**Indice**

[**1. Objetivo.............** 2](#_Toc163236260)

[**2. Definições e Abreviações 2**](#_Toc163236261)

[**4. Responsabilidades 4**](#_Toc163236262)

[**5. Procedimento.... 5**](#_Toc163236263)

[**6. Referências........ 8**](#_Toc163236264)

[**7. Histórico............. ……..8**](#_Toc163236265)

[**8. Anexos............... 8**](#_Toc163236266)

[**9. Validação........... 8**](#_Toc163236267)

# 1. Objetivo

Descrever diretrizes para geração de backup, arquivamento e restauração dos dados dos sistemas computadorizados considerados GxP, durante o seu ciclo de vida.

# 2. Definições e Abreviações

**Backups de software:** são feitos para garantir que, em caso de falha durante a operação ou falha após uma modificação, a versão mais recente do software validado para permitir a rápida recuperação do sistema.

Essas cópias serão feitas antes de liberar o sistema para produção, antes e depois de execução de uma alteração no software do computador / sistema. Eles serão arquivados e nomeados para identificar a data de realização e nome do equipamento / software. Deve se manter no mínimo duas gerações de cópias, a última gerada e a anterior.

**Backups de dados:** cópia de segurança dos dados. São criados para garantir que os registros GxP relevantes são mantidos em segurança durante todo o tempo de retenção definido conforme cada atividade específica.

Embora os dados sejam geralmente armazenados em sistemas com redundância, um sistema de backup adicional serve para evitar perdas dos dados em caso de desastre.

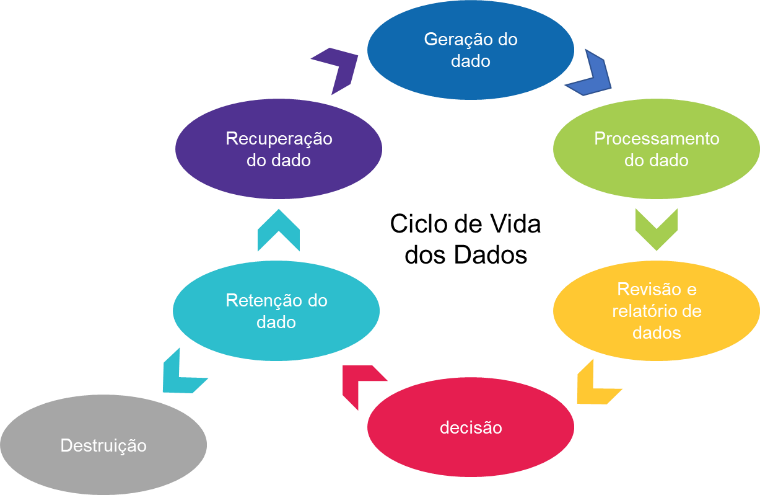
Deve ser definido quais dados são o GxP para fazer os backups. Os dados GxP consideram os dados do lote, a trilha de auditoria associada, o log de alarme, formatos, configurações do usuário e todos os registros relacionados com a qualidade do produto.

**Arquivo:** Uma área ou local seguro designado onde o próprio registro (por exemplo: armário, sala, prédio, sistema computadorizado ou documentos) a longo prazo, tenha retenção permanente de dados completos e metadados relevantes em sua forma final para fins de reconstrução do processo ou atividade.

**Backup (cópia de segurança):** Uma cópia dos dados atuais, metadados e configurações do sistema mantidos para fins de recuperação de desastres.

**BPD:** Boas Práticas de Documentação.

**Ciclo de Vida dos Dados**: Abrange todas as fases da vida dos dados (incluindo dados brutos), desde o início geração e gravação através do processamento (incluindo análise, transformação ou migração), uso, dados retenção, arquivo / recuperação e destruição. Veja a imagem abaixo:



**Dados brutos**: Registros e documentação originais, mantidos no formato originalmente gerado (ou seja, papel ou eletrônico) ou como uma "cópia fiel". Os dados brutos devem ser registrados simultaneamente e com precisão por meios permanentes.

**BPAD (*GDP*):** Boas Práticas de Distribuição.

**BPF (*GMP*):** Boas Práticas de Fabricação.

**Boas Práticas GxP:** No contexto deste documento, nos referimos apenas a Manufatura e Distribuição.

**Processamento de Dados**: Sequência de operações executadas nos dados para extrair, apresentar ou obter informações em um formato definido.

**Registros Dinâmicos:** Como registros eletrônicos, permitem um relacionamento interativo entre o usuário e o conteúdo do registro.

**Registros Híbridos**: É uma combinação de registros eletrônicos originais e registros em papel que compreender o conjunto total de registros que devem ser revisados e retidos.

**Metadados:** Metadados são dados que descrevem os atributos de outros dados e fornecendo contexto e significado. Normalmente, esses dados descrevem a estrutura, elementos de dados, inter-relacionamentos e outras características dos dados. Também permite que os dados sejam atribuíveis a um indivíduo (ou se automaticamente gerado, à fonte de dados original). Os metadados fazem parte integrante do registro original. Sem metadados, os dados não têm significado. Exemplos: hora, dia, escalas de grandezas.

**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 em papel original 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 não Tratados:** Registros e documentação originais, mantidos no formato em que foram originalmente gerados (ou seja, papel ou eletrônico) ou como uma 'cópia verdadeira'. Os dados brutos devem ser contemporâneos e gravados com precisão por meios permanentes.

**Dados Regulamentados:** Dados usados para fins GxP, exigidos pelos regulamentos GxP. No contexto deste. O documento GxP refere-se apenas a Manufatura e Distribuição. (por exemplo, dados que podem ter impacto sobre atributos de qualidade do produto).

**Registro Estático:** Um registro estático é um documento de dados fixos, como um registro em papel ou uma imagem eletrônica. Exemplos de um registro estático incluem: uma impressão em papel de uma balança ou uma imagem estática criada durante a aquisição de dados.

**Cópia Verdadeira:** Uma cópia exata de um registro original. As cópias verdadeiras podem ser estáticas (por exemplo, um registro ‘fixo’, como papel ou pdf) ou dinâmicas (por exemplo, um registro eletrônico com o qual o usuário / revisor possa interagir).

**Lista de tarefas:** Lista de atividades inseridas que serão realizadas no momento da manutenção, seja ela preventiva ou corretiva

# 4. Responsabilidades

* Garantir a conformidade com este procedimento nas áreas.
* Verificar a conformidade com este procedimento através da validação e manutenção do estado validado dos sistemas informatizados.
* Avaliar se as falhas apresentadas nos sistemas computadorizados afetam o estado validado.
* Avaliar se as alterações nos sistemas computadorizados afetam o estado validado do mesmo.
* Verificar, após a restauração do sistema computadorizado, se foi afetado o estado validado e estabelecer ações de correção em conjunto com o Dono e o Administrador do Sistema.
* Garantir que os sistemas computadorizados operem em conformidade com a validação e procedimentos operacionais atuais, assim como a manutenção do estado validado.
* Relatar falhas no sistema de acordo com o indicado no procedimento de uso de cada equipamento.
* Protejer os arquivos de dados GxP gerados durante os processos de desenvolvimento, fabricação, análise, armazenamento, distribuição e comercialização de produtos, quando não é possível fazer backup sejam eles dados brutos, não tratados, regulamentados ou registro estático.
* Verificar, após a restauração do sistema computadorizado, se foi afetado o estado validado e estabelecer ações de correção em conjunto com o Administrador do Sistema e a Validação.
* Estabelecer uma programação para a execução de cópias de segurança, de acordo com as capacidade e funcionalidade do sistema informatizado.
* Garantir a conformidade com a programação para gerar backups de sistemas informatizados.
* Proteger os backups em conformidade com os requisitos de integridade de dados.
* Proteger as licenças e cópias do software em conformidade com os requisitos de integridade de dados, se necessário para restaurar os sistemas.

# 5. Procedimento

5.1 Considerações gerais

* É necessário fazer backup de todos os dados chamados GxP para garantir sua integridade.
* Todos os registros considerados GxP devem ser protegidos contra danos ou destruição por incêndio, líquidos, pragas, umidade e acesso por pessoal não autorizado.
* A integridade dos dados deve ser incorporada desde a fase de projeto até o uso do sistema sendo aplicável para registros em papel e eletrônicos.
* Todos os registros devem ser rastreáveis e acessíveis durante todo o ciclo de vida do sistema.

5.2 Identificação da capacidade e modo de criação do backup do sistema computadorizado

5.2.1 Durante a validação do sistema computadorizado, definir a capacidade de armazenamento do sistema computadorizado e como deve ser gerado o backup.

5.2.2 Gerar uma rotina de backup em que a capacidade esteja incluída do sistema computadorizado e como gerar os backups.

5.2.3. Incluir, de acordo com o descrito no Anexo 1, a frequência de geração de backup de dados em um programa de geração de cópias de segurança da área correspondente.

5.2.4 Deve garantir que exista um procedimento ou rotina com as atividades para gerar cópias de backup de sistemas computadorizados.

5.3 Geração do programa de backup

5.3.1 Gerar uma rotina para a criação de backup e que deve incluir pelo menos os seguintes dados:

* Nome do sistema computadorizado;
* Localização do sistema computadorizado;
* Frequência de geração de backup;
* Método para obter o backup;
* A data em que as cópias de backup devem ser geradas.

5.4 Backup de dados através de cópias de segurança

5.4.1 Criar o backup, de acordo com a rotina correspondente ao sistema computadorizado.

5.5 Arquivamento dos dados

5.5.1 Extrair os registros e dados movendo-os para um local ou sistema diferente, protegendo-os da capacidade de serem alterados ou removidos. Também pode ser necessário reter aplicativos em arquivo (por exemplo, software e hardware associado) que suportam dados e registros GxP. Os registros arquivados devem ser facilmente recuperáveis para fins comerciais ou regulatórios e alinhados com a legislação. Esta extração deve ser registrada no roteiro de backup correspondente ao sistema computadorizado indicado local no qual o mesmo está sendo indexado

5.5.2 O administrador do sistema deve garantir que o local onde a cópia de backup dos registros e dados GxP são protegidas contra danos intencional ou acidental, durante todo o período de retenção necessário. Devem existir um backup duplicado das informações geradas pelos sistemas para ser usado em caso de perda ou extravio. Ambos os backups devem ser protegidos em locais diferentes, fisicamente ou logicamente, para a segurança destes e um deles será usado apenas se necessário.

5.5.3 No caso de backups físicos (dispositivos de armazenamento, por exemplo: discos rígidos, pendrive, cartões de memórias) deve estar bloqueado e identificado com o nome da área. Para backups eletrônicos, isso pode ser feito dentro da rede coorporativa através de uma pasta de arquivo restrita, com acesso apenas a pessoal autorizado.

5.5.4 Nomear o backup de maneira única: TAG do equipamento, tamanho do backup e data que o backup foi realizado.

5.5.5 Qualquer processo de backup físico ou eletrônico será documentado e identificado na rotina de backup, presente na rotina de manutenção preventiva que deve ser preenchido com nome de arquivo, local (nome do disco rígido e pasta), data de geração e tamanho do arquivo.

5.5.6 Estas ações devem ser preenchidas no momento da execução da atividade no roteiro de manutenção preventiva.

5.6 Recuperação dos dados

5.6.1 Abrir um desvio caso seja necessário um processo de recuperação de dados, para avaliar o impacto nos dados e no estado validado.

5.6.2 Informar à equipe de Validação para validar o processo de recuperação de dados realizado documentar todo o processo através da investigação do desvio.

5.7 Fornecimento final de dados e sistemas GxP (Proprietário do sistema)

5.7.1 O proprietário do sistema deve realizar uma análise de risco para avaliação dos dados que devem ser considerados para realização de backup avaliar o tempo de retenção necessário com base nos requisitos de retenção medidas regulatórias para garantir a integridade dos dados GxP.

5.8 Fluxograma para melhor entendimento do sequencial das tarefas e seu responsável mencionado nos itens anteriores



**Fluxograma 1**

# 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. Anexos

Não aplicável.

# 9. 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 |