

Este tópico contempla a descrição do objetivo, das atividades envolvidas e funcionalidades do sistema a ser validado.

As funcionalidades podem estar descritas no corpo do documento ou em anexo ao protocolo.

13.2.4 Procedimentos para a Execução dos Testes

Recomenda-se que os documentos que forneçam a base para elaboração do protocolo de testes sejam:

- Especificação Funcional;
- análise de riscos;
- procedimentos de operação do sistema;
- manuais do sistema/equipamento.

13.2.5 Instruções Gerais

- O início dos testes desta fase está condicionado à conclusão satisfatória da etapa anterior (Qualificação de Instalação);
- as verificações devem ser assinadas e datadas pelo executante e conferente. Quando houver comprovação dos resultados do teste, é facultativa a assinatura do conferente;
- os desvios, não-conformidades e/ou condições questionáveis detectados durante a execução da qualificação, devem ser registrados, investigados e controlados;
- todas as páginas adicionais devem ser anexadas e referenciadas no protocolo.

13.2.6 Conteúdo da Documentação

A documentação deve contemplar, no mínimo:

- controle da versão do protocolo;
- página contemplando assinatura dos revisores e aprovadores do protocolo;
- definição das responsabilidades pela execução das atividades de qualificação;
- desenvolvimento dos testes;
- descrição de forma clara e objetiva da metodologia e estrutura adotada para desenvolvimento dos testes.

13.2.7 Preenchimento e execução dos testes

Descrição da forma de preenchimento e roteiro dos testes, recomendando-se que contenha:

- identificação do número do protocolo;
- identificação da versão do documento;
- data de emissão;
- número do documento anexo (caso aplicável);
- número da página e total de páginas;
- registro de todo colaborador diretamente envolvido;
- resultado final de todos os passos do teste executado (aprovado/reprovado);
- cópia de tela, relatórios emitidos pelo sistema ou outra forma de comprovação dos resultados dos testes;
- registro de desvio, falha, não-conformidade ou resultado inaceitável no próprio teste.

13.2.8 Controle de Mudanças

Descrição das ações a serem tomadas para execução de uma alteração ou correção do sistema validado durante ou após o término da Qualificação de Operação.

13.2.9 Aprovação da Qualificação de Operação

O encerramento da Qualificação de Operação deve estar relacionado a uma conclusão que poderá ter a forma de relatório ou de um item do próprio protocolo.

13.2.10 Considerações Finais do Protocolo

Após a finalização da Qualificação de Operação verificar se:

- preenchimento de todos os campos do protocolo;
- campos em branco foram inutilizados;
- todos os colaboradores envolvidos na qualificação de Operação foram registrados;
- todos os anexos do protocolo foram registrados;
- todos os desvios de qualidade foram registrados, e devidamente finalizados;
- controles de mudanças originados no processo de qualificação de operação foram registrados.

13.2.11 Manutenção do Estado Validado

Após a conclusão da Qualificação de Operação, devem-se manter Planos e Procedimentos Operacionais de forma a assegurar que seja mantido o estado validado do sistema, garantindo a integridade dos dados e da documentação associada ao mesmo.

Os procedimentos para manutenção do estado de validado estão detalhados em capítulo posterior.

13.3 Protocolo de Qualificação de Desempenho (QD)

Recomenda-se que o Protocolo de Qualificação de Desempenho contenha a abordagem para a realização desta etapa da validação do sistema computadorizado no ambiente produtivo.

13.3.1Objetivo

A Qualificação de Desempenho (QD) tem como objetivo referenciar, verificar e documentar que o sistema computadorizado, após ser instalado no ambiente de produção e estar adequadamente parametrizado, cumpre satisfatoriamente com os requisitos pré-definidos pela Especificação de Requerimentos do Usuário e/ou Especificação Funcional.

13.3.2 Alcance

- Comprovar o atendimento aos requisitos do usuário e/ou especificação funcional;
- comprovar a existência de procedimentos aprovados para as funcionalidades com impacto em BPx;
- possibilitar a verificação de conformidade com as normas de BPx e outras normas técnicas aplicáveis;
- possibilitar o gerenciamento de segurança (por exemplo: concessão de acesso aos usuários do sistema computadorizado).

13.3.3 Descrição do Sistema

Descrição do objetivo, das atividades envolvidas e funcionalidades do sistema a ser validado.

As funcionalidades podem estar descritas no corpo do documento ou em anexo ao Protocolo.

13.3.4 Procedimentos para a Execução dos Testes

Recomenda-se que os documentos que forneçam a base para elaboração do protocolo de testes sejam:

- Requerimento do Usuário e/ou Especificação Funcional;
- análise de riscos;
- procedimentos de operação do sistema;
- manuais do sistema/equipamento.

13.3.5 Instruções Gerais

- O início dos testes desta fase está condicionado à conclusão satisfatória da etapa anterior (Qualificação de Operação);
- as verificações devem ser assinadas e datadas pelo executante e pelo conferente. Quando houver comprovação dos resultados do teste, é facultativa a assinatura do conferente;
- desvios, não-conformidades e/ou condições questionáveis detectadas durante a execução da qualificação, devem ser registrados, investigados e controlados;
- todas as páginas adicionais devem ser anexadas e referenciadas no protocolo.

13.3.6 Conteúdo da Documentação

A documentação deve contemplar, no mínimo:

- controle da versão do protocolo;
- página contemplando assinatura dos revisores e aprovadores do protocolo;
- definição das responsabilidades pela execução das atividades de qualificação;
- desenvolvimento dos testes
- descrição de forma clara e objetiva da metodologia e estrutura adotada para desenvolvimento dos testes.
- preenchimento e execução dos testes.

Descrição da forma de preenchimento e roteiro dos testes, recomendando-se que contenha:

- identificação do número do protocolo;
- identificação da versão do documento;
- data de emissão;
- número do documento anexo (caso aplicável);
- número da página e total de páginas;
- registro de todo colaborador diretamente envolvido;
- resultado final de todos os passos do teste executado (aprovado/reprovado);
- cópia de tela, relatórios emitidos pelo sistema ou outra forma de comprovação dos resultados dos testes;
- registro de desvio, falhas, não-conformidade ou resultado inaceitável no próprio teste.

13.3.7 Controle de Mudanças

Descrição das ações a serem tomadas após uma alteração ou correção do sistema validado durante ou após o término da Qualificação de Desempenho.

13.3.8 Aprovação da Qualificação de Desempenho

O encerramento da Qualificação de Desempenho deve estar relacionado a uma conclusão que poderá ter a forma de relatório ou inclusa no próprio protocolo.

13.3.9 Considerações Finais do Protocolo

Após a finalização da Qualificação de Desempenho, verificar se:

- todos os campos do protocolo foram preenchidos;
- os campos em branco foram inutilizados;
- todos os colaboradores envolvidos na qualificação de Desempenho foram registrados;
- todos os anexos do protocolo foram registrados;
- todos os desvios de qualidade foram registrados, e devidamente finalizados;
- os controles de mudanças originados no processo de Qualificação de Desempenho foram registrados.

13.3.10 Manutenção de Estado Validado

Após a conclusão da Qualificação de Desempenho, devem-se manter Planos e Procedimentos Operacionais de forma a assegurar que seja mantido o estado validado do sistema, garantindo a integridade dos dados e da documentação associada ao mesmo.

Vide capítulo específico que trata o assunto.

14. Matriz de Rastreabilidade

14.1 Introdução

14.2 Princípios

A Matriz de Rastreabilidade estabelece a relação entre dois ou mais documentos que são desenvolvidos durante o processo de validação. A Matriz assegura que:

- requisitos sejam atendidos e possam ser rastreados às respectivas configurações e/ou elementos de desenho do sistema;
- requisitos sejam verificados e possam ser rastreados para testar ou verificar atividades que demonstram que os requisitos foram atendidos.

Uma matriz também pode fornecer os seguintes benefícios:

- permitir maior efetividade no gerenciamento do risco;
- avaliar potencial impacto de uma mudança pretendida;
- facilitar gerenciamento de risco para uma mudança pretendida.

A Matriz de Rastreabilidade deve ser aprovada e deve ser integrada ao ciclo de vida do sistema.

14.3 Métodos para buscar a rastreabilidade

A rastreabilidade pode ser demonstrada de diversas formas, tais como, Matriz de Rastreabilidade, ferramentas automáticas de *software*s ou referências diretamente inseridas nos documentos.

Exemplo de Matriz de Rastreabilidade:

Requisitos	Análise de Riscos	Especificação Funcional	Especificação de Desenho	Testes
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	D3.3	T8.2

Figura 013 - Exemplo de Matriz de Rastreabilidade

14.4 Opções adicionais

A Matriz de Rastreabilidade pode ser aperfeiçoada com a utilização de colunas adicionais, tais como:

- breve descrição do requisito;
- referência do controle de mudanças;
- nível de criticidade;
- referência a procedimento;
- nível de teste;
- registro de manutenção ou calibração.

15. Relatório Final de Validação

O Relatório de Validação deve conter no mínimo os seguintes itens:

15.1 Introdução

Este item deve indicar a qual projeto se refere o relatório final de validação, bem como descrever seu escopo e objetivo.

15.2 Documentação e atividades geradas durante a validação

Mencionar, com suas respectivas identificações e descrições, todos os documentos gerados durante o projeto, tais como:

- análise de riscos;
- protocolos de testes;
- desvios;
- avaliação dos resultados dos testes;
- controles de mudanças;
- Matriz de Rastreabilidade;
- adendos da documentação de validação (se aplicável);
- referência a outros documentos.

15.3 Conclusão

A conclusão da validação do sistema deve ser elaborada levando-se em consideração os resultados obtidos nos testes aplicados nas qualificações de instalação, operação e desempenho.

Devem ser considerados ainda os requisitos para atendimento às normas regulatórias aplicáveis, conforme estratégia estabelecida no Plano de Validação.

A partir da data de aprovação do relatório final de validação, o sistema deve estar sujeito a controle de mudanças para quaisquer modificações ou implementações que porventura se façam necessárias.

16. Operação

Este capítulo trata dos itens da manutenção do estado de validação e administração e segurança do sistema.

16.1 Controle de Mudanças

Controles de mudanças devem fornecer um mecanismo eficaz e confiável para a rápida implementação de tecnologias e melhorias nos sistemas computadorizados, abordando especificações, desenvolvimento e verificações mencionadas no ciclo de vida.

A criticidade da mudança deve determinar a extensão e verificação das atividades e documentações necessárias sempre se baseando na análise de riscos e na complexidade da alteração a ser implementada.

O procedimento de controle de mudanças da empresa deve contemplar o gerenciamento e controle de todas as alterações relacionadas a sistemas computadorizados validados com o objetivo de assegurar que estes permaneçam neste estado.

As mudanças necessárias em um sistema computadorizado validado devem ser aprovadas por equipe multidisciplinar que envolva a Garantia de Qualidade.

Em caso de mudanças emergenciais, estas devem ser registradas e, ainda assim, analisadas quanto ao seu impacto e posteriormente analisadas e aprovadas pela Garantia de Qualidade. Os casos considerados emergenciais devem estar previstos no procedimento de controle de mudanças da empresa.

16.2 Administração do Sistema

Para manter um sistema computadorizado em estado validado, deve ser considerado o gerenciamento das atividades críticas de sua administração.

Deve haver um responsável por assegurar o planejamento, supervisão e/ou execução de todas as atividades administrativas do sistema. Este colaborador deve possuir conhecimento ou receber um suporte em questões relacionadas às BPx, a fim de poder avaliar, em tempo adequado, os possíveis efeitos das atividades de manutenção.

16.3 Administração da Segurança

Devem ser implementadas medidas que assegurem que o sistema e seus dados estejam protegidos adequadamente contra perdas, danos intencionais ou acidentais, ou alterações não autorizadas. Tais medidas devem assegurar o controle contínuo, integridade, disponibilidade e a confidencialidade de dados vinculados a atividades regulatórias.

Deve ser definido um procedimento ou política para a administração da segurança dos sistemas, levando em consideração os seguintes tópicos:

- segurança física: impedir o acesso físico não autorizado a áreas e sistemas restritos;
- segurança lógica: incluindo identificação do usuário e o controle da disponibilização de senhas. Recomenda-se que seja implementado um procedimento para atribuição e gerenciamento de contas de usuário, descrevendo como um usuário solicita uma conta, os critérios para concessão da conta, entre outros. Os usuários que não possuem mais acesso ao sistema devem ter suas contas desativadas ou excluídas logicamente. A exclusão lógica significa que a conta do usuário é apenas assinalada logicamente como excluída, mas o audit trail deve ser mantido e o ID do usuário não poderá ser reutilizado.
- segurança de rede: incluindo acesso e utilização de internet, acesso remoto, utilização de PC e notebooks, sistemas computadorizados externos e proteção a vírus.
- *log-out* automático: deve ser implementado um dispositivo que assegure que usuários não autorizados não possam acessar as estações de trabalho que sejam deixadas ligadas e disponíveis, tal como software aplicativo ou sistema operacional programados para interromper automaticamente.

O sistema computadorizado deve ter a capacidade de detectar tentativas repetidas não autorizadas de acessar o sistema.

16.4 Treinamento

Periodicamente, os usuários e o pessoal de suporte devem ser treinados. Deve ser mantido registro dos treinamentos realizados.

16.5 Gerenciamento de Desvios

Quaisquer desvios encontrados no sistema durante o ciclo de vida devem ser investigados e documentados.

As diretrizes e a metodologia para o programa de gerenciamento de desvios devem estar descritas em procedimento.

16.6 *Backup* e Restauração

O objetivo é proteger contra a perda física ou lógica dos dados do sistema.

Devem existir procedimentos que assegurem o processo de *backup*, restauração e manutenção dos registros.

Para a guarda do *backup* deve ser escolhida uma mídia adequada, levando-se em consideração: vida útil, condições de armazenamento da mídia e requisitos de verificação, atualização e regravação.

O processo de *backup* deve ser documentado e testado. A documentação do *backup* deve abranger:

- tipo de backup (total, incremental a cada hora,etc.) e periodicidade;
- número de gravações;
- o que fazer em caso de falhas;
- identificação da mídia;
- local de armazenamento com controle de acesso;
- ferramentas e procedimentos de backup;
- inspeção / verificação periódica do backup executado.
- simulação de restauração do sistema;

O processo de restauração do *backup* deve considerar:

- impactos e possíveis riscos (gerenciamento de controles de mudanças e desvios);
- sincronização em caso de sistemas interdependentes;
- aprovação para a atividade de restauração;
- descrição das medidas a serem tomadas em caso dos dados armazenados não poderem mais ser lidos devido a mudanças de software e/ou hardware.

Dados perdidos devem ser tratados como desvios.

16.7 Recuperação de Desastre

A recuperação de desastre tem por objetivo planejar as ações a serem adotadas para que sistemas computadorizados validados voltem a operar em ambiente de produção.

Deve existir um procedimento de recuperação após desastres, que considere:

- planos de contingência;
- conseqüências do sistema estar fora de serviço (impacto em BPx);
- responsabilidades;
- o restabelecimento do sistema e devido treinamento;
- simulação de restauração do sistema;
- especificação técnica de hardware e software necessários;

16.8 Revisão Periódica

A revisão periódica de sistemas computadorizados deve ser realizada com o objetivo de garantir que possíveis mudanças de processo, de componentes do sistema ou de manutenções, por exemplo, não tenham impactado no seu estado validado.

Deve ser determinado um cronograma de revisões para todos os sistemas. A freqüência de revisão para sistemas específicos deve ser baseada na sua criticidade. A revisão deve levar em consideração os seguintes aspectos:

- documentação de validação do sistema;
- documentação da revisão anterior;
- controles de mudanças emitidos;
- desvios ocorridos;
- procedimentos operacionais;
- controle de acesso ao sistema;
- execução correta do backup do sistema;
- status do sistema computadorizado (ex. espaço em disco, utilização RAM);
- status dos arquivos de histórico e trilhas de auditoria.

Caso seja encontrado algum problema no sistema, um plano de ação deve ser estabelecido.

16.9 Manutenção do Sistema Computadorizado

A manutenção deve ser conduzida regularmente, seguindo um plano de manutenção que deve contemplar, quando aplicável:

- calibrações de rotina;
- manutenções preventivas;
- condições ambientais (temperatura, umidade);
- no-breaks.

16.10 Arquivamento da Documentação de Validação

Tem por objetivo assegurar que toda a documentação envolvida no ciclo de vida de um sistema computadorizado validado seja devidamente arquivada, estando disponível a qualquer momento.

17. Particularidades de Validação por Tipo de Sistema

Devido à complexidade dos sistemas computadorizados, existe uma padronização global que visa classificá-los conforme sua atuação, facilitando o entendimento de sua aplicação.

A figura abaixo ilustra alguns deles:

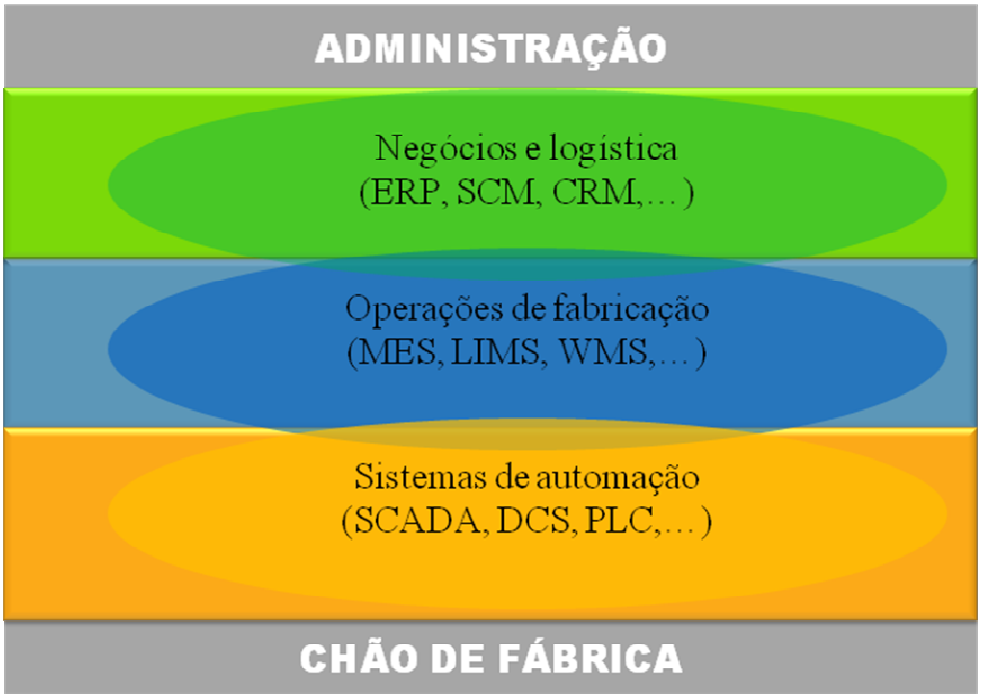

Figura 014

17.1 Particularidades de Validação para sistemas de gestão

17.1.1 Sistemas do tipo ERP

ERP (Enterprise Resource Planning) ou SIGE (Sistema Integrado de Gestão Empresarial) são sistemas computadorizados que integram um grande número de dados e processos de uma organização em um único sistema. A integração pode ser entre qualidade, finanças, contabilidade, recursos humanos, fabricação, marketing, vendas, compras, etc.

Quando se trata da validação de um novo ERP é recomendável seguir todo o ciclo de vida para sistemas computadorizados. Nestes casos é fundamental que na estratégia de validação seja contemplado o processo de migração dos dados, pois na maioria dos casos existe a necessidade de migrar para o novo sistema as informações gerenciadas pelo sistema a ser desativado ou gerenciar por um determinado período a consulta dos dados antigos.

As interfaces com o ERP também devem estar devidamente identificadas e ser consideradas na estratégia de validação.

17.1.2 Sistemas do Tipo CRM

Os sistemas do tipo CRM (*Customer Relationship Management*) gerenciam todo o processo de relacionamento com clientes que inclui SAC (serviços de atendimento ao cliente) e atividades de farmacovigilância.

Quando se trata da validação de um CRM é recomendável seguir todo o ciclo de vida para sistemas. Nestes casos é fundamental na estratégia de validação contemplar os processos relevantes às BPx.

17.1.3 Sistemas de Pesquisa Clínica

Sistema de Pesquisa Clínica pode estar inserido no PLM (Product Lifecycle Management). Sistemas do tipo PLM são aqueles que tratam do processo de desenvolvimento e estudos clínicos.

17.1.4 Sistemas do Tipo WMS

Os sistemas WMS (Warehouse Management System) utilizam normalmente tecnologias de código de barras, robotização, dispositivos móveis, redes locais sem fio, etc., para monitorar eficientemente o fluxo de materiais, endereçamento e inventário.

Quando se trata da validação deste tipo de sistema deve-se considerar todo o fluxo de materiais e produtos, inventário de estoques, gerenciamento e controle das movimentações, rastreabilidade e interfaces com o sistema.

17.1.5 Sistemas do tipo GED

Sistemas do tipo GED (Gerenciamento Eletrônico de Documentos) são sistemas computadorizados para o gerenciamento eletrônico de documentos que visam assegurar a integridade e controle das informações documentadas relacionadas a diversos processos críticos da empresa. Em alguns casos, esses sistemas também gerenciam o treinamento relativo aos documentos controlados por ele.

17.1.6 Sistemas Globais

São sistemas corporativos acessados remotamente por unidades locais visando assegurar a total integridade e globalização das informações da empresa.

Para estes tipos de sistemas é recomendável verificar os requisitos e riscos globais e locais contemplados no sistema, elaborando uma documentação local que identifique de forma geral os riscos envolvidos nos principais processos relacionados ao sistema.

Para sistemas globais já validados na matriz da empresa, é necessário identificar os eventuais desenvolvimentos ou adaptações locais executando a comprovação das verificações complementares à validação da matriz, bem como comprovar a segurança decorrente do acesso remoto.

18. Particularidades de validação para sistemas de controle e execução

18.1 Sistemas do tipo MES

Sistemas do tipo MES (*Manufacturing Execution System*) são aqueles que integram desde a automação no chão-de-fábrica até o gerenciamento de informação, potencializando as informações de controle de processo, para análise e interação, entre as diversas áreas da indústria.

Quando se trata da validação de um sistema deste tipo é recomendável considerar durante a estratégia de validação todos os controles, instrumentos e equipamentos que interagem com o mesmo, verificando os possíveis impactos nos processos produtivos e na qualidade final do produto.

Geralmente o MES é um sistema com menos funcionalidades que o ERP, porém de alta complexidade levando-se em consideração as interfaces com equipamentos e outros sistemas envolvidos na manufatura, entre eles, o próprio ERP, LIMS (Laboratory Information Management System), GED (Gerenciamento Eletrônico de Documentos) ou EDMS (Electronic Documents Management System), supervisórios, etc.

São funcionalidades clássicas dos sistemas tipo MES: sistemas de controle e gerenciamento de etapas de fabricação (pesagem, produção e embalagem); rastreabilidade de processo produtivo; documentação eletrônica de lote, controle e execução de receitas de fabricação eletrônica.

18.2 Sistemas do tipo LIMS

Sistemas do tipo LIMS (Laboratory Information Management System) são sistemas de laboratório de controle da qualidade responsáveis pela coleta e gerenciamento do fluxo dos dados analíticos, aprovação das análises, rastreabilidade de amostras e reagentes, registros de manutenção, etc.

Podem possuir interfaces com sistemas de dados cromatográficos, instrumentos analíticos, relatórios, outros sistemas, etc.

É importante ressaltar que fórmulas e decisões algorítmicas do sistema LIMS devem ser documentadas e verificadas durante a validação.

18.3 Gerenciamento de Dados

Devido à natureza critica dos dados arquivados no LIMS, deve-se assegurar a integridade destes. Os pontos críticos incluem, mas não se limitam a:

- produto/lote;
- código do produto;
- estabilidade;
- resultado analítico;
- especificação do material;
- número da amostra;
- data da amostra;
- horário da amostragem;
- status da amostra;
- metodologia de teste;
- data de reteste/validade.

19. Sistemas de chão de fábrica

19.1 Introdução

Sistemas de chão de fábrica são soluções de automação que utilizam informações oriundas da instrumentação da planta. São processadas por programas e dispositivos lógicos que usam algoritmos, seqüenciamentos, intertravamentos e acionam equipamentos utilizando-se de bombas, válvulas, etc. visando ao controle de processo e/ou seu gerenciamento.

19.2 Tipos de Sistemas de Controle de Processos

Os sistemas de controle de processos podem ser divididos em dois: sistemas embarcados *(embedded)* e sistemas individuais *(stand alone)*.

Sistemas embarcados são sistemas baseados em microprocessadores como Circuito Integrado Programado, Controlador Lógico Programável (CLP) ou computador pessoal, com o propósito de controle e monitoramento de uma parte de manufatura e é usualmente fornecido como parte integrada de um equipamento. Exemplos deste tipo de equipamento incluem máquinas de envase, de embalagem, etc.

Normalmente, os sistemas de chão de fábrica são compostos pelos sistemas embarcados nos equipamentos, somados aos sistemas individuais que são instalados de maneira independente pelo usuário ou podem estar integrados por um sistema em camada maior.

Exemplos de equipamentos com sistemas embarcados:

- autoclaves;
- drageadoras;
- liofilizadores;
- encartuchadoras.

Exemplos de sistemas individuais:

- anel de distribuição de água purificada;
- anel de distribuição de água para injetáveis;
- sistema de tratamento de ar;
- monitoramento ambiental.

A estrutura das atividades do ciclo de vida e documentação são as mesmas já descritas neste guia. Alguns detalhes específicos para os sistemas de automação serão descritos a seguir.

19.3 Detalhamento da documentação de Projeto

O projeto detalhado inclui a produção da especificação de *hardware*, *software* e instrumentação. Para sistemas embarcados isto pode incluir a preparação de desenhos contendo o detalhamento geral elétrico e mecânico.

19.4 Testes de Aceitação

Estes testes são efetuados para provar a correta operação do *software*, *hardware* e instrumentação como definido pelos requerimentos do usuário. Estes testes devem ser baseados em uma especificação de teste de aceitação do sistema revisado e aprovado.

Os testes nas dependências do fornecedor que são efetuados antes da entrega para o usuário são denominados “Teste de Aceitação de Fabrica”(*Factory Aceptance Test* – FAT), estes testes são efetuados para que se possam identificar problemas antes de se entregar o projeto ao usuário. Para sistemas independentes, devem ser realizados testes no fornecedor simulando situações reais.

O Teste de Aceitação Local (Site Acceptance Test – SAT) é executado para determinar que o sistema e quaisquer equipamentos associados não tenham sido danificados e as funções estejam corretas em seu ambiente de operação. O SAT normalmente constitui a repetição do FAT no ambiente de operação compreendendo os testes críticos envolvendo o processo, instrumentação de campo, interfaces e conexões estabelecidas.

As etapas de FAT e SAT não substituem as etapas de qualificação.

19.5 Inspeção dos instrumentos e calibração

A calibração dos sensores e instrumentos de controle e monitoramento deve seguir procedimentos, utilizando padrões de calibração que sejam rastreáveis. Os registros das calibrações devem detalhar os resultados dos ensaios e registrar os padrões de teste utilizados.

19.6 Componentes da arquitetura de automação

Neste tipo de arquitetura, é importante ressaltar que todos os componentes que são fontes de interface com a operação, IHM, supervisório e outros devem atender requisitos de segurança descritos neste guia, relativos à assinatura eletrônica, registro eletrônico e controle de acesso. Todos os componentes da arquitetura devem estar contemplados na validação, mesmo que fisicamente não estejam conectados.

20. Descontinuidade

20.1 Introdução

A descontinuidade do sistema abrange a retirada, descomissionamento do sistema, disposição e migração dos dados necessários.

A migração dos dados pode ser necessária quando um sistema existente é substituído por um novo sistema, quando um sistema operacional passa por uma mudança significativa ou quando o escopo de uso do sistema sofre uma modificação significativa. O processo de migração deve ser exato e completo. Deve haver verificação do processo de migração.

Devem ser estabelecidos procedimentos que contenham, mas não lse limitem a:

- retirada, descomissionamento e disposição do sistema;
- tratamento de registros com impacto em BPx (registros que devem ser mantidos, período de retenção e quais registros podem ser destruídos);
- avaliação da necessidade de migração dos registros para um novo sistema;
- avaliação da necessidade de arquivamento e método de consulta dos dados históricos.

20.2 Plano de Descontinuidade

O plano de descontinuidade deve conter:

- procedimentos para retenção de registros e requisitos de destruição para dados históricos ou registros;
- descrição do software e hardware atuais, incluindo interfaces, equipamentos, instrumentos, etc.

A estrutura do documento deve conter, no mínimo:

- introdução;
- Responsabilidades;
- Estratégia para descontinuidade do sistema;
- Avaliação do impacto da retirada;

21. Tratamento de Registros Eletrônicos, assinaturas eletrônicas e Controle de Acesso

21.1 Controle de Acesso

O controle de acesso é uma das partes mais importantes do processo de validação de sistemas computadorizados.

Deve ser entendido que nenhum sistema estará devidamente habilitado se o controle de acesso for feito de forma inadequada.

Todos os sistemas com impacto em BPx devem ter um rigoroso controle de acesso que deverá contar no mínimo com os requisitos abaixo:

- procedimento operacional padrão que defina a forma de concessão de acessos;
- fluxo de aprovação envolvendo tanto as áreas solicitantes dos acessos, quanto as áreas envolvidas ou afetadas pela utilização das funcionalidades atribuídas aos solicitantes, com avaliação sob a ótica das BPx;
- auditoria periódica para avaliação do cumprimento do procedimento operacional padrão de concessão de acessos;
- arquivamento de comprovação das requisições e aprovações do controle de acessos através de registros manuais ou sistemas eletrônicos capazes de recuperar as informações em casos de dúvidas;
- acessos individualizados por nome, de forma a se identificar inequivocamente o usuário que executou uma determinada ação no sistema;
- os privilégios de acesso devem ser documentados e parametrizados de acordo com as competências técnicas/atribuições dos usuários do sistema.

Durante o processo de validação do sistema, deverão ser desenvolvidos testes e desafios comprovando que as transações críticas em termos de BPx estejam exclusivamente associadas a usuários aptos e responsáveis por elas.

21.2 Assinaturas Eletrônicas

A assinatura eletrônica é uma forma de assinatura que substitui a manuscrita, desde que tenha a sua veracidade e validação devidamente executada, assegurando inequivocamente que seja inviolável, intransferível e adequadamente segura. Em nenhuma hipótese deve ser permitida a utilização de nomes de usuários e senhas coletivas, pois implicam em perda total da rastreabilidade.

Todo o processo de utilização de assinaturas eletrônicas deverá ser descrito em procedimento operacional padrão, independentemente do seu tipo.

Exemplos de assinatura eletrônica:

- registro do nome do usuário (por digitação, cartões de identificação, chip eletrônico, etc.) e a respectiva senha individual e secreta;
- leitura biométrica (digital, íris, timbre de voz, palma das mãos, etc.).

Recomenda-se que as senhas individuais e secretas utilizadas em conjunto com o nome do usuário sejam compostas por letras, números e caracteres especiais, devendo ser renovadas periodicamente.

Senhas expiradas deverão impedir o acesso dos usuários, obrigando-os a substituí-las antes do acesso ao sistema.

Após um determinado número de tentativas frustradas de acesso, o sistema deve bloquear o acesso do usuário e registrar estas tentativas.

As senhas devem ser armazenadas no banco de dados de forma encriptada. Adicionalmente, no momento de sua digitação pelo usuário, a senha não deve ser legível, podendo ser representada visualmente por asteriscos, por exemplo.

O sistema computadorizado deverá exigir a assinatura eletrônica para toda e qualquer funcionalidade crítica de BPx, de forma a garantir que o registro tenha sido autenticado no momento da conclusão pela pessoa autorizada, evitando-se, por exemplo, que o usuário tenha deixado seu posto de trabalho com o sistema aberto, e outro venha a executar e registrar uma operação em seu nome. Outra forma de se evitar o uso indevido de senhas é incluir no sistema computadorizado a função de desconexão automática do usuário após determinado tempo de inatividade.

Ao cadastrar um novo usuário no sistema, o Administrador deverá atribuir-lhe uma senha provisória de forma que este usuário seja obrigado a substituí-la no primeiro acesso.

21.3 Registros Eletrônicos com impacto em BPx

O Registro eletrônico é a forma que permite a substituição dos registros impressos por registros eletrônicos, desde que validado.

Todo o processo de utilização de registros eletrônicos deverá ser descrito em procedimento operacional padrão.

O registro eletrônico deverá atender aos seguintes preceitos:

- possibilidade de recuperação das informações registradas;
- garantia de recuperação de informações registradas ao menos pelo período de retenção, mesmo após a descontinuidade do sistema;
- segurança e inviolabilidade dos dados contidos nos bancos de dados do sistema, que não deverá ser acessível para modificações, mesmo que a impressão dos dados seja aplicável;
- criação de trilha de auditoria.

Trilha de auditoria é a capacidade do sistema de detectar e registrar qualquer alteração nos dados, especificando seu conteúdo, incluindo data, hora, usuário, campo alterado, parâmetro original, parâmetro novo e identificação do ponto de acesso do qual foi realizada a modificação.

21.4 Customização do sistema

A customização deverá levar em consideração os riscos específicos de privilégio de acesso, assinaturas e registros eletrônicos identificados na análise de riscos, pois dependendo de como a customização for realizada, perde-se a aderência às políticas de segurança tratadas neste capítulo.

22. Glossário / Siglário

As definições mencionadas abaixo têm aplicação exclusiva neste guia, independente de aparecerem em outros documentos.

Sigla	Descrição
Aplicativo	Sistema informatizado.
Backup	Cópia de uma base de dados ou do software efetuado em uma mídia externa capaz de garantir a restauração posterior quando necessário.
BMS	*Building Management System:* Sistema de controle que inclui monitoramento centralizado de equipamentos relacionado à parte predial e utilidades, como ar condicionado, ventilação, monitoramento ambiental de salas limpas, controle de acesso, combate à incêndio, estação de tratamento de efluentes, água purificada, água para injetáveis, vapor puro, etc.
BPx	Sigla de Boas Práticas, onde 'x' entende-se por Fabricação, Laboratório, Distribuição, etc.
Ciclo de Vida	Período compreendido entre a concepção do sistema e sua descontinuidade.
CLP	Controlador Lógico Programável.
Código-Fonte	Código do sistema em linguagem de programação utilizada para o desenvolvimento de aplicativos.
CPU	Unidade Central de Processamento.
CRM	*Customer Relationship Management*
DCS	*Distributed Control System* = Sistema de Controle Distribuído.
Descomissionamento	Corresponde às atividades para controlar a retirada do sistema.
Desenho	Modelagem e arquitetura do sistema.
Desvios	Qualquer evento não planejado, que ocorra em sistemas computadorizados, podendo colocar em risco a qualidade e/ou a segurança de um produto ou dado.
Disposição	Dados, documentação, software e hardware podem ser destruídos em diferentes períodos. Os dados e documentação não podem ser descartados até que atinjam o período de retenção do registro conforme especificado nas BPx aplicável.
EDMS	*Electronic Documents Management System*
ERP	*Enterprise Resource Planning*
ERU	Especificação de Requisitos do Usuário
Eventos adversos	Qualquer ocorrência médica não desejável, que pode estar presente durante um tratamento com um produto farmacêutico, sem necessariamente possuir uma relação causal com o tratamento. Todo evento adverso pode ser considerado como uma suspeita de reação adversa a um medicamento.
FAT	*Factory Aceptance Test*
Firmware	Sistema operacional interno de um equipamento.
Fornecedor	Responsável pelo desenvolvimento do sistema computadorizado e/ou validação podendo ser uma empresa terceirizada ou departamento interno da própria empresa.
GED	Gerenciamento Eletrônico de Documentos

HPLC	*High Performance Liquid Chromatography*
HVAC	*Heating, Ventilation and Air Conditioning* = o termo é relacionado a sistemas que utilizam as técnicas de "calefação, ventilação e ar condicionado".
IHM	Interface homem-máquina, equipamento que contém display utilizado pelo operador do sistema.
Interface	Inter relacionamento entre sistemas que permita enviar ou receber dados entre eles de forma eletrônica, automática ou acionada manualmente
LIMS	*Laboratory Information Management System*
MES	*Manufacturing Execution System*
Negócio	Objeto a ser estudado na validação, compreende gerenciamento de dados e materiais, atividades analíticas, processo produtivo, etc.
PLC	*Programmable Logic Controller* = Controlador Lógico Programável
PLM	*Product Lifecycle Management*
Projeto	Fase do ciclo de vida que define, valida e implementa o sistema.
QD	Qualificação de Desempenho.
QI	Qualificação de Instalação.
QO	Qualificação de Operação.
Rede Local	Rede de comunicação lógica restrita a uma área limitada, normalmente dentro da empresa.
Rede Remota	Rede de comunicação que interliga áreas geograficamente separadas.
Retirada	Corresponde à remoção das operações ativas do sistema (desativação de usuários, desabilitação de interfaces, etc.).
SAC	Serviço de Atendimento ao Cliente
SAT	Site Acceptance Test
SCADA	*Supervisory Control And Data Acquisition* = Sistema de Supervisão e Aquisição de Dados.
SCM	*Supply Chain Management* = sistema de planejamento e controle das operações da cadeia de suprimento.
SIGE	Sistema Integrado de Gestão Empresarial
Sistema Computadorizado	Consiste de hardware, software e componentes de rede de comunicação, junto com as funções controladas e documentação associada.
Sistema customizado	Sistemas ou subsistemas desenvolvidos para atender necessidades específicas da empresa.
Sistema embarcado	Sistema computadorizado de um equipamento.
Sistema legado	Sistema que se encontra em operação antes do início das atividades de validação.
Software Padrão	Sistema com arquitetura e funcionalidades pré-desenvolvidas pelo fornecedor para atender determinado processo ou aplicação de forma padrão, também conhecido popularmente como software de prateleira.
Supervisório	Software utilizado basicamente para a supervisão de processos industriais. Para tanto, são instalados em computadores conectados a uma rede de comunicação de um ou mais CLP's (controlador lógico programável) ligados a um equipamento, uma máquina ou até mesmo a um processo completo de fabricação.
TI	Tecnologia da Informação.

Trilha de auditoria (*Audit Trail*)	Capacidade do sistema em detectar e registrar qualquer alteração nos dados, especificando seu conteúdo, incluindo data, hora, usuário, campo alterado, parâmetro original, parâmetro novo e identificação do ponto de acesso do qual foi realizada a modificação.
Utilidades	Recursos utilizados direta ou indiretamente na produção que poderão ou não fazer parte dos produtos, como por exemplo, energia elétrica, água, vapor, ar comprimido, etc.
Validação/qualificação concorrente	Processo de validação executado em sistemas legados.
Validação/qualificação prospectiva de sistemas	Processo de validação executado em sistemas durante a implementação do sistema.
WMS	*Warehouse Management System*

23. Referências Bibliográficas

23.1 Guias

- ISPE GAMP5 A Risk-Based Approach to Compliant GxP Computarized Systems;
- PIC/S Guidance on Good Practices for Computarized Systems in Regulated "GxP" Environments (PI 011-3) September 2007;
- Good Manufacturing Practice Guide for Active Pharmaceutical Ingredients – Q7, International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH);
- Quality Risk Management – Q9, International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH);
- FDA Guidance for Industry Part11, Electronic Records; Electronic Signatures – Scope and Application (August 2003);

23.2 Norma

- ANSI/ISA-95.00.01-2000, Enterprise-Control System Integration Part 1: Models and Terminology;

23.3 Regulamento

- FDA 21 CFR Part11 – Electronic Records, Electronic Signatures.