# 1. Índice

[1. Índice 2](#_Toc157692454)

[3. Escopo 2](#_Toc157692455)

[4. Definições e Abreviações 3](#_Toc157692456)

[5. Responsabilidades 3](#_Toc157692457)

[6. Procedimento 4](#_Toc157692458)

[6.1. Categorizar os sistemas computadorizados conforme descrito no SOP 20013925 – Validação de Sistemas Computadorizados, em sua versão vigente. 4](#_Toc157692459)

[6.2. Após a aprovação do Controle de Mudanças, Criar o Plano de Validação para mapear os requisitos do projeto, conforme descrito no SOP 20013925 – Validação de Sistemas Computadorizados, em sua versão vigente. 4](#_Toc157692460)

[6.3. Validação de software do equipamento/sistema 4](#_Toc157692461)

[6.4. Configuração do Sistema 5](#_Toc157692462)

[6.5. Qualificação de Instalação 5](#_Toc157692463)

[6.6. Qualificação de Operação 9](#_Toc157692464)

[6.7. Qualificação de Desempenho (Performance) 20](#_Toc157692465)

[6.8. Relatório de Validação 22](#_Toc157692466)

[6.9. Matriz de rastreabilidade 22](#_Toc157692467)

[6.10. Geração e Arquivamento da Documentação de Validação. 22](#_Toc157692468)

[7. Referências 23](#_Toc157692469)

[8. Histórico 23](#_Toc157692470)

[9. Fluxograma 24](#_Toc157692471)

[10. Anexos 25](#_Toc157692472)

**2. Objetivo**

Fornecer os requisitos básicos para o gerenciamento da validação de software de equipamentos/sistemas dentro do escopo deste documento. As informações descritas devem ser usadas para gerar os documentos de validação de software do equipamento conforme 20378416 - Equipment Software Validation guideline versão 2.0. Os testes listados devem ser incluídos como parte dos documentos de validação do equipamento / sistema (quando aplicável), podendo ser incluídos testes adicionais, caso necessários.

# 3. Escopo

Aplicável aos equipamentos/sistemas classificados como Local CS para atividades GxP.

- Controle de Qualidade

- Tecnologia Farmacêutica

- Engenharia

# 4. Definições e Abreviações

Ciclo de vida dos dados – Todas as fases da vida dos dados, desde a geração e gravação até o processamento (incluindo análise, transformação ou migração), uso, retenção de dados, arquivamento / recuperação e destruição.

Dados brutos – São definidos como o registro (dados) original que pode ser descrito como a primeira captura de informações, registradas em papel ou eletronicamente. As informações capturadas originalmente em um estado dinâmico devem permanecer disponíveis nesse estado.

Validação – É a confirmação através de teste e evidência objetiva de que um requisito específico foi consistentemente cumprido para o uso pretendido.

Audit Trail – Trilha de Auditoria

ER – Electronic Records (Registro Eletrônico)

FRS – Functional Requirements Specification (Especificação de Requerimentos Funcionais)

FAT – Factory Acceptance Test (Tetes de Aceitação do Fabricante)

GPO – Global Policy Object (Objeto de Política Global)

GxP – Good Practices in general (Boas Práticas de Fabricação aplicáveis a p.ex. M = Manufatura, L = Laboratório, D = Distribuição)

IQ – Installation Qualification (Qualificação de Instalação - QI)

OQ – Operational Qualification (Qualificação de Operação - QO)

PQ – Performance Qualification (Qualiifcação de Performance - QP)

SW – Software

HW – Hardware

TI –Tecnologia da Informação

URS –User Requirements Specification (Especificação de Requerimentos do Usuário)

# 5. Responsabilidades

* 1. Engenharia-CSV:
* Fornecer orientação e suporte para a implementação deste procedimento.
* Executar os testes conforme descrito neste procedimento.
* Aprovar os testes
  1. Administradores de sistemas/Key users
* Executar os testes conforme descrito neste procedimento.
* Realizar os testes de desenvolvimento (FAT) após a aprovação do fornecedor, para auxiliar o entendimento do equipamento / software para o uso pretendido e atividades de validação.
  1. Proprietário do sistema
* Fornecer suporte para a realização das atividades de Validação.

# 6. Procedimento

## 6.1. Categorizar os sistemas computadorizados conforme descrito no SOP 20013925 – Validação de Sistemas Computadorizados, em sua versão vigente.

## 6.2. Após a aprovação do Controle de Mudanças, Criar o Plano de Validação para mapear os requisitos do projeto, conforme descrito no SOP 20013925 – Validação de Sistemas Computadorizados, em sua versão vigente.

## 6.3. Validação de software do equipamento/sistema

* + 1. Elaborar o protocolo de testes de validação conforme descrito neste procedimento e baseado na URS, FRS, Configuration Specification e / ou qualquer documento fornecido pelo fornecedor do software de prateleira. Os requisitos de IQ, OQ e PQ devem resultar no que foi estabelecido no Plano de Validação de acordo com a extensão e o uso pretendido do equipamento e software. O protocolo deve ser elaborado conforme o Template Brazil\_ Protocol QIQOQP\_Brazil - 20515589, em sua versão vigente. O protocolo depois de aprovado será o relatório de testes.

Observação: O teste não aplicável ao equipamento/sistema deverá ser removido do protocolo de testes.

* + - 1. Elaborar / aprovar o Relatório de Validação conforme descrito no SOP 20013925 – Validação de Sistemas Computadorizados, em sua versão vigente, após a execução do (s) protocolo (s) de testes de validação.
      2. Encerrar o Controle de Mudança após a conclusão de todas as atividades descritas no Plano de Validação.

6.3.2. Integridade de Dados

* + - 1. Garantir através dos testes de validação, a conformidade com os requisitos de integridade de dados conforme descrito no SOP 20665069 Integridade de dados, em sua versão vigente.
      2. Garantir o gerenciamento de acessos para impedir o acesso não autorizado ou alterações nos dados, conforme descrito no SOP 20291313 – Gerenciamento de Controle de Acesso e Perfil de Usuário, em sua versão vigente.
      3. Validar o equipamento/sistema computadorizado para o uso pretendido com testes específicos para garantir a integridade dos dados durante as operações, conforme descrito neste procedimento. Devem existir procedimentos locais ou globais para os seguintes processos:
    - Controle de acesso ao sistema e perfis de usuário.
    - Revisão do audit trail.
    - Arquivamento, backup e restauração.

## 6.4. Configuração do Sistema

* + 1. Registrar e manter atualizada a configuração do sistema durante o ciclo de vida do sistema. Este documento do fabricante deve incluir pelo menos: a configuração de hardware e software de cada componente relevante do sistema, a lista de todos os equipamentos do sistema e sua conexão com o componente do sistema, as configurações de senha configuradas, as políticas do sistema, as configurações de assinaturas eletrônicas (se aplicável), os registros eletrônicos gerados pelo sistema e seu (s) caminho (s), a referência do procedimento de backup e restauração em caso de falha do sistema, os níveis de acesso configurados e a matriz associada a cada grupo (ou tipo de usuário), referência à documentação de qualificação do equipamento, manual do usuário e manual de manutenção.

## 6.5. Qualificação de Instalação

* + 1. Realizar a qualificação de Instalação do sistema/equipamento. Registrar se os arquivos necessários foram carregados, se o sistema foi configurado conforme a especificação de configuração do fornecedor, se os procedimentos necessários foram elaborados / aprovados e os instrumentos calibrados. A Qualificação de Instalação é realizada antes da Qualificação de Operação.
    2. Documentação / Verificação do desenho-Tabela 1.

|  |  |
| --- | --- |
| Escopo do teste | 1. Verificar se os seguintes procedimentos estão presentes:  * Uso e manutenção do sistema (incluindo perfis e privilégios de usuário, gerenciamento de senhas, manutenção…) * Instalação e configuração do sistema * Gerenciamento de controle de mudanças * Gerenciamento de Desvios * Revisão periódica * Audit Trail e revisão de dados * Gerenciamento de Logbook * Gerenciamento de usuários * Backup * Descrição do processo de recuperação em caso de incidente * Processo e responsabilidades pelo archiving de dados * Locais aprovados para o armazenamento de dados  1. Verificar se os seguintes documentos estão presentes:  * Logbook do sistema * Documentação de treinamento do fornecedor * Manuais do sistema * Fichas técnicas relacionadas à interface / controladores, gerenciados pelo sistema (se aplicável) |
| Pré-requisito | N/A |
| Metodologia de teste | 1. Procedimentos  * Descrever os procedimentos detalhando o título, número, versão e data de efetivação (se aplicável)  1. Documentos  * Verificar se o logbook foi criado e conduzido de acordo com o procedimento da área sobre Gerenciamento de logbook. * Garantir que a matriz de funções esteja disponível e aprovada * Verificar a documentação de treinamento do fornecedor (se aplicável) * Descrever os manuais do sistema detalhando o título e número do código / versão * Relatar as fichas técnicas dos dados relacionadas à interface / controladores gerenciados pelo sistema (se aplicável) |
| Critério de aceitação | * Os procedimentos devem estar disponíveis pelo menos em draft * Os documentos devem estar disponíveis |

Tabela 1

* + 1. Verificação do Hardware/Equipamento -Tabela 2.

|  |  |
| --- | --- |
| Escopo do teste | * Verificar se as características de hardware do sistema e as conexões estão de acordo com os registros na documentação do fabricante, que descreve a especificação de configuração |
| Pré-requisito | N/A |
| Metodologia de teste | * Registrar as características de HW e comparar com as informações registradas na documentação que descreve especificação de configuração * Registrar as conexões HW |
| Critério de aceitação | * Os componentes de hardware do sistema estão instalados de acordo com a documentação que descreve a especificação de configuração |

Tabela 2

* + 1. Verificação do Software – Tabela 3.

|  |  |
| --- | --- |
| Escopo do teste | * Verificar se as versões do software, outro software necessário para o uso do sistema e do sistema operacional do cliente estão de acordo com a documentação do fabricante, que descreve a especificação de configuração |
| Pré-requisito | N/A |
| Metodologia de teste | * Registrar a identificação do PC, os sistemas operacionais, o software principal e software aplicativo (se aplicável) * Registrar o nome completo do SW, a versão do SW, a data de instalação do SW e o nome do fornecedor |
| Critério de aceitação | * O software está disponível e as versões relacionadas são compatíveis com a documentação que descreve a especificação de configuração * O sistema operacional do cliente está de acordo com a documentação que descreve a especificação de configuração |

Tabela 3

* + 1. Verificação da Configuração das Pastas -Tabela 4.

|  |  |
| --- | --- |
| Escopo do teste | * Verificar a presença de pastas utilizadas para salvar os dados, backup e archive * Verificar a programação de backup (Automatizado/periodicidade) * Verificar o nível de proteção da pasta * Verificar se as pastas não estão visíveis ou editáveis no aplicativo |
| Pré-requisito | N/A |
| Metodologia de teste | * Verificar e descrever se as pastas utilizadas para salvar os dados, archive e backup (no cliente local e no servidor) estão presentes * Verificar e descrever o roteiro de backup * Tentar excluir e modificar os dados em todas as pastas utilizadas para salvar os dados e o backup. Registre estas atividades * Tentar visualizar e / ou editar arquivos nas pastas no aplicativo. Registre estas atividades |
| Critério de aceitação | * Os dados são salvos nas pastas, conforme descrito na documentação do fabricante * O backup é realizado com métodos e horários que atendem às especificações * A pasta está protegida, os arquivos / dados não podem ser excluídos / modificados * As pastas não são visíveis e / ou editáveis no aplicativo |

Tabela 4

* + 1. Verificação da configuração de segurança de acesso/Antivírus – Tabela 5.

|  |  |
| --- | --- |
| Escopo do teste- segurança de acesso | * Verificar se as configurações de senha estão definidas de acordo com o SOP 20291313 – Gerenciamento de Controle de Acesso e Perfil de Usuário, em sua versão vigente, que descreve a configuração |
| Pré-requisito | N/A |
| Metodologia de teste | * Verificar e registrar os valores das configurações de senha:   + Expiração da senha   + Histórico de senhas   + Acesso negado   + As senhas devem ser alteradas no primeiro logon   + Complexidade da senha   + Logout automático do sistema |
| Critério de aceitação | * A configuração da senha é compatível com SOP 20291313 – Gerenciamento de Controle de Acesso e Perfil de Usuário, em sua versão vigente, que descreve a configuração |
| Escopo do teste- Antivírus | * Verificar se o SW antivírus está de acordo com a documentação do fabricante |
| Pré-requisito | * N/A |
| Metodologia de teste | * Relatar as informações de software antivírus (nome completo e versão do SW, data de instalação e nome do fornecedor) |
| Critério de aceitação | * O software está disponível no sistema e é compatível com o a documentação do fabricante * A versão do software antivírus e a data de instalação são registros informativos |

Tabela 5

* + 1. Verificação do Nível de Acesso – Tabela 6.

|  |  |
| --- | --- |
| Escopo do teste | * Verificar se o perfil do usuário e os privilégios relacionados estão configurados conforme a matriz de acessos aprovada |
| Pré-requisito | N/A |
| Metodologia de teste | * Verificar os usuários ativos do software e os privilégios da área relacionada |
| Critério de aceitação | * Os perfis de usuário e privilégios relacionados são configurados de acordo com a matriz de acessos aprovada |

Tabela 6

* + 1. Verificação de configuração de backup – Tabela 7.

|  |  |
| --- | --- |
| Escopo do teste | * Verificar a presença de pastas utilizadas para salvar os dados, backup e archive * Verificar a programação de backup (Automatizado/periodicidade) |
| Pré-requisito | N/A |
| Metodologia de teste | * Verificar e descrever se as pastas utilizadas para salvar os dados, archive e backup (no cliente local e no servidor) estão presentes * Verificar e descrever o roteiro de backup * Verificar se todas as pastas para salvar os backups possuem proteções para alteração e exclusão habilitadas. |
| Critério de aceitação | * Os dados são salvos nas pastas, conforme descrito na documentação do fabricante * O backup é realizado com métodos e horários que atendem às especificações * A pasta de backup está protegida, os arquivos / dados não podem ser excluídos / modificados * As pastas de backup não são visíveis e / ou editáveis no aplicativo |

Tabela 7

* + 1. Verificação de Instrumentos e Calibração – Tabela 8.

|  |  |
| --- | --- |
| Escopo do teste | * Verificar se os equipamentos/instrumentos foram calibrados/ |
| Pré-requisito | N/A |
| Metodologia de teste | * Verificar se o equipamento possui plano de calibração |
| Critério de aceitação | * Verificar se a calibração foi realizada conforme o plano de calibração |

Tabela 8

## Qualificação de Operação

* + 1. Realizar a qualificação de operação para verificar o correto funcionamento do equipamento / sistema, de acordo com a especificação dos requerimentos funcionais do fabricante. Realizar a Qualificação de operação após a conclusão da Qualificação de Instalação.
    2. Verificação do Gerenciamento de Usuários e Senhas -Tabela 9.

|  |  |
| --- | --- |
| Escopo do teste- Gerenciamento de usuários | * Verificar o gerenciamento de usuários |
| Pré-requisito | * Configurar o nível de acesso na Qualificação de Instalação * Criar um usuário para cada tipo de nível de acesso |
| Metodologia de teste | * Testar a criação de novo usuário: cadastrar do novo usuário, verificar que o usuário não pode ser duplicado, cadastrar usuário com o mesmo nome, mas com nível de acesso diferente * Testar alteração do nível de acesso de usuário * Testar desativação do usuário após tentativas malsucedidas de login * Testar de que o usuário não pode ser excluído, somente desativado |
| Critério de aceitação | * Cada nível de acesso opera conforme a matriz de acessos aprovada * O sistema opera conforme descrito na Especificação Funcional do fabricante * O Audit Trail é impresso e contém todas as ações executadas |
| Escopo do teste- Gerenciamento de senha | * Verificar se a configuração da senha está funcionando conforme descrito na documentação do fabricante (Especificação Funcional) |
| Pré-requisito | * Configurar a senha e o administrador do software durante a IQ, conforme SOP 20291313 – Gerenciamento de Controle de Acesso e Perfil de Usuário, em sua versão vigente |
| Metodologia de teste | * Testar as configurações de senha conforme descrito 20291313 – Gerenciamento de Controle de Acesso e Perfil de Usuário, número de caracteres, complexidade de senhas, expiração, histórico de senhas, acesso negado, alteração de senha no primeiro logon, senha padrão fornecida pelo fornecedor e logoff automático do sistema * Testar o acesso não autorizado: tentar fazer login no sistema sem inserir a senha, nome de usuário, senha incorreta, nome de usuário incorreto e com uma conta bloqueada * Testar sem o conhecimento da senha * Testar a possibilidade de alterar a senha em cada nível, de acordo com a matriz de funções |
| Critério de aceitação | * A configuração da senha opera como descrito na Especificação funcional do fabricante * O Audit Trail é impresso e contém todas as ações executadas |

Tabela 9

* + 1. Verificação do Gerenciamento de Grupo e Perfis de Usuários – Tabela 10.

|  |  |
| --- | --- |
| Escopo do teste | * Verificar a matriz de acessos |
| Pré-requisito | * Configurar o nível de acesso na Qualificação de Instalação * Criar um usuário para cada tipo de nível de acesso |
| Metodologia de teste | * Testar os diferentes perfis de acesso, conforme descrito na matriz de acesso aprovada e de acordo com a Especificação Funcional do fabricante. Verificar os diferentes níveis de acesso e as respectivas funcionalidades (sem acesso - somente leitura - gravação) * Testar todas as funcionalidades em cada nível de acesso - teste positivo (comportamento normal) e teste negativo (comportamento anormal) * Testar o acesso somente leitura para o usuário “convidado”, se aplicável |
| Critério de aceitação | * Cada nível de acesso opera conforme descrito na Especificação Funcional * O Audit Trail é impresso e contém todas as ações executadas |

Tabela 10

* + 1. Verificação do Gerenciamento de Lotes e Receitas/métodos – Tabela 11.

|  |  |
| --- | --- |
| Escopo do teste-Registros alterados | * Verificar a proteção do sistema contra alteração / exclusão de registros eletrônicos de Lotes e receitas/métodos. |
| Pré-requisitos | * Identificar todos os tipos de registros eletrônicos (ER) do sistema (exemplo: métodos, protocolos, receitas, dados brutos, relatórios, etc.) * Identificar o caminho de cada tipo de ER * Realizar o teste com todos os perfis de usuário |
| Metodologia de teste | * Tentar alterar os ERs (Lotes e Receitas/Métodos) pelo aplicativo * Tentar alterar os ERs (Lotes e Receitas/Métodos) pelo Sistema Operacional (pelo Windows Explorer) * Tentar alterar os ERs (Lotes e Receitas/Métodos) nas pastas de backup * Tentar renomear os ERs (Lotes e Receitas/Métodos) pelo aplicativo * Tentar renomear os ERs (Lotes e Receitas/Métodos) pelo Sistema Operacional (pelo Windows Explorer) * Tentar renomear os ERs (Lotes e Receitas/Métodos) nas pastas de backup * Tentar excluir os ERs (Lotes e Receitas/Métodos) pelo aplicativo * Tentar excluir os ERs (Lotes e Receitas/Métodos) pelo Sistema Operacional (pelo Windows Explorer) * Tentar excluir os ERs (Lotes e Receitas/Métodos) nas pastas de backup |
| Critério de aceitação | * Os dados eletrônicos (Lotes e Receitas/Métodos) do sistema são protegidos contra alterações / exclusões no sistema operacional e no software do aplicativo * O sistema está configurado conforme a Matriz de Funções aprovada |
| Escopo do teste-Inspeção de registros | * Verificar se o sistema gera cópias completas das informações contidas nos registros eletrônicos (Lotes e Receitas/Métodos) nos formatos eletrônico e impresso |
| Pré-requisitos | * Identificar todos os tipos de ERs do sistema (exemplo: métodos, protocolos, receitas, dados brutos, relatórios etc.) |
| Metodologia de teste | * Gerar uma cópia eletrônica (Lotes e Receitas/Métodos) para cada tipo de ER * Gerar uma cópia impressa para cada tipo de ERs (Lotes e Receitas/Métodos). |
| Critério de aceitação | * A cópia eletrônica e impressa foi gerada corretamente. * A cópia eletrônica e impressa contém as mesmas informações |

Tabela 11

* + 1. Verificação de Entradas inválidas – Tabela 12.

|  |  |
| --- | --- |
| Escopo do teste | * Verificar a capacidade do sistema para identificar entradas inválidas |
| Pré-requisitos | N/A |
| Metodologia de teste | * Verificar se cada campo de entrada de dados aceita apenas os valores do intervalo * Verificar se cada campo de entrada aceita apenas o formato configurado (por exemplo, numérico, alfabético) * Verificar os campos obrigatórios |
| Critério de aceitação | * O sistema não aceita valores incoerentes |

Tabela 12

* + 1. Verificação da Referência de Tempo -Tabela 13.

|  |  |
| --- | --- |
| Escopo do teste | * Verificar a função e a referência de hora |
| Pré-requisito | * Conectar à rede e configurar o GPO - objeto de política global (se aplicável) * Configurar o fuso horário na Qualificação de Instalação * Configurar a imagem do Windows (PCs stand alone) |
| Metodologia de teste | * Testar que o usuário não consegue alterar data / hora * Testar que somente o administrador do Windows consegue alterar a data / hora (acessando o GPO ou Windows security dos PCs stand alone) * Para sistemas conectados, testar a sincronização de data / hora com a rede * Testar que não há perda de dados após a alteração de data / hora |
| Critério de aceitação | * Data / hora bloqueada para o usuário * Data / hora acessíveis ao administrador do Windows * Data / hora sincronizada com a rede - servidor de data / hora (se aplicável) |

Tabela 13

* + 1. Verificação de Registros Alterados e Inspeção de Registros -Tabela 14.

|  |  |
| --- | --- |
| Escopo do teste- Registros alterados | * Verificar a proteção do sistema contra alteração / exclusão de registros eletrônicos |
| Pré-requisitos | * Identificar todos os tipos de registros eletrônicos (ER) do sistema (exemplo: métodos, protocolos, receitas, dados brutos, relatórios etc.) * Identificar o caminho de cada tipo de ER * Realizar o teste com todos os perfis de usuário |
| Metodologia de teste | * Tentar alterar os ERs pelo aplicativo * Tentar alterar os ERs pelo Sistema Operacional (pelo Windows Explorer) * Tentar alterar os ERs nas pastas de backup * Tentar renomear os ERs pelo aplicativo * Tentar renomear os ERs pelo Sistema Operacional (pelo Windows Explorer) * Tentar renomear os ERs nas pastas de backup * Tentar excluir os ERs pelo aplicativo * Tentar excluir os ERs pelo Sistema Operacional (pelo Windows Explorer) * Tentar excluir os ERs nas pastas de backup |
| Critério de aceitação | * Os dados eletrônicos do sistema são protegidos contra alterações / exclusões no sistema operacional e no software do aplicativo * O sistema está configurado conforme a Matriz de Funções aprovada |
| Escopo do teste-Inspeção de registros | * Verificar se o sistema gera cópias completas das informações contidas nos registros eletrônicos nos formatos eletrônico e impresso |
| Pré-requisitos | * Identificar todos os tipos de ERs do sistema (exemplo: métodos, protocolos, receitas, dados brutos, relatórios etc.) |
| Metodologia de teste | * Gerar uma cópia eletrônica para cada tipo de ER * Gerar uma cópia impressa para cada tipo de ERs |
| Critério de aceitação | * A cópia eletrônica e impressa foi gerada corretamente * A cópia eletrônica e impressa contém as mesmas informações |

Tabela 14

* + 1. Verificação do Procedimento de Backup de Sistema (Software) – Tabela 15.
       1. Geralmente, o backup de sistema é uma imagem de software para garantir a recuperação no caso de desastre. Gerar obrigatoriamente uma cópia do backup, a qual deverá ser armazenada em um sistema de armazenamento separado, caso os dados originais não permanecerem no sistema de origem, conforme descrito na figura 1.

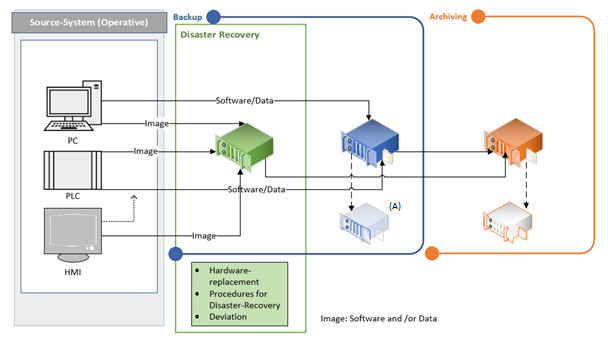


Figura 1: Ilustração dos termos: Backup, Recuperação de Desastres e Archive

|  |  |
| --- | --- |
| Escopo do teste | * Registro da rotina de backup de software (sistema) em um local de armazenamento seguro, conforme procedimento descrito na Qualificação de Instalação |
| Pré-requisito | * Realizar a avaliação de risco para determinar a frequência do backup de software conforme SOP 00150185 Gerenciamento de Backup, em sua versão vigente. |
| Metodologia de teste | * Testar todas as etapas de transferência de dados do backup de sistema, considerando todas as interfaces * Verificar que os dados backup de sistema foram transferidos corretamente (originais versus dados de backup) * Testar a autorização para o armazenamento do backup de sistema |
| Critério de aceitação | * O armazenamento é seguro e o acesso não autorizado não é possível * A transferência foi realizada corretamente. Os dados do backup de sistema permaneceram inalterados * O armazenamento está completo, todos os dados definidos na análise de risco (software, todos os dados originais e metadados, incluindo o audit trail) foram incluídos no (s) arquivo (s) de backup * Verificar a igualdade entre o check sum / atributos de dados dos dados originais e o backup (ex. tamanho do arquivo) |

Tabela 15

* + - 1. Se uma imagem for usada para fazer backup de software e ou dados, o formato dos dados originais e da imagem criada será diferente e não poderá ser comparado como descrito acima (ver item 6.6.7.1).
    1. Verificação do Procedimento de Restauração de Sistema – Tabela 16.
       1. A recuperação em desastres envolve um conjunto de políticas, ferramentas e procedimentos para permitir a recuperação ou continuação dos sistemas após um desastre natural ou induzido pelo homem. A recuperação de desastres concentra-se no suporte de TI para as funções críticas do negócio, em oposição à continuidade dos negócios, que envolve em manter todos os aspectos essenciais de uma empresa funcionando, apesar de eventos prejudiciais significativos. A recuperação de desastres pode, portanto, ser considerada como um subconjunto da continuidade dos negócios. Para executar uma recuperação, os dois processos principais podem ser usados e uma combinação dos dois pode ser estabelecida. Independentemente de como a recuperação é executada, é recomendável que haja um procedimento comum para o processo ou um específico para o sistema.

|  |  |
| --- | --- |
| Escopo do teste | * Recuperar o backup de sistema arquivados em um local seguro de armazenamento e archive |
| Pré-requisito | * O backup e archive de sistema estão disponíveis em um local seguro de armazenamento e archive |
| Metodologia de teste | * Testar todas as etapas de transferência de dados, considerando todas as interfaces (para backup e archive) * Testar a recuperação do sistema * Verificar se todos as informações do sistema foram transferidas corretamente * Testar a autorização para realizar a atividade |
| Critério de aceitação | * O teste de recuperação é realizado com sucesso. * A recuperação é completa. Todos as informações do sistema definidas na análise de risco (software, todos os dados originais e metadados, incluindo o audit trail) são recuperados * Os dados de backup e recuperação são idênticos (por exemplo, são idênticos via check sum ou tamanho de arquivo) * Após a recuperação, o sistema funciona conforme projetado |

Tabela 16

* + 1. Verificação do Procedimento de Backup e Arquivamento de Dados – Tabela 17.
       1. Geralmente, o backup é uma imagem de dados para garantir a recuperação no caso de perda de dados. Gerar obrigatoriamente uma cópia do backup, a qual deverá ser armazenada em um sistema de armazenamento separado, caso os dados originais não permanecerem no sistema de origem, conforme descrito na figura 1. Diferente do backup de dados, o archiving é o armazenamento de dados a longo prazo, onde o acesso direto não é mais necessário.

|  |  |
| --- | --- |
| Escopo do teste -backup de dados | * Recuperar o backup de dados arquivados em um local seguro de armazenamento e archive |
| Pré-requisito | * O backup e archive de dados estão disponíveis em um local seguro de armazenamento e archive |
| Metodologia de teste | * Testar todas as etapas de transferência de dados, considerando todas as interfaces (para backup e archive) * Testar de recuperação de dados únicos e recuperação total do sistema * Verificar se todos os dados foram transferidos corretamente * Testar a autorização para realizar a atividade |
| Critério de aceitação | * O teste de recuperação é realizado com sucesso. Os dados permanecem inalterados (para o backup e archive) * A recuperação é completa. Todos os dados definidos na análise de risco (software, todos os dados originais e metadados, incluindo o audit trail) são recuperados * Os dados de backup e recuperação são idênticos (por exemplo, são idênticos via check sum ou tamanho de arquivo) * Após a recuperação, o sistema funciona conforme projetado |
| Escopo do teste-arquivamento de dados | * Verificar a rotina de archive de dados e software para o processo de arquivamento |
| Pré-requisito | * Os dados relevantes são identificados (dados e metadados originais, incluindo audit trail) e estão disponíveis em backup * Técnico: O local de armazenamento é diferente do local de armazenamento principal |
| Metodologia de teste | * Testar todas as etapas de transferência de dados, considerando todas as interfaces * Verificar que todos os dados foram transferidos corretamente (originais versus dados de backup) * Testar a autorização para o armazenamento do achiving |
| Critério de aceitação | * O armazenamento é seguro e o acesso é limitado ao usuário autorizado * A transferência é realizada corretamente. Os dados permaneceram inalterados * O archive é concluído e todos os dados definidos foram incluídos pelo processo de arquivamento * Verificar a igualdade entre o check sum / atributos de dados dos dados originais e o backup (ex. tamanho do arquivo) |

Tabela 17

* + 1. Verificação do Procedimento de Restauração e Desarquivamento de Dados – Tabela 18.
       1. Uma imagem pode ser criada para garantir uma restauração rápida do sistema.
       2. Documentar a forma como a imagem do sistema é realizada, verificada e armazenada em um lugar seguro.
       3. Definir a frequência de geração de imagens baseada nos riscos e criticidade dos dados / sistema conforme SOP 00150185 Gerenciamento de Backup, em sua versão vigente.
       4. A imagem possivelmente terá um formato diferente dos dados originais. Portanto, a verificação da criação da imagem só pode ser realizada através da verificação de restauração.

|  |  |
| --- | --- |
| Escopo do teste-restauração de dados | * Verificar a criação da imagem e restauração de dados do sistema |
| Pré-requisito | * Técnico: O local de armazenamento é diferente do local de armazenamento principal |
| Metodologia de teste | * Testar todas as etapas de transferência de dados, considerando a criação e restauração de imagens * Verificar que todos os dados transferidos (dados originais versus dados restaurados) estão corretos * Testar a autorização para realizar o armazenamento de imagens |
| Critério de aceitação | * O armazenamento é seguro e o acesso é limitado ao usuário autorizado * A restauração de dados é realizada corretamente. Os dados permanecem inalterados * A restauração está completa e todos os dados definidos são incluídos pela restauração * Os dados de backup e recuperação são idênticos (por exemplo, idênticos via check sum ou tamanho de arquivo) * Após a recuperação, o sistema funciona conforme projetado |
| Escopo do teste-desarquivamento de dados | * Verificar a possibilidade de desarquivamentos dos dados após o processo de arquivamento |
| Pré-requisito | * Os dados relevantes são identificados (dados e metadados originais, incluindo audit trail) e estão disponíveis em backup * Técnico: O local de armazenamento é diferente do local de armazenamento principal |
| Metodologia de teste | * Testar todas as etapas de transferência de dados, considerando todas as interfaces * Verificar que todos os dados foram transferidos corretamente (originais versus dados de backup) * Testar a autorização para o desarquivamento dos dados. |
| Critério de aceitação | * O armazenamento é seguro e o acesso é limitado ao usuário autorizado * A transferência é realizada corretamente. Os dados permaneceram inalterados * O desarquivamento é concluído e todos os dados definidos foram incluídos pelo processo de desarquivamento no ambiente solicitado. * Verificar a igualdade entre o check sum / atributos de dados dos dados originais e o backup (ex. tamanho do arquivo) |

Tabela 18

* + 1. Verificação da Assinatura eletrônica – Tabela 19.

|  |  |
| --- | --- |
| Escopo do teste- alteração do registro de Assinatura eletrônica | * Verificar a proteção do sistema contra alteração / exclusão de registros eletrônicos de assinatura eletrônica |
| Pré-requisitos | * Identificar todos os tipos de registros de assinatura eletrônica (ER) do sistema * Identificar o caminho de cada tipo de ER * Realizar o teste com todos os perfis de usuário |
| Metodologia de teste | * Tentar alterar os ERs (assinatura eletrônica) pelo aplicativo * Tentar alterar os ERs (assinatura eletrônica) pelo Sistema Operacional (pelo Windows Explorer) * Tentar alterar os ERs (assinatura eletrônica) nas pastas de backup * Tentar renomear os ERs (assinatura eletrônica) pelo aplicativo * Tentar renomear os ERs (assinatura eletrônica) pelo Sistema Operacional (pelo Windows Explorer) * Tentar renomear os ERs (assinatura eletrônica) nas pastas de backup * Tentar excluir os ERs (assinatura eletrônica) pelo aplicativo * Tentar excluir os ERs (assinatura eletrônica) pelo Sistema Operacional (pelo Windows Explorer) |
| Critério de aceitação | * Os dados eletrônicos de assinatura eletrônica do sistema são protegidos contra alterações / exclusões no sistema operacional e no software do aplicativo * O sistema está configurado conforme a Matriz de Funções aprovada |
| Escopo do teste-Inspeção de registros de assinatura eletrônica | * Verificar se o sistema gera cópias completas das informações contidas nos registros de assinatura eletrônica nos formatos eletrônico e impresso |
| Pré-requisitos | * Identificar todos os tipos de assinatura eletrônica (ER) do sistema |
| Metodologia de teste | * Gerar uma cópia eletrônica para cada tipo de ER assinado eletronicamente. * Gerar uma cópia impressa para cada tipo de ERs assinado eletronicamente. |
| Critério de aceitação | * A cópia eletrônica e impressa foi gerada corretamente * A cópia eletrônica e impressa contém as mesmas informações |

Tabela 19

* + 1. Verificação da Proteção Audit Trail – Tabela 20.

|  |  |
| --- | --- |
| Escopo do teste | * Verificar se as alterações realizadas nas configurações do sistema / registro eletrônico são registradas automaticamente no audit trail e na configuração do sistema (por exemplo: acesso do usuário e alteração de horário se aplicável) * Verificar se há plano de revisão do audit Trail, conforme descrito no SOP 20658520 -Audit Trail Review, em sua versão vigente. |
| Pré-requisitos | * Identificar todos os tipos de ERs do sistema |
| Metodologia de teste | * Modificar a configuração do sistema (por exemplo: acesso do usuário e alteração de horário, se aplicável) * Verificar se os valores antigos e novos foram registrados * Verificar se o sistema registra o usuário, tipo de ação, data e hora da ação, valor antigo / novo e motivo da alteração * Tentar excluir ou modificar as informações do audit trail * Tentar desativar a funcionalidade da audit trail |
| Critério de aceitação | * O sistema rastreia automaticamente as modificações eletrônicas de registro e configuração no audit trail. Não é possível realizar modificações ou exclusões no audit trail |

Tabela 20

6.7. Qualificação de Desempenho (Performance)

* + 1. Verificação de que o equipamento e os sistemas auxiliares conectados executam as atividades de forma eficaz e reprodutível, baseado nos requerimentos dos usuários e métodos de processo aprovados. As Qualificações Operacionais e de Instalação devem ser executadas e concluídas antes do início da execução da Qualificação de Desempenho.
       1. Verificação de Documentação – Performance – Tabela 21.

|  |  |
| --- | --- |
| Escopo do teste | 1. Verificar se os procedimentos a seguir estão presentes   * Uso e manutenção do sistema (incluindo perfis e privilégios de usuário, gerenciamento de senhas, manutenção ...) * Instalação e configuração do sistema * Gerenciamento de mudanças * Gerenciamento de Desvios * Revisão periódica * Audit Trail e revisão de dados * Gerenciamento de Logbook * Verificação periódica de dados e restauração completa do sistema   2. Verificar se os usuários com acesso ao sistema possuem treinamento nos procedimentos |
| Pré-requisito | N/A |
| Metodologia de teste | 1. Procedimentos  * Descrever os procedimentos detalhando título, número, versão e data de efetivação  1. Verificar o treinamento nos procedimentos através da Plataforma de Treinamento / ManGo |
| Critério de aceitação | * Os procedimentos estão disponíveis, aprovados e efetivados no ManGo * Todos os usuários do sistema possuem treinamento nos procedimentos acima |

Tabela 21

* + - 1. Performance do Sistema (Corrida de Teste) – Tabela 22.
         1. Esse teste permite que o usuário final desafie o sistema no ambiente de produção. Os resultados deste teste serão usados para avaliar o desempenho do sistema.

|  |  |
| --- | --- |
| Escopo do teste | * Verificar o desempenho do sistema |
| Pré-requisito | * IQ concluído * OQ concluído * O sistema está pronto para a execução do primeiro lote |
| Metodologia de teste | * Executar o primeiro lote de acordo com os procedimentos locais |
| Critério de aceitação | * O Audit Trail contém todos os dados gerados durante a produção do primeiro lote * O sistema é capaz de operar como pretendido com as configurações definidas |

Tabela 22

* + - 1. Limpeza do Sistema (System Cleanup) – Tabela 23.

|  |  |
| --- | --- |
| Escopo do teste | * Realizar a limpeza dos dados criados durante a validação do software do equipamento (a ser executado antes ou depois do teste, conforme procedimento local) |
| Pré-requisito | * IQ concluído * OQ concluído |
| Metodologia de teste | * Com a conta de administrador e excluir as contas de usuário criados para a execução dos testes de OQ * Com a conta de administrador, excluir as receitas criadas para a execução dos testes de OQ, se aplicável * Com a conta de administrador, excluir os lotes criados para a execução dos testes de OQ, se aplicável |
| Critério de aceitação | * Todos os usuários do sistema são válidos e não existem usuários genéricos * Somente as receitas válidas estão configuradas * Apenas os lotes relevantes estão disponíveis |

Tabela 23

* + - 1. Testes de mitigação de riscos – Tabela 24.
         1. Permitir o desafio do sistema nas ações mitigatórias originadas na avaliação de riscos. Caso o processo de mitigação seja identificado antes da elaboração do protocolo de teste de QO os testes necessários serão incluídos no respectivo protocolo, caso contrário será inserido como anexo ao protocolo de testes.

|  |  |
| --- | --- |
| Escopo do teste | * Realizar os testes decorrentes das ações mitigatórias originadas na análise de risco do sistema |
| Pré-requisito | * Análise de risco do sistema * IQ concluído * OQ concluído |
| Metodologia de teste | * Gerar os testes referentes as ações mitigatórias descritas na análise de risco do sistema |
| Critério de aceitação | * O resultado do teste determina o controle do risco identificado na análise de risco |

Tabela 24

* 1. Relatório de Validação  
     1. Relatório resumido: documentar no relatório de validação os resultados, desvios, status final da validação e a autorização para o uso do sistema).

Nota: Para sistemas simples, a matriz de rastreabilidade e o relatório de validação podem ser combinados no mesmo documento.

* 1. Matriz de rastreabilidade  
     1. Descrever todos os testes realizados versus configuração, design, especificação funcional e requisitos do usuário, vinculando cada usuário e / ou requisito funcional a pelo menos um teste.
     2. Este documento deve ser usado para demonstrar que os requisitos do usuário e / ou funcionais foram testados.
  2. Geração e Arquivamento da Documentação de Validação.  
     1. Os documentos de Validação de Sistemas Computadorizados devem ser gerados eletronicamente no Sistema ManGo de acordo com SOP 20621886 - Gestão de Documentos de CSV e planilhas Merck Brasil no Sistema ManGo, em sua versão vigente e utilizando o template descritos nas referências. O protocolo de testes é aprovado conforme Tabela 8: Responsabilidades do SOP 20013925 – Validação de sistemas computadorizados em sua versão vigente.
     2. A documentação de Validação é arquivada no Sistema ManGo (Sistema Eletrônico de documentação), sendo de responsabilidade dos analistas/especialistas de Engenharia-CSV.
     3. O protocolo de Testes, após aprovado no sistema ManGo, deverá ser extraído utilizando o conteúdo primário (Primary Content) para o registro dos resultados dos testes (Fase execução). Caso necessário a utilização do protocolo em papel, utilizar o campo iniciais para inclusão da rubrica manuscrita do executor dos testes o revisor deverá incluir a assinatura/rubrica manuscrita na Conclusão Final dos Testes de Validação do protocolo de testes.
     4. Ao final do preenchimento eletrônico do protocolo de teste o executor deverá importar o documento no formato original para aprovação como relatório de teste (protocolo executado) no sistema ManGo conforme descrito no SOP 20621886 - Gestão de Documentos de CSV e planilhas Merck Brasil no Sistema ManGo, em sua versão vigente.
     5. O relatório de testes é aprovado conforme Tabela 8: Responsabilidades do SOP 20013925 – Validação de sistemas computadorizados em sua versão vigente

# 7. Referências

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

- SOP 20291313 - Gerenciamento de Controle de Acesso e Perfil de Usuário, em sua versão vigente;

- SOP 20621886 - Gestão de Documentos de CSV e planilhas Merck Brasil no Sistema ManGo-CARA, em sua versão vigente;

- SOP 00150185 - Gerenciamento de Backup, em sua versão vigente;

- SOP 20665069 - Integridade de dados, em sua versão vigente;

- SOP 20658520 -Audit Trail Review, em sua versão vigente;

- Módulo Corporativo 20378416 - Equipment Software Validation guideline, versão 2.0;

- Template Brazil\_ Protocol QIQOQP\_Brazil – 20515589, em sua versão vigente.

# 8. Histórico

|  |  |
| --- | --- |
| **VERSÃO** | **DESCRIÇÃO DA ALTERAÇÃO** |
| 1.0 | Versão Inicial |
| 2.0 | Item 5.2 – Inclusão do Controle de Mudanças.  Item 5.3.1 – Inclusão do template 20515589 e informação de que o protocolo QIQOQP depois de aprovado será o Relatório de testes.  5.5.2. Documentação / Verificação do desenho, Metodologia de teste, sub-item 2 – Documentos, alteração do texto para “procedimento da área”.  Exclusão do item 5.5.5. Verificação / ajuste de data/hora do sistema.  Renumeração dos subitens do item 5  Item 5.6.4. – Exclusão da nota. |
| 3.0 | Alteração no template do SOP com inclusão dos itens 1 (índice) e 9 (fluxograma).  Inclusão do item 6.10. Geração e Arquivamento da Documentação de Validação. |
| 4.0 | - Foi realizada a atualização do nome da área de Validação e Controle do Processo  para Garantia da Qualidade conforme TW 3365636. |
| 5.0 | - Alteração do autor de Jorge Ferreira para Luis Alberto Rodrigues  - Foi realizada a atualização das responsabilidades conforme TW 4206704.  - O item 6- procedimento foi reorganizado e incluído numeradores/marcadores e identificadores de tabelas.  - Foi atualizado o item 6.3.2.1 para descrição do SOP 20665069 - Integridade de Dados, em sua versão vigente.  - Foram atualizados os requerimentos do backup para a inclusão do SOP 00150185 - Gerenciamento de Backup, em sua versão vigente, nos itens 6.6.8.1- Tabela 14 e 6.6.11.3.  - Foi atualizado o escopo do teste de proteção de audit trail para a inclusão do SOP 20658520 -Audit Trail Review, em sua versão vigente, no item 6.6.13 – Tabela 19.  - Foi alterado o item 6.10 para atualização do processo de execução do protocolo de testes para contemplar o preenchimento em formato eletrônico.  - Atualização do Template Brazil\_ Protocol QIQOQP\_Brazil – 20515589 para alteração do layout e reorganização dos testes de CSV |

# 9. Fluxograma

Categorizar o Sistema

Aprovação do Controle de Mudança

Criação/Aprovação

do Plano de Validação

Elaboração/Aprovação

Protocolo de Testes

QI\_QO\_QP

Execução do Relatório de Testes

Elaboração/Aprovação

Relatório de Validação

Encerrar Controle de Mudança

# 10. Anexos

Não Aplicável.