ForMEQ

Fórum Internacional de
Metrologia e Examinologia em Química

Guia para sistemas informatizados em laboratórios

1ª edição

Out 2024

Guia para sistemas informatizados em laboratórios

Primeira edição

Este documento foi produzido pelo ForMEQ, fornecendo orientação para que os laboratórios possam fazer a gestão adequada dos seus sistemas informatizados.

Editores

Bruna Drielen Ferreira
Denise de Fátima Gonçalves
Kaique Dias Galera
Vitor Hugo Polisél Pacces (Responsável)

Grupo de trabalho

Alice Mosca
Bernardo José G. de Aragão
Bruna Drielen Ferreira
Carla Palma
Cecilia Cristina Marques dos Santos
Denise de Fátima Gonçalves
Elcio Cruz de Oliveira
Felipe Rebello Lourenço
Fernando Cordeiro Raposo
Florbela Dias
Jean Felipe de Faria Cardoso
Kaique Dias Galera
Marcio Ribeiro Machado
Otávio Arruda Heringer
Thábita Thiciana Bastos Marchezi
Tony Rogério de Lima Dadamos
Vanessa Morgado
Vitor Hugo Polisél Pacces (Responsável)

Como citar o guia

O presente guia deve ser citado como: Guia para sistemas informatizados em laboratórios (FORMEQ)

Sumário

1. PREÂMBULO 4
2. OBJETIVO 4
3. INTRODUÇÃO 4
4. GLOSSÁRIO 5
5. REQUISITOS 7
5.1. HARDWARE 7
5.1.1. GERAL 7
5.1.2. AQUISIÇÃO E AVALIAÇÃO 7
5.1.3. MANUTENÇÃO PREVENTIVA E CORRETIVA 8
5.1.4. BIOS E FIRMWARE 9
5.2. SEGURANÇA 9
5.2.1. ANTIVÍRUS 9
5.2.2. FIREWALL 10
5.3. SISTEMA OPERACIONAL 10
5.3.1. GERAL 10
5.3.2. MANUTENÇÃO 11
5.3.3. CONTROLE DE USUÁRIO 11
5.4. SOFTWARES DE BANCADA 11
5.4.1. GERAL 11
5.4.2. PLANILHAS 12
5.4.3. BANCO DE DADOS DE ESCRITÓRIO 13
5.4.4. EDITORES 14
5.5. DEMAIS SOFTWARES 15
5.5.1. GERAL 15
5.5.2. VALIDAÇÃO 15
5.5.3. APLICAÇÃO 17
5.6. REDES E ARMAZENAMENTO EM NUVEM 17
5.7. BACKUPS 18
5.8. PROCEDIMENTOS E MANUAIS 19
5.9. REGISTROS 19
5.10. CONTRATOS 20
6. REFERÊNCIAS 20

Guia para Sistemas Informatizados em Laboratório

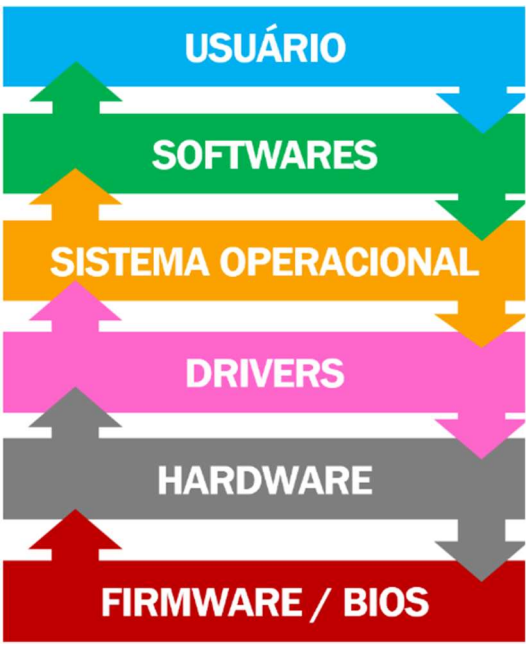
1. Preâmbulo

Considerando que o emprego de sistemas informatizados (Hardware + Softwares) nos laboratórios para obtenção, cálculo, processamento e armazenamento de dados pode afetar diretamente os resultados obtidos seja em um ambiente regido ou não por Sistemas de Gestão da Qualidade em laboratórios (como ISO/IEC 17025, ISO 17043, ISO 17034, ISO 15189); considerando ainda, a interdisciplinaridade do assunto, onde se torna necessário o conhecimento de três áreas: Sistema de Gestão, Informática e Laboratórios, fato que dificulta a compreensão, aplicação e avaliação destes requisitos relacionados às normas citadas, elaborou-se o presente guia.

2. Objetivo

Este guia fornece recomendações gerais e requisitos gerais para a correta utilização de sistemas informatizados em laboratórios que fazem uso de Sistemas de Gestão ou laboratórios que tenham preocupação da utilização correta destes sistemas, de forma que estes não interfiram adversamente nos resultados analíticos.

3. Introdução



Os sistemas informatizados são definidos por diferentes componentes, sendo classificados de maneira generalizada como hardwares e softwares. Portanto, pode ser definido especificamente como qualquer equipamento em que ocorra a realização das atividades de processamento, armazenamento, ou transmissão de dados utilizando-se de componentes eletrônicos e com capacidade de programação. Assim, a título de exemplo, podemos citar os desktops, laptops, tablets, celulares, equipamentos complexos de laboratório que possuam um software gerenciável, dentre outros. O Firmware / Bios são a peça fundamental pois controlam a inicialização e todas as funções básicas do hardware, que por sua vez relacionam-se diretamente com as atividades realizadas com os dados (processamento, armazenamento e transmissão). Para que estas operações sejam realizadas de forma coerente necessitamos de um “tradutor” para que as entradas e comandos realizados no Sistema Operacional possam ser realizadas a contento com relação aos dados. Este é o papel dos drivers. O Sistema Operacional por sua vez, facilita o acesso dos softwares e do próprio

usuário, podendo criar uma interface de comandos e ações para que não haja a necessidade de programação em linguagens próprias para se realizar as atividades com os dados. Os softwares por sua vez, são desenvolvidos para atuarem em um ou mais sistemas operacionais, fazendo o uso dos recursos nativos, facilitando a operação com os dados. O usuário é inerente aos sistemas informatizados por ser parte atuante do mesmo. Um comportamento inadequado deste indivíduo pode colocar em risco toda a cadeia apresentada anteriormente, mesmo que esta esteja adequada ao uso.

O presente guia foi desenvolvido para ser um documento orientativo. Para fins de utilização e a correta proteção e integridade dos dados, define-se os termos:

- **Deve:** este item é primordial para a garantia dos sistemas informatizados em todo ou em parte
- **Preferencialmente ou convém**: este item remete a práticas que auxiliam na integridade do sistema informatizado
- **Pode:** termos que utilizem podem oferecem alternativas ou permissões para determinadas atividades.
- **Quando aplicável:** se a condição for atendida, o mesmo assume a mesma caraterística do termo “deve”.

4. Glossário

Adware
Software que exibe anúncios indesejados em aplicativos ou navegadores.

Backup
Cópia de segurança dos dados importantes, geralmente armazenada em outro local para recuperação em caso de perda ou falha.

Benchmark
Teste de desempenho que compara o hardware ou software com padrões conhecidos.

BIOS (Basic Input/Output System)
Firmware embutido em placas-mãe que controla a inicialização do computador e configurações básicas.

Desktop
Computador pessoal projetado para uso em uma mesa ou estação de trabalho fixa.

Drivers
Programas que permitem a comunicação entre o sistema operacional e dispositivos de hardware específicos, como placas de vídeo, impressoras e teclados.

Firewall
Sistema de segurança que controla o tráfego de rede, permitindo ou bloqueando conexões com base em regras.

Firmware
Software embutido em dispositivos de hardware (como impressoras, placas-mãe, roteadores e unidades de armazenamento) que controla suas operações.

Funções
Blocos de código reutilizáveis que realizam tarefas específicas em programas ou scripts.

Hardware
Refere-se aos componentes físicos de um sistema computacional, como processadores, memória, placas-mãe, discos rígidos e periféricos.

Log
Registro detalhado de eventos ou atividades em um sistema, usado para diagnóstico e auditoria gerados automaticamente pelo software.

Malware
Termo genérico para software malicioso, incluindo vírus, worms e cavalos de Troia.

Manutenção Corretiva
Intervenções após falhas ou problemas, como reparos de hardware ou correções de software.

Manutenção Preventiva
Práticas regulares para evitar problemas futuros, como limpeza de poeira, atualizações de software e backups.

Mídias Físicas
Suportes físicos de armazenamento, como CDs, DVDs, Blu-rays ou pendrives, usados para instalar ou recuperar sistemas operacionais e aplicativos.

Notebook (Laptops)
Computador portátil e compacto, projetado para mobilidade e uso em qualquer lugar.

Objetos
Elementos de programação que representam dados ou funcionalidades em linguagens de programação.

Pasta Térmica
Material aplicado entre o processador e o dissipador de calor para melhorar a transferência de calor.

Reinstalação Limpa
Processo de formatar e reinstalar completamente o sistema operacional, eliminando quaisquer configurações ou programas antigos.

Sistemas Informatizados
Conjunto de hardware, software e dados que trabalham juntos para realizar tarefas específicas. Inclui sistemas operacionais, aplicativos e bancos de dados.

Sistemas Operacionais
Software que gerencia recursos de hardware e permite a execução de aplicativos. Exemplos incluem Windows, macOS, Linux e Android.

Software
Conjunto de programas, aplicativos e sistemas operacionais que executam tarefas específicas em um computador.

Spyware
Software malicioso que monitora atividades do usuário sem consentimento.

Terminal
Interface de linha de comando que permite interagir diretamente com o sistema operacional.

5. Requisitos

5.1. Hardware

5.1.1. Geral

5.1.1.1. Todo equipamento (hardware) deve possuir procedimentos para uso e manutenção, de modo a assegurar seu correto funcionamento e para evitar deterioração e/ou corrupção dos dados. Os sistemas informatizados, quando aplicável, deve apresentar identificação única e inequívoca.

5.1.1.2. Os equipamentos devem ser instalados em local apropriado, limpo, com condições ambientais controladas e sem interferentes (poeira, fontes de calor, umidade elevada, dentre outros) e com rede elétrica apropriada e/ou fonte de rede elétrica estabilizada. As mídias físicas e backups também devem atender o presente requisito.

5.1.1.3. Equipamentos que não estejam seguros, adequados ou sem manutenção periódica realizada no período apropriado e determinado em procedimento, devem ser identificados como tal e não poderão ser utilizados até que seu estado ideal seja retomado.

5.1.1.4. Os requisitos de hardware exigidos pelos softwares a serem utilizados, devem ser atendidos, não sendo permitidos requisitos menores dos que os estabelecidos como mínimos pelos softwares utilizados.

5.1.1.5. Deve existir um registro que relacione a identificação do sistema informatizado com as peças, acessórios e periféricos que o compõe.

5.1.2. Aquisição e avaliação

5.1.2.1. Deve-se assegurar que sejam utilizados somente equipamentos adequados, de fornecedores avaliados e que tais equipamentos tenham sido verificados quanto aos requisitos mínimos quando da sua chegada ao laboratório e antes da sua utilização. Estas atividades devem ser descritas em procedimento e registradas.

5.1.2.2. Serviços de manutenção externos podem ser utilizados, desde que realizado por empresas idôneas e de atuação na área de manutenção.

5.1.3. Manutenção Preventiva e Corretiva

5.1.3.1. Devem existir procedimentos que garantam quais avaliações e manutenções preventivas devem ser aplicadas aos hardwares, definindo a periodicidade destas atividades e registrando-as quando realizadas.
Nota: *As atualizações de hardware são entendidas como manutenções necessitando ser registradas, porém sem a necessidade de serem descritas em procedimento, uma vez que decorrem da avalição da necessidade frente a utilização ou requisitos mínimos de softwares. Incluem-se nestas manutenções verificações da saúde do disco, limpezas internas dos gabinetes (desktops ou notebooks), troca de pasta térmica, testes de benchmark, entre outros.*

5.1.3.2. As manutenções preventivas ou corretivas devem ser antecedidas de backup dos dados analíticos ou registros digitais relativos ao Sistema de Gestão.

5.1.3.3. Após qualquer manutenção ou troca de equipamento deve ser avaliada a adequação do sistema informatizado de acordo com os presentes requisitos. O mesmo se aplica quando houver a necessidade de recuperação emergencial utilizando-se os backups. Esta atividade deve ser descrita em procedimento e registrada. Devem ser avaliados os impactos, registradas todas e quaisquer perdas de dados ocorridas em função da recuperação emergencial, bem como as medidas tomadas a respeito.

5.1.3.4. Caso ocorram problemas que não possam ser resolvidos imediatamente e que levem à inutilização dos sistemas e, caso os trabalhos não possam ser interrompidos, devem existir outras formas de se garantir o registro de dados de forma segura e conforme descrito em procedimento. Retornar estes dados o mais prontamente possível para o sistema, registrando as atividades.

5.1.3.5. Quando os equipamentos forem enviados para manutenções preventivas ou corretivas externas ao laboratório, a confidencialidade e integridade dos dados deve ser preservada.
Nota: *A confidencialidade pode ser acautelada, por exemplo, por meio de cláusulas contratuais juridicamente vinculativas. Quanto à integridade pode ser garantida por meio de backups.*

5.1.3.6. É recomendável que os sistemas operacionais e todo o conjunto de softwares de cada terminal passe por uma reinstalação limpa, com uma dada periodicidade.
Nota: A instalação de alguns aplicativos, a desinstalação de softwares, desligamentos incorretos, quedas de energia e outros comportamentos anormais, podem originar erros nos registros do Sistema Operacional, fragmentos e arquivos corrompidos no armazenamento, entre outros.

Estas situações provocam travamentos, lentidão e comportamentos não ideais nestas máquinas, comprometendo assim a integridade dos dados do laboratório nelas presentes.

5.1.4. Bios e Firmware

5.1.4.1. As BIOS e os Firmwares devem estar atualizados para garantir a correta compatibilidade e segurança dos equipamentos. As atualizações devem ser realizadas por pessoal habilitado e devidamente autorizado. Periodicamente devem ser verificadas novas atualizações.

5.2.Segurança

5.2.1. Antivírus

5.2.1.1. Deve existir um software antivírus atualizado, ativo e instalado nas máquinas que obtenham, calculem, processem e/ou armazenem dados analíticos ou registros digitais relativos ao sistema de gestão.
Nota: *Não devem ser utilizados antivírus gratuitos pois estes são destinados ao uso pessoal e domiciliar.*

5.2.1.2. O banco de dados do antivírus deve ter atualização automática e ser realizada no mínimo de forma diária.

5.2.1.3. Devem ser realizadas verificações da presença de vírus de forma rápida (verificação do Sistema Operacional, memória e arquivos de configuração) ao menos uma vez ao dia, e de forma completa e, no mínimo, uma vez na semana. As verificações podem ser realizadas de forma automatizada e agendadas.

5.2.1.4. O antivírus deve possuir proteção ativa e contínua do computador com prevenção às intrusões.

5.2.1.5. Devem ser mantidos relatórios e logs dessas atividades, podendo ser dentro do próprio programa de antivírus.

5.2.1.6. O mesmo antivírus poderá atuar como antispyware, antiadware, antimalware e firewall. No entanto, se o antivírus não cobrir estas atuações deverão existir programas para prevenir e eliminar estes malwares, igualmente descritas em procedimento e registradas.

5.2.1.7. O antivírus deverá ser capaz de remover os malwares quando localizados. Caso o antivírus não seja suficiente para a remoção dos malwares, devem ser registradas quais as ações adicionais que foram executadas para esse fim.

5.2.2. Firewall

5.2.2.1. Deve existir um firewall ativo para evitar ataques a rede ou dados encaminhados de forma inapropriada.
Nota: *O mesmo antivírus poderá atuar como firewall. No entanto, se o antivírus não cobrir esta atuação deve existir um programa para prevenir e eliminar ataques de rede.*

5.2.2.2. Devem ser mantidos relatórios e logs dessas atividades, podendo ser dentro do próprio programa de antivírus ou outro programa que exerça esta tarefa.

5.3. Sistema Operacional

5.3.1. Geral

5.3.1.1. O Sistema Operacional e demais softwares que são executados utilizando-o como base devem ser originais, não sendo admitidas cópias piratas ou subterfúgios para utilização de cópias não autorizadas. O Sistema Operacional deve estar ativado.

5.3.1.2. O Sistema Operacional deve ser compatível com o hardware onde é instalado atendendo pelo menos aos requisitos mínimos preconizados para o mesmo.

5.3.1.3. Os softwares a serem instalados no computador devem ser compatíveis com o Sistema Operacional utilizado.

5.3.1.4. A Edição do Sistema Operacional utilizada (por exemplo, para PCs: Windows 8.1, Windows 10 ou Windows 11; para Computadores Apple: macOS 14: Sonoma; macOS 13: Ventura macOS 12: Monterey) deve estar em vigência de acordo com o ciclo de vida do Sistema Operacional.
Nota: *Exemplo de ciclo de vida de Sistema Operacional: https://learn.microsoft.com/pt-br/lifecycle/products/windows-11-home-and-pro*

5.3.2. Manutenção

5.3.2.1. O Sistema Operacional deve ser atualizado com a última versão disponível, preferencialmente tendo seu mecanismo de atualização automática ativado.
Nota: *não confundir edição (por exemplo, Windows 11, Windows 10 e similares) com versão (por exemplo, 23H2, 22H1 e similares)*

5.3.2.2. Os drivers dos dispositivos instalados devem estar atualizados com a última versão disponibilizada pelo fabricante.

5.3.2.3. Não devem existir conflitos ou problemas com os dispositivos instalados na máquina (verificar a existência em um gerenciador de dispositivo).

5.3.2.4. Devem existir procedimentos que descrevam como são realizadas as manutenções e avaliações preventivas referentes aos sistemas operacionais.
Nota: *entende-se que ao descrever esta atividade em procedimento, devem existir evidências de sua execução, podendo ser a partir dos "logs" dos próprios softwares.*

5.3.2.5. Qualquer Restauração ou Recuperação do Sistema Operacional, deve ser seguida de uma verificação, assegurando-se que nenhum dispositivo, aplicativo ou arquivo foi perdido ou danificado, durante esse processo.

5.3.3. Controle de usuário

Deve haver controle de usuário que impeça pessoas não autorizadas de acessar computadores que obtenham, calculem, processem e/ou armazenem dados analíticos ou registros digitais relativos ao Sistema de Gestão.

5.4. Softwares de bancada

5.4.1. Geral

5.4.1.1. Somente os pacotes tipo "office" (de escritório) são considerados softwares de bancadas e, portanto, validados. Este tipo de pacote está disponível comercialmente e contém planilhas eletrônicas, bancos de dados e/ou editores de texto. Os outros tipos de softwares devem ser tratados como "Demais Softwares" neste documento e atender aos presentes requisitos.

5.4.1.2. Não devem ser utilizadas versões não originais, não licenciadas, não sendo admitidas cópias piratas ou subterfúgios para utilização de cópias não autorizadas destes softwares, devendo ser mantidos registros de compra ou aquisição destes ou outra forma que garanta sua legitimidade.

5.4.1.3. O pacote dos softwares de escritório deve ser atualizado periodicamente. Essa periodicidade deve ser definida em procedimento e registrada.

5.4.1.4. As modificações, inserções e exclusões realizadas nos dados (registros eletrônicos) devem conter a identificação de quem as realizou, a data e, se aplicável (por exemplo, por requisição de algum procedimento interno, guia ou norma), a justificativa das mesmas. O dado anterior a exclusão ou modificação deve ser passível de verificação.
Nota: *Para registros técnicos, principalmente os contendo resultados ou observações analíticas, este item deve ser integralmente aplicado. Para registros relacionados a gestão, que não contenham resultados ou observações analíticas, este requisito é apenas preferencial. Não há necessidade de se aplicar este requisito para procedimentos, instruções ou documentos similares, uma vez que são cobertos pelo histórico de modificações destes.*

5.4.1.5. No caso de se utilizar programação como complemento às planilhas, aos bancos de dados ou aos documentos (por exemplo, uso de VBA – Visual Basic for Application ou Python), os requisitos a serem aplicados devem ser os mesmos quando da criação ou aquisição de software para uma determinada finalidade, seguindo os requisitos do item 5.5 Demais Softwares.

5.4.1.6. Caso os documentos gerados (planilhas, banco de dados, documentos e outros) precisem ser utilizados por um determinado usuário ou grupo de usuários, deve existir uma forma de controle de acesso (somente leitura ou permitindo controle total) restringindo-se apenas a estes usuários ou grupos.

5.4.2. Planilhas

5.4.2.1. Antes das planilhas serem colocadas em uso, devem ser validadas e as células contendo cálculos (fórmulas) devem ser bloqueadas com senhas para evitar alterações (com exceção das células em que ocorrerão entradas de dados).

5.4.2.2. Todos os cálculos (fórmulas) devem ser verificados com relação à exatidão dos resultados apresentados e a célula correta de origem dos dados utilizados nos cálculos. Considerar valores numericamente baixos e valores numericamente altos, decimais e inteiros e, em casos específicos, números em notação científica, dentro do intervalo de utilização da planilha. As verificações devem ficar registadas.

5.4.2.3. Fórmulas que utilizem comandos e expressões condicionais ('contar se', 'se', 'somar se',...), operadores lógicos ('e', 'ou', 'não', 'é verdadeiro', 'é falso',...), formatações condicionais que utilizem cores, fontes, símbolos, marcadores ou outra forma de apresentação da avaliação de resultados e/ou comandos de outras linguagens de programação, devem ser testadas através de diferentes entradas que resultem em células, contemplando as diferentes avaliações dos comandos e expressões condicionais. As verificações devem ficar registadas.

5.4.2.4. Quando gráficos forem gerados, devem ser verificados frente aos valores entrados e calculados.

5.4.2.5. Ao utilizar o recurso autocompletar presente nas planilhas eletrônicas não será necessário verificar todas as células que fizeram uso desse recurso a partir de uma 'fórmula mãe'. Porém, deve-se avaliar algumas células geradas automaticamente, incluindo a célula que contém a 'fórmula mãe'.
Nota: *entende-se por 'fórmula mãe', a fórmula que foi utilizada na célula de referência para o comando autocompletar.*

5.4.2.6. Deve ser mantido histórico das versões após as modificações destas planilhas.

5.4.2.7. Deve ser elaborado um relatório da validação destas planilhas contendo todas as verificações realizadas de acordo com estes requisitos. A pessoa responsável deverá autorizar o uso desta planilha aprovando e assinando esse relatório.

5.4.3. Banco de dados de escritório

5.4.3.1. Deve-se avaliar os objetos e funções presentes em cada janela e definir testes de inserção, eliminação, alteração e pesquisa de informações com o objetivo de verificar se o programa funciona conforme o uso pretendido.

5.4.3.2. Para objetos ou conjuntos de objetos que estão relacionados com a inserção e criação de novos dados, deve-se inserir uma nova informação no banco de dados e verificar se esta foi devidamente salva.
Nota: *podem ser incluídas novas informações (inexistentes) na base de dados ou, se aplicável, realizar testes de redundância (inserir informações*

que já existam; por exemplo, tentar inserir outro usuário com a mesma identificação para verificar o tratamento da situação).

5.4.3.3. Para edição e alteração de dados, realizar a alteração de um dado fictício previamente inserido. Pesquisar a nova informação verificando se a alteração foi realizada.

5.4.3.4. Para objetos ou conjuntos de objetos relacionados a exclusão de dados inserir um dado fictício e depois removê-lo utilizando os objetos em estudo. Pesquisar a informação previamente deletada, verificando se ela está ausente e se é retornada uma mensagem sobre tal ausência.

5.4.3.5. Para objetos ou conjuntos de objetos que realizam pesquisa ou retorno de dados, deve-se pesquisar informações existentes e inexistentes. Avaliar se a resposta recebida corresponde ao que foi pesquisado. Considerar pesquisas de palavras ou objetos similares para que não ocorram falsos positivos. Considerar respostas únicas e múltiplas.

5.4.3.6. Fórmulas que utilizam condicionais e operadores lógicos (‘e’, ‘ou’, ‘não’, ‘é verdadeiro’, ‘é falso’,...), formatações condicionais que utilizam cores, fontes, símbolos, marcadores ou outra forma de apresentação de avaliação de resultado e/ou comandos de outras linguagens de programação, devem ser testadas diferentes entradas que resultem em células, contemplando os diferentes resultados das condicionais e comandos. Registrar estas verificações.

5.4.3.7. Deve-se registrar no relatório de validação todos os testes realizados e respectivos resultados, bem como a conclusão sobre a aplicação do banco de dados ou não.

5.4.4. Editores

5.4.4.1. Basicamente, se os documentos aplicados (procedimentos, formulários, instruções ou documentos similares) criados em editores de textos forem armazenados somente em formato digital, esses devem ser controlados de forma a conter a identificação de quem os criou / modificou e em qual data. Caso seja aplicável (por exemplo, se o laboratório atuar em um Sistema de Gestão ou por requisição de algum procedimento interno, guia ou norma) devem ser incluídas as justificativas de tais alterações.

5.4.4.2. Deve existir um histórico das versões anteriores destes documentos (anterior às modificações) de forma organizada.

5.4.4.3. Documentos que necessitem de assinaturas e sejam armazenados somente eletronicamente, não existindo na forma física, devem possuir alguma forma de assinatura eletrônica, podendo envolver certificações de identidade ou assinaturas controladas por meio de logins e senhas, devidamente registradas no próprio documento ou em um software para este fim. São admitidas assinaturas de recursos do próprio software.

5.5.Demais Softwares

5.5.1. Geral

5.5.1.1. Independentemente de os softwares serem desenvolvidos sob demanda, adquiridos de terceiros ou desenvolvidos internamente, todos devem atender aos requisitos presentes nesse guia.

5.5.1.2. Os softwares devem ser instalados considerando, ao menos, os requisitos mínimos de software (Sistema Operacional, frameworks, complementos e outros similares) e de hardware.

5.5.1.3. Todo software deve ter números de versões controlados e estes números devem estar disponíveis no próprio software, podendo ser facilmente consultado. Cada alteração do software disponibilizada deve receber um novo número de versão.

5.5.1.4. Ao finalizar uma versão modificada, o software deve ser validado novamente, total ou parcialmente, dependendo da extensão das modificações seguindo os presentes requisitos antes de ser disponibilizado para uso.

5.5.2. Validação

5.5.2.1. A Validação deve ser realizada por objeto ou por funcionalidade (contendo vários objetos com um mesmo propósito e presente em uma mesma página ou janela). Funcionalidades diferentes ou janelas ou páginas diferentes devem ser avaliadas de forma individual.

5.5.2.2. Quando são realizados os cálculos, independentemente de serem simples ou complexos, os mesmos devem ser verificados utilizando-se outra fonte de cálculo, avaliando-se os resultados apresentados pelo software. Considerar valores numéricos baixos e valores numéricos altos, decimais e inteiros e, em casos específicos, números científicos, dentro do intervalo de utilização do software. Registrar estas verificações.

5.5.2.3. Funcionalidades que utilizam comandos e expressões condicionais (‘se’, ‘execute enquanto’,... em comandos relativos a linguagem utilizada), operadores lógicos (‘e’, ‘ou’, ‘não’, ‘é verdadeiro’, ‘é falso’,... em comandos relativos a linguagem utilizada), formatações condicionais que utilizam cores, fontes, símbolos, marcadores ou outra forma de apresentação de avaliação de resultado e/ou comandos de outras linguagens de programação, devem ser testadas com diferentes entradas contemplando os diferentes resultados dos comandos e expressões condicionais. As verificações devem ficar registadas.

5.5.2.4. Quando forem gerados gráficos referentes aos dados ou resultados, estes devem ser verificados .

5.5.2.5. Deve-se avaliar os objetos e funções presentes em cada janela e definir testes de inserção, eliminação, alteração e pesquisa de informações com o objetivo de verificar se o programa funciona conforme o uso pretendido.

5.5.2.6. Para objetos ou conjuntos de objetos que estão relacionados com a inserção e criação de novos dados, deve-se inserir uma nova informação no banco de dados e verificar se esta foi devidamente salva.
Nota: *podem ser incluídas novas informações (inexistentes) na base de dados ou, se aplicável, realizar testes de redundância, como inserir informações que já existam (por exemplo, tentar inserir outro usuário com a mesma identificação para verificar o tratamento da situação)*

5.5.2.7. Para edição e alteração de dados, realizar a alteração de um dado fictício previamente inserido. Pesquisar a nova informação, verificando se a alteração foi realizada.

5.5.2.8. Para objetos ou conjuntos de objetos relacionados com a exclusão de dados, inserir um dado fictício e depois removê-lo utilizando os objetos em estudo. Pesquisar a informação previamente eliminada, verificando se está ausente e se é retornada uma mensagem sobre tal ausência.

5.5.2.9. Para objetos ou conjuntos de objetos que realizam pesquisa ou retorno de dados, deve-se pesquisar informações existentes e inexistentes. Avaliar se a resposta recebida é correspondente ao que foi pesquisado. Considerar pesquisas de dados e informações similares para que não ocorram falsos positivos. Considerar respostas únicas e múltiplas.

5.5.2.10. O relatório de validação do software deve conter evidência de todos os testes realizados, bem como a conclusão e extensão de uso do software. Caso alguma funcionalidade, objeto ou janela apresentem erros nos testes que inviabilizem seu uso, mas não o uso parcial do restante do software, deve-se enfatizar estas informações no relatório. Caso não seja possível bloquear funcionalidades, objetos ou janelas que apresentem problemas ou erros no próprio software, deve-se informar estes problemas no procedimento de uso do software ou em seu manual.

5.5.3. Aplicação

5.5.3.1. Se os mesmos softwares forem instalados em diferentes computadores ou terminais, não há necessidade de se avaliar se os mesmos são executados de forma adequada, desde que os requisitos mínimos para uso desse software sejam verificados e aplicados os demais requisitos do presente guia.

5.5.3.2. Os usuários do software devem ter treinamento adequado para as funções que forem desempenhar com relação a este software.

5.5.3.3. O software deve conter controle de identificação de usuário para que possa registrar quem fez as modificações nos dados.

5.5.3.4. Caso haja necessidade da utilização de assinatura eletrônica ou a necessidade de se controlar o acesso às funcionalidades, áreas ou registros, o software deve prover esse controle de usuário.

5.6. Redes e Armazenamento em Nuvem

5.6.1. Uma rede pode possuir um ou mais servidores gerenciando a rede, podem existir computadores conectados entre si ou ainda pode haver computadores que não farão parte da rede. Independentemente da sua conexão ou não, todos os requisitos presentes neste documento devem ser aplicados caso estas máquinas obtenham, calculem, processem e/ou armazenem dados analíticos ou registros digitais relativos ao Sistema de Gestão.

5.6.2. Caso existam dados ou softwares gerenciados ou mantidos fora das instalações (por exemplo, armazenamento em nuvem), deve-se assegurar que estes são mantidos com segurança contra ataques, malwares e perdas acidentais, além de se garantir a confidencialidade e integridade das informações.

Nota: *Podem ser aceitas certificações de órgãos reguladores ou entidades similares que garantam estes requisitos, por exemplo, ISAE 3402 (International Standard on Assurance Engagements).*

5.6.3. Caso a empresa que fornece o serviço de armazenamento em nuvem (software e/ou dados) não possua certificação, a mesma deve ser avaliada quanto à segurança e integridade dos dados periodicamente e às garantias a respeito da segurança contra ataques, malwares e perdas acidentais de dados devem ser definidas em contrato, assim como as garantias quanto a confidencialidade e integridade das informações.

5.7.Backups

5.7.1. Devem ser realizados backups de dados analíticos ou registros digitais relativos ao Sistema de Gestão. Os dados podem estar:

a) Em um ou mais servidores;

b) Em computadores conectados entre si sem um servidor;

c) Uma forma híbrida das opções anteriores, ou seja, parte deles dispersos nos computadores da rede e parte armazenados no servidor.

No primeiro caso (a), onde os dados mencionados estão presentes somente no(s) servidor(es), basta apenas o backup deste(s) servidor(es). No segundo caso (b), o backup deve ser realizado em cada máquina que possua os dados mencionados anteriormente. No terceiro caso (c) devem ser efetuados os backups de forma independente, tanto do servidor como das máquinas que contenham os dados mencionados.

5.7.2. O Backup não deve ser armazenado na mesma máquina que o gerou.

5.7.3. Caso o backup seja realizado em nuvem, devem ser seguidos os respectivos requisitos do presente documento.

5.7.4. Backups armazenados em mídias físicas não devem ser guardados na mesma sala das máquinas que deram origem a estes. Devem ser armazenados em locais seguros e protegidos contra acesso não autorizado, danos físicos. Considerar o armazenamento de backups físicos em locais geograficamente distintos (off-site) para proteção contra desastres locais (incêndios, inundações, etc.). Devem ser implementados controles de acesso aos backups, garantindo que apenas pessoal autorizado possa acessar e restaurar os dados.

5.7.5. Os backups devem ser realizados de forma periódica. Esta periodicidade deve ser inversamente proporcional ao volume de dados gerados diariamente ou sua importância, ou seja, laboratórios com grande volume de dados digitais devem ter periodicidade de backup diária ou mesmo várias vezes ao dia. A periodicidade deve ser inferior a uma semana. Justificar a escolha da periodicidade do backup em procedimento ou registro relacionado.

Nota: *Convém, onde possível, implementar soluções automatizadas de backup para reduzir a dependência de intervenções manuais e minimizar o risco de erro humano.*

5.7.6. Devem ser realizados testes regulares de recuperação de dados a partir dos backups para garantir que estes possam ser restaurados com sucesso.

5.7.7. Devem ser implementados procedimentos para o descarte de backups antigos com segurança, incluindo a destruição segura de mídias físicas e a exclusão segura de dados em mídias digitais.

5.7.8. Devem ser mantidos registros da realização desta atividade.

5.8. Procedimentos e Manuais

5.8.1. Devem existir, no mínimo, procedimentos descritos que contemplem as atividades de Manutenção (preventiva e corretiva), Aquisição e Avaliação de Hardwares, Segurança, Validação de Softwares e de Produtos de Pacote de Escritório (como por exemplo, planilhas e bancos de dados gerados), Controle de Rede e Backups.

5.8.2. Nos procedimentos devem ser claramente identificados os responsáveis que irão executar as tarefas relacionadas neste documento.

5.9.Registros

5.9.1. Devem existir registros que evidenciem que as atividades requeridas para cada um dos requisitos do presente guia foram realizadas de forma adequada, seguindo os procedimentos internos, além de atender normas, leis, regulações, resoluções e documentos similares aplicados.

5.10. Contratos

É recomendável que os contratos de prestação de serviço firmados entre o laboratório e empresas fornecedoras de software ou armazenamento de dados tenham as informações a seguir, assim como os respectivos registros.

a. Certificado, declaração ou documento equivalente que confirme que o desenvolvedor validou o software quanto suas funcionalidades.
b. Que o desenvolvedor irá atualizar o certificado, declaração ou documento equivalente comprovando que foram realizadas com resultado positivo a validação do produto sempre que houver atualizações.
c. Sempre que aplicável, o laboratório deve garantir aos profissionais envolvidos no processo de atualização do produto apenas o acesso estritamente necessário ao servidor para a realização desta tarefa.
d. Quais processos são implementados para proteção de perda ou alteração do produto no servidor.
e. Qual o procedimento utilizado para assegurar a integridade dos dados
f. Como as falhas do sistema são identificadas e corrigidas

6. Referências

ABNT NBR ISO/IEC 17025:2017, “Requisitos gerais para competência de laboratórios de ensaio e calibração” – Associação Brasileira de Normas Técnicas (2017)

ABNT NBR ISO 15489-1:2018 Informação e documentação-Gestão de documentos de arquivo. Parte 1: Conceitos e princípios – Associação Brasileira de Normas Técnicas (2018)

ABNT NBR ISO 9001:2015 – Sistemas de Gestão da Qualidade - Associação Brasileira de Normas Técnicas (2015)

ABNT ISO/TR 21946:2020 - Informação e documentação - Avaliação para a gestão de documentos de arquivo - Associação Brasileira de Normas Técnicas (2020)

Brasil (BR)- Lei Nº 13.853 de 08.07.2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. DOU nº 246, Seção 1, 20 dez 2019

ISBN: 978-65-01-47519-6

ForMEQ

Fórum Internacional de
Metrologia e Examinologia em Química

ISBN: 978-65-01-47519-6