# 1. Índice

[1. Índice 2](#_Toc153280924)

[2. Objetivo 3](#_Toc153280925)

[3. Escopo 3](#_Toc153280926)

[4. Definições e Abreviações 3](#_Toc153280927)

[5. Responsabilidades 4](#_Toc153280928)

[6. Procedimento 5](#_Toc153280929)

[**6.1** **Considerações Gerais** 5](#_Toc153280930)

[**6.2** **Geração do programa de Backup de Dados** 6](#_Toc153280931)

[**6.3** **Arquivamento dos Dados Eletrônicos e Backups** 6](#_Toc153280932)

[**6.4** **Revisão da Execução do Backup** 6](#_Toc153280933)

[**6.5** **Revisão do Backup de dados** 7](#_Toc153280934)

[**6.6** **Recuperação dos Dados/Sistema (Administrador do sistema)** 7](#_Toc153280935)

[**6.7** **Retenção dos Dados GxP** 7](#_Toc153280936)

[**6.8** **Destruição dos Dados GxP** 7](#_Toc153280937)

[**6.9** **Documentação da Revisão do Backup** 7](#_Toc153280938)

[**6.10** **Frequência da Revisão de Backup** 8](#_Toc153280939)

[**6.11** **Análise do Risco de Backup de Dados** 8](#_Toc153280940)

[**6.12** **Revisão Backup de Sistema:** 12](#_Toc153280941)

[**6.13** **Gerenciamento de Incidentes** 14](#_Toc153280942)

[7. Referências 14](#_Toc153280943)

[8. Histórico 15](#_Toc153280944)

[9. Fluxograma 16](#_Toc153280945)

[10. Anexos 17](#_Toc153280946)

# Objetivo

Descrever diretrizes para Gerenciamento de Backups dos dados dos sistemas GxP da Merck Brasil, durante o seu ciclo de vida.

# Escopo

Engenharia

Produção

Tecnologia Farmacêutica

Controle de Qualidade

Garantia da Qualidade

# Definições e Abreviações

* 1. **Definições:**

**Backups de software/sistema:** 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.

**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.

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

**Ciclo de Vida dos Dados (*Data Lifecycle*)**: 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 figura 1:

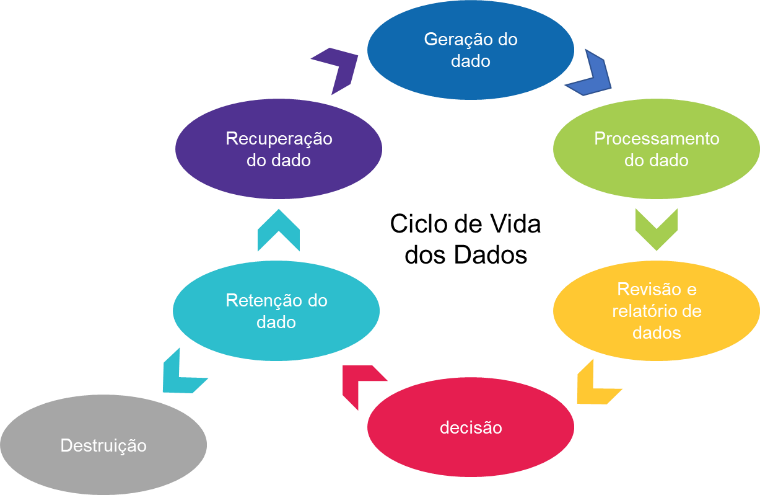


Figura 1

* 1. **Abreviações:**

GHO- Global Healthcare Operations

CS- Sistema Computadorizado

TI- Tecnologia da Informação

CSV-Validação de Sistemas Computadorizados

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

# Responsabilidades

* 1. **Direção do site, gerentes, coordenadores e supervisores:**
     1. Garantir a conformidade com este procedimento nas áreas de GHO (Global Healthcare Operations) da Merck Brasil / Rio
  2. **Engenharia- CSV:**
     1. Verificar a conformidade com este procedimento através da validação e manutenção do estado validado dos sistemas informatizados.
     2. Avaliar se as falhas apresentadas nos sistemas computadorizados afetam o estado validado.
     3. Avaliar se as alterações nos sistemas computadorizados afetam o estado validado.
     4. 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.
     5. Aprovar e verificar a aderência ao Plano de Backup.

**Dono do sistema (Engenharia, Tecnologia Farmacêutica e Controle de Qualidade):**

* + 1. Garantir que os sistemas computadorizados operem em conformidade com a validação e procedimentos operacionais atuais, assim como a manutenção do estado validado.
    2. Relatar falhas no sistema de acordo com o indicado no procedimento de uso de cada equipamento.
    3. Proteger os arquivos de dados 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.
    4. 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.
    5. Garantir que o processo de backup seja realizado.
  1. **Administrador do sistema:**
     1. Suportar as atividades de backup e realizar o backup para sistemas sem backup automático
     2. Realizar o backup de sistema ao realizar alteração no software do computador / sistema.
  2. **Dono dos dados- responsável pelo processo (Produção,** **Tecnologia Farmacêutica e Controle de Qualidade):**
     1. Gerenciar todas as atividades durante todo o ciclo de vida do dado incluindo a verificação da integridade, exatidão e disponibilidade dos dados.
  3. **Garantia da Qualidade**
     1. Aprovar e efetivar o Plano de Backup.

# Procedimento

* 1. **Considerações Gerais** 
     1. É necessário fazer backup de todos os dados chamados GxP para garantir sua integridade conforme SOP 20665069 – Integridade de Dados em sua versão vigente.
     2. O processo de geração, frequência de execução do backup, frequência de revisão de backup, armazenando e destruição dos backups deverão ser baseados em risco conforme SOP 20064096 – Gerenciamento de Riscos à Qualidade, em sua versão vigente.
     3. Todos os dados considerados GxP devem ser protegidos contra danos ou destruição por incêndio, líquidos, pragas, umidade e acesso por pessoal não autorizado.
     4. 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.
     5. Todos os registros devem ser rastreáveis e acessíveis durante todo o ciclo de vida do sistema.
     6. Identificação da capacidade e modo de criação do backup do sistema computadorizado
     7. Deve ser definida a capacidade de armazenamento do sistema computadorizado e como deve ser gerado o backup.
     8. Gerar uma rotina de backup de dados em que a capacidade esteja incluída do sistema computadorizado e como gerar os backups.
     9. As áreas donas dos sistemas devem garantir que exista um procedimento ou rotina com as atividades para gerar cópias de backup de sistemas computadorizados.
  2. **Geração do programa de Backup de Dados** 
     1. Gerar uma rotina para a criação de backup de dados e incluir no plano de backup, 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;
  + Localização da retenção do backup dados/sistema;
    1. A Garantia da Qualidade deve aprovar e efetivar o Plano de Backup.
    2. O Dono dos Dados e a Engenharia-CSV devem verificar a aderência ao Plano de Backup.
  1. **Arquivamento dos Dados Eletrônicos e Backups**
     1. É necessário 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
     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.
     3. O administrador do sistema deve garantir que a migração de dados para seja realizada para um local aprovado que possua os requisitos de segurança de acesso e proteção contra exclusão não autorizada.
     4. 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, esta solução deverá ser utilizada quando não houver outros recursos de armazenamento disponíveis.
     5. Os backups deverão ser identificados para fins de armazenamento.
     6. Qualquer processo de backup físico ou eletrônico deverá ser documentado.
  2. **Revisão da Execução do Backup** 
     1. A Revisão da Execução dos Backups deve realizada pelo dono dos dados para garantir que o processo de execução e arquivamento do backup são realizados.
  3. **Revisão do Backup de dados** 
     1. Os backups devem ser revisados pelo dono dos dados para a verificação da integridade e exatidão.
  4. **Recuperação dos Dados/Sistema (Administrador do sistema)** 
     1. O processo de restauração de dados deverá ser documentado pelo administrador.
     2. Em caso de incidentes onde a restauração do sistema seja necessária um desvio deverá ser aberto conforme SOP 20016001 – “Gerenciamento de Desvios”, em sua versão vigente.
     3. Em caso de incidentes onde a restauração do sistema seja necessária a avaliação do status validado deverá ser documentada conforme SOP 20013925 – Validação de Sistemas Computadorizados, em sua versão vigente.
  5. **Retenção dos Dados GxP** 
     1. O dono dos dados deve gerenciar o tempo de retenção dos dados conforme SOP 20015511 “Indexação, Arquivamento, Armazenamento e Descarte (ou Destruição) de Documentos e Registros da Fábrica Rio, Unidade da Qualidade e Sistemas de Gestão de Saúde, Segurança e Meio Ambiente” e listagem 20495853 - Listagem Tempo Mínimo de Arquivamento dos documentos relacionados à Qualidade, ambas suas versões vigentes para garantir a integridade dos dados GxP.
  6. **Destruição dos Dados GxP** 
     1. O dono dos dados deve solicitar a destruição dos dados GxP ao final do tempo de retenção programado.
     2. O processo de destruição dos dados eletrônicos deverá ser documentado.
  7. **Documentação da Revisão do Backup**
     1. Instruções:
        1. Os requerimentos para revisão do backup, independentemente do tipo, devem ser descritos em procedimentos.
        2. Os procedimentos devem providenciar claras instruções sobre:
  + Quais dados devem ser revisados (quanto a exatidão e integridade);
  + Em quais detalhes e qual frequência (por exemplo, período para revisão, e qual o critério de aceitação para a exatidão.);
  + O método para obter os dados requeridos, e possíveis especificações para recuperação;
  + As possíveis especificações para recuperação do sistema;
  + Documentação de checks seja em formato eletrônico ou papel e a conclusão de revisão bem-sucedida ou falhada, incluindo ações de acompanhamento, quando necessário;
  + Autorização/Qualificação para realização da revisão de backup;
  + Responsabilidade pela revisão de backup;
  + Como a revisão de backup deve ser documentada.

Observação 1: Um template de revisão de backup ou check-list pode ajudar e facilitar a documentação da atividade de revisão de backup.

* + 1. Registros
       1. Os resultados da revisão devem ser documentados de acordo com procedimentos aprovados. Esses registros devem ser considerados GxP relevantes, seguindo as regras de documentação preconizadas no SOP 20034479 - Gerenciamento de Documentação da Qualidade, em sua versão vigente.
  1. **Frequência da Revisão de Backup**
     1. A abordagem para frequência de condução da revisão de backup deve garantir que requerimentos GxP sejam atingidos, controles apropriados sejam implementados, e a confiabilidade da revisão comprovada.
     2. Caso a frequência de revisão de backup estejam especificadas em regulamentações GxP relevantes, torna-se mandatório aderir a frequência de revisão de backup nela estabelecida.
     3. Caso a frequência de revisão dos backups não seja especificada em regulamentações GxP relevantes, a frequência de revisão do backup deve ser determinada usando conhecimento do processo e baseado em risco.
  2. **Análise do Risco de Backup de Dados**
     1. A frequência e extensão da execução/revisão do backup deve ser proporcional com o nível de risco combinado entre criticidade do dado e do sistema. A decisão sobre a frequência e a extensão da revisão deve ser suportada por uma análise de risco documentada, conforme SOP 20064096 - Gerenciamento de Riscos à Qualidade, em sua versão vigente.
     2. Em casos nos quais é definido que não há necessidade de revisão de backup, um racional válido baseado em risco deve ser documentado e revisado durante a revisão periódica do sistema computadorizado para suporte da decisão.
     3. A estrutura do processo de execução/revisão de backup deve considerar as capacidades atuais de segurança dos sistemas e sua validação (por exemplo, não é necessário checar a ativação do backup se o CS não permite a desativação).
     4. Criticidade dos dados:
        1. A criticidade dos dados é determinada pelo impacto deles na tomada de decisão e qualidade do produto.
        2. A criticidade dos dados deve seguir o SOP 20665069 “Integridade de dados” em sua versão vigente.
     5. Complexidade do sistema (Vulnerabilidade do Sistema):
        1. A complexidade do sistema (ou vulnerabilidade, em relação ao backup): é baseada no grau no qual os dados de backup podem ser livremente configurados e, potencialmente, dados podem ser manipulados.
        2. Considerando a definição anterior, a seguinte escala é definida (Tabela 1):

|  |  |
| --- | --- |
| **Escala de Complexidade/ Vulnerabilidade do Sistema** | |
| Alta | Backup pode ser desabilitado por um usuário operacional do CS. Ou Usuário operacional do CS pode modificar ou deletar backup durante operação normal (disco local ou servidor) E Atividades do Backup são realizadas pelo administrador são registradas em caderno em papel |
| Média | Backup é automaticamente gerado e não pode ser desabilitado pelo usuário operacional do CS mas necessita de intervenção humana para arquivamento (Transferência do backup)  E  Usuário operacional do CS não pode modificar ou deletar o backup durante operação normal (disco local ou servidor)  E Atividades do Backup são realizadas pelo administrador ficam registradas no sistema ou em caderno em papel |
| Baixa | O Backup é gerado automaticamente e não pode ser desabilitado pelo usuário operacional do CS E O backup é arquivado sem nenhuma intervenção humana. (Transferência do backup)  E  Usuário operacional do CS não pode modificar ou deletar o backup durante operação normal (disco local ou servidor)  E  Atividades do Backup ficam registradas no sistema. |

Tabela 1

* + 1. Matriz de avaliação de riscos backup de dados
       1. Para determinar o risco geral do sistema, a seguinte matriz é definida (Tabela 2):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Complexidade do sistema/ Vulnerabilidade do sistema | Alta |  |  | Alta |
| Média |  | Média |  |
| Baixa | Baixa |  |  |
|  |  | Baixa | Média | Alta |
|  |  | Nível de criticidade dos dados | | |

Tabela 2

* + 1. Execução/Revisão de Backup de dados
       1. O backup/revisão deve ser executado de acordo com instruções de trabalho, descrevendo tarefas específicas a serem completadas pelo revisor e critérios de aceitação relacionados.
       2. Backup deve ser executado por pessoa qualificada com treinamento no respectivo sistema computadorizado, procedimentos aplicáveis, conhecimento provado do processo e sem conflito de interesse.
       3. Revisão do backup deve ser executada por pessoa qualificada com treinamento no respectivo sistema computadorizado, procedimentos aplicáveis, conhecimento provado do processo.
       4. O escopo do processo de revisão de backup de dados deve ser focado, em garantir a integridade e exatidão do backup.
       5. A análise de risco deve conter avaliação da criticidade do dado, mecanismos de controle de dados e impacto do dado na qualidade.
       6. Uma vez que os registros eletrônicos (ER) e seus sistemas associados possuam nível de risco identificados de acordo com a tabela 2, o dono do dado e Engenharia-CSV vão determinar o esforço (frequência e profundidade) da revisão da execução do backup, revisão de backup baseados no racional providenciado tabelas 3,4, 5 e 6 deste procedimento. A revisão de backup pode ter diferentes frequências de revisão.
       7. Com base nos resultados da análise de risco de cada sistema, a revisão de backup deve ser executada de acordo com um dos seguintes métodos:
    2. Revisão de backup periódica de dados: revisão realizada de forma periódica. Dono dos dados/Operações da Qualidade devem definir a frequência associada, baseado na frequência de uso do sistema e a relevância GxP dos registros. A revisão de backup periódica deve ser executada em 1 arquivo de dado para cada pasta e subpasta com a finalidade de garantir que a ferramenta de backup conseguiu atingir todas as pastas da estrutura de arquivos.
    3. Revisão eventual do backup de dados: não possui requerimento rotineiro e necessária com base eventual somente para suportar outros processos PQS como por exemplo investigação, auditorias internas, ou inspeções. A revisão de backup eventual deve ser executada mediante uma solicitação definida de processo de investigação, auditorias ou inspeções.
       1. Execução do Backup Automático de dados (Tabela 3)

|  |  |  |
| --- | --- | --- |
| Frequência de uso do sistema | Risco do sistema para Execução de Backup Automático arquivado sem interação humana. | |
| Baixo | Médio |
| Diária/ Semanal | Semanal | Diario |
| Mensal | 2 meses | Mensal |
| Menor que mensal | 4 meses | 2 Meses |

Tabela 3

* + - 1. Execução de backup de dados Manual ou automático com transferência de arquivo com interação humana (Tabela 4)

|  |  |  |  |
| --- | --- | --- | --- |
| Frequência de uso do sistema | Risco do sistema para Execução de backup Manual ou automático com transferência de arquivo com interação humana*.* | | |
| Baixo | Médio | Alto |
| Diária/ Semanal | 6 meses | 3 meses | Mensal |
| Mensal | 9 meses | 6 meses | 3 meses |
| Menor que mensal | 12 meses | 9 meses | 6 meses |

Tabela 4

Observação 2: O prazo de execução do backup deve ser reduzido devido a capacidade de armazenamento do sistema.

* + - 1. Revisão da Execução do Backup de Dados (Tabela 5)

|  |  |  |
| --- | --- | --- |
| Risco do sistema para revisão da Execução de backup | | |
| Baixo | Médio | Alto |
| 3 meses | 2 meses | Semanal |

Tabela 5

Observação 3: para sistemas com a Execução de backup Manual ou Automático com transferência de arquivo com interação humana onde o processo de revisão da execução é realizado e documentado no momento da atividade não será necessária a Revisão da execução do Manual ou automático com transferência de arquivo com interação humana (tabela 5).

* + - 1. Revisão de Backup de Dados (Tabela 6):

|  |  |  |  |
| --- | --- | --- | --- |
| Frequência de uso do sistema | Risco do sistema para Revisão de Backup de Dados | | |
| Baixo | Médio | Alto |
| Diária/ Semanal | Baseada em evento | 2 anos | 1 anos |
| Mensal | Baseada em evento | 4 anos | 2 anos |
| Menor que mensal | Baseada em evento | 6 anos | 4 anos |

Tabela 6

* + - 1. Revisão de Backup de Dados - Sistemas fora de uso (descomissionado) (Tabela 7):

|  |  |  |
| --- | --- | --- |
| Risco do sistema para Revisão de Backup de Dados sistemas fora de uso. | | |
| Baixo | Médio | Alto |
| Baseada em evento | 8 anos | 6 anos |

Tabela 7

Observação 4: Deverá ser executada uma revisão de backup de dados para sistema classificado com Baixo, conforme tabela 7, antes da descontinuação do sistema.

* 1. **Revisão Backup de Sistema:**
     + 1. O escopo do processo de revisão de backup de sistema deve ser focado, em garantir que o sistema possa ser recuperado em caso de desastre, nos casos que a revisão necessite da restauração completa do sistema um plano de recuperação de desastre deve ser implementado com o prazo para a execução do Teste de recuperação de desastre.
       2. A revisão backup de sistema deve ser incorporada ao plano de backup.
       3. O Teste de recuperação de desastre poderá ser realizado internamente ou empresa contratada/fornecedor.
       4. Para sistemas/e ou aplicação que possuem ferramentas de verificação da integridade do backup o Teste de Recuperação de Desastre não precisará ser executado periodicamente somente será necessária a verificação periódica da integridade do backup através da ferramenta de verificação.
       5. O Teste de recuperação de desastre deve ser executado em ambiente de qualidade sempre que disponível, caso o teste seja realizado em ambiente produtivo deve se avaliar o risco e esforço necessário e a maturidade, conhecimento específico e treinamento dos envolvidos no processo de restauração.
       6. A verificação da integridade do backup de sistema poderá ser realizada por outros processos de verificação de integridade de arquivos, mídia ou imagem caso o teste de restauração não seja viável em ambiente de produção.
       7. Avaliação de Risco revisão periódica de backup de sistema
          1. Utilizar a Complexidade do sistema/ Vulnerabilidade do sistema, conforme Tabela 1
          2. Criticidade do sistema em relação ao negócio (Tabela 8)

|  |  |  |
| --- | --- | --- |
| Nível de criticidade do sistema para o negócio | | |
| Baixo | Médio | Alto |
| Há sistema substituto disponível e a recuperação pode ser realizada internamente ou externamente. | Não há sistema substituto disponível e a recuperação pode ser realizada internamente ou há contrato externo ativo de serviço para restauração | Não há sistema substituto disponível e a recuperação não pode ser realizada internamente e não há contrato externo ativo de serviço para restauração |

Tabela 8

* + - * 1. Matriz de avaliação de riscos backup de sistema

• Para determinar o risco geral de criticidade do sistema, a seguinte matriz é definida (Tabela 9):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Complexidade do sistema/ Vulnerabilidade do sistema (Tabela 1) | Alta |  |  | Alta |
| Média |  | Média |  |
| Baixa | Baixa |  |  |
|  |  | Baixa | Média | Alta |
|  |  | Nível de criticidade do sistema para o negócio | | |

Tabela 9

* + - * 1. Com base nos resultados da análise de risco de cada sistema, a revisão de backup de sistema deve ser executada de acordo com um dos seguintes métodos:
        2. Revisão de backup periódica de sistema: revisão realizada de forma periódica. Dono do sistema/Operações da Qualidade devem definir a frequência associada, baseado na frequência de uso do sistema e a criticidade do sistema.
        3. Revisão eventual do backup de sistema: não possui requerimento rotineiro e necessária com base eventual somente para suportar a continuidade do negócio.

|  |  |  |  |
| --- | --- | --- | --- |
| Frequência de uso do sistema | Risco do sistema para *Revisão de Backup de sistema*. | | |
| Baixo | Médio | Alto |
| Diária/ Semanal | Baseada em evento | 5 anos | 3 anos |
| Mensal | Baseada em evento | 7 anos | 5 anos |
| Menor que mensal | Baseada em evento | 9 anos | 7 anos |

Tabela 10

* + - * 1. A revisão de backup de sistema deverá ser realizada conforme tabela 10, somente para sistemas em uso no último backup de sistema realizado.
  1. **Gerenciamento de Incidentes**
     1. Quaisquer variações significativas do resultado esperado encontradas durante a revisão de execução de backup e/ou revisão de backup devem ser totalmente investigadas e registradas conforme SOP 20016001 - Gerenciamento de Desvios, em sua versão vigente

# Referências

- SOP 20016281– Emissão, Aprovação e Distribuição de Procedimentos de Operação Padrão e Instrução de Trabalho;

- SOP 20665069 – Integridade de Dados, em sua versão vigente;

- SOP 20064096 – Gerenciamento de Riscos à Qualidade, em sua versão vigente;

- SOP 20016001 – Gerenciamento de Desvios, em sua versão vigente;

- SOP 20015511 “Indexação, Arquivamento, Armazenamento e Descarte (ou Destruição) de Documentos e Registros da Fábrica Rio, Unidade da Qualidade e Sistemas de Gestão de Saúde, Segurança e Meio Ambiente”, em sua versão vigente;

- SOP 20013925 – Validação de Sistemas Computadorizados, em sua versão vigente;

- SOP 20034479 - Gerenciamento de Documentação da Qualidade, em sua versão vigente;

- Listagem 20495853 - Listagem Tempo Mínimo de Arquivamento dos documentos relacionados à Qualidade, em sua versão vigente.

# Histórico

|  |  |
| --- | --- |
| **VERSÃO** | **DESCRIÇÃO DA ALTERAÇÃO** |
| 1.0 | Versão Inicial conforme TW: 4236641 |

# Fluxograma

* 1. Fluxograma Backup de dados

* 1. Backup de sistema

# Anexos

Não aplicável