FACULDADE DE COMPUTAÇÃO DE MONTES CLAROS
CURSO DE SISTEMAS DE INFORMAÇÃO

Helberth Oliveira Silva

REGISTROS E ASSINATURAS ELETRÔNICAS NOS SISTEMAS COMPUTADORIZADOS VALIDADOS DAS INDÚSTRIAS FARMACÊUTICAS

Montes Claros/MG
2009

Livros Grátis

http://www.livrosgratis.com.br

Milhares de livros grátis para download.

HELBERTH OLIVEIRA SILVA

REGISTROS E ASSINATURAS ELETRÔNICAS NOS SISTEMAS COMPUTADORIZADOS VALIDADOS DAS INDÚSTRIAS FARMACÊUTICAS.

Trabalho Conclusão de Curso, apresentado como requisito parcial para obtenção do Diploma de Bacharel em Sistemas de Informação da Faculdade de Computação de Montes Claros.

Orientador do projeto: Professor(a): Douglas Andrey De Oliveira Araújo. Graduação em Administração de Empresas – UNIMONTES, ano de 1996. Pós-Graduação em Tecnologias Da Computação – UFMG, ano de 2001. MBA em Gestão de Empresas, FGV, ano de 2005.

Montes Claros – MG
2009

HELBERTH OLIVEIRA SILVA

REGISTROS E ASSINATURAS ELETRÔNICAS NOS SISTEMAS COMPUTADORIZADOS VALIDADOS DAS INDÚSTRIAS FARMACÊUTICAS

Trabalho de Conclusão de Curso, apresentado como requisito parcial para obtenção do Diploma de Bacharel em Sistemas de Informação, da Faculdade de Computação de Montes Claros.

Aprovado em:

BANCA EXAMINADORA:

Ass._____

1º Exam.: Douglas Andrey De Oliveira Araújo – Graduação em Administração de Empresas – UNIMONTES - Pós-Graduação em Tecnologias Da Computação - UFMG

Ass._____

2º Exam.: Bruno Rodrigues Lima – Engenheiro Mecânico – CEFET-MG

Graduação em licenciatura CEFET-MG

Pós-Graduação em Manutenção – CEFET-MG

Ass._____

3º Exam.: Jose Expedito de Freitas **–** Mestrado em Informática (Conceito CAPES 7) **-** Pontifícia Universidade Católica do Rio de Janeiro, PUC/RJ, Brasil

Montes Claros /MG
2009

DEDICATÓRIA

À minha esposa Rosemary Soares de Barros, por toda a força e incentivo que contribuiu para o meu sucesso.

Ao meu pai Francisco de Assis Oliveira Silva que sempre esteve presente cobrando meu empenho nos momentos de desânimo.

À minha mãe Anália leal oliveira que muito contribuiu para que esta etapa fosse vencida.

Ao meu avô (in memorian) Gerônimo Inácio da Silva que sempre guardo em meus pensamentos a sua capacidade de perseverança e insistência para vencer desafios.

AGRADECIMENTOS

Primeiramente a Deus, pois sem ele nada teria conseguido em minha vida, à Facomp onde encontrei um ambiente acolhedor e com ótima infra-estrutura. Minha família, por todo incentivo e apoio nas horas mais difíceis.

Agradeço também a todos que direta ou indiretamente contribuíram para realização deste trabalho, a todos os meus professores, ao orientador Douglas Andrey De Oliveira Araújo, colegas e demais funcionários desta instituição.

“Para conhecermos os amigos é necessário passar pelo sucesso e pela desgraça. No sucesso, verificamos a quantidade e, na desgraça, a qualidade”.

Confúcio, filósofo chinês (551 a.C. - 479 a.C.).

RESUMO

Este estudo tem como objetivo apresentar as assinaturas e registros eletrônicos em função da validação de sistemas computadorizados e suas etapas que dependem das normas FDA 21 CFR Part. 11, do guia GAMP5 e no Brasil, as recomendações da ANVISA, descrevendo os conceitos e modelos utilizados nas indústrias farmacêuticas e sua metodologia, classificação, rastreabilidade dos dados e modelos de segurança, como forma de não apenas oferecer qualidade aos produtos finais, mas também a garantia de produtos contínuos.

A área de TI suporta ativamente todas as etapas desde a chegada da matéria-prima até o produto final, e está embarcada nas diversas áreas e equipamentos que compõe o processo produtivo.

Palavras-chave: sistemas computadorizados, validação, registros, segurança.

ABSTRACT

This study aims to present the signatures and electronic records according to the validation of computer systems and their stages which depend on the FDA 21 CFR Part. 11, the guide GAMP5 and Brazil, the recommendations of ANVISA, describing the concepts and models used in the pharmaceutical and its methodology, classification, data traceability and security models as a way to not only provide quality final products, but also ensuring solid products.

The IT department actively supports all the steps from the arrival of raw material to finished product, and is embedded in different areas and equipment that make up the production process.

Keywords: computer systems, validation, records, security.

SUMÁRIO

INTRODUÇÃO **11**

CAPITULO I – ASSINATURAS **13**

1.0 Assinaturas eletrônicas 13
1.0.1 Identidade de um usuário de uma assinatura eletrônica 13
1.0.2 Validade da assinatura eletrônica 14
1.1.0 Logs de tempo para uma assinatura eletrônica 14
1.1.1 Sessões 14
1.2.0 Assinaturas manuais 15

CAPITULO II - REGISTROS **16**

2.0 Registros eletrônicos 16
2.0.1 Ciclo de vida do registro eletrônico 16
2.0.2 Cópias de registros eletrônicos 16
2.0.3 Substituição/Fechamento dos sistemas 17
2.0.4 controle para sistemas fechados 17
2.0.5 Controle para sistemas abertos 18
2.0.6 Registros de dados 18
2.0.7 Reconhecimento 19

CAPITULO III – NORMAS **20**

3.0 A Norma 21 CFR PART 11 20
3.0.1 Abrangência 20
3.0.2 Impacto legal do uso de assinaturas eletrônicas 21
3.0.3 Segurança dos sistemas 21
3.0.4 Emprego e adequação da norma 21CFR PART11 no Brasil 21
3.0.5 Anvisa 21
3.0.6 Rastreabilidade dos dados e registros eletrônicos (AUDIT TRAIL) 22
3.0.7 Requerimentos de regras de predicados para Audit Trail 23
3.0.8 Requerimentos GXP 23
3.0.9 GAMP5®(Boas Práticas Fabricação Automatizadas) na indústria farmacêutica 24

CAPITULO IV – PRÉ-REQUISITOS PARA VALIDAÇÃO DE SISTEMAS COMPUTADORIZADOS **26**

4.0 Segurança nos sistemas computadorizados 26
4.0.1 Usuário final 26
4.0.2 Administrador do sistema 26
4.0.3 Administrador do banco de dados e Infra-estrutura tecnológica 26
4.1 Qualificação e auditoria de fornecedores 27
4.1.1 Pré-seleção de fornecedores 27
4.1.2 Auditoria de pré-contrato 27
4.1. 3 Auditoria de acompanhamento 28
4.1. 4 Auditoria periódica 28
4.2 Especificação de projeto 28
4.2.1 Especificação do sistema 28
4.2.2 Especificação de software 28
4.2.3 Especificação de hardware 29
4.2.4 Co-construção 29
4.3 Desenvolvimento e construção do sistema 29
4.3.1 Testes de desenvolvimento 30
4.3.2 Implementação e início de operação 31
4.4.0 Qualificação da infra-estrutura 31

CAPITULO V - VALIDAÇÃO DE SISTEMAS COMPUTADORIZADOS 33

5.0 DOCUMENTAÇÃO DE VALIDAÇÃO DOS SISTEMAS COMPUTADORIZADOS 33
5.0.1 CLASSIFICAÇÃO DOS SISTEMAS COMPUTADORIZADOS 34
5.0.2 SISTEMAS DE INFORMAÇÃO 34
5.0.3 SISTEMAS DE AUTOMAÇÃO 35
5.0.4 COMITÊ DE VALIDAÇÃO 35
5.0.5 EQUIPE DE VALIDAÇÃO 35
5.0.6 PROPRIETÁRIO DO SISTEMA 36
5.0.7 REQUISITOS E ESPECIFICAÇÕES DO USUÁRIO (USER REQUIREMENTS SPECIFICATION) 36
5.0.8 ESPECIFICAÇÃO FUNCIONAL 37
5.0.9 PLANO MESTRE DE VALIDAÇÃO 39
5.1 TIPOS DE VALIDAÇÃO 39
5.1.1 VALIDAÇÃO PROSPECTIVA 39
5.1.2 VALIDAÇÃO RETROSPECTIVA 40
5.2 CICLO DE VIDA DE SISTEMAS COMPUTADORIZADOS 40
5.2.1 VALIDAÇÃO DO CICLO DE VIDA DE SISTEMAS COMPUTADORIZADOS 41
5.2.2 SISTEMAS EMBARCADOS E SISTEMAS AUTÔNOMOS 41
5.3.0CRITÉRIOS PARA INCLUSÃO E PRIORIZAÇÃO EM INVENTÁRIO DE SISTEMAS COMPUTADORIZADOS 41
5.4 QUALIFICAÇÃO DA INSTALAÇÃO (IQ) 42
5.4.2 QUALIFICAÇÃO DA OPERAÇÃO (OQ) 42
5.4.3 QUALIFICAÇÃO DO DESEMPENHO (PQ) 43
5.5.0 RELATÓRIO FINAL DE VALIDAÇÃO DE SISTEMAS COMPUTADORIZADOS 43
5.5.1 USO E MANUTENÇÃO DOS SISTEMAS COMPUTADORIZADOS VALIDADOS 44
5.5.2 GERENCIAMENTO DE PROBLEMAS 44
5.5.2.1 MANUTENÇÕES PREVENTIVAS 44
5.5.2.2 MANUTENÇÕES CORRETIVAS 45
5.5.2.4 CÓPIA DE SEGURANÇA E RESTAURAÇÃO 45
5.5.2.4 GERENCIAMENTO DE MUDANÇAS 45
5.5.3 PLANO DE MIGRAÇÃO DE DADOS E ENCERRAMENTO DO USO DO SISTEMA 46

6.0 CONCLUSÃO 47

7.0 ELEMENTOS PÓS-TEXTUAIS 50

7.1 GLOSSÁRIO 50
7.2 REFERÊNCIAS 52

INTRODUÇÃO

A intenção deste trabalho visa demonstrar que a integridade dos dados de registros e assinaturas eletrônicas é fator de importância, uma vez que devido aos controles rígidos, deve-se garantir que no processo automatizado e computadorizado não haja perda de dados durante e depois da execução dos processos.

Os Sistemas de controle de processos são todos aqueles que adquirem dados, processam e os utilizam para controlar máquinas e equipamentos do processo.

Um Sistema Computadorizado é a combinação de componentes de hardware e software que interagem para automatizar tarefas que são programadas ou configuradas especificamente para satisfazer exigências do usuário e envolve documentação (especificações, instruções, manuais e documentação de validação) e treinamento de pessoal.

Uma série de normas estabelecidas direciona a fabricação dos remédios para sua integridade e eficácia nos mais variados tipos de tratamento de saúde, dentre elas a 21CFR PART 11 do FDA que é a agência norte americana que estabelece os controles para alimentos e medicamentos, sendo adaptada a cada país através de suas agências reguladoras como no Brasil, a ANVISA.

Para estabelecer um padrão de qualidade na produção das medicações, a validação na indústria farmacêutica é um mecanismo que assegura que um sistema de fabricação esteja capaz de fornecer de uma forma constante e consistente artigos medicamentosos, atendendo às especificações farmacêuticas.

A validação, ou qualificação, de um determinado sistema farmacêutico requer evidências documentadas de que todas as seqüências de processos, equipamentos, componentes e dispositivos de controle que possam influenciar na qualidade, potência, integridade e eficácia do produto estejam validados / qualificados, de modo a assegurar que o produto seja fabricado de acordo com especificações pré-definidas, com alto grau de confiança e de maneira reprodutível.

Devido ao uso de normas nacionais e internacionais e a concorrência no setor farmacêutico juntamente com sua expansão faz com que as indústrias busquem constantes melhorias em processos e produtos, para garantir qualidade e segurança para o usuário do medicamento.

A indústria farmacêutica deve atender aos regulamentos sanitários nacionais, porém, para exportação de produtos acabados, deve também conhecer e atender os requisitos estabelecidos por órgãos internacionais.

Um dos principais deveres das indústrias farmacêuticas é garantir a integridade das informações relacionadas a todo ciclo de vida de um medicamento, desde a fase de pesquisa, desenvolvimento, registro, produção, distribuição e eventuais devoluções, sendo conhecido como rastreabilidade, ou seja, o fato de realizar ações, investigações e tomar decisões com base nas informações obtidas por um equipamento e / ou software validados.

Parte destas informações, relacionadas à rastreabilidade, encontram-se hoje baseadas em Sistemas Computadorizados, e estes devem oferecer a garantia de que seus dados continuarão íntegros e seguros, desta forma, surge a necessidade de validação destes sistemas afim de que esta segurança dos dados seja testada e comprovada de acordo com os requisitos legais e normas pertinentes.

CAPITULO I – ASSINATURAS

Assinaturas eletrônicas são compilações de dados computadorizados de quaisquer símbolos ou série de símbolos executados, adotados ou autorizados por um indivíduo para ser legalmente equivalente à assinatura do mesmo feito à mão.

1.0 Assinaturas eletrônicas

Assim, uma assinatura eletrônica é uma entrada feita por um usuário em um sistema computadorizado, que o identifica sem qualquer ambigüidade, e é utilizada legalmente e obrigatoriamente como a assinatura manual do mesmo indivíduo.

1.0.1 Identidade de um usuário de uma assinatura eletrônica

Somente um usuário por vez deverá possuir ***login*** único e senha única e este não deverá ceder seu acesso a outrem, caso isto aconteça, quaisquer alterações indevidas executadas por outra pessoa utilizando seus dados de acesso ficarão registradas e este poderá responder por eventuais alterações;

> Cada assinatura eletrônica deve ser única para um indivíduo e não deve ser reutilizada por ou reatribuída para qualquer outro.
> Pessoas que usam assinaturas eletrônicas devem, sob requisição da agência, prover certificação adicional ou testemunho que uma assinatura eletrônica específica é o equivalente legal de uma assinatura manuscrita do assinante.
> (FDA 21CFR PART 11, § 11.100)

Quando uma assinatura de dois componentes é utilizada, o código de identificação do usuário deve ser um código único, que o identifique sem equívocos.

O código de identificação do usuário pode ser composto de suas iniciais (como usado em algumas empresas para identificar os funcionários), nunca deve, obrigatoriamente, ser re-utilizado por outro usuário. O proprietário do sistema deve manter um registro do código de identificação do usuário, e o período pelo qual este teve acesso ao sistema computadorizado.

1.0.2 Validade da assinatura eletrônica

O sistema computadorizado deve ser capaz de determinar se qualquer assinatura eletrônica aplicada é válida para aquele sistema, e se o usuário da assinatura tem a autorização para usar uma assinatura eletrônica naquele ponto de aplicação específico no sistema.

Assinaturas inválidas e de uso não-autorizado devem ser rejeitadas pelo sistema computadorizado.

1.1.0 *Logs* de tempo para uma assinatura eletrônica

Quando uma assinatura eletrônica for utilizada, o sistema computadorizado deve registrar a hora, data e ações para cada uso de uma assinatura eletrônica.

> Para prevenir falsificação de registros, a data e o horário registrados em cada operação serão gerados pelo sistema computadorizado e não inseridos pelo usuário da assinatura eletrônica. (FDA 21 CFR PART 11, § 11.101).

Deve ser assegurado que a data e o horário sejam rastreados em tempo real para o assinante do sistema, os quais são acessáveis de lugares em diferentes fusos horários.

1.1.1 Sessões

Quando um usuário necessita aplicar assinaturas repetidas durante um processo contínuo simples, não é necessário entrar com todos os dados novamente.

Os dados devem ser inseridos na primeira ação de registro da assinatura eletrônica.

Em todos os registros subseqüentes durante o período contínuo de uso, apenas a parte confidencial (senha) da assinatura é necessária.

> Componentes e controle de assinatura eletrônica.
> (a) Assinaturas eletrônicas que não são baseadas em biometria devem: (1) Empregar pelo menos dois componentes de identificação distintos, como um código de identificação e senha.
> (i) Quando um indivíduo executa uma série de assinaturas durante um único período contínuo de acesso controlado ao sistema, a primeira assinatura deve ser executada usando todos os componentes eletrônicos; assinaturas subseqüentes devem ser executadas usando pelo menos um componente de assinatura eletrônica que só pode ser executado e que foi projetado para ser usado somente pelo

> indivíduo.
> (ii) Quando um indivíduo faz uma ou mais assinaturas não executadas durante um único período contínuo de acesso controlado aos sistemas, cada assinatura deve ser executada usando todos os componentes de assinatura eletrônica.
> (FDA 21 CFR PART 11, § 11.200).

Como a norma estabelece, se um usuário acessou um sistema para executar qualquer ação, além de ser gerado um ***log*** com seus dados de acesso, é conveniente que seja criada uma sessão pelas telas onde este estiver obtendo acesso às informações, salvo em situações que podem causar alterações no processo o acesso deste usuário deve ser solicitado novamente para confirmar a ação.

1.2.0 Assinaturas manuais

Onde uma assinatura é requerida, mas se a funcionalidade assinatura eletrônica não estiver implementada, assinaturas manuais em cópias em papel do registro eletrônico são aceitas desde que um link seguro entre a assinatura manual e a assinatura eletrônica possa ser estabelecida e mantida.

Este link deve ter um mínimo de segurança como a identidade do sistema computadorizado utilizado, o registro eletrônico, a data de impressão e qualquer outra informação necessária para identificar a assinatura eletrônica assinada.

Antes de aplicar uma assinatura manual, o assinante deve, obrigatoriamente, assegurar que a impressão é uma representação completa e fiel da assinatura eletrônica relevante armazenada no sistema.

> Uma assinatura manual, que é capturada eletronicamente por escâner ou algum outro método eletrônico sem qualquer verificação do sistema computadorizado, não é considerada uma assinatura eletrônica. (FDA 21 CFR PART 11, § 11.112).

CAPITULO II - REGISTROS

Os registros podem ser definidos como qualquer combinação de textos, gráficos, dados, áudio, desenhos ou outro tipo de informação em forma digital, criados, modificados, mantidos, arquivados, recuperados ou distribuídos por um sistema computacional são considerados registros eletrônicos,

2.0 Registros eletrônicos

Um registro eletrônico é criado quando dados são salvos em um meio de gravação durável (ex. disco ou fita).

Instrumentos ou equipamentos de laboratórios que armazenam dados em memória volátil (ex. EPROM ou RAM) e depois realizam cálculos nestes dados para produzir um resultado na tela ou em cópia impressa, não criam uma assinatura eletrônica.

Um registro eletrônico pode conter dados que sejam gravados automaticamente, como o resultado de um cálculo, gravados por um operador ou qualquer combinação desses.

2.0.1 Ciclo de vida do registro eletrônico

Todo registro eletrônico no sistema computadorizado deve ser mantido através do período de retenção em formato aplicável para utilizações futuras. As abordagens para isto, incluindo requisitos específicos para a manutenção do registro eletrônico, como a norma FDA 21 CFR PART 11 assim descreve.

O período de retenção pode ser dividido em fases específicas que juntas constituem o ciclo de vida do registro eletrônico. O objetivo primário de descrever o ciclo de vida do registro eletrônico é assegurar que o conteúdo e o significado do mesmo estejam preservados através do período de retenção.

2.0.2 Cópias de registros eletrônicos

Procedimentos devem estar em condições que assegurem a classificação dos registros eletrônicos e que cópias dos mesmos possam ser geradas, preservando o seu conteúdo e significado de uma forma adequada para inspeção, revisão e cópia, através do período requerido de retenção.

Quando o sistema computadorizado possuir a habilidade para procurar, classificar ou gerar gráficos com os registros eletrônicos, as cópias destes devem prover da mesma capacidade, se razoável e tecnicamente possível.

Isto deve ser assegurado por atribuições validadas no sistema computadorizado.

Cópias dos registros eletrônicos devem ser geradas em formatos eletrônicos comuns e portáteis ex, em PDF, XML, SGML, ASCII ou outro quando tecnicamente possível.

Quando for copiado de um sistema/plataforma/formato/meio para outro, o processo de transferência deve incluir um mecanismo de verificação que assegure a preservação da autenticidade, integridade, confidencialidade, não-repúdio e outros atributos do registro como aplicáveis.

2.0.3 Substituição/Fechamento dos sistemas

Acrescentando-se aos requisitos gerais de retenção para registro eletrônico considerações específicas devem estar endereçadas quando substituição ou encerramento dos sistemas.

Neste instante deve, obrigatoriamente, ser decidido como o conteúdo e significado do registro eletrônico no sistema devem ser assegurados através do período de retenção do registro. O registro eletrônico pode ser transferido para o sistema novo desde que o processo de transferência seja validado. Quando tal processo de transferência é realizado, o formato e layout do registro eletrônico no novo sistema não necessitam ser mantido. Onde aplicável a reprocessabilidade deve ser assegurada.

Onde o registro eletrônico não é migrado para um novo sistema computadorizado, mas permanece no sistema computadorizado gerador, o proprietário do sistema deve, obrigatoriamente, assegurar continua legibilidade do registro eletrônico através do período de retenção do registro eletrônico. Isto inclui preservação da documentação do sistema e procedimentos/ instruções relevantes requeridos para o uso do sistema computadorizado e manter usuários treinados no sistema.

2.0.4 controle para sistemas fechados

Um sistema deve considerado fechado quando um indivíduo possui acesso para modificar seus dados, conforme descrito na norma 21CFR PART 11da FDA:

> § 11.10 Controle para sistemas fechados.
> Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade de registros eletrônicos, e para assegurar que o assinante não pode prontamente rejeitar o registro assinado como não genuíno.

Isto significa que os sistemas devem ser controlados por acesso somente a pessoas responsáveis pelo conteúdo dos mesmos. Recomenda-se a utilização de licenças únicas para o software e utilizando-se também a segurança do Windows NT/XP/2XXX para controlar o acesso estes arquivos. Também é a definição para os registros eletrônicos, pelos quais devem ser armazenados os nomes de usuários, e todas as seqüências de operações ou alterações realizadas por estes, de modo que se mantenha um rastreamento de todas as operações realizadas por estes usuários registrados no sistema.

Este rastreamento é feito através de "***logs***" de eventos criados automaticamente a cada operação executada dentro do sistema.

2.0.5 Controle para sistemas abertos

Fica a critério de o utilizador implementar seus procedimentos de segurança quanto a estes registros, portanto devem ser seguros e possibilitar registros confiáveis, como por exemplo, gerar relatórios com dados precisos e livres de qualquer manipulação por parte dos usuários.

> Controle para sistemas abertos.
> Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos, deverão empregar procedimentos e controles projetados para garantir a autenticidade, integridade e quando apropriado, a confidencialidade de registros eletrônicos, desde sua criação até seu recebimento. (FDA 21CFR PART 11, § 11.30)
> Estes procedimentos e controles deverão incluir medidas adicionais como encriptação de documentos e o uso de padrões de assinatura digital apropriados para garantir, quando necessário sob as circunstâncias, a autenticidade integridade e confidencialidade dos registros. (FDA 21CFR PART 11, § 11.30).

2.0.6 Registros de dados

Os registros devem ser armazenados em uma base de dados relacional segura, nunca se devendo incluir rotinas para exclusão ou destruição dentro do banco de dados, mas sim, somente a inclusão de novos dados. Devendo qualquer acesso ser gravado em um sistema de registros com o nome do utilizador, com data, dia e horário do acesso, e, além disso, haver

um registro de eventos automático. Recomenda-se também a utilização de backups periódicos. Quaisquer saídas de dados para consulta devem ser no formato PDF.

2.0.7 Reconhecimento

Ação de fornecer uma identidade na gravação de um registro ou aprovações que não requeiram uma assinatura. A ação de reconhecimento deve conter identificação do usuário e/ou senha. Onde a regra de predicado dita que um indivíduo desempenhando uma ação relacionada a um registro eletrônico deve, obrigatoriamente, ser identificado, mas, a regra de predicado não especifica esta identificação através do uso de uma assinatura. Um reconhecimento pode ser utilizado no lugar da assinatura.

Nos capítulos seguintes serão abordados todos os passos para validação dos sistemas computadorizados quanto ao uso das assinaturas e registros eletrônicos bem como o impacto legal sobre o processo de validação.

CAPITULO III – NORMAS

As normas abordadas neste trabalho são utilizadas como referência e como padrão para diversas empresas do ramo farmacêutico, sendo que além destas ainda existem diversas que regem cada etapa do processo, neste trabalho serão abordados, GAMP5, FDA 21 CFR PART 11 e ANVISA.

3.0 A Norma 21 CFR PART 11

Em 1991, membros da indústria farmacêutica americana realizaram um encontro com a FDA (Food and Drug Administration) para determinar como eles poderiam acomodar sistemas de registro eletrônico de documentos (sem o uso de papel) de acordo com as normas 210 e 211 da "Current Good Manufacturing Practice" (prática atual para a manufatura de bens).

A FDA criou uma Força-Tarefa para Assinatura/Identificação Eletrônica para desenvolver um conjunto de diretrizes uniforme para a agência aceitar registros e assinaturas eletrônicas em todas as áreas deste programa.

O resultado final providenciaria um critério segundo qual a FDA iria considerar registros eletrônicos equivalentes a registros em papel, e assinaturas eletrônicas equivalentes às assinaturas manuscritas tradicionais.

3.0.1 Abrangência

As empresas que atendem às normas da FDA adquirem segurança e controle dos registros eletrônicos, confirmados por assinaturas eletrônicas, permitindo impressão ou transferência eletrônica.

Nos laboratórios das indústrias, os softwares que controlam ou gerenciam equipamentos para análise devem possuir funcionalidade para atender às regulamentações sobre validação, cópias de registros disponíveis, acesso limitado ao sistema, seguimento de auditoria e controle de permissões e de documentos.

O primeiro aspecto a ser considerado quando se deseja avaliar se os sistemas devem atender à norma 21 CFR PART 11, ou seja, quais informações ou atividades serão por ele gerenciadas ou realizadas, desta forma, somente sistemas que envolvam operações e/ou informações críticas devem ser considerados.

3.0.2 Impacto legal do uso de assinaturas eletrônicas

Assinatura eletrônica é o equivalente legal à assinatura manual para todos os sistemas onde a função de assinaturas eletrônicas foi implementada. Isto significa que:

- Usuários devem ter conhecimento que o uso de assinaturas eletrônicas é um mandatório legal e eles devem ser treinados nesta conseqüência.
- Os usuários devem manter em confidencial a parte secreta de uma assinatura eletrônica e nunca dividir as suas assinaturas eletrônicas com outro usuário.

3.0.3 Segurança dos sistemas

A norma 21 CFR PART 11 exige a necessidade de se utilizar um sistema de controle com segurança tal que inclua ***login*** de usuário, ***logout*** automático por inatividade e outros procedimentos garantindo que os usuários que operam o sistema sejam realmente os responsáveis pelo seu uso e não um falso usuário.

A segurança nos sistemas computadorizados é de vital importância, pois ela assegura que um sistema seja protegido contra quaisquer tipos de violações que possam afetar a integridade dos registros armazenados ou do controle por este desempenhado sobre o processo produtivo.

3.0.4 Emprego e adequação da norma 21CFR PART11 no Brasil

Baseado na norma 21CFR PART 11 do FDA, o sistema deve primeiramente, estar validado para que atenda a todos os requisitos que lhes são exigidos. Esta validação visa garantir que além de seguros e confiáveis, o sistema esteja integro e com informações reais de tudo aquilo que ele processa ou armazena em tempo real.

3.0.5 Anvisa

No Brasil, o órgão que gerencia as atividades das indústrias do setor é a ANVISA, e em sua Resolução da Diretoria Colegiada (RDC) número 210, de 04 de agosto de 2003. Menciona em seu anexo 1 Item14.1.8 que:

> Os dados podem ser registrados através de sistema de processamento eletrônico ou por meios fotográficos ou outros meios confiáveis. As fórmulas mestras/fórmulas padrões e os Procedimentos Operacionais Padrão – POPs relativos ao sistema em uso devem estar disponíveis, assim como a exatidão dos dados registrados conferidos. Se o registro dos dados for feito através de processamento eletrônico, somente pessoas designadas podem modificar os dados contidos nos computadores. Deve haver registro das alterações realizadas. O acesso aos

> computadores deve ser restrito por senhas ou outros meios. A entrada de dados considerados críticos deve ser conferida por outra pessoa designada. Os registros eletrônicos dos dados dos lotes devem ser protegidos por transferência de cópias em fita magnética, microfilme, impressão em papel ou outros meios. É particularmente importante que, durante o período de retenção, os dados estejam prontamente disponíveis.

A ANVISA também menciona as formas de registrar os dados e como esses dados podem ser considerados válidos. Descreve também a maneira de restrição de acesso, somente por pessoas designadas e autorizadas a tal. Sendo que para o Brasil a única menção a registros eletrônicos e assinaturas é desta resolução da ANVISA, servindo apenas como uma recomendação para boas práticas de fabricação.

Mas, devido a exigências de diversos órgãos internacionais, inclusive se a empresa pretende expor seus produtos para o mercado europeu ou norte-americano, esta deve se adequar a seus órgãos pertinentes, por isso a adequação a norma FDA e outras européias.

3.0.6 Rastreabilidade dos dados e registros eletrônicos (AUDIT TRAIL)

Assegurar que o audit trail gerado pelo sistema computadorizado tenha um mínimo exigido como entradas do operador, ação criada, modificar ou apagar um registro eletrônico.

Para cada entrada ou ação do operador, o processo de audit trail deve conter:

- A data gerada pelo computador e o tempo impresso da entrada do operador ou ação;
- A identificação do operador;
- O tipo de ação onde aplicável (ex. um comando para abrir uma válvula);
- Se for requerido por regra de predicado, o audit trail também deve conter a razão para a alteração.

Se o conteúdo de um registro eletrônico for modificado ou apagado, então o conteúdo anterior do registro deverá ser mantido arquivado. Os registros apagados devem estar disponíveis para acesso, entretanto identificados como inválidos.

Não deverá, obrigatoriamente, ser possível por nenhum usuário modificar ou deletar o audit trail.

Deve estar obrigatoriamente, garantido que a data e hora do sistema estejam configuradas para uma referência escolhida e dentro de intervalos pré-definidos, prevenindo registros impressos fora de seqüência quando o tempo do sistema for reiniciado.

3.0.7 Requerimentos de regras de predicados para Audit Trail

A regra de predicado dita se uma assinatura é requerida ou não. Se uma regra de predicado requer que um dado registro seja assinado, então aquele registro se for eletrônico por natureza, deve, obrigatoriamente, ser eletronicamente assinado.

3.0.8 Requerimentos GXP

As atuais boas práticas de fabricação estabelecem normas que devem ser seguidas pelas empresas farmacêuticas para estarem em conformidade quanto aos requisitos de limpeza e documentação. As indústrias farmacêuticas devem estar em conformidade com as cGXPs estabelecidas pelos Órgãos regulatórios de cada país.

Um software terá relevância GXP se satisfazer uma das seguintes questões:

- O sistema controla ou monitora diretamente a qualidade do produto?
- O sistema afeta os registros de produção (ex. BOM, ***Batch Records***, Mestre de Itens, etc.)?
- O sistema produz um arquivo ou registro oficial?
- O sistema é parte integral de um equipamento usado na manufatura, embalagem, testes, armazém e/ou distribuição do produto?
- O sistema define os materiais a serem usados (ex. matéria-prima, material de embalagem, granéis, etc)?
- O sistema é usado para recall de produtos, rastreabilidade de estoque e histórico do produto?
- O sistema considera informações de estoque, status do local, localizações ou tempo de estocagem?
- Os dados do sistema são utilizados para suportar a liberação de produtos?
- O sistema interage com as reconciliações, uso parcial de componentes ou quebra de lotes?
- O sistema de alguma maneira impacta ou afeta a pureza do produto, tamanho, esterilidade, identidade, status qualidade ou localização?

Conforme a legislação ANVISA Resolução RDC nº 210, de 04 de agosto de 2003 aborda com relação às boas práticas de fabricação e sobre validações que abrangem também os sistemas computadorizados como partes integrantes do processo fabril.

> 2.1 Boas Práticas de Fabricação é a parte da Garantia da Qualidade que assegura que os produtos são consistentemente produzidos e controlados, com padrões de qualidade apropriados para o uso pretendido e requerido pelo registro. O cumprimento das BPF está dirigido primeiramente à diminuição dos riscos inerentes a qualquer produção farmacêutica, os quais não podem ser detectados através da realização de ensaios nos produtos terminados. Os riscos são constituídos essencialmente por: contaminação-cruzada, contaminação por partículas e troca ou mistura de produto. (ANVISA Resolução RDC nº 210, de 04 de agosto de 2003)
>
> 2.2. As BPF determinam que:
>
> (a) todos os processos de fabricação devem ser claramente definidos e sistematicamente revisados em função da experiência adquirida. Além disso, devem mostrar ser capazes de fabricar medicamentos, dentro dos padrões de qualidade exigidos, atendendo às respectivas especificações; (b) as etapas críticas dos processos de fabricação e quaisquer modificações significativas devem ser sistematicamente validadas.(ANVISA Resolução RDC nº 210, de 04 de agosto de 2003)

Estas recomendações da resolução da ANVISA aplicam-se também à sistemas computadorizados.

3.0.9 GAMP5®(Boas Práticas Fabricação Automatizadas) na indústria farmacêutica

Segundo histórico apresentado pelo ISPE (Associação Internacional de Engenharia Farmacêutica) sobre o GAMP5, as diretrizes regulamentares relativas à utilização de tais sistemas automatizados estivessem disponíveis há algum tempo, os sistemas tinham sido sujeitos a controle regulamentar menor do que outras áreas de produção e eram considerados menos maduros do que áreas mais convencionais.

Um grupo da indústria foi criado para promover a compreensão das exigências da indústria. Esse grupo era composto por grandes fabricantes de produtos farmacêuticos e tornou-se o chamado guia GAMP5 ®.

No ano 2000, o GAMP5 ® tornou-se formalmente afiliado ao ISPE como um subcomitê técnico dentro da organização.

O Guia de Validação de sistemas automatizados foi lançado em dezembro de 2001, em Amsterdam. Ele pretende ajudar as indústrias de cuidados da saúde validar em conformidade os seus sistemas computadorizados.

Ele fornece orientações para os fornecedores desses sistemas automatizados no seu desenvolvimento e manutenção, seguindo as boas práticas, e auxilia os fornecedores na produção da documentação necessária para apoiar a validação.

O guia é um avanço significativo em versões anteriores deste amplamente aceite orientações sobre validação de sistemas automatizados. O documento completo está sendo revisado e aperfeiçoado de modo a refletir as expectativas atuais de regulação e de boas práticas. Ele foi consideravelmente melhorado e reestruturado.

O próximo capítulo descreve os requisitos necessários para o início da validação dos sistemas computadorizados e sua relação às normas descritas neste capítulo.

CAPITULO IV – PRÉ-REQUISITOS PARA VALIDAÇÃO DE SISTEMAS COMPUTADORIZADOS

Neste capítulo serão abordados os pré-requisitos para a validação de sistemas de computadorizados, conceitos e definições de como o GAMP5 e o FDA estabeleceram as seqüências e desenvolvimento da validação.

4.0 Segurança nos sistemas computadorizados

A segurança deve estabelecer controles tecnológicos garantindo a integridade, autenticidade, confiabilidade e confidencialidade das informações, garantindo processos confiáveis e controle contra fraudes mais eficazes.

4.0.1 Usuário final

Deve haver procedimentos para este solicitar acessar os sistemas computadorizados. O acesso se dá por meio de uma senha individual ou por controles de acesso do tipo token ou biométrico (ex: impressão digital). Assinatura de um termo de responsabilidade de confidencialidade pela manipulação nas informações destes sistemas.

4.0.2 Administrador do sistema

De acordo com o capítulo 1 do guia de validação do FDA é necessário haver procedimentos claros para criação, alteração e desativação de contas de usuários. Prevenção de fraudes (bloquear o usuário por senha incorreta). Controle de acesso a funções e das telas do sistema, isso pode ser feito pelo perfil do usuário (cargo e responsabilidades desempenhadas).

4.0.3 Administrador do banco de dados e Infra-estrutura tecnológica

Manutenção da integridade e confidencialidade das informações, procedimentos para restringir e controlar o acesso ao banco de dados. Procedimentos para criação e manutenção das interfaces. Backup e retenção de registros eletrônicos, proteção contra vírus, contra acesso externo através de firewall.

Instalações físicas de informática devem ser protegidas com controle de acesso e restrição a pessoas não autorizadas, deve haver procedimentos definidos.

Manutenção da integridade e confidencialidade das informações resguardadas (backup, retenção de registros históricos). Proteção adequada contra vírus e contra acesso externo através de firewall, mecanismos de controle de acesso aos componentes da infra-estrutura.

Controle de acesso às instalações físicas de informática (salas de servidores, gabinetes e cabeamento, antenas de telecomunicações).

4.1 Qualificação e auditoria de fornecedores

O GAMP5 possui um questionário detalhado que pode ser usado como base para realização das auditorias, demais informações estão dispostas na norma ISO 10011. O objetivo desse processo é averiguar a existência de um sistema de gerenciamento da qualidade que assegure que as práticas de desenvolvimento, teste, validação, suporte e manutenção do sistema computadorizado estejam de acordo com as práticas GXP e outros regulamentos aplicáveis.

São consideradas quatro etapas durante o processo de auditoria de fornecedores:

4.1.1 Pré-seleção de fornecedores

Permite selecionar o grupo de fornecedores potenciais.

- Certificações do fornecedor (ISO, IEC, etc.)
- Tempo no mercado
- Resultados de auditorias anteriores realizadas por outros clientes

4.1.2 Auditoria de pré-contrato

Avaliação final que objetiva certificar as informações enviadas pelo fornecedor durante a pré-seleção, devendo ser executada antes da confirmação do pedido de compra como parte do processo de seleção de fornecedor.

A auditoria realizada nas instalações do fornecedor deve contemplar

- Agendamento prévio
- Acordo de confidencialidade
- Envio da lista de documentos exigidos

4.1. 3 Auditoria de acompanhamento

Avaliação das observações encontradas durante a auditoria pré-contrato com o objetivo de certificar a implementação das ações corretivas acordadas.

4.1. 4 Auditoria periódica

Avaliação periódica realizada com o objetivo de certificar a manutenção dos padrões exigidos e acordados em contrato.

4.2 Especificação de projeto

Pode ser utilizada a mesma categorização de software descrita na especificação funcional, porém na especificação de projeto são definidos os requisitos de infra-estrutura, hardware e software, é criada após a aprovação da especificação funcional.

Para sistemas de baixa complexidade, pode-se adotar a estratégia de elaboração em um único documento de especificação funcional e de projeto.

4.2.1 Especificação do sistema

Fornecendo uma visão geral de todos os componentes do sistema, infra-estrutura, hardware e software e suas iterações contendo breve descrição de cada componente (rede, servidores, PLC, sistema operacional, base de dados). Tendo por objetivo detalhar o projeto do sistema e como ele interage dentro da infra-estrutura existente. Ou com outros sistemas ou interfaces externas.

4.2.2 Especificação de software

Segundo critérios do GAMP5, o detalhamento da arquitetura de software, módulos, interfaces, fluxograma e dicionário de dados deve ser elaborado de maneira que o desenvolvedor ou programador seja capaz de desenvolver o software aplicativo sem consultar o usuário e que possa ser utilizado como referência para os planos de teste.

Define os dados do sistema, base de dados, arquivos, tabelas, estrutura dos arquivos e tabelas, estrutura dos registros, tipos de dados e faixas de valores.

Descrição dos módulos interfaces e interações com outros módulos, tratamento de mensagens de erro, dados manipulados durante sua operação, outras variáveis ambientes utilizadas.

4.2.3 Especificação de hardware

Segundo o modelo de especificação do GAMP5, o qual inclui a infra-estrutura de rede, servidores, PLCs, sensores, instrumentos e demais periféricos. Para sistemas instalados sobre uma infra-estrutura existente, o projeto de hardware deve mostrar claramente de que forma o novo sistema irá se adequar a ela.

Os principais componentes a serem considerados são os seguintes:

- Servidores (dados, arquivamento, aplicativos, impressão, acesso remoto).
- Componentes da infra-estrutura de rede (cabeamento, rádio, switches, roteadores).
- Interfaces com usuários e operadores (pc's, painéis touch screen, terminais).
- Periféricos (impressoras, leitores de código de barras).
- Equipamentos de laboratório (HPLC, estufas, espectrofotômetro, autoclaves, lavadoras)
- Hardware de automação industrial (balanças, CLP, sistemas de visão, HVAC, FMS, BMS)
- Equipamentos mecânicos, sistemas hidráulicos e pneumáticos;
- Sensores e atuadores;
- Instrumentos de medição;
- Equipamentos de qualificação térmica, umidade relativa e pressão barométrica.
- Especificação do hardware do computador (CPU, armazenamento de dados, periféricos, conexões. Além do detalhamento das entradas e saídas (I/O);
- Descrição das condições ambientais exigidas pelo hardware, incluindo segurança física, a prova de explosões, incêndio e desastres ambientais.

4.2.4 Co-construção

Nesta fase são executadas todas as tarefas necessárias para que o sistema adquira as características definidas durante a fase de planejamento da implantação.

- Revisão dos processos;
- Instalação do software no ambiente de teste;

4.3 Desenvolvimento e construção do sistema

O desenvolvimento ou configuração do software deve estar baseado em metodologias que garantam sua confiabilidade e robustez e utilizem técnicas de programação modular de fácil compreensão para garantir sua manutenção, adotando comentários das funções no código-fonte.

Padrões de codificação (programação)

Cada projeto de desenvolvimento de software deve identificar os padrões de codificação de programas e as convenções de nomes que serão seguidos ao longo da fase de desenvolvimento, devendo ser descrito de maneira clara, de forma que qualquer programador esteja apto a manter e a aprimorá-lo sempre que necessário.

Convenções de nomes são utilizadas para variáveis, arquivos, módulos e funções e devem estar bem definidos, de modo a descrever de forma clara sua utilização.

O formato e o estilo da estrutura de codificação devem ser consistentes e padronizados, de modo a permitir a inspeção eficiente e reduzir o tempo e esforços para o desenvolvimento e manutenção dos códigos.

Os comentários devem ser estruturados, seguindo padrões de codificação intenção e estrutura. A codificação deve considerar o tratamento de erros, emitindo alertas ao operador e permitindo uma recuperação documentada e segura por meio de registro histórico dos erros. Na ocorrência de erros o software não deverá prosseguir seu processamento.

Os programas de instalação, bibliotecas, código-fonte e sua respectiva documentação devem ser tratados como um documento controlado, ser mantido sob controle de versões e seguir as práticas de gerenciamento de documentos e de configuração.

4.3.1 Testes de desenvolvimento

Os testes devem contemplar a execução do software por meio de casos de testes predeterminados e a verificação objetiva dos resultados com relação aos critérios de aceitação, sendo que somente após a sua execução e aprovação o sistema poderá ser liberado para instalação no usuário.

- Testes de unidade verificam a funcionalidade de um programa ou função de forma isolada;
- Testes de integração verificam que os módulos, programas e funções funcionam de forma integrada;
- Estes testes devem confrontar funções, desempenho, condições críticas e consistência de dados.

4.3.2 Implementação e início de operação

Para o projeto de validação de sistemas de automação são levados em consideração todos os seus componentes (humanos, mecânicos, hidráulicos, elétricos, ambientais, etc.) e devem fazer parte do plano de implementação.

FAT (***factory acceptance test***), através deste teste é verificado a fidelidade com o atendimento aos requisitos do usuário (URS) e identificam-se possíveis problemas encontrados durante o desenvolvimento e as respectivas soluções. São testes realizados pelo cliente nas instalações do fornecedor.

No SAT (***system acceptance test***) são verificadas as funcionalidades e sua capacidade de integração e comportamento no ambiente final.

Para sistemas de automação que existe a interação entre sistema computadorizado e equipamentos automatizados, deve-se considerar o FAT e o SAT.

Para sistemas computadorizados que não interagem com equipamentos automatizados, apenas o SAT é suficiente e os testes realizados podem ser considerados como parte da documentação previstos nas próximas etapas que são as qualificações da operação.

4.4.0 Qualificação da infra-estrutura

Verifica se todos os componentes foram instalados corretamente de acordo com as especificações de projeto e que todos os procedimentos de operação e manutenção estão implantados.

Nesta qualificação verifica-se o hardware e o software, componentes de rede, sistema operacional, banco de dados atendem às normas internas da empresa.

Deve ser elaborado um protocolo de qualificação da infra-estrutura que descreve como verificar a concordância dos componentes com o especificado em projeto. Requisitos de acesso físico, controles de segurança implementados limitam o acesso de pessoas não autorizadas.

Requisitos elétricos e de cabeamento estruturado para verificar se o sistema elétrico e a rede suporta todos os componentes de hardware.

Recuperação de desastres atende às normas pertinentes e se existe um procedimento descrevendo todo o processo para tal.

Verificação de todos os procedimentos, manuais e diagramas técnicos ***P&ID*** estão disponíveis.

O desenvolvimento é o processo que deixa apto ao início da validação propriamente dita, conforme descrito no capítulo a seguir, onde será detalhado como efetuar todas as tarefas e planos de testes necessários para que um sistema possa estar apto a funcionar devidamente qualificado.

CAPITULO V - VALIDAÇÃO DE SISTEMAS COMPUTADORIZADOS

A etapa de validação de sistemas computadorizados deve ser suportada ativamente pela área de TI (tecnologia da informação) que é responsável pela manutenção e infra-estrutura desses sistemas. Documenta que o equipamento, sistemas, procedimentos analíticos, processos e processamento de dados estão sob controle e são confiáveis.

Conseqüentemente, fornece resultados de processo e produto de acordo com os requisitos especificados e as expectativas das agências regulatórias.

> Validar é o ato de comprovar, de acordo com as normas, e padrões previamente estabelecidos, de que os processos de fato conduzem aos resultados esperados e projetados.
> A validação consiste em estabelecer evidências documentadas, com alto nível de segurança, de que um processo específico terá desempenho efetivo e produzirá consistentemente um resultado que atenda suas especificações e características previamente determinadas.
> (Moraes, Regina Lúcia de Oliveira, Validação, dezembro 2006.)

Procedimentos específicos devem ser elaborados para suportarem todas as atividades referentes à validação destes sistemas, seguindo normas nacionais e internacionais de acordo com o propósito de abrangência do produto.

Esses procedimentos devem conter o treinamento específico de todos os usuários do sistema e que suas funções devem estar envolvidas com a manutenção e operação desses sistemas.

5.0 Documentação de validação dos sistemas computadorizados

Segundo a resolução da diretoria colegiada ANVISA - RDC Nº. 249, DE 13 DE SETEMBRO DE 2005, a documentação envolvendo todo o processo de validação segue uma estrutura pré-definida, sendo definido pela ANVISA e ficando a critério do executante responsável pela validação do processo ou equipamento determinar a melhor estratégia de validação, desde que atenda aos requisitos legais. Conforme a ANVISA, GAMP55 e demais órgãos a que se submetem:

> ANVISA, RDC Nº. 249, DE 13 DE SETEMBRO DE 2005
> 12.3. Documentação
> 12.3.1. Plano Mestre de Validação
> 12.3.1.1. Deve existir um plano mestre de validação que contenha, no mínimo, os seguintes tópicos:
> a) objetivo (e os requisitos prévios);

b) apresentação dos processos por meio de fluxograma, diagrama de blocos ou descritivo destacando etapas críticas;
c) estrutura organizacional das atividades de validação, evidenciando as responsabilidades;
d) motivo para inclusão ou exclusão de determinada validação;
e) sistema de rastreabilidade para referências e revisões;
f) indicação de Treinamentos necessários para o programa de validação;
g) planejamento e cronograma das atividades a serem realizadas;
(h) referência cruzada a outros documentos;
(i) periodicidade e critérios para Revalidação;
(j) apresentar relação de equipamentos e instalações que devem ser qualificados;
(k) previsão de elaboração de relatórios de validação.
12.3.1.2. O Plano Mestre de Validação deve abranger:
(a) Métodos analíticos
(b) Limpeza
(c) Processos Produtivos
(d) Utilidades
(e) Sistemas Computadorizados.
12.3.2. Protocolo de Validação
12.3.2.1. Deve ser estabelecido um protocolo de validação que especifique como o processo de validação será conduzido. O protocolo deve ser aprovado pela Unidade da Qualidade.
12.3.2.2. O protocolo de validação deve especificar:
a) descrição do processo;
b) descrição dos equipamentos e instalações;
c) variáveis a serem monitoradas;
d) amostras a serem coletadas (local, freqüência, quantidade e procedimento de amostragem);
e) características/atributos e desempenho a serem monitorados, especificando os métodos analíticos;
f) limites aceitáveis;
g) definição de responsabilidades;
h) descrição dos métodos utilizados para registro e avaliação dos resultados, incluindo análise estatística;
i) etapas críticas do processo;
j) critérios de aceitação;
k) tipo de validação a ser conduzida;
l) treinamentos necessários para o programa de validação.
12.3.2.3. Devem ser identificados os pontos críticos, estabelecendo probabilidade, extensão, origem, prioridades e avaliação final.
12.3.2.4. A validação deve ser prospectiva quando realizada no estágio de desenvolvimento do produto intermediário ou insumo farmacêutico. Deve ser detalhada cada etapa do processo, tendo como base experiências anteriores para determinar situações críticas.

5.0.1 Classificação dos Sistemas Computadorizados

Os sistemas computadorizados são classificados pelo GAMP5 em dois tipos distintos de sistemas:

5.0.2 Sistemas de Informação

São sistemas que interagem com banco de dados (criam, recuperam, modificam ou excluem registros) e automatizam o fluxo de informações nas áreas onde estão implantados.

Como exemplo pode-se citar:

Softwares ERP, LIMS.

5.0.3 Sistemas de Automação

São compostos por equipamentos utilizados nos processos produtivos, tais como pesagem, produção, laboratório, etc. Estes interagem com software supervisório ou controlador lógico programável (CLP).

São exemplos: ***Scada, BMS, FMS***.

A validação aplica-se a todos os sistemas que tenham impacto sobre processos regulados por normas vigentes.

5.0.4 Comitê de validação

Trata-se de um grupo multidisciplinar criado quando da execução do projeto de validação afim de que seja responsável em definir, formalizar e divulgar a estratégia para a validação de sistemas computadorizados. Assegurando que a estratégia esteja consistente com o plano mestre de validação da organização e garante o cumprimento dos cronogramas estabelecidos, prioridades e execução das atividades.

O perfil dos integrantes do comitê deve incluir o conhecimento dos processos produtivos e suas interações com os sistemas computadorizados.

5.0.5 Equipe de Validação

Trata-se de um grupo multidisciplinar responsável pela execução das atividades. Coordena a execução das atividades dos fornecedores, fornece as informações técnicas requeridas para construção do sistema e garante o cumprimento dos cronogramas.

Além de assegurar que toda a documentação da validação contempla todas as variáveis do processo a ser automatizado e garante que os sistemas computadorizados, equipamentos e instrumentos que compõe o sistema satisfazem as especificações funcionais e expectativas de desempenho em cumprimento com os requisitos regulatórios.

O perfil destes integrantes deve incluir o conhecimento técnico de TI, automação industrial, engenharia, processos, qualidade e regulamentos aplicáveis. Devendo possuir capacitação técnica suficiente para realizar a análise dos riscos envolvidos e determinar a extensão da validação.

5.0.6 Proprietário do sistema

O proprietário do sistema é responsável pelas informações gerenciadas pelo sistema computadorizado ou pelo resultado alcançado na automação de um processo. Ele documenta todos os requisitos do processo e mantem atualizada a documentação. Atua como administrador do sistema, incluindo o gerenciamento de controle de acesso e o gerenciamento de configuração. Está também ativamente no comitê de validação como aprovador das melhorias propostas ou das modificações necessárias para a manutenção do sistema.

5.0.7 Requisitos e especificações do Usuário (*User Requirements Specification*)

Segundo os órgãos reguladores da indústria farmacêutica, os requisitos podem ser desenvolvidos internamente pelo fornecedor (no caso de desenvolvimento de produto).

Os requisitos devem definir com clareza e precisão o que o sistema deve fazer e indicar quaisquer restrições. Os requisitos devem ser revistos e aprovados pelas partes interessadas e os especialistas no assunto. Ou podem também ser fornecidos pelos clientes (para um produto configurado, o pedido personalizado, ou um serviço.

Alterações nos requisitos devem ser controladas, alterações em documentos posteriores que afetam a especificação dos requisitos devem conduzir a uma atualização dos mesmos. Os requisitos devem ser escritos de modo que possam ser testados. Necessidades individuais devem ser rastreáveis através do ciclo de vida.

Para os produtos configurados e aplicações personalizadas, a empresa regulada deve descrever os processos de negócio a ser automatizado. No caso de produtos configurados, esses processos devem estar alinhados com a funcionalidade do produto a ser utilizado.

Esta elaboração deve descrever clara e precisamente os requisitos de um processo e as funcionalidades esperadas do sistema (o que o usuário deseja que o sistema faça). Este documento deve ser elaborado pelo proprietário do sistema, baseando-se no mapeamento dos processos utilizando fluxograma, considerando entradas, saídas regras e recursos.

Definindo-se a seguir:

- As exigências do sistema e a descrição atual e desejada
- Objetivos e benefícios principais
- Áreas envolvidas da empresa

- Requisitos de GXP e demais regulamentos aplicáveis
- Funções e dados que o sistema processará
- Baseadas nos processos do usuário
- Requisitos para manipulação de dados-entrada, processamento e saída em linguagem não técnica;
- Ambientes de operação
- Requisitos de segurança e integridade dos dados, bem como direitos e níveis de acesso ao sistema;
- Período em que dados históricos devem ser mantidos

Para cumprimento desta exigência, a norma orienta que se deve dar ênfase às funções exigidas e não como serão feitas.

Ambiente operacional incluindo Infra-estrutura, interfaces do sistema, interfaces do usuário, interfaces com outros sistemas ou equipamentos e requisitos de desempenho dos sistemas.

Cada requisito deve ser estabelecido e codificado de forma a permitir sua rastreabilidade com os demais documentos que compõem o pacote de validação, especificando quais são imprescindíveis e quais os desejáveis.

5.0.8 Especificação funcional

A especificação funcional é requisito das boas práticas de automação sendo definida pelo GAMP55 como modelo que detalha o conteúdo recomendado considerando questões e impactos legais e habilidades e qualificações atuais dos usuários, podendo ser utilizado como pré-requisito para a especificação de projeto auxiliando a equipe de desenvolvimento ou fornecedor durante sua elaboração e que servirá como base para deixar o sistema apto a ser validado.

Uma função pode ser interpretada como uma rotina que executa um processamento específico das informações, o resultado gerado pode ser utilizado por outra função, por um equipamento, disponibilizado em forma de relatório ou consulta, ou armazenado na base de dados.

Para ***firmware*** (categoria dois do GAMP5) e sistemas comerciais (categoria três do GAMP5), a especificação do sistema pode ser entregue na forma de manual do sistema. Caso esses sistemas não atendam a todos os requisitos do usuário.

Para os sistemas configuráveis (categoria quatro do GAMP5) e customizados (categoria cinco do GAMP5), um documento de especificação funcional deve ser escrito.

Cada uma das funções do sistema deve ser codificada de tal forma que permita sua rastreabilidade com os demais documentos que compõe o pacote de validação.

Os pontos principais para este documento são:

Resumo das funções principais e interfaces com outros sistemas, devendo haver um detalhamento de cada função dentro do sistema e sobre sua utilização, definição das funções configuráveis, limites e regras dentro das configurações, cálculos e algoritmos, segurança, incluindo ações no caso de falha de hardware, redundância, restrições no acesso, interrupções e recuperação de dados. Além das premissas ou limitações de projeto de sistema ou especificações e do atendimento às normas reguladoras pertinentes.

Definição dos dados e parâmetros com que o sistema irá trabalhar, considerando as informações a serem armazenadas, especificando tipos (numérico, texto, alfabético) e tamanhos, faixas de operação, requisitos e as configurações de acesso, incluindo níveis de segurança, volume de dados, tempo de retenção e os detalhes do arquivamento de dados, utilização de assinaturas eletrônicas e de controles sobre os registros eletrônicos.

Desenho das interfaces do sistema e interfaces com usuários, incluindo o formato geral das telas e relatórios, tratamento de erros, formas de acesso (via web, cliente servidor). Interfaces com outros sistemas, a natureza da interação (envio/recebimento de dados) e os métodos e regras que a regem. As interfaces com os equipamentos devem incluir a listagem de entrada e saída (I/O) para sistemas de controle de processo.

Arquitetura do ambiente operacional que o sistema operará infra-estrutura (redes, servidores, comunicações, internet, etc.). Condições físicas e ambientais (umidade, partículas, temperatura, vibração, energia). Limitações do sistema, levando em consideração a compatibilidade com o sistema anterior, se forem o caso de substituição, compatibilidade com sistemas e padrões existentes na empresa confiabilidade, incluindo períodos máximos admissíveis de parada do sistema.

5.0.9 Plano Mestre de Validação

Segundo o guia GAMP5, e o FDA capítulo II e Resolução RDC nº 210, de 04 de agosto de 2003, o Plano Mestre de Validação é o planejamento das atividades da validação que tem objetivos, prazos, responsabilidades e procedimentos definidos. Deve abranger todos os sistemas computadorizados em uso e define seu impacto GXP e a priorização para execução da validação de acordo com os níveis de riscos associados que devem compreender:

- Papéis e responsabilidades das áreas envolvidas;
- Categorização do Software de acordo com o GAMP5
- Cronogramas de validação
- Critérios para avaliação de criticidade dos desvios e suas respectivas ações corretivas

A ANVISA Resolução RDC nº 210, de 04 de agosto de 2003, estabelece que:

> §19.9 Plano Mestre de Validação
> O Plano Mestre de Validação de um processo específico deve conter, no mínimo, os seguintes tópicos:
> 1. Objetivo (e os requisitos prévios).
> 2. Apresentação da totalidade do processo e dos sub-processos, fluxograma, pontos críticos / riscos.
> 3. Estrutura organizacional das atividades de validação
> 4. Motivo para inclusão ou exclusão de determinada validação
> 5. Sistema de rastreabilidade para referências e revisões
> 6. Treinamentos necessários para o programa de validação
> 7. Tipo de validação definido para cada sistema ou processo
> 8. Planejamento e cronograma das atividades a serem realizadas
> 9. Referência cruzada a outros documentos
> O Plano Mestre de Validação deve incluir a validação dos procedimentos de limpeza e dos métodos analíticos.

5.1 Tipos de validação

5.1.1 Validação Prospectiva

Os projetos de implementação de novos sistemas computadorizados devem incluir as atividades de validação desde sua concepção.

> A validação prospectiva é um ato documentado, baseado na execução de um plano de testes previamente definidos, que demonstre que um novo sistema, processo, equipamento ou instrumento, ainda não operacionalizado, satisfaz as especificações funcionais e expectativas de desempenho.
> ANVISA – RDC 210, de 04 de agosto de 2003, Item 19.4.1

5.1.2 Validação Retrospectiva

A validação retrospectiva consiste na elaboração ou revisão da documentação requerida (plano de validação, especificação de requisitos do usuário, especificação de desenho, protocolos de testes) certificando a sua precisão e atualização com relação ás práticas vigentes.

> ANVISA – RDC 210, de 04 de agosto de 2003, Item 19.4.1.3
> Se, ao final do processo de validação, os resultados são aceitáveis, o processo é satisfatório. Se os resultados forem insatisfatórios deve-se buscar modificação no processo até que o mesmo apresente resultados aceitáveis. Esta forma de validação é essencial para limitar o risco de erros que ocorrem em escala de produção industrial.

5.2 Ciclo de vida de sistemas computadorizados

De acordo com o IEEE Std. 1012-1986 cap. 7 [7.4.1] o ciclo de vida de um software deve descrever todos os aspectos do ciclo de vida de um sistema computadorizado que consiste em planejamento, especificação design construção, teste, implementação e aceitação, operação em curso e arquivamento do sistema, quando substituído.

O GAMP5 fornece um modelo conforme a ***fig.1***, o lado direito do ciclo de vida em 'V' é composto pelo protocolo de testes e seu devido uso para desafiar o sistema..

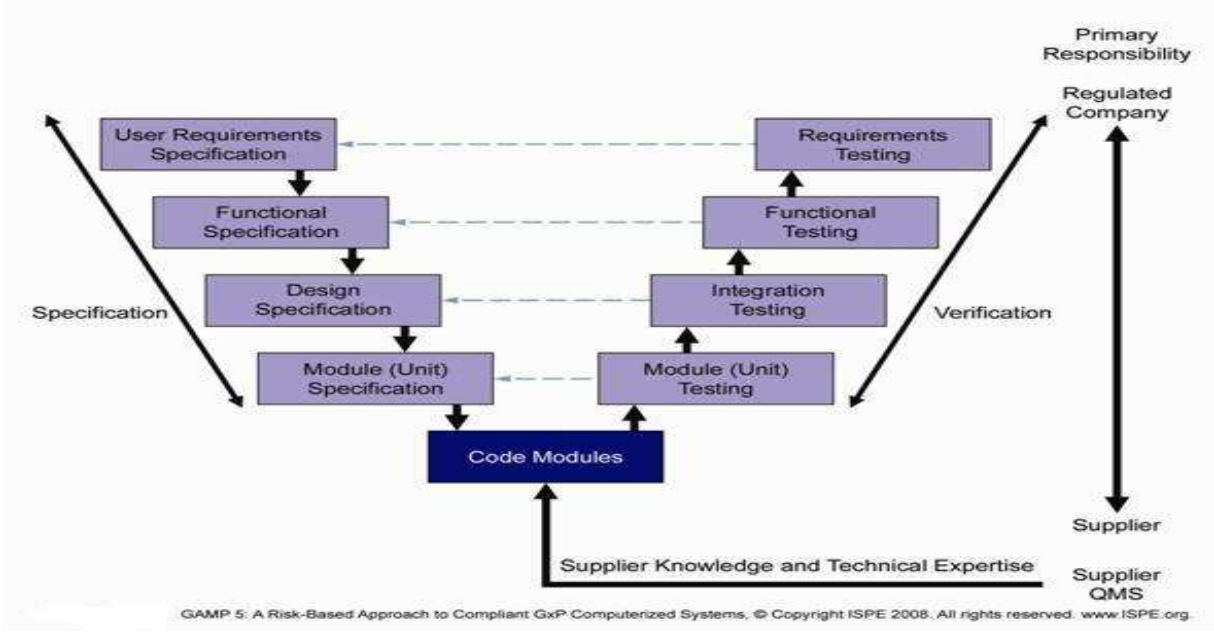

Fig. 1
Ciclo de vida de um sistema computadorizado.

5.2.1 Validação do ciclo de vida de sistemas computadorizados

Os usuários devem verificar se a documentação de apoio do ciclo de vida atende as expectativas da empresa, o que normalmente é feito através de uma auditoria de fornecedores. Cada empresa deve ter uma política definida em matéria de sistemas automatizados.

Qualquer sistema requer uma cooperação entre fornecedores e usuários. É vantajoso que o fornecedor utilize um sistema formal de gestão para controlar a documentação, incluindo a produção de pacote de software.

5.2.2 sistemas embarcados e sistemas autônomos

O GAMP5 diferencia sistemas embarcados e sistemas de controle de processo autônomos.

Sistemas embarcados são sistemas baseados em microprocessador, como programação em circuitos integrados (memórias flash, e2prom) controladores Lógicos Programáveis (PLC) ou PC com o único propósito de controle ou acompanhamento parte do processo ou equipamentos analíticos.

Sistemas autônomos são personalizados ou configurados independentemente, que são componentes de uma aplicação automatizada nos processos de fabricação.

Eles são distribuídos livremente como sistemas informáticos, para os equipamentos da planta. Os pré-requisitos para a validação com custos mínimos para os dois tipos de sistema são os mesmos, seguir os mesmos princípios básicos de vida do sistema.

5.3.0Critérios para inclusão e priorização em inventário de sistemas computadorizados

Para a realização da classificação e gerenciamento de riscos pode ser utilizado como referência o GAMP5 e documento do FDA Q9 ***Quality Risk Management***.

Deve-se definir o critério para inclusão e priorização em inventário, grau de extensão e profundidade das atividades de validação de sistemas computadorizados. Nestes documentos estão descritos os critérios para cada tipo de sistemas em relação às normas e ao risco potencial deste afetar a qualidade e a segurança do produto durante as fases em que este é monitorado por sistemas computadorizados. Por exemplo: software acoplado às

máquinas de produção, equipamentos de laboratório, sistemas de gestão de estoque, controle produtivo, sistemas automatizados que monitoram variáveis de processo, etc.

5.4 Qualificação da instalação (IQ)

A qualificação da instalação, conhecida como IQ (***Installation Qualification***) é a etapa da validação que verifica a conformidade de todos os componentes do projeto e equipamento associados estão conforme o especificado e instalados.

Protocolos de IQ atestam a conformidade das instalações com os documentos de compra e aceitação, documentação técnica que compreende manuais do usuário, administração, instalação, lista de componentes do sistema (***component list***), instalação técnica, SOP's, ***logbook's***, planos de manutenção e de recuperação de desastres.

É nesta fase que todos os critérios são desafiados, caso haja desvios em relação ao especificado, que não satisfaçam aos critérios de aceitação, deve-se registrar um desvio, o processo de validação é interrompido e através de uma não-conformidade mais conhecida por VNC (***validation non conformity***) o desvio deve ser tratado e solucionado afim de que se possa prosseguir com as demais etapas do processo. Caso haja desvios que podem ser considerados não críticos, pode-se prosseguir à execução da próxima etapa.

5.4.2 Qualificação da operação (OQ)

Nesta etapa detalha-se e documenta-se todo o correto funcionamento do sistema, conhecida como OQ (***Operational qualification***). Execução de testes de operação do sistema sob condições operacionais normais, através de cenários de operação normal do sistema.

Desafiando o sistema através de testes de execução, testes de alarmes do sistema sob as mais variadas condições possíveis e passíveis de ocorrerem, de acordo com as especificações de alarmes.

Os testes podem ser executados com documentos impressos com a descrição do alarme que ocorrerá em tal situação e o resultado pode ser anotado no documento como "aprovado/'reprovado', ou impressão de tela e relatórios de resultados. Testes funcionais podem ser executados pelas mesmas pessoas que desenvolveram o sistema. Os testes FAT e SAT podem substituir a documentação de qualificação da operação, caso estes tenham sido

executados satisfatoriamente. Mas algumas empresas preferem não usá-los, para que haja mais garantia na qualidade dos testes.

Caso haja desvios em relação ao especificado, que não satisfaçam aos critérios de aceitação deve-se registrar um desvio, o processo de validação é interrompido e através de uma não-conformidade mais conhecida por VNC (***validation non conformity***) o desvio deve ser tratado e solucionado afim de que se possa prosseguir com as demais etapas do processo.Caso haja desvios que podem ser considerados não críticos, pode-se prosseguir à execução da próxima etapa.

5.4.3 Qualificação do desempenho (PQ)

Também conhecida como PQ (***Performence Qualification***) esta etapa comprova que o sistema e suas funções operam de forma integrada com eficiência e constante durante sua operação normal.

Este teste tem enfoque nos processos e não nas funções, nele se observa os resultados esperados e os observados. Os resultados devem ser observados de forma descritiva e não apenas como 'aprovado/reprovado'.

Também poderão ser inclusos usuários que foram treinados nos sistema e nos processos e não poderão executar os testes aquelas pessoas que desenvolveram o sistema. Neste caso, os desvios devem ser documentados em listas de desvios e, para cada desvio haverá um plano de ação correspondente contendo responsáveis e prazos definidos.

Depois de sanados todos os desvios, caso ocorram, e aprovação final deste relatório, o sistema computadorizado pode ser considerado qualificado e liberado para produção.

5.5.0 Relatório final de validação de sistemas computadorizados

Este documento resume todas as atividades realizadas durante todo o processo de validação do sistema computadorizado, levando-se em conta todos os testes aprovados e o sistema liberado para produção. Devendo conter todos os documentos exigidos ao longo do processo e das atividades realizadas, protocolos, lista de alarmes, lista de componentes do sistema, etc.

Estes documentos devem ser armazenados em arquivos do tipo corta-fogo, devendo ser catalogados, e mantidos sob condições ambientais controladas, e como boas práticas

devem ser utilizadas canetas com tintas especiais nos documentos onde é necessária escrita manual dos resultados esperados nos testes executados.

5.5.1 Uso e manutenção dos sistemas computadorizados validados

Depois de concluída a validação do sistema computadorizado e o mesmo liberado para uso em produção / processo, deve ser avaliado periodicamente o seu estado validado. Esta avaliação visa garantir a integridade do sistema, evitando alterações no software sem a devida justificava caso haja necessidade de adequação aos negócios da empresa.

Neste caso, toda e qualquer alteração deve ser devidamente documentada e detalhada com a devida justificava que motivou a alteração. Algumas empresas adotam um método chamado PSE (***Periodic Evalution System***) ou avaliação periódica do sistema. Nestes testes é realizado o ***BASELINE***, que examina o sistema desde sua configuração de infra-estrutura até o software e programas instalados avaliados desde a validação ou última qualificação.

Quaisquer intervenções por ocorrências de problema de hardware, substituição de componentes do sistema devem ter um plano de impacto, examinando quais podem ser considerados críticos para o sistema. Os componentes substituídos devem ser de mesma especificação do anterior, não importando o fabricante, desde que atenda a configuração exata do anterior.

5.5.2 Gerenciamento de problemas

O plano de recuperação de desastres estabelece os procedimentos que garantem a disponibilidade das informações históricas dos sistemas computadorizados caso haja algum desastre. Devem definir as atividades, mecanismos tecnológicos, papéis e responsabilidades e o período requerido para a recuperação das informações.

5.5.2.1 Manutenções preventivas

Para assegurar que o estado validado do sistema é constantemente monitorado, faz-se necessário acordo entre as partes, manutenção e proprietários do sistema, neste caso podem ser criadas alternativas que garantem a execução sistemática, tais como:

Lista de componentes críticos do sistema, contrato de manutenção periódica (por exemplo, SLA (***Service Level Agreement***), que garante que a manutenção será realizada seja interna ou por outra empresa externa, para os componentes de hardware da data da última e / ou manutenção seguinte devem ser visíveis ou facilmente recuperáveis, toda a manutenção

deve ser documentada (ordens de serviços e ***logbooks***) no caso da manutenção preventiva levar a mudanças, um controle de alterações deve ser criado e o impacto dessas alterações deverá ser avaliado com a necessidade de abertura de não conformidades.

5.5.2.2 Manutenções corretivas

Cada problema deve ser registrado sob um único número ou código, que citam o problema, a data, o número do registro de hardware, a solução escolhida, por quem ele foi tratado etc.

Se a solução de um problema leva a uma mudança de hardware ou software, os procedimentos para controle de mudanças devem ser seguidos e um controle de alterações deve ser criado e o impacto dessas alterações deverá ser avaliado com a necessidade de abertura de não conformidades.

5.5.2.4 Cópia de segurança e Restauração

Todos os sistemas computadorizados devem possuir procedimentos específicos para a realização das atividades de cópia de segurança e restauração das informações e do software. Devendo ser periodicamente testados.

Além da tecnologia utilizada, tipo e identificação da mídia, procedimentos para solicitação de restauração de informações, além do local e condições ambientais da mídia de backup.

5.5.2.4 Gerenciamento de Mudanças

Segundo o GAMP5, o gerenciamento de mudanças é um processo que deve estabelecer os procedimentos para a solicitação, aprovação e implementação de alterações nos sistemas computadorizados e na infra-estrutura que os suportam. Toda alteração que afete GXP e modifique os requisitos e/ou as especificações originais, realizadas durante o processo de validação ou até mesmo após sua conclusão, deve gerar o controle de mudanças de forma a minimizar os riscos e atender aos regulamentos vigentes, devendo também ser documentadas e avaliado o grau de impacto na validação a fim de definir a extensão das atividades de requalificação do sistema computadorizado.

Principais atividades a serem consideradas em um controle de alterações são:

- Definição de responsáveis pelo controle de mudanças (área, comitê).

- Avaliação de impacto das mudanças sobre a funcionalidade do sistema
- Obter a aprovação do usuário responsável pelo sistema antes de efetivar as alterações;
- Realizar testes adequados ao impacto da mudança em ambientes de testes;
- Atualizar a documentação do sistema;
- Atualizar a condição dos usuários.

5.5.3 Plano de migração de dados e encerramento do uso do sistema

Este plano deve descrever todos os eventos que podem ocorrer durante o processo de transferência das informações e dados históricos de um sistema para outro, por motivos de substituição ou atualização de versões. Deve conter os ambientes de origem e de destino, a estratégia de migração, papéis e responsabilidades dos membros da equipe.

6.0 CONCLUSÃO

A utilização de assinaturas e registros na forma eletrônica pelas indústrias farmacêuticas impacta em toda sua cadeia produtiva não bastando existirem controles de acessos aos sistemas ou até mesmo a inviolabilidade dos mesmos, e precisam ser desafiados e colocados às mais diversas situações de usabilidade por meio de testes e avaliações que lhes garantam serem confiáveis íntegros e seguros.

> As indústrias farmacêuticas vêm apresentando necessidade crescente de registrar informações referentes aos seus processos e monitorar ambientes de fabricação e armazenamento. Indústrias deste segmento passaram a investir mais neste sentido, com resultados mais precisos, atribuindo a devida importância e dimensão aos registros de temperatura, pressão diferencial de salas, umidade dos ambientes, entre outras variáveis igualmente importantes para cada processo produtivo.
>
> Um sistema de registro e monitoramento deve possuir as aplicações básicas como registro de tendências das variáveis do processo envolvido, gerar armazenamento destes dados, produzir relatórios de acordo com as necessidades de cada aplicação, acesso aos dados históricos com segurança e confiabilidade, possibilidade de configuração e parametrização do hardware de coleta de dados, geração de alarmes, etc. Estes são alguns recursos básicos exigidos pela indústria farmacêutica para a citada finalidade.
>
> No sentido de atender às exigências e aos requisitos regulatórios relevantes ao segmento farmacêutico, as indústrias buscam sistemas de registro e monitoramento que possuam registro de dados em todos os níveis da planta, que jamais percam seus dados de registro múltiplos e com backup de segurança.
>
> Além de atender aos requisitos da norma 21 CFR Part11 do FDA - visando segurança nos registros eletrônicos e nas assinaturas eletrônicas, proporcionando a manutenção de contas e senhas dos usuários, facilitando e minimizando o tempo de validação e testes do referido sistema - e apresentar conformidade com as diretrizes do GAMP - Guide for Validation of Automated Systems – Guia de Validação para Sistemas Automatizados - que se tornaram o padrão para as Boas Práticas de Fabricação Automatizada (Good Automated Manufacturing Practice – GAMP) nas indústrias farmacêuticas. Em geral, a necessidade dos registros eletrônicos é proporcionar dados extremamente seguros, os quais podem oferecer níveis de confiabilidade e devem oferecer significativa segurança para recuperação e armazenamento de dados.
>
> (**Autor:** Sub-comitê GAMP Calibração - Ivan Canever - Inca Consultoria e Qualidade. Newton Bastos - Presys Instrumentos e Sistemas. Vander Gonçalves - Boehringer-Ingelheim. Luiz Antonio Rocha - Nycomed. Nicolás Cosentino – Giltece ngenharia. Marcelo Chagas - Bayer Healthcare).

A decisão pela substituição dos registros em papéis por registros eletrônicos deve ser suficientemente bem planejada e avaliada.

Fica a cargo de a própria empresa avaliar suas estratégias de mercado, se o destino final de seus produtos tratar-se de países onde haja norma que regulamente tal exigência.

No Brasil, como foi citado neste trabalho, não existe ainda uma norma clara quanto à sua utilização, já que o órgão responsável por regulamentar o setor farmacêutico é a ANVISA.

> Marcelo Decanio de Oliveira, chefe de automação, energias e qualificação da Boehringer Ingelheim e chairman do comitê GAMP5 – ISPE Afiliada Brasil comenta que a validação adequada gera menos correções após implantação, e isso é importante para a competitividade do negócio.
>
> Em termos regulatórios, ele acredita em exigências crescentes no mercado nacional, com possível aprofundamento quando da próxima edição da RDC 210 da ANVISA. "Acredito que a validação de sistemas computadorizados vai ser enfatizada exigindo-se mais detalhamento".
>
> PAZ, Alberto – SBCC (Sociedade Brasileira de Controle de Contaminação).

Embora citado neste trabalho, as novas tendências mundiais são de um mercado em plena expansão, o que obriga as empresas a serem mais competitivas e responsáveis quanto àquilo que produzem, devem oferecer um produto com qualidade.

As etapas de validação dos sistemas computadorizados são, hoje em dia, práticas usuais nestas empresas, não apenas porque a lei obriga, mas por questões de desempenho produtivo, evitando paradas de produção por erros inesperados que poderiam ter sido descobertos ainda na etapa de testes funcionais ou nas qualificações.

A área de TI atua efetivamente em todas as etapas do negócio, visando qualidade e a garantia desta, afinal o elemento computadorizado será o responsável pelas informações corretas e registros de eventos que acontecerem durante a produção, indicando inclusive os participantes do processo, operadores, técnicos que realizarem quaisquer intervenções no processo, através de sua rastreabilidade através das assinaturas eletrônicas.

A validação de sistemas computadorizados deve ser suportada por uma equipe multidisciplinar, envolvendo diversos profissionais com conhecimentos abrangentes, tanto do processo a ser automatizado e validado quanto da automação utilizada neste.

Podendo ser adotadas, algumas etapas de padrões de gerência de projetos, por exemplo, o PMBOK.

A fig.2 abaixo ilustra o processo descrito neste trabalho, a Tecnologia da informação como suporte a todo processo desde a concepção do projeto até a fase de produção, com os meios legais e apoio técnico.

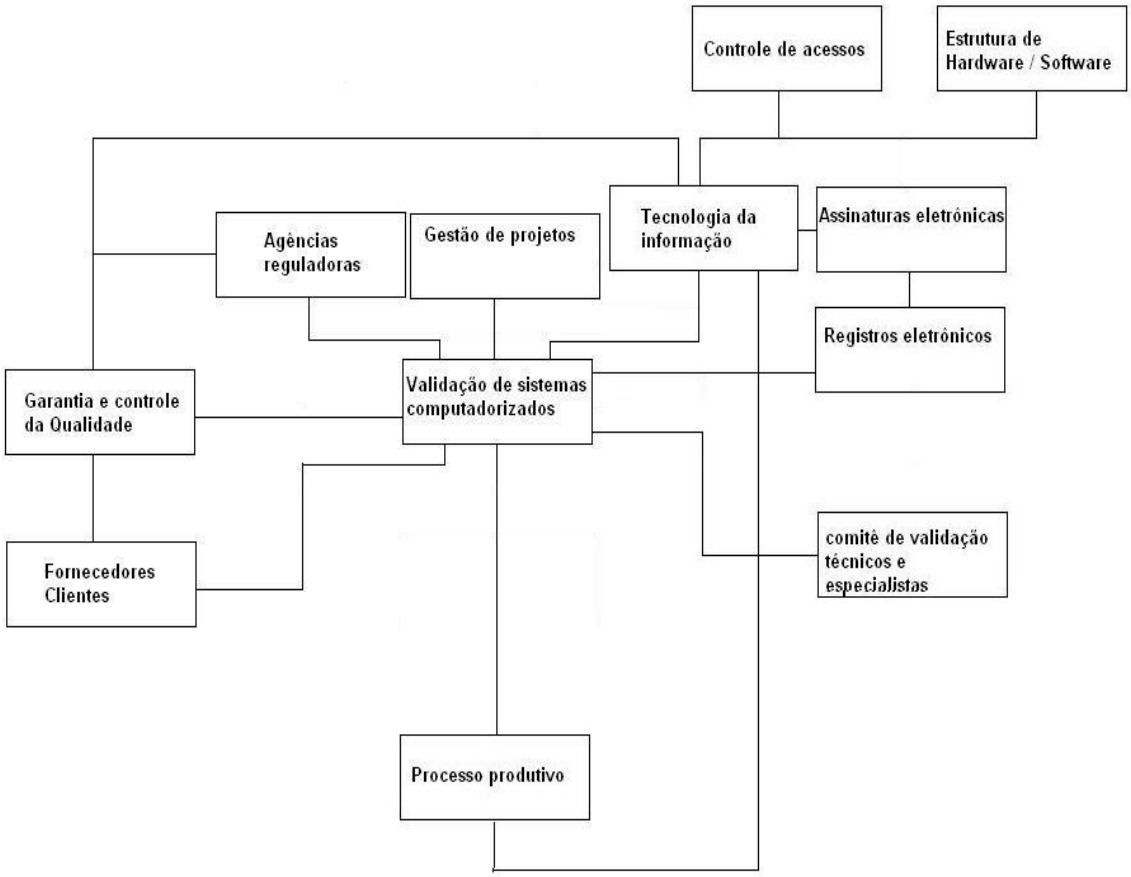
Controle de acessos
Estrutura de Hardware / Software
Tecnologia da informação
Assinaturas eletrônicas
Agências reguladoras
Gestão de projetos
Registros eletrônicos
Validação de sistemas computadorizados
Garantia e controle da Qualidade
comitê de validação técnicos e especialistas
Fornecedores Clientes
Processo produtivo

Fig. 2

7.0 ELEMENTOS PÓS-TEXTUAIS

7.1 GLOSSÁRIO

21 CFR Part 11: Edição 21 do Code of Federal Regulations e a Part 11 trata exclusivamente dos registros e assinaturas eletrônicas na área farmacêutica.

ANVISA: Agência Nacional de Vigilância Sanitária

Audit Trail *(Trilha de auditoria)* - Histórico das transações de sistemas que estão disponíveis para a avaliação a fim de aprovar a correção de sua execução comparada com os procedimentos ditados pela política de segurança. Relacionam-se a uma chave ou transação que permite que as quebras na segurança sejam detectáveis.

BASELINE : O baseline é um método de avaliação periódica de hardware e software em um sistema computadorizado, servindo para verificar alterações realizadas e o impacto dessas alterações para o estado validado da entidade.

BMS : Sistema de monitoramento predial

BOM : (Bill of Material) A BOM, ou estrutura de produto é uma das informações fundamentais da manufatura, pois nela registram-se as informações de produtos utilizadas por todos os setores e processos envolvidos com a manufatura do produto.

BPF: Boas Práticas de Fabricação.

DMA: Danish Medicines Agency: Agência dinamarquesa que regulamenta a produção e comercialização de produtos farmacêuticos.

FDA: (Food and Drug Administration) orgão governamental Norte Americano que regula a fabricação e distribuição dos alimenos (humano e animal), suplementos alimentares, medicamentos (humano e animal), cosméticos e equipamentos médicos, materiais biológicos

e produtos derivados do sangue humano. Criada em 15 de Maio de 1862 e atual designação inciada em 27 de Maio de 1930.

FIRMWARE: É o conjunto de instruções operacionais programadas diretamente no hardware de um equipamento eletrônico. É armazenado permanentemente num circuito integrado de memória de hardware, como uma ROM, PROM, EPROM ou ainda EEPROM e memória flash, no momento da fabricação do componente.

FMS : Sistema de monitoramento de facilidades

GAMP5: (Good Automated Manufacturing Practices edition 5.0) Guia utilizado para validação de sistemas computadorizados e sistemas automatizados, é utilizado para realizar especificações e projetos de validação, além da definição de responsabilidades ao longo do projeto.

GMP: (Good Manufacturing Practices) Derivação de GxP: Generic Trem for Good 'x' Practice, where 'x' may represent Testing, Documentation, Engineering or Manufacturing. (Termo Genérico para Boas Práticas de Teste, Documentação, Engenharia ou Fabricação).

P&ID: Diagrama de tubulação e Instrumentação

PLC: controladores Lógicos Programáveis

SCADA: (Supervisory Control and Data Acquisition) São sistemas que utilizam software para monitorar e supervisionar as variáveis e os dispositivos do sistema de controle conectados através de drives específicos.

7.2 REFERÊNCIAS

FDA Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application 28. Agosto 2003.

Glossary of Computerized System and Software Development Terminology (Division of 325 Field Investigations, Office of Regional Operations, Office of Regulatory Affairs, FDA 326 1995.

Good Practice and Compliance for Electronic Records and Signatures –-ISPE – versão 1 "21 CRF Part 11 – Electronic Record, Electronic Signatures," Section 1.10(e), Department of Food and Drug Administration, US Government, March 20, 1997 .

Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software. International Organization for Standardization, 1997.

IEEE Std 1012-1986, Software Verification and Validation Plans, Institute for Electrical and Electronics Engineers, 1986.

ISO 9000-3:1997, Quality management and quality assurance standards - Part 3:

ISO/IEC 12119:1994, Information technology – Software packages – Quality requirements and testing, Joint Technical Committee ISO/IEC JTC 1, International Organization for Standardization and International Electrotechnical Commission, 1994.

ISO/IEC 17799:2000 (BS 7799:2000) Information technology – Code of practice for 347 information security management (ISO/IEC, 2000).

Moraes, Regina Lucia de Oliveira Uso de risco na validação de sistemas baseados em componentes -- Campinas, [S.P. s.n.], 2006.

The Good Automated Manufacturing Practice (GAMP5) Guide for Validation of 344 Automated Systems, GAMP5 (ISPE/GAMP5 Forum, 2001-2008).

**** Este trabalho está licenciado sob uma Licença Creative Commons Atribuição-Vedada a Criação de Obras Derivadas 3.0 Brasil. Para ver uma cópia desta licença, visite http://creativecommons.org/licenses/by-nd/3.0/br/ ou envie uma carta para Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA***

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Administração
Baixar livros de Agronomia
Baixar livros de Arquitetura
Baixar livros de Artes
Baixar livros de Astronomia
Baixar livros de Biologia Geral
Baixar livros de Ciência da Computação
Baixar livros de Ciência da Informação
Baixar livros de Ciência Política
Baixar livros de Ciências da Saúde
Baixar livros de Comunicação
Baixar livros do Conselho Nacional de Educação - CNE
Baixar livros de Defesa civil
Baixar livros de Direito
Baixar livros de Direitos humanos
Baixar livros de Economia
Baixar livros de Economia Doméstica
Baixar livros de Educação
Baixar livros de Educação - Trânsito
Baixar livros de Educação Física
Baixar livros de Engenharia Aeroespacial
Baixar livros de Farmácia
Baixar livros de Filosofia
Baixar livros de Física
Baixar livros de Geociências
Baixar livros de Geografia
Baixar livros de História
Baixar livros de Línguas

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo