SUMÁRIO

1 OBJETIVO

Esta Norma estabelece requisitos complementares à NIT-Dicla-035 a serem utilizados pelas instalações de teste e adotados pela Cgcre para reconhecimento da conformidade destas instalações aos Princípios das Boas Práticas de Laboratório – BPL.

2 CAMPO DE APLICAÇÃO

Este documento aplica-se à Cgcre, aos inspetores e especialistas e às instalações de teste que possuem ou pretendem obter o reconhecimento da conformidade aos Princípios das Boas Práticas de Laboratório – BPL.

3 RESPONSABILIDADE

A responsabilidade pela revisão desta Norma é da Dicla.

4 HISTÓRICO DAS REVISÕES

Revisão	Data	Itens revisados
2	SET/2011	- Foi feita a substituição do acrônimo Cgcre/Inmetro por Cgcre - Foi alterada a denominação do Inmetro para Instituto Nacional de Metrologia, Qualidade e Tecnologia
3	JUL/2019	- Atualização da marca da Cgcre no cabeçalho. - Incluído capítulo de Documentos Complementares. - O Anexo foi atualizado com a tradução da nova publicação da OECD Number 17 "Application of GLP Principles to Computerised Systems", 2016.

5 DOCUMENTOS COMPLEMENTARES

ABNT NBR ISO 9001	Sistemas de gestão da qualidade - Requisitos
NIE-Cgcre-020	Elaboração de Documentos do Sistema de Gestão da Cgcre
NIT-Dicla-035	Princípios das boas práticas de laboratório - BPL
NIT-Dicla-072	Estabelecimento e Controle de Arquivos que Operam em Conformidade com os Princípios das BPL

6 SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BPF	Boas Práticas de Fabricação
BPL	Boas Práticas de Laboratório
Cgcre	Coordenação Geral de Acreditação
COTS	Sistemas Comerciais Off-The-Shelf
Dicla	Divisão de Acreditação de Laboratórios
LIMS	*Laboratory Information Management System* (Sistema de Gestão de Informações do Laboratório)
NBR	Norma Brasileira
NIE	Norma Inmetro Específica
NIT	Norma Inmetro Técnica
OECD	*Organization for Economic Cooperation and Development (*Organização de Cooperação e Desenvolvimento Econômico – OCDE)
OGM	Organismos Geneticamente Modificados
POP	Procedimento Operacional Padrão
TI	Tecnologia da Informação

7 CONSIDERAÇÕES GERAIS

7.1 Os Princípios das Boas Práticas de Laboratório são aplicados a instalações de teste que realizam estudos exigidos por órgãos regulamentadores para o registro de produtos agrotóxicos, farmacêuticos, aditivos de alimentos e rações, cosméticos, veterinários, produtos químicos industriais, organismos geneticamente modificados – OGM, visando avaliar o risco ambiental e a saúde humana dos mesmos.

7.2 A Cgcre se utilizou da versão de documentos publicados pela Organization for Economic Cooperation and Development – OCDE para estabelecer procedimentos e documentos normativos utilizados no reconhecimento da conformidade de instalações de teste aos princípios das BPL.

/ANEXO A

ANEXO A
VERSÃO BRASILEIRA DA PUBLICAÇÃO OECD Number 17 "Application of GLP Principles to Computerised Systems", 2016.

Nota: Por tratar-se de tradução de documento em língua estrangeira, este documento não segue as prescrições da NIE-Cgcre-020.

A APLICAÇÃO DOS PRINCÍPIOS BPL AOS SISTEMAS COMPUTADORIZADOS

SUMÁRIO

Introdução

Este documento introduz uma abordagem de ciclo de vida para a validação e operação de sistemas computadorizados. Ele enfatiza a avaliação de risco como o elemento central de um processo de validação ajustável, econômico e eficaz com foco na integridade dos dados. O objetivo deste documento é fornecer uma diretriz para permitir que as instalações de teste desenvolvam uma estratégia adequada para a validação e operação de qualquer tipo de sistema computadorizado, independente de sua complexidade, em um ambiente de BPL.

1.1 Escopo e definição dos termos

Os termos relevantes estão definidos no Glossário no Apêndice 2.

1.1.1 Sistema Computadorizado

Esta diretriz aplica-se a todos os tipos de sistemas computadorizados usados nas atividades reguladas em BPL, independente de sua complexidade (desde dispositivos simples, como balanças, até dispositivos mais complexos, tais como PC independentes que controlam instrumentos de laboratório e sistemas complexos, como sistemas de gestão de informações de laboratório). O sistema computadorizado consiste de hardware, software e as interfaces ao seu ambiente operacional. O hardware consiste de componentes físicos do sistema computadorizado; inclui a própria unidade do computador e seus componentes periféricos. O software é o programa ou programas que controlam a operação do sistema computadorizado. Portanto, todos os princípios de BPL relacionados a equipamento aplicam-se tanto a hardware como software. Durante o planejamento, condução, relato e arquivamento dos estudos, poderá haver diversos sistemas computadorizados em uso por uma série de motivos. Tais motivos podem incluir a captura direta ou indireta de dados de instrumentos automatizados, operação/controle de equipamentos automatizados e o processamento, relato e armazenamento de dados. Consequentemente, convém haver procedimentos adequados para controlar, manter e operar sistemas computadorizados.

1.1.2. Validação

A demonstração de que um sistema computadorizado é adequado ao longo do seu ciclo de vida para o seu uso pretendido é de importância fundamental e é referida como validação de sistemas computadorizados. Convém que todos os sistemas computadorizados usados para geração, medição, cálculo, avaliação, transferência, processamento, armazenamento ou arquivamento de dados para submissão a órgãos regulamentadores ou para apoiar decisões regulatórias sejam validados, operados e mantidos em conformidade com os Princípios das BPL. O mesmo requisito também se aplica a sistemas computadorizados usados para produzir outros dados relevantes para BPL, tais como registros de dados brutos, condições ambientais, registros de pessoal e treinamento, documentação de manutenção etc. Convém que o processo que um sistema computadorizado executa seja confiável e adequado ao propósito. O processo de validação deve fornecer um alto grau de garantia de que um sistema computadorizado atenda às especificações predeterminadas. Convém realizar a validação por meio de um plano de validação formal e executá-la antes do uso operacional.

Convém realizar prospectivamente a validação de sistemas computadorizados recém-estabelecidos. Dependendo do tamanho, criticidade e novidade do sistema, convém realizar o teste, se possível, em um ambiente de validação dedicado antes da transferência para o ambiente de laboratório. Deve-se assegurar que o ambiente de validação seja equivalente ao ambiente de laboratório para simulação apropriada. Convém utilizar um controle apropriado de alterações por todo o ciclo de vida do sistema até ser retirado de uso.

A validação retrospectiva não é permitida, a menos que o escopo de uso tenha mudado ou um sistema existente tenha se tornado relevante para a BPL (por exemplo, a necessidade de conformidade com os Princípios das BPL não foi prevista ou especificada). Quando isso ocorrer, convém haver uma justificativa documentada antes do uso do sistema em um estudo BPL. Isso deve envolver uma avaliação retrospectiva para avaliar a adequação que começa com a coleta de registros históricos relevantes relacionados ao sistema computadorizado. Convém revisar esses registros e elaborar um resumo escrito. Convém que este resumo retrospectivo especifique quais evidências estão disponíveis e quais requisitos adicionais devem ser testados durante o teste de aceitação formal para atingir o status de validado.

1.1.3. Qualificação

A qualificação formal, em vez da validação, pode ser aceitável para Sistemas Comerciais Off-The-Shelf (COTS), equipamentos automatizados de baixa complexidade ou sistemas pequenos. Devido ao seu uso extensivo, a validade do software incorporado pode ser assumida nos casos em que nenhuma customização é executada. É feita referência à respectiva orientação da área das Boas Práticas de Fabricação (BPF), como por exemplo, o Anexo 15 das Diretrizes da UE para Boas Práticas de Fabricação de Medicamentos para Uso Humano e Veterinário, com relação à “Qualificação e Validação”.

Exemplos de COTS de baixa complexidade, equipamento automatizado ou sistemas pequenos podem ser: equipamentos analíticos como pipetas eletrônicas, balanças, fotômetros e dispositivos de armazenamento como refrigeradores, freezers, etc.

A gerência da instalação de teste deve decidir e definir critérios para quando aplicar as abordagens de validação de sistemas computadorizados e/ou de qualificação. Convém aplicar uma abordagem baseada no risco para definir os parâmetros críticos do processo e as ações usadas para monitorar cada processo para garantir que ele permaneça em um estado de controle durante todo o ciclo de vida do sistema computadorizado. Portanto, espera-se que medidas rigorosas de calibração e manutenção sejam implementadas, juntamente com o uso de referências ou padrões internos com especificações estritas predefinidas. A aplicação de ferramentas estatísticas de controle de processo (por exemplo, cartas de controle) é recomendada e a rastreabilidade de longo prazo dos resultados de monitoramento é esperada. Foco especial e monitoramento são esperados com relação ao controle do fluxo de dados onde as interfaces com outros sistemas são estabelecidas. Devem existir procedimentos padrão que descrevam claramente as etapas definidas de processo e controle.

As atividades de requalificação devem ser realizadas com base em períodos de tempo predefinidos, levando em consideração os riscos identificados. Convém que a abordagem de qualificação seja detalhada nos procedimentos.

Os planos e relatórios de qualificação existentes podem ser referenciados quando vários exemplos do mesmo equipamento são usados dentro da instalação de teste.

1.1.4 Ciclo de vida

Convém que a abordagem de validação seja baseada em riscos e a gerência da instalação de teste tem a liberdade de escolher qualquer modelo de ciclo de vida apropriado. Deve assegurar que as atividades de validação sejam definidas e executadas de forma sistemática desde a concepção, compreendendo os requisitos, passando pelo desenvolvimento, liberação, uso operacional, até a retirada do uso do sistema. Convém documentar e definir todas as fases relevantes do ciclo de vida. Isso pode incluir a compra, especificação, projeto, desenvolvimento e teste, implementação, operação e desativação de sistemas computadorizados. Convém dimensionar as atividades do ciclo de vida com base na avaliação de risco documentada. Atividades mínimas podem ser requeridas para processos simples, como pesar em uma balança independente; atividades mais extensas podem ser necessárias para sistemas complexos, como sistemas interfaceados de gerenciamento de informações de laboratório.

1.2. Gerenciamento de risco

Convém aplicar o gerenciamento de risco durante todo o ciclo de vida de um sistema computadorizado, levando em conta a necessidade de garantir a integridade dos dados e a qualidade dos resultados do estudo. O gerenciamento de riscos consiste na identificação de riscos, avaliação de riscos, mitigação de riscos e controle de riscos. Convém que as decisões sobre a extensão dos controles de validação e integridade de dados sejam baseadas em uma justificativa documentada e em uma avaliação de risco documentada. Convém que o gerenciamento de riscos esteja vinculado a outros procedimentos relevantes (por exemplo, gerenciamento de configuração e mudança, processos de gerenciamento de dados, riscos de negócios, etc.).

A avaliação de risco deve ser usada para desenvolver uma estratégia de validação adequada e reduzir os esforços de validação. Convém direcionar esforço de validação para o uso pretendido do sistema e para os possíveis riscos à qualidade dos dados e à integridade dos dados. O resultado do processo de avaliação de risco deve gerar a elaboração de atividades de validação apropriadas para sistemas computadorizados ou funcionalidades de sistemas computadorizados. O uso apropriado de avaliações de risco é de suma importância para uma abordagem de validação eficaz e eficiente. Se os resultados da avaliação de riscos forem usados adequadamente, eles fornecerão à gerência da instalação de teste uma metodologia adequada para validar sistemas simples de laboratório, bem como sistemas complexos de gerenciamento de dados de laboratório.

Convém que a avaliação de risco de sistemas computadorizados que são usados tanto para estudos BPL como para estudos não-BPL inclua qualquer impacto potencial de atividades não relacionadas a ambos os casos. Os mesmos requisitos para validação aplicam-se a sistemas como os sistemas computadorizados que são usados exclusivamente em estudos de BPL. Deve haver uma clara diferenciação entre dados BPL e dados não-BPL.

1.3 Pessoal, funções e responsabilidades

Os Princípios das BPL exigem que uma instalação de teste ou uma unidade de teste possua pessoal qualificado e experiente e que existam programas de treinamento documentados com tarefas específicas, incluindo treinamento no local de trabalho e, quando apropriado, participação em cursos de treinamento externos. Registros de todos esses treinamentos devem ser mantidos. As mesmas disposições também se aplicam a todo o pessoal envolvido com sistemas computadorizados. Convém que as tarefas e responsabilidades de gerenciamento de instalações de teste, garantia da qualidade, diretor de estudo e pessoal de estudo que usam ou mantêm sistemas computadorizados sejam definidas e descritas.

Convém que para validar um sistema e operar um sistema validado, haja estreita cooperação entre todos os funcionários relevantes, se possível, como a gerência da instalação de teste, o diretor de estudo, o pessoal de garantia de qualidade, o pessoal de TI e o pessoal de validação. Todo o pessoal deve ter qualificações apropriadas, ser provido de níveis adequados de acesso e ter responsabilidades definidas para desempenhar as suas funções.

Os funcionários que validam, operam e mantêm sistemas computadorizados são responsáveis por realizar suas atividades de acordo com os Princípios das BPL e normas e guias sobre boas práticas (consulte "Referências" no Capítulo 5 abaixo).

Convém que durante a validação de sistemas computadorizados e a condução de estudos de BPL, os papéis e responsabilidades sejam definidos e controlados através de restrições de acesso ao sistema, treinamento e requisitos gerais de BPL. Convém que registros de treinamento e autorizações de acesso ao sistema de usuários estejam disponíveis e demonstrem que o pessoal tem conhecimento e direitos de acesso suficientes para cumprir suas respectivas funções de maneira compatível com as BPL.

Convém que contratos relevantes ou acordos de nível de serviço detalhem os requisitos de treinamento BPL para equipes de TI globais ou corporativas ou para provedores de serviços de TI internos e externos que possam trabalhar de acordo com sistemas de gerenciamento de qualidade diferentes das BPL.

Funções e Responsabilidades são descritas no Apêndice 1.

1.3.1. Gerência da instalação de teste

A gerência da instalação de teste tem a responsabilidade geral de garantir que as instalações, equipamentos, pessoal e procedimentos estejam em vigor para alcançar e manter sistemas computadorizados validados.

Isso inclui:
a) a responsabilidade de estabelecer procedimentos para assegurar que os sistemas computadorizados sejam adequados à sua finalidade pretendida e sejam operados e mantidos de acordo com os Princípios das BPL;
b) a nomeação e organização eficaz de um número adequado de pessoal devidamente qualificado e experiente; e
c) a obrigação de assegurar que as instalações, equipamentos e procedimentos de manuseio de dados sejam de um padrão adequado.

A gerência da instalação de teste deve assegurar que os procedimentos necessários para alcançar e manter o status validado dos sistemas computadorizados sejam compreendidos e seguidos, e garantir que o monitoramento efetivo da conformidade ocorra.

A gerência da instalação de teste deve designar pessoal com responsabilidade específica para o desenvolvimento, validação, operação e manutenção de sistemas computadorizados. Tal pessoal deve ser adequadamente qualificado, com experiência relevante e treinamento apropriado para desempenhar suas funções de acordo com os Princípios das BPL.

É responsabilidade geral da gerência local da instalação de teste garantir que os sistemas computadorizados fornecidos dentro de uma empresa mais ampla sejam operados e mantidos localmente de acordo com os Princípios das BPL. Acordos escritos entre a gerência local da instalação de teste e a organização mãe devem claramente atribuir responsabilidades para a validação, manutenção do status validado e a operação em conformidade com as BPL dos sistemas computadorizados. A gerência da instalação de teste pode delegar responsabilidades total ou parcialmente a um indivíduo ou a um grupo de profissionais adequadamente treinados (por exemplo, delegar a responsabilidade geral pela conformidade de BPL de sistemas computadorizados a um proprietário do sistema ou no caso de um sistema computadorizado específico, para um diretor de validação).

Convém que a gerência da instalação de teste defina funções e responsabilidades para as atividades de validação e a operação de rotina de cada sistema computadorizado, independentemente do seu nível de complexidade. Convém que potenciais conflitos de interesses associados a funções e responsabilidades sejam considerados para evitar riscos à integridade dos dados (por exemplo, convém que o pessoal analítico não esteja no controle das configurações da trilha de auditoria do sistema com o qual está trabalhando).

1.3.2. Diretor de Estudo

O diretor do estudo é responsável pela condução geral e pela conformidade BPL dos estudos. O diretor de estudo tem a responsabilidade de garantir que todos os sistemas computadorizados usados nos estudos sejam validados e usados de maneira apropriada. A responsabilidade do diretor de estudo pelos dados eletrônicos é a mesma dos dados registrados em papel (os dados devem ser atribuíveis, legíveis, contemporâneos, originais, exatos, completos, consistentes, duradouros e disponíveis). Convém que antes do início de um estudo de BPL, a confirmação do status de validação de todos os sistemas computadorizados que serão utilizados seja verificada pelo diretor de estudo.

1.3.3. Garantia da Qualidade

Convém que o pessoal de garantia da qualidade esteja ciente dos sistemas computadorizados relevantes para BPL em sua instalação de teste ou unidade de teste. As responsabilidades de garantia da qualidade para sistemas computadorizados devem ser definidas pela gerência da instalação de teste e descritas em procedimentos escritos. Convém que a garantia da qualidade seja capaz de verificar o uso válido de sistemas computadorizados. Convém que o programa de garantia da qualidade inclua procedimentos e práticas que verifiquem se os padrões estabelecidos são atendidos para todas as fases do ciclo de vida de um sistema. As tarefas para verificar os padrões de validação, operação e manutenção de sistemas computadorizados podem ser delegadas a especialistas ou auditores especializados (por exemplo, administradores de sistemas, proprietários de sistemas, especialistas externos, etc.). O pessoal de garantia da qualidade deve receber um nível apropriado de treinamento e acesso para permitir que eles inspecionem os processos específicos do computador, se necessário (revisão da trilha de auditoria, técnicas de análise de dados, etc.).

Se durante as inspeções de estudo, os dados estiverem disponíveis somente dentro de um sistema computadorizado, convém que o pessoal da garantia da qualidade tenha acesso direto somente à leitura dos dados.

Os diretores de estudo e pessoal da garantia da qualidade devem ter treinamento suficiente para entender os procedimentos relevantes no uso adequado de sistemas computadorizados relevantes para as BPL.

1.4. Instalação

Convém que seja dada a devida consideração à localização física do hardware do computador, componentes periféricos, equipamentos de comunicação e mídia de armazenamento eletrônico. Convém evitar extremos de temperatura e umidade, poeira, interferência eletromagnética e proximidade a cabos de alta tensão, a menos que o equipamento seja especificamente projetado para operar sob tais condições.

Também deve ser considerada a alimentação elétrica para equipamentos de informática e, quando apropriado, suprimentos de reserva ou ininterruptíveis para sistemas computadorizados cuja falha súbita afetaria os resultados de um estudo. Convém fornecer instalações adequadas para a retenção segura de mídia de armazenamento eletrônico.

1.5. Inventário

Convém que seja mantida uma listagem atualizada (inventário) de todos os sistemas computadorizados relevantes para as BPL e suas funcionalidades. Convém que a lista cubra todos os sistemas computadorizados relevantes para as BPL, independentemente da sua complexidade. Convém que os sistemas computadorizados usados em estudos de BPL sejam rastreados a partir do plano de estudo ou método relevante para o inventário. Convém que o inventário contenha o status de validação, marca, modelo ou versão como relevante e o proprietário do processo de negócios e o proprietário do sistema de TI (pessoas responsáveis ou responsáveis pelo sistema).

1.6. Fornecedor

Quando fornecedores (por exemplo, terceiros, fornecedores, departamentos internos de TI, provedores de serviços, incluindo provedores de serviços de hospedagem) são usados para fornecer, instalar, configurar, integrar, validar, manter, modificar, descomissionamento ou reter um sistema computadorizado ou para serviços como processamento de dados, armazenamento de dados, arquivamento ou serviços de nuvem devem existir acordos escritos (contratos) entre a instalação de teste e o fornecedor. Convém que esses acordos incluam declarações claras descrevendo as responsabilidades do fornecedor, bem como declarações claras sobre a propriedade dos dados.

Convém que a competência e a confiabilidade de um fornecedor sejam avaliadas pela gerência da instalação de teste. A necessidade e a extensão da avaliação do fornecedor devem se basear em uma avaliação de risco, levando-se em consideração a complexidade do sistema computadorizado e a criticidade do processo de negócio suportado pelo sistema computadorizado. A necessidade de uma auditoria deve ser baseada em uma avaliação de risco documentada. É responsabilidade da gerência da instalação de teste justificar a necessidade e o tipo de auditoria com base no risco.

Se o escopo da avaliação do fornecedor incluir uma parte técnica e a conformidade, convém que seja considerado o envolvimento de pessoal técnico especialista e do pessoal da garantia da qualidade. Convém que a gerência da instalação de teste seja capaz de fornecer aos inspetores informações sobre os sistemas de qualidade dos fornecedores, dependendo dos serviços que estão prestando. Os fornecedores não precisam estar em conformidade com os regulamentos das BPL, mas devem operar em um sistema de qualidade documentado, considerado aceitável pela gerência da instalação de teste, com informações da unidade de garantia de qualidade.

Para sistemas providos pelo fornecedor, é provável que grande parte da documentação criada durante o desenvolvimento esteja retida com o fornecedor. Se a documentação for retida no local do fornecedor, convém que a gerência da instalação de teste garanta que ela seja armazenada com segurança. Isso pode exigir um contrato formal entre o fornecedor e a instalação de teste. Nesse caso, convém que a evidência de uma avaliação formal e / ou auditorias do fornecedor esteja disponível na instalação de teste. O teste de aceitação formal pela instalação de teste dos sistemas fornecidos pelo fornecedor é necessário.

Convém que a gerência da instalação de teste defina, em acordos escritos, as interfaces entre seus procedimentos de validação e quaisquer atividades fornecidas por um fornecedor. Convém que tais interfaces sejam aplicáveis à fase de validação e à fase operacional. Por exemplo, convém que quaisquer atividades de teste executadas por um fornecedor sejam avaliadas pela gerência da instalação de teste.

Convém que os serviços hospedados (por exemplo, plataforma, software, armazenamento de dados, arquivamento, backup ou processos como um serviço) sejam tratados como qualquer outro serviço de fornecedor e exijam acordos escritos descrevendo as funções e responsabilidades de cada parte. É responsabilidade da gerência da instalação de teste avaliar o serviço relevante e estimar os riscos à integridade dos dados e à disponibilidade dos dados. Convém que a gerência da instalação de teste esteja ciente dos possíveis riscos resultantes do uso não controlado de serviços hospedados.

Uma instalação de teste pode incluir o departamento de TI da empresa como parte de sua instalação de BPL. Em tais casos, o departamento de TI deve se reportar à gerência da instalação de teste.

1.7 Produtos Comerciais Off-The-Shelf (COTS)

Um sistema computadorizado pode depender total ou parcialmente de produtos COTS. Os produtos COTS podem ser usados sem modificação, com configuração limitada, com configuração pesada ou mesmo codificação personalizada. Como acontece com qualquer outro tipo de software, os produtos COTS exigem validação apropriada, dependendo do risco e da complexidade de qualquer personalização. Se um aplicativo (por exemplo, uma planilha eletrônica) não for complexo, pode ser suficiente verificar as funções em relação às especificações de requisitos do usuário.

As especificações de requisitos do usuário devem ser escritas para qualquer aplicativo que seja baseado em um produto COTS. Convém que a documentação fornecida com um produto comercial pronto para uso (COTS) seja verificada pela gerência da instalação de teste para garantir que ele possa atender às especificações de requisitos do usuário.

Modelos de planilhas para cálculos usando fórmulas predefinidas, equações auto escritas ou macros devem ser considerados como aplicativos desenvolvidos internamente. Os requisitos de validação para estes são descritos nas seções 2 e 3 e dependerão do risco e da complexidade. O produto COTS básico exigirá uma forma adequada de qualificação e documentação. Somente a qualificação do produto COTS básico não é suficiente.

1.8 Controle de mudança e configuração

Convém que quaisquer alterações a um sistema computadorizado sejam feitas de maneira controlada e de acordo com os procedimentos de controle de alteração por escrito. Convém que os procedimentos de controle de alteração cubram a fase de validação, a fase operacional (incluindo arquivamento) e a fase em que o sistema é retirado de uso. A gerência da instalação de teste deve definir os papéis e responsabilidades dos envolvidos nas atividades de controle de alterações. Convém que as decisões sobre requisitos de controle de alterações sejam baseadas em riscos e dependerão da complexidade e da criticidade da mudança na integridade de dados ou nos processos de negócios suportados pelo sistema computadorizado. A avaliação de riscos usada no controle de alterações pode utilizar a categorização de software conforme descrito na orientação atual do ISPE (International Society for Pharmaceutical Engineering) GAMP (Good Automated Manufacturing Practice).

Convém que o controle de alterações abranja qualquer item submetido à revisão, aprovação e teste e que seja relevante para uma configuração definida de um sistema computadorizado. Convém que o controle de alterações garanta que a configuração de um sistema seja descrita e documentada com exatidão em todos os momentos. Convém que atividades específicas de estudo (por exemplo, captura de dados, cálculo de dados, etc.) sejam rastreáveis a uma configuração específica dos sistemas computadorizados, se a configuração for relevante para os resultados. Convém que o controle de alterações seja interfaceado com avaliação de risco, teste, liberação e procedimentos adequados de documentação.

1.9 Requisitos de documentação

Convém que os requisitos de documentação para sistemas computadorizados sejam incluídos no sistema de gestão da qualidade e convém que eles cubram todos os sistemas computadorizados relevantes para as BPL. A profundidade da documentação necessária irá variar dependendo da complexidade e estratégia de validação do sistema computadorizado. Convém que para cada sistema computadorizado, haja documentação cobrindo tipicamente:

a) o nome e a versão do software ou código de identificação do sistema computadorizado e uma descrição detalhada e clara da finalidade do sistema computadorizado;
b) o hardware no qual o software opera;
c) o sistema operacional e outro software de sistema (por exemplo, ferramentas) utilizado em conjunto com o sistema computadorizado;
d) a (s) linguagem (s) de programação do sistema computadorizado e / ou ferramentas da base de dados utilizadas apenas quando apropriado;
e) as principais funções desempenhadas pelo sistema computadorizado;
f) uma visão geral do tipo e fluxo de dados associados ao sistema computadorizado;
g) estruturas de arquivos, mensagens de erro e alarme associadas ao uso do sistema computadorizado;
h) os componentes de software do sistema computadorizado com números de versão; e
i) os canais de configuração e comunicação entre módulos do sistema computadorizado e equipamentos e outros sistemas.

Convém que o uso de sistemas computadorizados seja documentado adequadamente. Essa documentação geralmente cobre, mas não está limitada a:

a) procedimentos para o funcionamento de sistemas computadorizados (hardware e software) e as responsabilidades do pessoal envolvido;
b) procedimentos para medidas de segurança para detectar e impedir o acesso não autorizado ou alterações de dados;
c) alterar os procedimentos de controle, descrevendo os processos de autorização, teste e documentação de alterações nos equipamentos (hardware e software);
d) procedimentos para a avaliação periódica para o correto funcionamento do sistema completo ou seus componentes e o registro desses testes;
e) procedimentos que cubram a manutenção preventiva de rotina e o reparo de falhas (esses procedimentos devem detalhar claramente as funções e responsabilidades do pessoal envolvido. Para sistemas COTS, o uso de políticas e procedimentos do fornecedor para a execução do trabalho, quando apropriado, é aceitável. Convém que isto seja detalhado em um acordo escrito relacionado ao nível de serviço);
f) procedimentos para desenvolvimento de software, testes de aceitação e outros testes relevantes e o registro de todos os testes;
g) procedimentos de back-up e continuidade de negócios;
h) procedimentos para o arquivamento e “recuperação” de todos os dados eletrônicos, versões de software e documentação da configuração do computador e evidência de todas as atividades;
i) procedimentos de monitoramento e auditoria de sistemas computadorizados e evidências de todas as atividades; e
j) procedimentos e autorização para a desativação do sistema.

Convém que procedimentos adicionais de gerenciamento e validação sejam descritos se relevantes e podem incluir, mas não se limitar a: aquisição; gerenciamento de riscos; gerenciamento de serviços; planejamento de validação; especificação de requisitos; especificação de design; instalação; liberação do sistema; rastreabilidade; gerenciamento de incidentes; gerenciamento de configurações; gerenciamento de registros; pessoal; funções e responsabilidades do pessoal e gestão de documentos.

Convém que registros e procedimentos que descrevam com suficiente detalhe a validação e uso do sistema computadorizado estejam disponíveis. Tais registros podem incluir, mas não estão limitados a: avaliação de risco; avaliação de fornecedores; acordos de nível de serviço; especificações de requisitos; teste; liberação para uso; treinamento de pessoal e usuários; descrições de incidentes e mudanças; configuração e operação.

Convém que a documentação completa da validação e operação de um sistema computadorizado esteja disponível desde que os dados do estudo gerados com o sistema tenham que ser arquivados de acordo com os regulamentos aplicáveis.

2. FASE DO PROJETO

2.1 Validação

Convém que os sistemas computadorizados sejam projetados e demonstrados como adequados para o propósito em um ambiente de BPL e introduzidos de uma maneira pré-planejada. Convém que a validação de um sistema computadorizado, sua documentação e relatórios cubram as etapas relevantes do ciclo de vida, conforme definido pela gerência das instalações de teste com base na complexidade e no uso pretendido de um sistema. O trabalho de validação pode ser dimensionado e adaptado ao tipo de sistema justificado por uma avaliação de risco documentada. A gerência da instalação de teste pode confiar na orientação das boas práticas ao dimensionar o trabalho de validação. A gerência da instalação de teste deve ser capaz de justificar o ciclo de vida, a estratégia, os padrões de validação, os protocolos, os critérios de aceitação, os procedimentos, os registros e os entregáveis correspondentes com base em uma avaliação de risco. Por exemplo, os entregáveis referentes à validação realizada pela gerência da instalação de teste podem ser limitados às especificações de requisitos do usuário, um plano de validação, teste de aceitação do usuário e um relatório de validação, se puder ser justificado pela avaliação de risco.

Convém que haja evidência de que o sistema foi adequadamente testado quanto à conformidade com os critérios de aceitação estabelecidos pela instalação de teste antes de ser colocado em uso rotineiro. O teste de aceitação formal requer a realização de testes seguindo um plano predefinido e a retenção de evidências documentadas de todos os procedimentos de teste, dados de teste, resultados de testes, um resumo formal de testes e um registro de aceitação formal.

2.2 Controle de alterações durante a fase de validação

Convém que um processo de controle de alterações e gerenciamento de desvio esteja em vigor desde o início do processo de validação. Convém que se os registros de controle de alteração e desvios não forem considerados relevantes, isto seja justificado pela gerência da instalação de teste com base em uma avaliação de risco (por exemplo, uma abordagem de validação simplificada de um sistema menos complexo [ou seja, simples]).

Convém que o controle de alterações durante o desenvolvimento e a validação de um sistema seja claramente distinguido do controle de alterações durante a operação do sistema. Convém que a documentação de validação inclua registros de controle de alterações (se aplicável) e relatórios de todos os desvios observados durante o processo de validação.

2.3 Descrição do sistema

Convém que esteja disponível uma descrição do sistema detalhando os arranjos físicos e lógicos, fluxos de dados e interfaces com outros sistemas ou processos, quaisquer pré-requisitos de hardware e software e medidas de segurança. Convém que uma descrição atualizada do sistema seja mantida durante todo o ciclo de vida do sistema, conforme descrito no capítulo 1.9. Para sistemas simples com baixa complexidade, uma descrição menos complexa seria aceitável.

2.4. Especificações de requisitos do usuário

As especificações de requisitos do usuário são de suma importância para todas as atividades de validação e convém que sejam geradas para todos os sistemas computadorizados relevantes para as BPL, independentemente da complexidade do sistema. Convém que as especificações de requisitos do usuário descrevam as funções de um sistema e sejam baseadas em um processo de negócios documentado para o sistema e nos requisitos regulamentares aplicáveis. Convém que uma avaliação inicial de risco da validação seja baseada em um entendimento dos processos de negócios, especificações de requisitos do usuário e requisitos regulamentares.

Convém que as especificações de requisitos do usuário cubram todas as funções relevantes para BPL de um sistema e sejam usadas na avaliação de riscos para identificar funções críticas e atividades de teste apropriadas. Dependendo da complexidade do sistema, convém que as especificações dos requisitos do usuário sejam rastreáveis a qualquer documento de especificação adicional, se aplicável, e à documentação de teste gerada ao longo do ciclo de vida.

Se um sistema fornecido (comprado ou hospedado por um fornecedor) contiver mais funções que o necessário, somente as funções relevantes para BPL precisam ser testadas. Convém que a validação também inclua funções que possam ser usadas em estudos não-BPL e que possam interferir com o uso do sistema computadorizado em estudos de BPL. Convém que as outras funções e / ou funcionalidades que estão fora do escopo (ou seja, não destinadas a serem usadas) sejam identificadas, mas não requerem testes.

2.5 Sistema de Gestão da Qualidade e procedimentos de suporte

Convém que tanto o desenvolvimento de um sistema computadorizado como o processo de validação sejam governados por um sistema de gestão da qualidade. Convém que haja documentação adequada de que um sistema foi desenvolvido de maneira controlada e, de preferência, de acordo com padrões técnicos e de qualidade reconhecidos (por exemplo, ABNT NBR ISO 9001). Se um sistema for desenvolvido por um fornecedor, é responsabilidade da gerência da instalação de teste avaliar o sistema de gestão da qualidade de desenvolvimento do sistema do fornecedor. Convém que a gerência da instalação de teste confie na avaliação de risco ao definir a estratégia de avaliação.

2.6 Sistemas personalizados

Sistemas personalizados são desenvolvidos para um uso específico por uma instalação de teste específica (por exemplo, sistemas de captura de dados específicos do estudo BPL, modelos de planilhas com fórmulas ou macros, consultas, aplicativos estatísticos ou sistemas de avaliação de dados, etc.). Tais sistemas computadorizados podem também ser configurados ou codificados especificamente para um ou mais estudos BPL. Como nenhuma experiência de uso anterior ou paralelo está disponível, os sistemas personalizados apresentam o maior risco intrínseco. Convém que haja um processo para a validação de sistemas computadorizados personalizados que garanta a avaliação formal e a comunicação de medidas de qualidade e desempenho para todos os estágios do ciclo de vida do sistema.

É necessário um acordo por escrito entre o fornecedor do sistema personalizado e a gerência da instalação de teste, descrevendo papéis e responsabilidades relevantes para o sistema e sua validação. Convém que o trabalho de validação da gerência da instalação de teste considere todas as atividades relevantes de qualidade do fornecedor, mesmo no local de negócios do fornecedor. Convém que quaisquer atividades terceirizadas ou atividades de fornecedores internos façam parte do ciclo de vida do sistema computadorizado.

Se um aplicativo hospedado for um aplicativo personalizado, codificado ou configurado, convém que o sistema seja tratado tanto como um sistema personalizado como um provido externamente.

2.7 Testes

Convém que os testes (por exemplo, testes de instalação, testes de aceitação do usuário) sejam realizados para garantir que um sistema atenda aos requisitos predefinidos. É responsabilidade da gerência da instalação de teste entender a necessidade de testes e garantir a completude dos testes e da documentação de teste. Convém que os testes se baseiem no conhecimento do processo de negócios e no uso pretendido do sistema. Convém que os procedimentos descrevam como os testes são conduzidos e definam claramente os papéis e responsabilidades e os requisitos de documentação. É responsabilidade da gerência da instalação de teste decidir sobre a profundidade e a amplitude dos testes, orientados pela avaliação de riscos. Convém que a gerência da instalação de teste garanta que todos os sistemas, incluindo os sistemas COTS, sejam testados e avaliados. Os testes feitos pelo fornecedor e a documentação podem auxiliar a gerência da instalação de teste no trabalho de validação e podem suplementar ou substituir os testes executados na instalação de teste. Convém que a gerência da instalação de teste retenha evidências de testes, independentemente de o teste ser realizado pela instalação de teste ou por um fornecedor, demonstrando que métodos e cenários de testes apropriados foram empregados. Em particular, convém que os limites de parâmetros do sistema (processo), limites de dados e tratamento de erros sejam considerados.

Convém que a gerência da instalação de teste considere um teste de aceitação de usuário específico para demonstrar que o sistema é adequado para realizar um determinado estudo BPL (por exemplo, provar a adequação de um sistema que executa uma determinação analítica típica, incluindo calibração, medições, cálculos e transferência de dados para um LIMS).

Convém que exista uma interface para alterar os procedimentos de controle. Quando o teste leva a alterações no sistema, convém que elas sejam gerenciadas por meio do controle de alterações. Evidências de testes adequados podem ser fornecidas pela manutenção de registros de resultados de testes internos ou registros de auditoria de fornecedores.

2.8 Migração de dados

A migração de dados pode ocorrer no decorrer de um estudo de BPL ou após um estudo ter sido finalizado. Convém que a migração de dados faça parte do escopo de validação da gerência da instalação de teste se os dados relevantes às BPL forem afetados, independentemente do status de qualquer projeto de estudo de BPL. Se os registros do estudo forem arquivados em um sistema eletrônico, a migração de dados pode se tornar relevante.

Quando os dados eletrônicos forem transferidos de um sistema para outro, o processo deve ser documentado. É responsabilidade da gerência da instalação de teste assegurar e demonstrar que os dados não sejam alterados durante o processo de migração. Convém que a conversão de dados para um formato diferente seja considerada como migração de dados (por exemplo, de um formato de dados proprietário para PDF). Quando os dados são transferidos para outro meio, convém que os dados sejam verificados como uma cópia exata antes de qualquer destruição dos dados originais.

Os esforços de migração de dados podem variar muito em complexidade e riscos. Exemplos incluem:

a) atualizações de versão;
b) conversões de dados (de um banco de dados para outro; para outro formato de dados; atualização de software relacionada à mudança de formato);
c) mesma migração do sistema (movimentação de aplicativos; dados de um servidor para outro); e
d) migração de uma fonte para um sistema de destino.

Convém que os dados migrados permaneçam utilizáveis e mantenham seu conteúdo e significado. Convém que o valor e / ou significado de links entre uma trilha de auditoria do sistema e assinaturas eletrônicas sejam assegurados em um processo de migração. Cabe à gerência da instalação de teste manter a ligação entre a trilha de auditoria legível ou as assinaturas eletrônicas e os dados auditados.

2.9 Intercâmbio de dados

Comunicações relacionadas a sistemas computadorizados geralmente se dividem em duas categorias: entre computadores ou entre computadores e componentes periféricos. Dados relevantes para GLP podem ser transportados automaticamente, unidirecionalmente ou bidirecionalmente, de um sistema para outro (por exemplo, de um sistema remoto de captura de dados para um banco de dados central, de planilhas para um LIMS, de um sistema de gerenciamento de dados cromatográficos para LIMS, ou de uma planilha eletrônica para um aplicativo de software estatístico). Todos os links de comunicação são possíveis fontes de erro e podem resultar na perda ou corrupção de dados. Controles apropriados de interfaces para segurança e integridade do sistema devem ser adequadamente abordados durante o desenvolvimento, validação, operação e manutenção. Convém que o intercâmbio eletrônico de dados entre sistemas inclua verificações internas apropriadas para a entrada e o processamento corretos e seguros dos dados. Convém que a infraestrutura de rede seja qualificada. Entretanto, este requisito não pretende solicitar a validação da infraestrutura de comunicação padrão e seus procedimentos (por exemplo, a linguagem de comunicação básica da Internet TCP / IP [Protocolo de Controle de Transmissão / Protocolo da Internet]).

3. FASE OPERACIONAL

Convém que todos os sistemas computadorizados sejam operados e mantidos de forma a garantir a continuidade do estado validado.

3.1 Checagens de exatidão

Convém que a gerência da instalação de teste esteja ciente de todos os dados relevantes BPL inseridos manualmente nos sistemas eletrônicos. É responsabilidade da gerência da instalação de teste controlar adequadamente qualquer sistema de entrada de dados eletrônicos, independentemente de sua complexidade. Convém que a avaliação de risco seja aplicada para identificar o potencial de entrada incorreta de dados e para avaliar a criticidade e as consequências de dados digitados erroneamente ou incorretamente. Convém que estratégias de mitigação de risco sejam descritas e implementadas. Isso pode resultar na necessidade de verificações manuais e / ou eletrônicas adicionais para a precisão dos dados inseridos por um segundo operador ou sistema eletrônico. Convém que quando usadas, as verificações automatizadas na entrada de dados sejam incluídas na validação de um sistema computadorizado (por exemplo, scripts de validação aplicados automaticamente durante a entrada de dados manual), a profundidade dos trabalhos de validação seja dimensionada com base na avaliação de risco. Convém que o uso de sistemas de entrada de dados invalidados não seja permitido (por exemplo, o uso não controlado de planilhas). Se forem aplicados procedimentos de controle manual para entrada manual de dados, convém que o procedimento seja assegurado por documentação adequada que facilitará a reconstrução das atividades.

3.2 Dados e armazenamento de dados

Quando os dados (dados brutos, dados derivados ou metadados) são armazenados eletronicamente, convém que os requisitos para fins de backup e arquivamento sejam definidos. Convém que o backup de todos os dados relevantes seja realizado para permitir a recuperação após falhas que comprometam a integridade do sistema.

Convém que os dados armazenados sejam protegidos por meios físicos e eletrônicos contra perda, dano e/ou alteração. Convém que os dados armazenados sejam verificados quanto à capacidade de restauração, acessibilidade, legibilidade e exatidão. Convém que os procedimentos de verificação de dados armazenados sejam baseados em risco. Convém que o acesso aos dados armazenados seja assegurado durante todo o período de retenção.

As alterações no sistema de hardware e software devem permitir o acesso contínuo e a retenção dos dados sem qualquer risco à integridade dos dados. Quando um sistema ou software é atualizado, deve ser possível ler dados armazenados pela versão anterior ou outros métodos devem estar disponíveis para ler os dados antigos. Convém que as informações de suporte (por exemplo, registros de manutenção, registros de calibração, configuração, etc.) que são necessárias para verificar a validade de dados brutos ou para reconstruir um estudo inteiro ou partes dele sejam armazenadas em *backup* e retidas nos arquivos. Convém que o software seja mantido no arquivo, se necessário, para ler ou reconstruir dados.

Em relação aos registros eletrônicos, convém que a gerência da instalação de teste tenha:

a) quaisquer registros eletrônicos relevantes do estudo identificados (por exemplo, dados brutos, dados derivados). É necessário que os dados brutos sejam identificados para cada sistema computadorizado, não importando o quanto os dados brutos estejam associados a ele (por exemplo, por armazenamento em um meio de armazenamento eletrônico, por meio de impressões de computador ou instrumento etc.);
b) avaliado a criticidade dos registros eletrônicos para a qualidade dos resultados do estudo;
c) avaliado riscos potenciais para os registros eletrônicos;
d) procedimentos de mitigação de risco estabelecidos; e
e) monitorado a eficácia da mitigação de risco ao longo do ciclo de vida.

Com relação aos procedimentos, convém que a gerência da instalação de teste descreva como os registros eletrônicos são armazenados, como a integridade do registro é protegida e como a legibilidade dos registros é mantida. Para qualquer período de tempo relevante para BPL, isso inclui, mas pode não estar limitado a:

a) controle de acesso físico à mídia de armazenamento eletrônico (por exemplo, medidas para controlar e monitorar o acesso de pessoal a salas de servidores, etc.);
b) controle de acesso lógico (eletrônico) a registros armazenados (por exemplo, conceitos de autorização para sistemas computadorizados como parte da validação de sistema computadorizada que define funções e privilégios em qualquer sistema computadorizado relevante para as BPL);
c) proteção física dos meios de armazenamento contra perda ou destruição (por exemplo, incêndio, umidade, falhas elétricas destrutivas ou anomalias, roubo, etc.);
d) proteção de registros eletrônicos armazenados contra perda e alteração (por exemplo, validação de procedimentos de back-up, incluindo a verificação de dados de back-up e armazenamento adequado de dados de backup; aplicação de sistemas de trilha de auditoria); e
e) garantir acessibilidade e legibilidade dos registros eletrônicos, proporcionando um ambiente físico adequado, bem como um ambiente de software adequado.

Convém que o armazenamento de dados seja considerado para cada sistema computadorizado usado para realizar estudos BPL durante a fase de estudo e período de arquivamento. Não é necessário incluir a avaliação na documentação do estudo. No entanto, convém que a gerência da instalação de teste tenha uma política para explicar como os dados são armazenados e como os requisitos de armazenamento são atendidos. Convém que essas informações façam parte do conjunto de documentação de validação do sistema. Se a instalação de teste entregar os dados do estudo eletrônico a um patrocinador, a responsabilidade pelos dados será transferida para o patrocinador.

3.3 Impressões

Se os dados forem impressos para representar dados brutos, convém que todos os dados eletrônicos, incluindo dados derivados, bem como metadados e (informações sobre alterações de dados, se tais alterações forem necessárias para manter o conteúdo e o significado corretos dos dados), sejam impressos. Alternativamente, convém que todos os registros eletrônicos sejam verificáveis na tela em formato legível e retidos. Isso inclui todas as informações sobre alterações feitas nos registros, se tais alterações forem relevantes para o conteúdo e o significado corretos.

3.4 Trilhas de auditoria

Uma trilha de auditoria fornece evidência documental de atividades que afetaram o conteúdo ou o significado de um registro em um ponto de tempo específico. É necessário que as trilhas de auditoria estejam disponíveis e sejam convertíveis para uma forma legível por humanos. Dependendo do sistema, pode-se considerar que os arquivos de log satisfazem este requisito (ou pode-se agregá-los a um sistema de trilha de auditoria). Qualquer alteração nos registros eletrônicos não deve obscurecer a entrada original e ter hora e data marcadas e deve ser rastreável à pessoa que fez a alteração.

Convém que a trilha de auditoria de um sistema computadorizado seja habilitada, configurada apropriadamente e reflita os papéis e responsabilidades do pessoal do estudo. Convém que a capacidade de fazer modificações nas configurações da trilha de auditoria seja restrita ao pessoal autorizado. Convém que qualquer pessoal envolvido em um estudo (por exemplo, diretores de estudo, chefes de departamentos analíticos, analistas, etc.) não seja autorizado a alterar as configurações da trilha de auditoria.

Convém que haja um sistema em vigor que garanta uma análise baseada em risco das funções da trilha de auditoria, suas configurações e as informações registradas. A gerência da instalação de teste pode considerar, mas convém que não se limite a, eventos individuais (por exemplo, comportamento do usuário, problemas suspeitos de integridade de dados) para revisar os registros da trilha de auditoria. Completude e adequação das funções e configurações da trilha de auditoria podem ser consideradas. Convém que o pessoal de garantia de qualidade BPL esteja envolvido. Convém que uma revisão das funções da trilha de auditoria seja baseada no entendimento do uso do sistema, na capacidade de modificar o registro e nos controles que impedem alterações maliciosas dos registros.

Convém que o sistema seja capaz de realçar as alterações feitas nos dados inseridos anteriormente, tanto na tela quanto em qualquer cópia impressa. Convém que as entradas originais e modificadas sejam retidas pelo sistema. As trilhas de auditoria podem existir em alguns sistemas como um registro de alterações suplementares à exibição dos dados (na tela ou impressos). Convém que os dados originais sejam armazenados juntos com os dados modificados. Por exemplo, qualquer cromatograma reintegrado modificado para fins de recálculo deve ser marcado irrevogavelmente.

3.5 Gerenciamento de alterações e gerenciamento de configuração

Convém que a gerência da instalação de teste tenha procedimentos apropriados para gerenciamento de configuração e gerenciamento de alterações na fase operacional. Tanto o gerenciamento de alterações quanto de configurações deve ser aplicado ao hardware e software. Convém que as medidas de controle de alteração garantam que as alterações na configuração do sistema computadorizado que podem afetar o status de validação sejam introduzidas de maneira controlada. Convém que uma alteração seja rastreável para registros apropriados de controle de alterações e configurações. Convém que os procedimentos descrevam o método de avaliação usado para determinar a extensão do reteste necessário para manter o status validado do sistema.

Convém que os procedimentos de controle de alterações definam claramente as funções e responsabilidades para acessar e aprovar alterações e procedimentos detalhados para avaliar a alteração. Independentemente da origem da alteração (fornecedor ou sistema desenvolvido internamente), informações apropriadas precisam ser fornecidas como parte do processo de controle de alterações. Convém que os procedimentos de controle de alterações garantam a integridade dos dados.

Convém que a configuração de um sistema computadorizado seja conhecida a qualquer momento durante seu ciclo de vida, desde as etapas iniciais do desenvolvimento até a aposentadoria. A conformidade documentada da configuração de um instrumento analítico com as disposições da validação do método é necessária para demonstrar o uso adequado de um sistema computadorizado em um estudo BPL - independentemente de sua complexidade. Qualquer resultado do estudo BPL deve ser rastreável à configuração do sistema relevante e validado para permitir a verificação das configurações, conforme fornecido pelo plano de estudo ou pelo método relevante.

Mudanças podem ser necessárias em resposta a incidentes ou a propósitos específicos da instalação / estudo. Após a modificação ou reparo, o status de validação do sistema deve ser verificado e documentado.

Convém que as modificações implementadas pela automação de rotina (por exemplo, *patches* de proteção contra vírus ou sistema operacional) façam parte do controle formal de alterações ou do gerenciamento de configurações. Convém que a ausência de gerenciamento de alterações para um sistema computadorizado seja justificada e baseada na avaliação de risco.

3.6 Análise crítica periódica

Convém que os sistemas computadorizados sejam revisados periodicamente para confirmar que eles permanecem em um estado validado, estão em conformidade com as BPL e continuam a atender aos critérios de desempenho declarados (por exemplo, confiabilidade, capacidade de resposta, capacidade etc.). Convém que a análise crítica periódica inclua, quando apropriado, a faixa atual de funcionalidade, registros de desvio, incidentes, histórico de atualizações, desempenho, confiabilidade e segurança que podem ter afetado o status de validação do sistema. Convém que a frequência e a profundidade da análise crítica periódica sejam determinadas com base em uma avaliação de risco considerando a complexidade e a criticidade das BPL. Convém que a análise crítica periódica leve em conta qualquer evento inesperado relatado que possa ter afetado o status de validação de um sistema. Convém que a adequação das atividades de revisão e o envolvimento de pessoal especializado, bem como de pessoal relevante para BPL (por exemplo, gerência de instalações de teste, garantia de qualidade, pessoal de suporte de TI, fornecedor, etc.) sejam justificados. Convém que as responsabilidades do pessoal envolvido em análise crítica periódica do status de validação de sistemas computadorizados sejam definidas. A necessidade de uma interação entre as atividades de análise crítica periódica e o sistema de notificação de incidentes pode ser considerada dependendo de uma avaliação de risco. Convém que os resultados das atividades de análise crítica periódica e, quando aplicável, as ações corretivas sejam documentadas.

Sistemas computadorizados de menor criticidade e menor complexidade podem ser excluídos da análise crítica se a exclusão for justificada com base no risco. Uma análise crítica periódica pode ser desnecessária quando as principais atividades de (re)validação ocorreram recentemente e poderiam, portanto, ser postergadas. Se nenhum evento inesperado que possa ter afetado o status validado tiver sido relatado, sistemas COTS automatizados podem ser excluídos da revisão. Convém que uma análise crítica periódica do usuário seja feita quando necessário (por exemplo, no caso de mudanças organizacionais) ou pelo menos uma vez por ano, já que pessoas e funções de acesso podem mudar. Convém que a análise crítica periódica do usuário também seja feita para COTS.

3.7 Segurança física, lógica e integridade de dados

Convém que os procedimentos de segurança documentados autorizados pelo gerenciamento da instalação de teste estejam em vigor para a proteção de hardware, software e dados contra corrupção, modificação não autorizada ou perda. Convém que sejam implementados controles físicos e / ou lógicos apropriados, dependendo da complexidade e da criticidade de um sistema e dos requisitos da organização na qual o sistema é operado.

Métodos de controle adequados para impedir o acesso físico não autorizado ao sistema (por exemplo, hardware, equipamentos de comunicação, componentes periféricos e mídia de armazenamento eletrônico) podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria ou acesso restrito a equipamento informático (por exemplo, áreas de armazenamento de dados, interfaces, computadores, salas de servidores, etc.). Convém que a criação, alteração e cancelamento de autorizações de acesso sejam registrados. Convém que os registros de autorização sejam periodicamente revisados com base na criticidade do processo suportado pelo sistema computadorizado e em caso de mudanças organizacionais relevantes na instalação de teste.

Como a manutenção da integridade dos dados é um objetivo primário dos Princípios das BPL, convém que a gerência da instalação de teste garanta que os funcionários estejam cientes da importância da segurança de dados, dos procedimentos e recursos do sistema disponíveis para fornecer segurança apropriada e as consequências das violações de segurança. Tais características do sistema podem incluir a vigilância de rotina do acesso ao sistema, a implementação de rotinas de verificação de arquivos e relatórios de exceção e / ou tendências.

Para equipamentos não mantidos em “salas de computadores” específicas (por exemplo, computadores pessoais e terminais), convém que haja controles de acesso à área onde o hardware está localizado (por exemplo, controle de acesso a um prédio, área de laboratório ou sala específica). Onde tal equipamento estiver localizado remotamente (por exemplo, componentes portáteis e ligações de modem), podem ser tomadas medidas adicionais que convém sejam justificadas e baseadas no risco (por exemplo, controle criptográfico).

É essencial que apenas versões qualificadas e aprovadas de software estejam em uso. Qualquer introdução de dados ou software de fontes externas deve ser controlada. Esses controles podem ser fornecidos pelo sistema operacional do computador, por rotinas de segurança específicas, por rotinas incorporadas nos aplicativos ou por combinações dos itens acima. Convém que os sistemas de dados e armazenamento de documentos sejam projetados para registrar a data, hora e identidade dos operadores que entram, alteram, confirmam ou excluem dados.

Convém que o potencial de corrupção de dados por um código malicioso ou outros agentes seja abordado se for considerado necessário. Convém que medidas de segurança sejam *tomadas para garantir a integridade dos dados em caso de falha do sistema a curto e longo* prazo.

Convém que uma política de autorização adequada e bem mantida especifique os direitos de acesso lógico a domínios, computadores, aplicativos e dados. Convém que os privilégios de usuário sejam definidos para sistemas operacionais e aplicativos, e sejam adaptados conforme exigido pela organização da instalação de teste e em combinação com os requisitos de um estudo BPL em particular. Convém que os papéis e responsabilidades do pessoal que concede privilégios de usuário sejam definidos.

Convém que os privilégios de usuário dentro de um sistema computadorizado não interfiram nos requisitos de integridade de dados. Convém que as atividades de qualquer pessoal do estudo de BPL sejam rastreáveis aos privilégios e atividades do usuário dentro de todos os sistemas computadorizados relevantes e sejam refletidas nos documentos de controle de privilégio do usuário. Convém que os direitos de administrador não sejam concedidos a pessoas com potencial interesse nos dados (por exemplo, a função de laboratório 'analista' não é compatível com a função do sistema 'administrador' em um sistema de gerenciamento de dados de cromatografia). Convém que um usuário não tenha uma segunda função em um sistema específico que possa interferir nos requisitos de integridade de dados.

3.8 Gerenciamento de Incidentes

Durante a operação diária do sistema, convém que os registros sejam mantidos de quaisquer problemas ou inconsistências detectadas e qualquer ação corretiva tomada. Convém que o diretor de estudo, a gerência da instalação de teste, a garantia da qualidade e, se apropriado, o patrocinador sejam informados sobre os incidentes que exigem ação corretiva. O diretor de estudo é responsável por definir a criticidade dos incidentes e por avaliar o impacto no estudo. Convém que a causa raiz de um incidente que requer ação corretiva seja identificada e forme a base de ações corretivas e preventivas. Convém que a prioridade para ações corretivas e preventivas seja determinada. Convém que seja possível rastrear todos os incidentes que exigem ação corretiva informada para um sistema computadorizado aos estudos BPL afetados e vice-versa.

Convém que os registros de incidentes sejam mantidos com a documentação do sistema e periodicamente arquivados. Convém que os registros de incidentes sejam arquivados e armazenados com a documentação relevante do sistema (validação), pois os relatórios de incidentes são necessários para monitoramento e análise crítica periódica. Convém que a gerência da instalação de teste tenha o gerenciamento de incidentes interfaceado ou integrado ao gerenciamento de alterações, gerenciamento de configuração, revisão periódica e treinamento. Convém que a revisão de incidentes faça parte de uma avaliação periódica do sistema.

3.9 Assinatura Eletrônica

Registros eletrônicos podem ser assinados eletronicamente com a aplicação de uma assinatura eletrônica.

Espera-se que as assinaturas eletrônicas:

a) tenham as mesmas consequências legais que uma assinatura manuscrita, pelo menos dentro dos limites da instalação de teste;
b) estejam permanentemente vinculadas ao(s) respectivo(s) registro(s);
c) incluam a hora e a data em que foram aplicadas; e
d) permitam a identificação do signatário e o significado da assinatura.

Convém que uma função de assinatura eletrônica de um sistema computadorizado seja abordada nos requisitos do sistema e validada e descrita nos procedimentos do sistema. Convém que a gerência da instalação de teste tenha identificado os registros que requerem uma assinatura escrita à mão ou uma assinatura eletrônica. É uma decisão da gerência da instalação de teste confiar em uma função de assinatura eletrônica se outros meios forem possíveis (por exemplo, impressão e assinatura manual). Convém que o procedimento aplicado seja descrito adequadamente.

Convém que a gerência da instalação de teste assegure o estabelecimento de uma política de assinatura eletrônica, a fim de garantir o uso adequado e a manutenção das funções de assinatura eletrônica de um sistema computadorizado. Convém que o pessoal autorizado a assinar eletronicamente seja claramente identificado por nome e vinculado por nome à política de assinatura eletrônica. Convém que o papel de uma pessoa em um estudo BPL seja refletido pelo significado da assinatura eletrônica correspondente aplicada por um sistema computadorizado relevante do estudo e seja rastreável à política de autorização do sistema. Pode ser necessário adaptar o conceito de autorização de um sistema computadorizado para estudar requisitos específicos.

Convém que a gerência da instalação de teste assegure que a assinatura eletrônica seja equivalente à assinatura manuscrita e sua autenticidade seja indiscutível, pelo menos, dentro dos limites da instalação de teste ou do local de teste. Convém que a redigitação de senha seja considerada como um requisito mínimo para uma assinatura eletrônica. Convém que o acionamento de uma tecla de função por uma pessoa conectada a um sistema não seja considerado uma assinatura eletrônica.

Convém que os metadados que estão associados ao registro assinado eletronicamente sejam claramente identificados (por exemplo, configurações de método e configuração do sistema, se relevante para o resultado analítico assinado eletronicamente etc.). Convém que a função de assinatura do sistema computadorizado garanta a prontidão do *link* entre o registro assinado eletronicamente e os metadados de suporte. Convém que não seja possível para o usuário alterar uma assinatura eletrônica aplicada nem o *link* para os metadados associados. Se ocorrer uma alteração em um registro assinado eletronicamente ou nos metadados de suporte, convém que isso seja explicado (eletronicamente) e datado pela pessoa responsável pela alteração. Convém que o impacto da alteração em um registro assinado eletronicamente ou nos metadados de suporte da assinatura eletrônica seja avaliado, pois a alteração invalida a assinatura eletrônica.

A gerência da instalação de teste pode aplicar um procedimento “em meio físico” para assinar registros que são impressos a partir do sistema eletrônico. Deve-se observar que as impressões em papel de um registro eletrônico podem não conter todas as informações necessárias para reconstruir totalmente as atividades ou fornecer o significado completo dos dados. Certos metadados de suporte relevantes para o registro impresso / assinado podem ser mantidos eletronicamente em uma solução híbrida. Convém que o uso de tal sistema híbrido seja totalmente explicado nos procedimentos das instalações e justificado por meio de avaliação de risco. Com base em uma avaliação de risco, convém que a impressão seja feita com uma compreensão clara do processo e das informações que não serão capturadas na impressão. Convém que a solução híbrida seja descrita claramente para identificar todos os registros eletrônicos adicionais ou metadados de suporte que são representados pela versão impressa e assinada de um registro. Convém que um sistema apropriado para o controle de versão garanta a prontidão da ligação entre o registro impresso / assinado e os registros mantidos eletronicamente. Convém que seja possível o acesso a registros modificados ou substituídos para rastreabilidade de alterações e documentação de resultados inválidos. No entanto, convém que esses registros sejam excluídos do uso rotineiro. Se um conjunto completo de registros eletrônicos e seu análogo impresso forem mantidos em paralelo, convém que a gerência da instalação de teste especifique o tipo de registro regulado para aplicar o procedimento de controle apropriado (por exemplo, se o conjunto completo de informações de um sistema analítico for impresso e mantido eletronicamente em paralelo, convém que se defina qual conjunto de informações é o regulado).

3.10 Aprovação de dados

Se um procedimento incluir um processo de aprovação eletrônica de dados, convém que a funcionalidade de aprovação de dados seja incluída como parte da validação do sistema. Convém que o processo de aprovação seja descrito nos procedimentos das instalações e ser realizado eletronicamente no sistema.

3.11 Arquivamento

Com relação ao arquivamento, este documento de recomendação suplementa o Documento Consultivo número 15 da OCDE “Estabelecimento e Controle de Arquivos que Operam em Conformidade com os Princípios das BPL”.

Quaisquer dados relevantes para BPL podem ser arquivados eletronicamente. Convém que os Princípios de BPL para arquivamento sejam aplicados de maneira consistente a dados eletrônicos e não eletrônicos. Portanto, é importante que os dados eletrônicos sejam armazenados com os mesmos níveis de controle de acesso, indexação e "recuperação" expedita que os dados não eletrônicos.

A visualização de registros eletrônicos sem a possibilidade de alteração ou exclusão dos registros eletrônicos arquivados ou de replicação dentro de um sistema computadorizado ou para outro sistema computadorizado não constitui “recuperação” de registros. Somente quando existir a possibilidade de alteração ou exclusão do registro arquivado, deve ser considerado acesso, retirada, “recuperação” ou remoção de registros e materiais. Convém que o arquivista seja capaz de controlar a atribuição de acesso "somente visualização" aos dados eletrônicos arquivados, a fim de verificar se os requisitos para os dados arquivados são atendidos.

Convém que os dados eletrônicos sejam acessíveis e legíveis, e sua integridade mantida, durante o período de arquivamento. Se uma solução híbrida for escolhida (ou seja, dados “baseados em papel” e dados eletrônicos mantidos em paralelo), convém que a gerência da instalação de teste especifique os registros regulamentados para relevância no arquivamento.

Convém que o arquivamento eletrônico seja considerado como um procedimento independente o qual convém seja validado apropriadamente. Convém que uma avaliação de risco seja aplicada ao projetar e validar o procedimento de arquivamento. Convém que sistemas de hospedagem e formatos de dados relevantes sejam avaliados quanto à acessibilidade, legibilidade e influências na integridade dos dados durante o período de arquivamento. Pode ser necessário considerar o arquivamento de dados eletrônicos em um formato aberto que seja independente do formato de arquivo proprietário, por exemplo, de um fabricante de instrumentos. Onde a conversão de dados é necessária, os requisitos da seção 2.8 se aplicam. O arquivista, que detém a responsabilidade exclusiva, pode delegar tarefas durante o gerenciamento de dados eletrônicos a pessoal qualificado ou processos automatizados (por exemplo, controle de acesso). Para funções e responsabilidades no processo de arquivamento, consulte o Documento Consultivo número 15 da OCDE sobre BPL (NIT-Dicla-072).

Convém que os procedimentos sejam implementados para garantir que a integridade a longo prazo dos dados armazenados eletronicamente não seja comprometida. Se a mídia de dados, formatos de dados, hardware ou software de sistemas de arquivamento (não os sistemas de coleta de dados) mudarem durante o período de arquivamento, convém que a gerência da instalação de teste garanta que não haja influência negativa na acessibilidade, legibilidade e integridade dos dados arquivados. Convém que a habilidade contínua de recuperar os dados seja assegurada e testada. Onde problemas com acesso de longo prazo aos dados são vislumbrados ou quando os sistemas computadorizados precisam ser desativados, convém que procedimentos para assegurar a legibilidade continuada dos dados sejam estabelecidos. Isso pode, por exemplo, incluir a produção de cópias impressas ou a conversão de dados em um formato diferente ou a transferência de dados para outro sistema. Se a migração de dados, incluindo a conversão para um formato de dados ou impressão diferente, for relevante, convém que os requisitos deste guia para migração de dados sejam atendidos. Convém que sejam considerados a avaliação de riscos, o controle de alterações, o gerenciamento de configuração e o regime de testes, como procedimentos padrão relevantes quando são requeridas alterações no sistema de arquivamento. Como convém que o conteúdo e o significado de quaisquer dados eletrônicos sejam preservados durante o período de arquivamento, convém que o pacote completo de informações seja identificado e arquivado (por exemplo, dados brutos, metadados necessários para entender corretamente o significado de um registro ou para reconstruir sua origem, assinaturas eletrônicas, trilhas de auditoria, etc.).

Se um registro assinado eletronicamente for arquivado eletronicamente, convém que sua integridade seja assegurada pelo período de tempo relevante. Convém que a verificação da integridade do registro assinado, os metadados de apoio e a assinatura eletrônica sejam possíveis e submetidos à avaliação dentro do período de arquivamento. Convém que a periodicidade da avaliação seja justificada pelo gerenciamento da instalação de teste com base na avaliação de risco.

No relatório do estudo, convém que o diretor do estudo identifique todos os dados eletrônicos relevantes para as BPL que estão sujeitos a arquivamento eletrônico e a localização do arquivo eletrônico.

Convém que quaisquer dados mantidos em suporte a sistemas computadorizados relevantes, como código-fonte, desenvolvimento, validação, operação, manutenção e registros de monitoramento, sejam mantidos pelo menos enquanto houver registros de estudos associados a esses sistemas.

Convém que nenhum dado armazenado eletronicamente seja destruído sem a autorização da gerência da instalação de teste e, quando aplicável, do patrocinador e sem que haja a documentação relevante.

3.12 Continuidade de negócios e recuperação de desastres

Convém que sejam tomadas precauções para garantir a continuidade do apoio a sistemas computadorizados que são utilizados para processos relevantes às BPL no caso de uma falha do sistema (por exemplo, uma introdução manual de dados ou um sistema computadorizado alternativo). Convém que o tempo necessário para pôr em prática os arranjos alternativos se baseie numa avaliação de riscos que seja adequada a um determinado sistema e ao processo empresarial que apoia. Convém que esses arranjos sejam adequadamente documentados e testados.

Convém que haja procedimentos em vigor que descrevam as medidas a tomar em caso de falha parcial ou total de um sistema computadorizado. As medidas podem variar da redundância de hardware planejada até a transição para um sistema alternativo. Todos os planos de contingência precisam ser bem documentados e validados e convém que garantam a continuidade da integridade dos dados e que o estudo não seja comprometido de forma alguma. Convém que o pessoal BPL esteja ciente desses planos de contingência.

Os procedimentos para a recuperação de um sistema computadorizado podem depender da criticidade do sistema, mas é essencial que as cópias originais ou de backup de todos os softwares na versão relevante para o sistema computadorizado validado sejam mantidas, garantidas ou disponibilizadas pelo acordo de nível de serviço. Se os procedimentos de recuperação implicarem alterações no hardware ou no software, os requisitos de validação deste documento serão aplicados.

Quando for aplicado um procedimento alternativo de captura de dados, se os dados gravados manualmente forem inseridos posteriormente no computador, convém que ele seja claramente identificado como tal. Convém que o processo de entrada de dados seja validado e haja uma declaração de que os dados entrados são equivalentes aos dados brutos gravados manualmente. Convém que os dados brutos registrados manualmente sejam mantidos como o registro original e arquivados como tal. O período de retenção total dos dados brutos gravados manualmente é necessário. Convém que procedimentos alternativos de backup sirvam para minimizar o risco de perda de dados e garantir que esses registros alternativos sejam mantidos.

4 FASE DE DESATIVAÇÃO

A desativação do sistema deve ser considerada como uma fase do seu ciclo de vida. Convém que seja planejada, baseada em riscos e documentada. Se a migração ou o arquivamento de dados relevantes para as BPL for necessário, convém que os riscos para os dados sejam mitigados e os requisitos desta diretriz se aplicam.

5 REFERÊNCIAS

"Good Practices for Computerised Systems in Regulated GxP Environments" [effective 25.09.2007] PIC/S PI 11-3

"Computerised Systems used in Nonclinical Safety Assessment: Current Concepts in Validation and Compliance" [published 2008, DIA, Red Apple II]."

"GAMP 5 - A Risk Based Approach to Compliant GxP Computerised Systems" ISPE Good Automated Manufacturing Practice © ISPE 2007

"Establishment and Control of Archives that Operate in Compliance with the Principles of GLP", [ENV/JM/MONO(2007)10], OECD GLP Advisory Document Number 15.

The rules governing medicinal products in the European Union. Volume 4 - Guidelines for good manufacturing practices for medicinal products for human and veterinary use. Annex 15 to the EU Guide of GMP "Qualification and Validation" October 2015.

Apêndice 1: Funções e responsabilidades

Função	Responsabilidade
Proprietário do processo de negócios	O indivíduo ou organização responsável por fornecer os recursos para um processo de negócios (por exemplo, um estudo pré-clínico)
Pessoal de TI	Pessoal envolvido na compra, instalação e manutenção de um sistema computadorizado. A responsabilidade inclui, por exemplo, operar e manter o hardware e o software, realizar backups, resolver problemas, etc.
Pessoal	Qualquer pessoa envolvida na validação, operação ou suporte de um sistema computadorizado.
Garantia da qualidade	(*ver* ENV/MC/CHEM(98)17 “OECD Principles of GLP”, (1997), 2.2.8. – NIT-Dicla-035, 2.2.8 do Anexo)
Patrocinador	(*ver* ENV/MC/CHEM(98)17 “OECD Principles of GLP”, (1997), 2.2.5. – NIT-Dicla-035, 2.2.5 do Anexo)
Diretor de estudo	(*See* ENV/MC/CHEM(98)17 “OECD Principles of GLP”, (1997), 2.2.6. – NIT-Dicla-035, 2.2.6 do Anexo)
Fornecedor	Terceiros (Terceira parte), fornecedores, departamentos internos de TI, provedores de serviços, incluindo provedores de serviços hospedados, etc.
Proprietário do sistema / proprietário de TI	O indivíduo que é responsável pela disponibilidade, suporte e manutenção de um sistema e pela segurança dos dados que residem nesse sistema. O proprietário do sistema é responsável por garantir que o sistema computadorizado seja suportado e mantido de acordo com os procedimentos aplicáveis. O Proprietário do Sistema atua em nome da gerência da instalação de teste. Os sistemas globais de TI podem ter um proprietário de sistema global e proprietários de sistemas locais para gerenciar a implementação local (ver GAMP 5).
Gerência da instalação de teste	(*ver* ENV/MC/CHEM(98)17 “OECD Principles of GLP”, (1997), 2.2.3. – NIT-Dicla-035, 2.2.3 do Anexo).
Usuário	O pessoal que opera o sistema computadorizado em um estudo de BPL.
Diretor de Validação	Uma pessoa designada responsável por um projeto de validação.

Apêndice 2: Glossário

Termo	Definição
Critério de aceitação	Os critérios documentados que convém serem cumpridos para concluir com sucesso uma fase de teste ou para atender aos requisitos de entrega.
Teste de aceitação	Teste formal de um sistema computadorizado em seu ambiente operacional previsto para determinar se todos os critérios de aceitação da instalação de teste foram atendidos e se o sistema é aceitável para uso operacional.
Conceito de autorização	Um conceito de autorização é um procedimento formal para definir e controlar direitos de acesso e privilégios em um sistema computadorizado.
Back-up	Disposições feitas para a recuperação de arquivos de dados ou software, para o reinício do processamento ou para o uso de equipamentos de computador alternativos após uma falha do sistema ou desastre.
Controle de alterações	Avaliação e documentação contínuas das operações e alterações do sistema para determinar se um processo de validação é necessário após quaisquer alterações no sistema computadorizado.
Gerenciamento de alterações	O gerenciamento de alterações é o processo de controle do ciclo de vida de alterações.
Produto comercial pronto para uso (COTS)	O software ou hardware é um produto pronto para uso comercial (COTS) se fornecido por um fornecedor ao público em geral, se disponível em várias cópias idênticas, e se implementado pela gerência da instalação de teste sem ou com alguma personalização.
Sistema computadorizado	“Um sistema computadorizado é uma função (processo ou operação) integrada a um sistema de computador e executada por pessoal treinado. A função é controlada pelo sistema do computador. O sistema computadorizado de controle é composto de hardware e software. A função controlada é composta de equipamentos a serem controlados e procedimentos operacionais executados pelo pessoal. ”PIC / S PI 11-3“ Boas Práticas para Sistemas Computadorizados em Ambientes Regulados em BPx”
Configuração	Uma configuração é um arranjo de unidades funcionais e pertence à escolha de hardware, software e documentação. Afeta a função e o desempenho do sistema.
Gerenciamento de configuração	O gerenciamento de configuração compreende as atividades necessárias para definir com precisão um sistema computadorizado em um determinado momento.

Continua

Função controlada	É um processo ou operação integrada a um sistema de computador e executada por pessoas treinadas.
Ações corretivas e preventivas	O conceito de ações corretivas e preventivas enfoca a investigação sistemática das causas-raiz dos problemas ou riscos identificados, na tentativa de prevenir sua recorrência ou impedir sua ocorrência.
Sistema computadorizado customizado	Um sistema computadorizado projetado individualmente para se adequar a um processo de negócios específico.
Dados (dados derivados)	Os dados derivados dependem de dados brutos e podem ser reconstruídos a partir de dados brutos (por exemplo, concentrações finais calculadas por uma planilha que depende de dados brutos, tabelas de resultados conforme resumidas por um LIMS, etc.).
Dados (dados brutos)	Dados (dados brutos) podem ser definidos como atributos mensuráveis ou descritivos de uma entidade, processo ou evento físico. Os Princípios das BPL definem dados brutos como todos os registros e documentação de laboratório, incluindo dados inseridos diretamente em um computador através de uma interface de instrumento automática, que são os resultados das principais observações e atividades em um estudo e que são necessários para a reconstrução e avaliação do relatório daquele estudo.
Aprovação de dados	A aprovação de dados significa bloquear os dados após a coleta, verificação e, por exemplo, a transformação para tornar os dados adequados para uso em registros.
Captura de dados	Captura de dados são ações que normalmente ocorrem para planejar, coletar e verificar dados e elementos de metadados associados.
Migração de dados	Migração de dados é a atividade de, por exemplo, transportar dados eletrônicos de um sistema de computador para outro, transferindo dados entre meios de armazenamento ou simplesmente a transição de dados de um estado para outro [por exemplo, conversão de dados para um formato diferente]. O termo "dados" refere-se a "dados brutos", bem como "metadados".
Gerenciamento de desvio (incidente)	O gerenciamento de desvio (incidente) compreende as atividades para identificar, documentar, avaliar e, quando apropriado, investigar a fim de determinar as causas originárias do desvio (incidente) para evitar a recorrência.
Registro eletrônico	Qualquer combinação de texto, gráficos, dados, áudio, imagens ou outras representações de informações em formato digital criadas, modificadas, mantidas, arquivadas, recuperadas ou distribuídas por um sistema de computador.

Continua

Assinatura eletrônica	Uma medida eletrônica que pode ser substituída por uma assinatura manuscrita ou iniciais com a finalidade de significar aprovação, autorização ou verificação de entradas de dados específicas.
Solução híbrida (sistema)	Coexistência de componentes em papel e registro eletrônico e assinatura. Exemplos incluem combinações de papel (ou outras mídias não eletrônicas) e registros eletrônicos, registros em papel e assinaturas eletrônicas, ou assinaturas manuscritas vinculadas a registros eletrônicos.
Ciclo de vida	Uma abordagem para o desenvolvimento de sistemas computadorizados, que começa com a identificação dos requisitos do usuário, continua por meio do design, integração, qualificação, validação do usuário, controle e manutenção, e termina quando o sistema é retirado de uso.
Modelo de ciclo de vida	Um modelo de ciclo de vida descreve as fases ou atividades de um projeto desde a concepção até o produto ser retirado de uso. Ele especifica as relações entre as fases do projeto, incluindo critérios de transição, mecanismos de feedback/realimentação, marcos, linhas de base, revisões e entregas.
Metadado	Metadados são dados acerca de dados. Metadados é qualquer informação usada para a identificação, descrição e relacionamentos de registros eletrônicos ou seus elementos. Os metadados fornecem significado aos dados, fornecem contexto, definem estrutura e permitem a capacidade de recuperação em todos os sistemas e a usabilidade, autenticidade e capacidade de auditoria ao longo do tempo.
Sistema operacional	Um programa ou conjunto de programas, rotinas e sub-rotinas que controlam o funcionamento de um computador. Um sistema operacional pode fornecer serviços como alocação de recursos, agendamento, controle de entrada / saída e gerenciamento de dados.
Componentes auxiliares periféricos	Qualquer instrumentação interfaceada, ou componentes auxiliares ou remotos, como impressoras, modems e terminais, etc.
Processo	Um processo é uma série de ações projetadas para produzir um resultado especificado. Um processo define as atividades necessárias e as responsabilidades do pessoal designado para realizar o trabalho. Ferramentas e equipamentos apropriados, procedimentos e métodos definem as tarefas e relações entre as tarefas.
Qualificação	Ação de provar que qualquer equipamento, incluindo o software, funciona corretamente e é adequado ao seu propósito.
Normas técnicas reconhecidas	Normas conforme publicadas por organizações nacionais ou internacionais de definição de normas (ISO, IEEE, ANSI, etc.)

Continua

Registros regulamentados	É um registro requerido por regulamentos BPL de ser mantido ou submetido a órgãos regulamentadores. Um registro regulamentado pode ser mantido em formatos diferentes, por exemplo, eletrônico, em papel ou ambos.
Risco	Combinação da probabilidade de ocorrência de danos e a gravidade desse dano.
Análise de risco	Estimativa do risco associado aos perigos identificados. É o processo qualitativo ou quantitativo de vincular a probabilidade de ocorrência e gravidade dos danos.
Avaliação de risco	A avaliação de risco consiste na identificação de perigos e na análise e avaliação dos riscos associados à exposição a esses perigos. A avaliação de risco é seguida pelo controle de risco.
Controle de risco	Processo através do qual decisões são tomadas e medidas de proteção são implementadas para reduzir riscos, ou manter riscos dentro de níveis especificados.
Identificação de risco	Um uso sistemático de informações para identificar perigos referentes à questão de risco ou descrição do problema. As informações podem incluir dados históricos, análises teóricas, opiniões informadas e as preocupações das partes interessadas.
Gerenciamento de risco	O conceito de gestão do risco da qualidade é descrito como “um processo sistemático” para avaliação, controle, comunicação e revisão de riscos à qualidade.
Mitigação de risco	Ações tomadas para diminuir a probabilidade de ocorrência de danos e a gravidade desse dano.
Segurança	A proteção de hardware e software de computador contra acesso acidental ou mal-intencionado, uso, modificação, destruição ou divulgação. A segurança também se refere ao pessoal, dados, comunicações e à proteção física e lógica das instalações de computadores.
Software	Um programa adquirido ou desenvolvido, adaptado ou adaptado aos requisitos das instalações de teste com a finalidade de controlar processos, coleta de dados, manipulação de dados, relatório de dados e / ou arquivamento.
Código fonte	Um programa de computador original expresso em forma legível (linguagem de programação) que deve ser traduzido em formato legível por máquina antes de poder ser executado pelo computador.
Especificações de requisitos do usuário	As especificações de requisitos do usuário definem por escrito o que o usuário espera que o sistema computadorizado possa fazer.
Análise crítica do usuário	Análise crítica dos direitos e privilégios de acesso do usuário
Validação	Ação de provar que um processo leva aos resultados esperados. A validação de um sistema computadorizado requer garantia e demonstração da adequação ao seu propósito.
Estratégia de validação	A estratégia de validação define em um documento o processo e todas as atividades relacionadas a cada estágio de validação do sistema computadorizado.