# 1. Índice

[1. Índice 1](#_Toc163235213)

[2. Objetivo 2](#_Toc163235214)

[3. Definições e Abreviações 2](#_Toc163235215)

[4. Responsabilidades 3](#_Toc163235216)

[5. Procedimento 4](#_Toc163235217)

[5.1. Considerações iniciais 4](#_Toc163235218)

[5.2. Ciclo de Vida de Dados 6](#_Toc163235219)

[**5.3. Prevenção de Lapsos de Integridade de Dados** 11](#_Toc163235220)

[5.4. Requerimentos para Registros em Papel 15](#_Toc163235221)

[**5.5. Requerimentos para Registros Eletrônicos** 17](#_Toc163235222)

[**5.6. Requerimentos para Registros e Sistemas Híbridos** 17](#_Toc163235223)

[**5.7. Registros e suas Cópias Verdadeiras** 18](#_Toc163235224)

[**5.8. Não conformidade dos Dados** 20](#_Toc163235225)

[**5.9. Garantia de Integridade de Dados para Atividades Terceirizadas** 21](#_Toc163235226)

[6. Referências 21](#_Toc163235227)

[7. Histórico 22](#_Toc163235228)

[8. Fluxograma 22](#_Toc163235229)

[9. Anexos 23](#_Toc163235230)

[10. VALIDAÇÃO 25](#_Toc163235231)

# 2. Objetivo

Estabelece os requisitos de integridade de dados gerados. Também define as atividades que irão garantir a integridade, consistência e precisão de todos os dados (eletrônicos e impressos) gerados nas áreas e instalações com impacto em Boas Práticas (GxP). Os dados devem ser gerados de acordo com os princípios do ALCOA+ (atribuíveis, legíveis, contemporâneos, originais, precisos, contemporâneos, disponíveis, completos e consistentes).

# 3. Definições e Abreviações

3.1. Definições

Integridade de dados: é a extensão em que todos os dados são completos, consistentes e precisos durante todo o ciclo de vida dos dados e produtos relacionados. Os dados devem ser de acordo com o ALCOA+, onde:

A - Atribuível à pessoa que gera os dados

L - Legível e permanente

C - Contemporâneo

O - Registro original (ou 'cópia verdadeira')

A - preciso

+ - contemporâneos, disponíveis, completos e consistentes

Trilha de auditoria: uma trilha de auditoria é um processo que captura detalhes como acréscimos, exclusões ou alterações de informações em um registro, em papel ou eletrônico, sem obscurecer ou sobrescrever o registro original. Uma trilha de auditoria facilita a reconstrução da história de tais eventos relativos ao registro independentemente de sua mídia, incluindo o “quem, o quê, quando e por quê” da ação.

Backup: uma cópia dos dados atuais, metadados e configurações do sistema mantidos para fins de recuperação de desastres

Ciclo de vida de dados: o ciclo de vida de dados cobre todas as fases da vida dos dados (incluindo dados brutos), desde a geração inicial e gravação até o processamento (incluindo transformação ou migração), uso, retenção de dados brutos, arquivamento / recuperação e destruição.

Processamento de dados: seqüência de operações realizadas em dados para extrair, apresentar ou obter informações em um formato definido.

Revisão de dados: deve haver um procedimento que descreva o processo de revisão e aprovação dos dados. A revisão de dados também deve incluir uma revisão de metadados relevantes, incluindo trilhas de auditoria. A revisão deve ser baseada nos dados originais ou em uma cópia verdadeira.

Registro original: dados como o arquivo ou formato em que foram gerados originalmente, preservando a integridade (precisão, integridade, conteúdo e significado) do registro, por exemplo, registro original em papel de observação manual ou arquivo eletrônico de dados brutos de um sistema computadorizado. Esses dados devem permitir a reconstrução completa das atividades que resultam na geração dos dados.

Dados brutos: registros e documentação originais, retidos no formato que eles geraram originalmente (ou seja, papel ou eletrônico), ou como uma "cópia verdadeira". Os dados brutos devem ser registrados contemporaneamente e com precisão por meios permanentes.

Dados regulamentados: Dados usados ​​para fins GxP, exigidos pelos regulamentos GxP. No contexto deste documento, GxP se refere apenas à Fabricação e Distribuição

3.2. Abreviações.

GxP – Sigla em inglês para Boas Práticas de x = Fabricação, Laboratórios e Distribuição.

# 4. Responsabilidades

* Fornecer orientação e apoio para a implementação dos requerimentos de Integridade de Dados;
* Avaliar a eficácia e conformidade do programa de integridade de dados por meio da auditoria interna.
* Garantir que os funcionários sejam devidamente treinados e informados sobre os requisitos de integridade de dados;
* Garantir que os princípios e padrões de integridade de dados sejam mantidos, incluindo a implantação de sistemas para evitar falhas de integridade de dados;
* Garantir a adesão a esta diretriz por meio de monitoramento periódico e auditorias internas
* Garantir a conformidade com este procedimentos.
* Gerar dados confiáveis, precisos, completos e contemporâneos.
* Ser responsável pela integridade dos dados, incluindo geração, registro, relatório e arquivo nas suas próprias atividades.
* Ser transparente e aberto para relatar quaisquer desvios, erros, omissões e resultados inadequados em todos os níveis da organização.

# 5. Procedimento

## 5.1. Considerações iniciais

5.1.1. É essencial que haja um processo de gerenciamento de integridade de dados em vigor.

5.1.2. O processo de integridade de dados deve garantir que:

* Os dados são completos, consistentes, precisos, confiáveis ​​e confiáveis ​​e que essas características dos dados são mantidas durante todo o ciclo de vida dos dados,
* Os dados devem ser coletados e mantidos de forma segura, de forma que sejam atribuíveis, legíveis, registrados contemporaneamente, originais ou uma cópia verdadeira e precisa
* A integridade deve ser garantida por meio de sistemas adequados de gestão de riscos e qualidade, incluindo a adesão aos princípios científicos e às boas práticas de documentação.

5.1.3. ALCOA+: Atributos de integridade de dados

5.1.3.1. Os registros regulamentados representados em papel, híbrido e eletrônico devem atender aos requisitos da ALCOA+:

* Atribuível: Atribuível à pessoa que gera os dados. As informações devem ser capturadas identificando a fonte dos dados. Por exemplo: Quem executou a ação e quando? Se um registro for alterado, quem o fez e por quê?. Isso também se aplica a alterações feitas em registros, incluindo correções, exclusões, alterações, etc.
* Legível: as informações do registro devem ser legíveis e permanentes. Os dados devem ser gravados permanentemente em um meio durável, acessível durante todo o ciclo de vida dos dados e sempre legíveis.
* Contemporâneo: As evidências de ações, eventos ou decisões devem ser registradas no momento em que ocorrem. Essa documentação deve servir como um atestado preciso do que foi feito, ou do que foi decidido e por quê.
* Original (ou cópia verdadeira que preserva o conteúdo ou significado): O registro original pode ser descrito como a primeira captura da informação, seja ela gravada em papel (estática) ou eletronicamente (dinâmica). Todos os dados capturados originalmente devem ser retidos, em vez de substituídos ou excluídos. Os dados devem ser usados ou apresentados como quando foram criados.
* Exatos: os resultados e registros devem ser corretos e precisos. Sem erros e sem edição sem alterações documentadas / entradas de trilha de auditoria por pessoal autorizado.
* Completo: todas as informações críticas para recriar um evento são importantes ao tentar entendê-lo. O nível de detalhe necessário para que o conjunto de informações seja considerado completo dependeria da criticidade das informações. Um registro completo de dados gerados eletronicamente inclui metadados relevantes.
* Consistente: Boas Práticas de Documentação devem ser aplicadas em todo o processo, sem exceção, incluindo desvios que possam ocorrer durante o processo. Isso inclui a captura de todas as alterações feitas nos dados
* Duradouro: Os registros devem existir para todo o período durante o qual podem ser necessários. Isso significa que eles precisam permanecer intactos e acessíveis como um registro indelével / durável.
* Disponível: os registros devem estar disponíveis para revisão a qualquer momento durante o período de retenção exigido, acessíveis em um formato legível para todo o pessoal aplicável que é responsável por sua revisão, seja para decisões de liberação de rotina, investigações, tendências, relatórios anuais, auditorias ou inspeções. Eles devem ser criados e retidos por um período de tempo definido na norma apropriada.

## 5.2. Ciclo de Vida de Dados

5.2.1. Considerações:

5.2.1.1. O ciclo de vida dos dados descreve o fluxo de dados em todas as suas fases, conforme item 9, fluxograma. O princípio ALCOA+ deve ser aplicado em todo o ciclo de vida dos dados.

5.2.1.2. O ciclo de vida dos dados deve ser documentado para garantir que os riscos à integridade dos dados sejam identificados e mitigados.Todos os dados GxP relevantes adquiridos, processados ou calculados devem ser retidos em um ambiente seguro, em mídia duradoura e devem estar disponíveis em forma legível para análise ou auditoria para todo o período de retenção aplicável.

5.2.2. Geração / Gravação:

* Todos os documentos e registros eletrônicos devem ter um número de identificação único (incluindo o número da versão) e devem ser verificados, aprovados, assinados e datados.
* O uso de documentos não controlados e práticas de registro temporário é proibido.
* O documento deve fornecer espaço suficiente para entradas manuais de dados e deixar claro quais dados devem ser inseridos.
* Os documentos e registros eletrônicos devem ser armazenados de forma a garantir o controle de versão apropriado.
* A cópia original (em cópia papel ou eletrônica) deve ser impedida de alterações não autorizadas ou inadvertidas.
* A captura e o registro de dados devem ser atribuíveis, legíveis, contemporâneos, originais, precisos e completos

5.2.3. Processamento:

* Os dados são processados para obter e apresentar informações no formato necessário.
* A transferência manual de dados deve ser evitada sempre que possível, as interfaces usadas para transferir dados entre dois sistemas eletrônicos devem ser validadas.
* As versões atualizadas devem ser distribuídas em tempo hábil.
* Documentos mestre obsoletos e arquivos devem ser arquivados e seu acesso restrito.
* A emissão do documento deve ser controlada por procedimentos escritos, incluindo os seguintes controles: Uso de um carimbo seguro ou outro sistema apropriado, garantir que apenas a versão aprovada atual esteja disponível para uso, a cópia deve ser única, deve haver reconciliação e manutenção de cópias distribuídas
* A emissão do documento em sistemas computadorizados deve ser controlada por procedimentos aprovados, incluindo o seguinte:

- Os controles de acesso do usuário, tanto físicos quanto eletrônicos, devem ser configurados para proibir o acesso não autorizado, alteração e exclusão de dados.

- IDs de login e senhas individuais devem ser configuradas e atribuídas a todos os funcionários que precisam acessar o registro.

- Credenciais de login compartilhadas não são permitidas para rastreabilidade ao indivíduo que realizou a atividade.

- A entrada de dados e alterações nos registros computadorizados devem ser feitas apenas por pessoal autorizado. A lista de indivíduos autorizados e seus privilégios de acesso para cada sistema eletrônico em uso deve ser mantida.

- O acesso do administrador aos sistemas de computador usados para executar aplicativos deve ser controlado. Os usuários em geral não têm acesso a aspectos críticos do software, por exemplo, relógios do sistema, funções de exclusão de arquivo, etc.

- Os administradores do sistema devem ser independentes dos usuários que executam a tarefa, e não devem ter envolvimento ou interesse no resultado dos dados gerados ou disponíveis no sistema eletrônico. Indivíduos fora das organizações de qualidade e produção (por exemplo, administradores de tecnologia de negócios) podem servir como administradores de sistema e ter níveis de permissão aprimorados. Pode ser permitido a uma pessoa nomeada manter o acesso como administrador do sistema; entretanto, nesses casos, o acesso de administrador não deve ser usado para realizar operações de rotina e o usuário deve possuir um segundo acesso restrito para realizar operações de rotina.

- Para adicionar novos usuários, novos privilégios remover usuários, uma solicitação deve ser emitida, aprovada e encaminhada ao administrador do sistema informatizado de forma rastreável de acordo com o procedimento aplicável

6.2.4. Verificação, Uso e Reporte:

* A verificação, o reporte e o uso de dados devem ser realizados de acordo com processos definidos e verificados e procedimentos aprovados.
* Os registros das etapas críticas do processo devem ser:

- Revisado / testemunhado por pessoal qualificado designado de acordo com os procedimentos aprovados (por exemplo: supervisor de produção ou designado) no momento da ocorrência das operações.

- Revisado por uma pessoa autorizada antes de enviá-los para o departamento de Unidade de Qualidade.

- Revisado e aprovado pela Unidade da Qualidade de antes da liberação ou distribuição do lote produzido.

- Os registros das etapas não críticas do processo devem ser revisados de acordo com os procedimentos aprovados. A revisão deve ser realizada após a execução da tarefa / atividade e assinada ou rubricada e datada.

- A verificação de que todos os campos foram preenchidos corretamente usando os modelos atuais (aprovados) e que os dados foram comparados com os critérios de aceitação devem ser preenchidos e documentados por assinatura e data.

- Uma vez identificados, os dados críticos devem ser verificados pelo usuário para determinar se as operações foram realizadas corretamente e se alguma alteração (modificação, exclusão ou substituição) foi feita nas informações originais nos registros. Todas as alterações devem ser devidamente autorizadas.

* Todos os registros devem ser armazenados no local especificado de maneira rastreável e acessível. Os sistemas devem garantir que todos os registros GxP relevantes sejam armazenados por períodos que atendam aos requisitos
* Todos os registros devem ser protegidos de danos ou destruição por: Fogo; Líquidos e Umidade; Roedores e / ou insetos; Acesso de pessoal não autorizado, que pode tentar alterar, destruir ou substituir registros;
* As assinaturas eletrônicas usadas no lugar das assinaturas manuis devem ter controles apropriados para garantir sua autenticidade e rastreabilidade até a pessoa específica que assinou eletronicamente o registro.
* Trilhas de auditoria: As funcionalidades da trilha de auditoria para sistemas baseados em eletrônicos devem ser configuradas para capturar eventos gerais do sistema, bem como quaisquer atividades relacionadas à aquisição, exclusão, sobrescrita e alterações nos dados para fins de auditoria. Para sistemas que não estão equipados com trilhas de auditoria; ações alternativas devem ser implementadas para verificar a veracidade dos dados, por exemplo, procedimentos administrativos, verificações e controles secundários. As trilhas de auditoria devem ser verificadas durante a validação do sistema. As funcionalidades da trilha de auditoria devem estar ativadas e bloqueadas o tempo todo, por exemplo, o indivíduo envolvido na entrada e nas alterações dos dados não deve ter acesso para habilitar e desabilitar a trilha de auditoria conforme desejado. A frequência da revisão da trilha de auditoria e logs do sistema deve ser definida em procedimentos apropriados.

6.2.5. Armazenamento, Retenção e Recuperação:

* Os dados devem ser armazenados de forma segura.
* Os dados retidos devem ser originais ou uma cópia verdadeira e incluir metadados e trilhas de auditoria, quando disponíveis.
* Os dados devem estar prontamente disponíveis durante todo o período de retenção necessário.
* Os dados devem ser copiados e a restauração de dados de backup deve ser testada periodicamente.
* Os dados arquivados devem ser recuperáveis caso sejam necessários novamente no ambiente ativo.
* Armazenamento de dados deve incluir todos os dados originais, incluindo trilhas de auditoria, usando um processo seguro e validado. Se o backup dos dados for feito ou se forem feitas cópias deles, o backup e as cópias também devem ter os mesmos níveis apropriados de controles, de modo a proibir o acesso não autorizado, as alterações e a exclusão dos dados ou sua alteração. Algumas considerações adicionais para o armazenamento e backup de dados incluem:

- Cópias verdadeiras de registros eletrônicos dinâmicos podem ser feitas, com a expectativa de que todo o conteúdo (ou seja, todos os dados são incluídos) e o significado dos registros originais sejam preservados.

- As cópias de backup de rotina devem ser armazenadas em um local remoto (fisicamente separado) em caso de desastre.

- Os dados de backup devem ser legíveis pelo período definido por procedimentos regulamentares e apropriados, mesmo se uma nova versão do software foi atualizada ou substituída.

* Deve haver a possibilidade de imprimir registros legíveis e significativos de todos os dados gerados por um sistema informatizado. Se uma alteração for realizada nos registros, o sistema deve ser capaz de imprimir o registro alterado, indicando quando e como os dados originais foram alterados.

6.2.6. Destruição:

* Quaisquer documentos físicos emitidos e não utilizados devem ser destruídos.
* Os controles devem estar em vigor para garantir que os registros atuais não sejam destruídos por acidente.
* Os dados originais não devem ser destruídos ou descartados intencionalmente.
* O registro do documento destruído, quem e quando foi destruído deve ser mantido.

**5.3. Prevenção de Lapsos de Integridade de Dados**

5.3.1. Uma abordagem de gerenciamento de risco deve ser usada para evitar lapsos de integridade de dados e, consequentemente, garantir a conformidade com os princípios ALCOA+. Isso só pode ser alcançado pela aplicação de controles comportamentais, processuais e técnicos apropriados para gerenciar os riscos identificados, conforme descrito na tabela 1.

|  |  |  |
| --- | --- | --- |
| **Comportamental** | **Procedimental** | **Técnico** |
| Promovendo a cultura de responsabilidade pelo dado durante todo o seu ciclo de vida.  Treinamento de pessoal na importância dos princípios de integridade de dados.  Criação de um ambiente de trabalho que:  - Permite a visibilidade de erros, omissões e resultados atípicos (aberrantes);  - Incentiva a investigação e análise transparentes. | Estabelecimento de procedimentos para minimizar o risco potencial à integridade dos dados (por exemplo, revisão da trilha de auditoria, registro de dados, revisão e aprovação de dados, emissão de logbooks). | - Validação de sistemas informatizados para uso pretendido, qualificação de infraestrutura e equipamentos de apoio.  - Trilhas de auditoria.  - Acesso controlado a sistemas informatizados.  - Backup automatizado. |

Tabela 1

5.3.2. Cultura de Qualidade e Integridade de Dados

5.3.2.1. A qualidade é alcançada por meio de procedimentos que definem os elementos-chave necessários para garantir a confiabilidade e integridade dos dados e informações. Eles também garantem que todos os indivíduos sejam responsáveis ​​por garantir a segurança do paciente e qualidade do produto. Para tal, todos os colaboradores devem coletar, analisar, relatar e reter informações e dados de uma maneira que represente de forma precisa, verdadeira e completa o que realmente ocorreu em papel ou formato eletrônico.

5.3.2.2. Esses padrões de ética e integridade devem ser estabelecidos e conhecidos por cada funcionário e essas expectativas devem ser comunicadas de forma frequente e consistente. As políticas existentes e os elementos do sistema de qualidade, incluindo procedimentos e treinamento, garantem que o pessoal esteja ciente da importância de sua função em garantir a integridade dos dados e a implicação de suas atividades relacionadas à qualidade do produto e à segurança do paciente.

5.3.3. Gerenciamento de Riscos

5.3.3.1. O gerenciamento de risco deve ser aplicado em todo o ciclo de vida dos dados, considerando a segurança do paciente, a integridade dos dados e a qualidade do produto. A extensão dos controles procedimentais e técnicos (por exemplo, validação) e esforços e recursos relacionados devem ser proporcionais ao risco. A avaliação de risco deve considerar a criticidade dos dados, bem como o risco dos dados, conforme tabela 2 – Criticidade do Dado x Risco do Dado.

|  |  |
| --- | --- |
| **Criticidade do Dado** | **Risco do Dado** |
| A criticidade dos dados é determinada pelo impacto dos dados na tomada de decisões e na qualidade do produto.  Qual decisão os dados influenciam?  por exemplo. decisão de liberação do lote versus registros de limpeza do armazém.  Qual é o impacto na qualidade ou segurança do produto?  por exemplo. Ensaio API vs. friabilidade do comprimido | Vulnerabilidade dos dados a alteração, falsificação, exclusão, perda ou recriação involuntária ou deliberada e a probabilidade de detecção de tais ações.  Considerar:  Complexidade do processo  Métodos de geração, armazenamento e retirada de dados e sua capacidade de garantir a precisão, legibilidade e indelébilidade dos dados  Consistência do processo e grau de automação/interação humana  Subjetividade do resultado |

Tabela 2 – Criticidade do Dado x Risco do Dado

5.3.3.2. O Anexo 1 descreve as definições de criticidade de dados e exemplifica o risco de dados.

5.3.4. Revisão e Aprovação do Dado

5.3.4.1. A revisão e a aprovação dos dados devem ser baseadas em riscos e devem incluir a revisão de metadados relevantes, incluindo trilhas de auditoria. A revisão deve ser baseada em registros originais ou cópias verdadeiras.

5.3.4.2. Os procedimentos para revisão e aprovação de dados devem estar em vigor e incluir o seguinte:

* Escopo/objetivo da revisão (ou seja, o revisor deve entender o significado de sua assinatura)
* O que deve ser revisado/aprovado, por quem e quando
* Ações a serem tomadas quando forem identificados erros, discrepâncias ou omissões

5.3.4.3. A revisão de dados deve ser formalmente documentada, incluindo o resultado da revisão, por exemplo, passar, falhar, se algum problema/erro foi encontrado, etc.

5.3.4.4. Qualquer correção ou esclarecimento necessário durante o processo de revisão deve ser documentado usando boas práticas de documentação.

5.3.4.5. A revisão de dados (verificação de impressão ou outro registro eletrônico) deve ser o principal método usado para garantir a exatidão da entrada de dados. O método de verificação de dados (princípio dos 4 olhos) deve ser usado apenas quando a revisão de dados não for possível (ou seja, sem impressão disponível ou sem retenção de registros eletrônicos).

5.3.4.6. A verificação/revisão em segunda pessoa é necessária sempre que os dados são registrados manualmente, a tabela 3 abaixo apresenta orientação sobre verificação/revisão em segunda pessoa.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **Alta Criticidade de Dados** | **Média Criticidade de Dados** | **Baixa Criticidade de Dados** |
| **Exemplo** | **Gravação manual de dados sem um segundo formato controlado (por exemplo, gravação de um valor de um display, sem impressão disponível ou sem retenção de registro eletrônico)** | | | |
| **Duplo Check de Entrada de Dados** | Que ação? | Verificar à quatro olhos: Revisão completa em tempo real e revisão completa da unidade de qualidade para garantir que os requisitos sejam atendidos | Revisão completa de que os dados brutos atendem aos requisitos | Verificação geral da adesão às boas práticas de documentação, mas nenhuma verificação de precisão necessária |
| Quem? | Verificação em tempo real por uma segunda pessoa.  Revisão completa da unidade de qualidade | Revisão de uma segunda pessoa | Revisão de uma segunda pessoa |
| Quando? | Verificação em tempo real por uma segunda pessoa.  Revisão completa da unidade de qualidade antes da disposição do lote | Antes da próxima etapa crítica do processo ou antes da liberação do lote, conforme apropriado | Antes da liberação do lote ou dentro do prazo especificado nos procedimentos |
| **Exemplo** | **Transcrição de dados em um sistema eletrônico (de impressão ou outro registro eletrônico)** | | | |
| **Duplo Check de Entrada de Dados** | Que ação? | Revisão completa dos dados manuais inseridos no sistema eletrônico correspondem aos dados brutos originais da impressão ou gravação manual | | Não aplicável |
| Quem? | Supervisor ou Unidade da Qualidade | Duplo Check | Não aplicável |
| Quando? | Antes da liberação do lote (uma vez que os dados brutos originais estão disponíveis, a verificação do registro de dados não precisa ser em tempo real) | | Não aplicável |

Tabela 3

## 5.4. Requerimentos para Registros em Papel

5.4.1. Os registros em papel devem ser controlados e devem permanecer atribuíveis, legíveis, indeléveis / duráveis, contemporâneos, originais e precisos (ALCOA+) ao longo do ciclo de vida dos dados.

5.4.2. As seguintes regras para documentos criados em formato de papel devem ser aplicadas:

* Documentos e procedimentos principais são criados, revisados ​​e aprovados para uso.
* A geração, distribuição e controle de modelos usados ​​para registrar dados (mestre, logs, etc.) devem ser definidos.
* Os registros em estado inativo devem ser arquivados em locais seguros (com acesso restrito e condições ambientais adequadas) para evitar danos ou perdas, de forma que sejam facilmente rastreáveis e recuperáveis e garantam que sejam duráveis por toda a vida útil do arquivo.
* Processo controlado e rastreável para geração de cópias de trabalho de documentos para uso rotineiro, com ênfase específica em cópias de documentos, por ex. POPs estão em vigor.
* Orientação para o preenchimento de documentos em papel, especificando a identificação de operadores individuais, formatos de entrada de dados e alterações em vigor.
* Os documentos são revisados ​​rotineiramente quanto à precisão, autenticidade e integridade.
* Os processos de preenchimento, recuperação, retenção, arquivamento e eliminação de registros estão em vigor, incluindo a captura e retenção de formulários incompletos e / ou errôneos como parte do registro permanente, juntamente com a justificativa para sua substituição.
* Os dados originais são mantidos de acordo com as políticas de retenção de registros aplicáveis ​​e não são destruídos nem descartados intencionalmente.
* A integridade dos dados é mantida durante todo o ciclo de vida dos dados.

5.4.3. Emissão e reconciliação de formulários (em branco)

5.4.3.1. A entrada ou processamento de dados GxP (incluindo dados brutos) em notas adesivas, papel de rascunho ou outro formato temporário, como blocos de notas ou diários não oficiais, é estritamente proibido. Os dados GxP devem ser registrados e processados ​​em formulários controlados.

5.4.3.2. Formulários/templates para registro e/ou processamento de dados altamente críticos (por exemplo, registros de lote, folhas de teste de Controle de Qualidade) devem ser emitidos por uma unidade designada e ter um identificador exclusivo. A impressão desses registros deve ser controlada, ou seja, um número especificado de pessoas autorizadas pela unidade de qualidade a imprimir, com total rastreabilidade do número de cópias impressas, quando foram impressas e por quem. A reconciliação completa do registro, incluindo folhas extras ou páginas adicionais, é necessária após o uso. Procedimentos de destruição de formulários não utilizados (em branco) devem estar em vigor e podem ser executados pela unidade emissora.

5.4.3.3. Formulários para dados de média criticidade (por exemplo, calibração, equipamento/qualificação de sistema computadorizado/protocolo de testes de validação), não é necessário um identificador exclusivo para o registro. A impressão controlada deve garantir que os modelos sejam impressos por um número limitado de pessoas autorizadas pela unidade de qualidade. Embora seja permitido um número ilimitado de cópias do modelo, um processo deve ser implementado para evitar o uso indevido, incluindo o uso de formulários expirados ou desatualizados. A reconciliação completa de registros e páginas com base na quantidade emitida é garantida. Procedimentos de destruição de formulários não utilizados devem estar em vigor e podem ser executados pela unidade operacional ou unidade emissora.

5.4.3.4. Formulários para dados pouco críticos (por exemplo, registros de treinamento) podem ser impressos pelo usuário final sem um identificador único e nenhuma atividade de reconciliação é necessária após o uso. O número de cópias que podem ser impressas não é limitado, e quaisquer formulários não utilizados podem ser descartados pelo usuário sem que a unidade de qualidade esteja diretamente presente no processo.

**5.5. Requerimentos para Registros Eletrônicos**

5.5.1. Sistemas computadorizados, desde sistemas autônomos a grandes sistemas integrados e complexos, que têm impacto na qualidade dos produtos fabricados, devem ser gerenciados de acordo com os requisitos de GxP para garantir que os sistemas sejam protegidos contra atos de manipulação, modificação ou qualquer outra atividade acidental ou deliberada que possa afetar a integridade dos dados. Os sistemas determinados como tendo um impacto GxP devem ser projetados, configurados e validados.

5.5.2. Devem ser aplicadas as seguintes regras para documentos criados em formato eletrônico:

* Os processos de recuperação e recuperação de desastres para registros são definidos
* Os documentos são revisados ​​rotineiramente quanto à precisão, autenticidade e integridade
* Os processos de preenchimento, recuperação, retenção, arquivamento e eliminação de registros estão em vigor, incluindo a captura e retenção de formulários incompletos e / ou errôneos como parte do registro permanente, juntamente com a justificativa para sua substituição
* Os dados originais são mantidos de acordo com as políticas de retenção de registros aplicáveis ​​e não são destruídos nem descartados intencionalmente, fora dessas políticas
* A integridade dos dados é mantida durante todo o ciclo de vida dos dados

**5.6. Requerimentos para Registros e Sistemas Híbridos**

5.6.1. O uso de sistemas híbridos deve ser evitado, pois a abordagem híbrida provavelmente trará complexidade e riscos adicionais do que uma abordagem totalmente eletrônica.

5.6.2. Uma abordagem híbrida pode ser usada excepcionalmente para assinar registros eletrônicos quando o sistema não tiver recursos para assinaturas eletrônicas, desde que haja controles adequados.

5.6.3. O uso de sistemas híbridos também pode ser necessário como mitigações provisórias quando controles técnicos apropriados não estiverem disponíveis ou viáveis, por exemplo, em sistemas eletrônicos legados.

5.6.4. Os sistemas híbridos exigem controles específicos e adicionais devido à sua complexidade adicional e potencial maior vulnerabilidade à manipulação de dados:

* Uma descrição do sistema de todo o sistema deve estar disponível que descreva todos os principais componentes do sistema (automatizado e manual) e a função de cada componente
* Devem existir procedimentos para gerenciar e controlar adequadamente a interface entre os elementos manuais (papel) e automatizados (eletrônicos).
* A saída em papel deve estar ivinculada aos registros eletrônicos subjacentes usados para produzi-la. Esse link deve ser mantido durante todo o período de retenção de registros para garantir a consistência dos elementos eletrônicos e em papel.
* Os dados originais devem ser revisados e retidos após a transcrição e processamento.

**5.7. Registros e suas Cópias Verdadeiras**

5.7.1. Registros em Papel – para – Eletrônico

5.7.1.1. Se uma cópia verdadeira dos registros em papel original for feita pela digitalização do registro em papel original e conversão em uma imagem eletrônica (por exemplo, PDF), medidas adicionais para proteger a imagem eletrônica de outras alterações, exclusão ou destruição não controlada devem estar em vigor.

5.7.1.2. Registros eletrônicos (por exemplo, imagem em PDF) devem ser autenticados como Cópias Verdadeiras de registros em papel usando assinatura eletrônica.

Observação: se for utilizado papel sensível à temperatura, fotossensível ou facilmente oxidável para registro original, é obrigatória a criação de sua cópia fiel (eletrônica ou em papel).

5.7.1.3. Cópia verdadeira no lugar do registro original: uma cópia fiel dos registros originais pode ser retida no lugar dos registros originais somente se todas as seguintes condições forem cumpridas:

* A cópia verdadeira é gerada seguindo um processo definido e procedimento aprovado.
* A cópia é autenticada como Cópia Verdadeira, ou seja, foi comparada com os registros originais e verificada para conter todo o conteúdo e significado dos registros originais.
* O registro original não contém marca d'água ou outro identificador que não possa ser reproduzido eletronicamente com precisão.
* Caso o registro original seja considerado um dado altamente crítico (ver anexo 2), a cópia fiel é autenticada pela unidade de qualidade.
* A destruição do original é um processo controlado e documentado (que documento, por quem, quando e quem aprovou a destruição).

5.7.2. Registros em Eletrônico – para – Papel

5.7.2.1. Os registros em papel devem ser autenticados como Cópias Verdadeiras de registros eletrônicos com assinatura manual.

5.7.2.2. Cópia verdadeira no lugar do registro original: Uma cópia fiel dos registros originais pode ser retida no lugar dos registros originais somente se todas as seguintes condições forem cumpridas:

* A cópia é autenticada como Cópia Verdadeira, ou seja, foi comparada com os registros originais e verificada para conter todo o conteúdo e significado dos registros originais, incluindo metadados aplicáveis e trilhas de auditoria necessárias para a reconstrução de um determinado conjunto de dados brutos.
* O registro eletrônico original está em formato estático.
* Caso o registro original seja considerado um dado altamente crítico, a cópia fiel é autenticada pela unidade de qualidade.
* A destruição do original é um processo controlado e documentado (que documento, por quem, quando e quem aprovou a destruição).

5.7.3. Registros em Eletrônico – para – Eletrônico

5.7.3.1. Uma cópia fiel dos registros originais pode ser retida no lugar dos registros originais somente se todas as seguintes condições forem cumpridas:

* A cópia é autenticada como Cópia Original através do processo de validação, ou seja, foi comparada com os registros originais e verificada para conter todo o conteúdo e significado dos registros originais, incluindo metadados aplicáveis e trilhas de auditoria necessárias para a reconstrução de um determinado conjunto de dados brutos.
* O processo de cópia deve manter o formato dos dados (por exemplo, dinâmico ou estático).
* Se a destruição do original for necessária e for um processo manual, ela deve ser controlada e documentada (qual documento, por quem, quando e quem aprovou a destruição). Se a destruição for um processo automatizado, ela deve ser validada.

**5.8. Não conformidade dos Dados**

5.8.1. Ao ocorrer falha no gerenciamento dos dados gerados, um desvio deve ser aberto.

5.8.2. Se houver erros ou inconsistências encontradas durante a revisão de dados, incluindo a revisão de trilha de auditoria, o revisor deve obter esclarecimentos apropriados do registrador dos dados (por exemplo, operador ou analista), para verificar as correções feitas aos dados ou iniciar uma investigação.

5.8.3. Qualquer violação de integridade de dados detectada deve ser investigada (de acordo com os procedimentos aprovados) pelo departamento / indivíduos apropriados, incluindo o representante da Unidade de Qualidade relevante. Além disso, qualquer incidente de integridade de dados será usado como um evento de aprendizado que aumentará a compreensão da importância da integridade de dados e evitará erros de integridade de dados.

**5.9. Garantia de Integridade de Dados para Atividades Terceirizadas**

5.9.1. Empresas terceirizadas (por exemplo, fornecedores, prestadores de serviços usados ​​para fornecer, instalar, configurar, integrar, validar, manter, monitorar ou reter um sistema informatizado ou serviço relacionado para processamento de dados) que fornecem ou prestam serviço(s) devem cumprir requisitos de integridade de dados.

5.9.2. As responsabilidades do doador e do destinatário do contrato devem ser claramente descritas em acordos escritos para tratar dos processos de integridade de dados de ambas as partes. O acordo escrito deve indicar que as atividades não podem ser terceirizadas para subcontratados de terceiros sem a aprovação prévia do contratante.

5.9.3. A avaliação, frequência e abordagem para monitorar ou avaliar periodicamente o contratado devem ser baseadas em avaliação de risco documentada que inclui uma avaliação dos processos de dados. Fornecedores e prestadores de serviços devem ser avaliados periodicamente por meio de auditorias e processos de qualificação.

5.9.4. Para serviços terceirizados de armazenamento de dados/documentos:

* Os dados devem ser transferidos, armazenados e restaurados de maneira segura (por exemplo, criptografia de dados).
* Os controles devem estar em vigor para garantir a integridade dos dados ao longo de seu ciclo de vida.

# 6. Referências

* **RDC 430 Nº 430/2020 (ANVISA)** - Dispõe sobre as Boas Práticas de Distribuição, Armazenagem e de Transporte de Medicamentos;
* **Guia de Validação de Sistemas Computadorizados nº 33/2020**, 1ª Versão ANVISA,
* **GAMP5, PIC/S, 21 CFR Part 11**

# 7. Histórico

|  |  |  |  |
| --- | --- | --- | --- |
| **DATA** | **REVISÃO** | **DESCRIÇÃO DA ALTERAÇÃO** | **OBSERVAÇÃO** |
| 05/04/2024 | 000 | Criação | N/A |

# 8. Fluxograma

# 9. Anexos

**Anexo 1:**

- Definições de criticidade de dados:

|  |  |
| --- | --- |
| **Criticidade** | **Definição** |
| **Alto** | Quando o uso pretendido dos dados afeta diretamente a qualidade e/ou a segurança do produto:   * Monitoramento da qualidade do produto e controle dos processos que podem ser responsáveis por causar variabilidade durante a fabricação, liberação ou distribuição impactando atributos críticos de qualidade, atributos críticos de materiais, parâmetros críticos de processo ou controles críticos de processo, incluindo aqueles que pode estar vinculado ao dossiê de registro do produto (quando aplicável). * Monitoramento da segurança do produto e controle dos processos que garantem gerenciamento de alertas, recalls, reclamações ou eventos adversos |
| **Médio** | Quando o uso pretendido dos dados estiver relacionado a atributos de qualidade, atributos de material, parâmetros de processo, parâmetros de processo chave ou controles de processo que não são CQAs/Processos Críticos (CPs)/CPPs e podem ou não estar no dossiê de registro do produto; isso inclui parâmetros do processo de fabricação que podem não estar diretamente ligados a atributos críticos de qualidade do produto, mas precisam ser fortemente controlados para garantir a consistência do processo. |
| **Baixo** | Quando o uso pretendido dos dados for fornecer evidências de conformidade com as GxPs ou relacionar, monitorar e controlar os processos que não se enquadram na Categoria Alta ou média |

- Exemplos de risco de dados (Data risk):

|  |  |
| --- | --- |
| **Categorias** | **Exemplos** |
| **Gerenciamento de Dados** | * Transcrição manual de dados. * Revisões periódicas pouco frequentes e gerenciamento de mudanças com base no uso pretendido. * Uso de sistemas híbridos (por exemplo, discrepâncias entre impressão em papel e registro eletrônico correspondente, duplicação de dados). * Tecnologia de fabricação nova ou complexa (causando erros repetidos). * Capacidade de substituir dados eletrônicos existentes. * Validação inadequada do sistema. * Controles do sistema insuficientes relacionados à exportação de dados, cálculo, relatório, transferência, arquivamento e recuperação. * Tecnologias com elementos de integridade de dados inadequados relacionados ao controle de acesso, trilha de auditoria, backup e restauração de dados, revisão eletrônica de dados, carimbo de data e hora, dentre outros (por exemplo, planilhas, LIMS). * Discrepâncias inexplicáveis entre dados brutos eletrônicos e dados relatados. |
| **Fator Humano** | * Falta de revisão de supervisão, * Observações ou medições manuais (por exemplo, pesagem), * Repetir erros humanos (por exemplo, devido à multitarefa, alta rotatividade de pessoal, treinamento inadequado, pressões de tempo), * Treinamento e procedimentos (complexos, longos, pouco claros, incompletos ou de difícil acesso instruções), * Definição de função pouco clara ou segregação de funções, * Cultura (medo, frustração, intenção, práticas de documentação local inaceitáveis), |
| **Processo GxP** | * Execuções abortadas (por exemplo, devido à falta de planejamento, compreensão da operação do sistema, adequação do equipamento e processo). * Processo complexo (por exemplo, muitas interfaces, alto nível de intervenção humana, alto níveis de entrada manual de dados), * Fluxos de dados e propriedade não bem definidos. * Verificações de folga de linha inadequadas. * Tendências negativas relacionadas a mudanças, desvios, fora de especificação, alarmes, fora de calibração. * Processos novos ou complexos (causando erros repetidos). * Comutação de operação (GxP vs. não GxP). * Indisponibilidade de dados relacionados à qualidade solicitados durante inspeções regulatórias. |

# 10. VALIDAÇÃO

|  |  |  |  |
| --- | --- | --- | --- |
| **Elaborado por:** | **Tatiana Gonçalves**  Responsável |  | 05/04/2024 |
| **Revisado por:** | **XXXXXXXX**  Coordenador Operacional |  | xx/xx/xxxx |
| **Aprovado por:** | **XXXXXXX**  Gerente Operacional |  | xx/xx/xxxx |