Guia RELACRE 15

GARANTIA DA QUALIDADE

DE

SISTEMAS INFORMÁTICOS

EM

LABORATÓRIOS

RELACRE
Associação de Laboratórios Acreditados de Portugal

FICHA TÉCNICA

TÍTULO:

Guia RELACRE 15

GARANTIA DA QUALIDADE DE SISTEMAS INFORMÁTICOS EM LABORATÓRIOS

EDIÇÃO: RELACRE

DESIGN GRÁFICO: RELACRE

CAPA: Alda Rosa

IMPRESSÃO: Espaço 2 Gráfico

TIRAGEM: 250 exemplares

DEPÓSITO LEGAL: 154306/00

ISBN: 972 8574-04-5

Guia RELACRE 15

EDIÇÃO: JUNHO 00

GARANTIA DA QUALIDADE DE SISTEMAS INFORMÁTICOS EM LABORATÓRIOS

A presente edição foi elaborada pelo grupo de trabalho **GT04** "Garantia da Qualidade de Sistemas Informáticos" da Comissão Técnica CTR01 da RELACRE "Garantia da Qualidade nos Laboratórios".

O Conteúdo é da responsabilidade dos que colaboraram na sua elaboração.

É intenção da RELACRE proceder à revisão deste documento sempre que se revele oportuno.

Na elaboração da presente edição colaboraram:

Fátima Inglês (*Coordenadora)*	ARSENAL DO ALFEITE
Helena Torgal	ICAT
Luísa Calhau	INETI
Martinha Rebelo	DGFCQA
Paulo Tavares	ICAT
Teresa Cipriano	PETROGAL

ÍNDICE

1. OBJECTIVO

Este documento tem como objectivo ser um guia de orientação, para os Laboratórios que pretendam cumprir os requisitos da Garantia da Qualidade e que utilizam sistemas informáticos nas suas actividades.

Salienta-se que, como qualquer outro guia de orientação, não é de cumprimento obrigatório.

2. ÂMBITO

Aplica-se aos Laboratórios que utilizem sistemas informáticos incluindo os computadores integrados noutros equipamentos ou sistemas quando a sua utilização possa afectar a integridade, qualidade, segurança e emissão dos resultados.

Alguns exemplos são:

- Aquisição de dados, processamento, transferência, armazenamento e arquivo.
- Bases de dados, folhas de cálculo, processamento de texto que integre dados adquiridos durante as medições e ensaios.
- Sistemas de gestão da informação do Laboratório
- Instrumentos ou sistemas controlados por computadores ou microprocessadores

Este guia foi elaborado para cobrir as necessidades de todos os Laboratórios independentemente da sua dimensão e campo de actividade. As orientações deste documento podem ser implementadas a diferentes níveis ou detalhe para diferentes Laboratórios. Em alguns casos pode ser adequado encontrar soluções mais simples e noutros estas orientações podem ser redundantes devido à dimensão ou tipo de actividade em questão.

A decisão da aplicação deste guia não deve ser tomada com base na complexidade dos sistemas mas sim na sua relevância para a qualidade dos resultados. Desta forma, os processadores de texto e as calculadoras de bolso podem ser objecto de aplicação das orientações deste guia: uma má utilização do processador de texto, na emissão de relatórios a partir de outros já existentes pode introduzir erros; nas

calculadoras de bolso a determinação do desvio padrão pode dar resultado nulo devido a limitações de arredondamento interno.

Por forma a decidir o tipo de controlo a efectuar aos sistemas informáticos, é necessário uma pré-avaliação do risco, tendo em atenção a necessidade de assegurar a integridade dos dados, a confidencialidade e a disponibilidade dos dados dos sistemas.

Existem casos onde o equipamento de ensaio, que pode ser considerado como um sistema informático, é usado como uma única entidade, por vezes conhecida como "caixa preta". Nestes casos nem sempre é relevante separar o sistema nos seus componentes individuais, pois tal pode não se traduzir numa melhoria e pode inclusivamente não ser suficiente.

Muitas vezes é conseguida uma razoável garantia do correcto funcionamento, de uma tarefa específica, através do teste ao funcionamento do sistema completo. É no entanto importante que essa "caixa preta" seja testada em todas as gamas que poderão ocorrer na prática e que as limitações do sistema estejam estabelecidas.

3. DEFINIÇÕES

Arquivo[1] - Armazenagem de ficheiros de salvaguarda e de diários[1] associados, geralmente durante um determinado período de tempo.

Backup, ficheiro de salvaguarda, ficheiro de segurança[1] - Cópia de um ficheiro feita com vista a uma eventual reconstituição do ficheiro.

Dados brutos - dados que são utilizados como entrada para uma operação computadorizada no Laboratório não podendo ser derivados ou recalculados a partir de outros.

Diário[1] – Registo cronológico das operações de processamento de dados. O diário pode ser utilizado para reconstruir uma versão anterior ou actualizada de um ficheiro.

Firmware, suporte lógico permanente[2] - Conjunto ordenado de instruções e dados associados, armazenados de um modo funcionalmente independente da memória principal, normalmente numa memória ROM.

Hardware, equipamento informático[2] - Totalidade ou parte dos componentes físicos de um sistema de processamento de informação.

Integridade dos dados[1] - Qualidade dos dados que existe enquanto não ocorrer a sua destruição, alteração ou perda, de uma forma acidental ou intencional.

Outsourcing - utilização de recursos externos para assumir a responsabilidade de uma função da entidade.

Password, senha, palavra-passe[1] - Cadeia de caracteres que permite ao utilizador ter acesso parcial ou total a um sistema ou a um conjunto de dados.

Qualidade dos dados [1] - Correcção, actualidade, exactidão, exaustividade, relevância e acessibilidade que tornam os dados próprios para utilização.

Segurança do sistema de processamento de dados[1] - Conjunto de medidas técnicas e administrativas aplicadas a um sistema de processamento de dados para proteger o equipamento, o suporte lógico e os dados de modificação, destruição ou divulgação acidental ou intencional.

Software, suporte lógico[2] - Totalidade ou parte dos programas, procedimentos, regras e documentação associada, pertencentes a um sistema de processamento de informação.

Teste de aceitação[1] - Teste normalmente efectuado pelo comprador no seu próprio local, com a participação do vendedor, após a instalação de um sistema ou unidade funcional, para assegurar o cumprimento das exigências contratuais.

Validação de dados[1] - Processo utilizado para determinar se os dados são incorrectos, incompletos ou falsos.

Verificação dos dados[1] - Operação utilizada para verificar a qualidade dos dados e a integridade dos dados.

4. REFERÊNCIAS

[1] NP 3003-08: 1991 - Computadores e tratamento da informação. Vocabulário. Parte 08: Controlo, integridade e segurança

[2] NP 3003-1:1997 - Tecnologias da informação. Vocabulário. Parte 1: Termos fundamentais.

[3] ISO/IEC 17025: 1999 – General requirements for the competence of testing and calibration laboratories.

[4] DL 290-D/99 de 2 de Agosto - Regime jurídico dos documentos electrónicos e da assinatura digital.

5. ORGANIZAÇÃO E GESTÃO

5.1 ORGANIZAÇÃO

Em muitas organizações, um sistema informático é acessível a entidades, isto é, pessoas, organizações ou máquinas, não abrangidas pelo Sistema da Qualidade do Laboratório. Todos os acessos devem ser devidamente autorizados e controlados.

Se o Laboratório tiver de partilhar o sistema com outras áreas da organização tal deve ser feito de forma que qualquer alteração introduzida ao sistema pelas outras áreas não afecte a parte do sistema usada pelo Laboratório.

Basicamente, o sistema informático utilizado no âmbito das actividades da acreditação deve estar sob o controlo do Laboratório.

Este requisito pode ser difícil de aplicar na prática, tendo em consideração que situações como o *outsourcing*, a gestão remota de sistemas e a utilização de sistemas de dados distribuídos se têm tornado cada vez mais comum. Por exemplo, uma entidade subcontratada, terá o seu próprio sistema da qualidade para controlo de alterações. A responsabilidade do Laboratório é assegurar que quando os serviços são realizados fora do controlo directo do Laboratório, existe um contrato ou outro tipo de controlo que assegure a integridade.

O Laboratório deverá estabelecer políticas e procedimentos documentados para a especificação, aquisição, instalação, verificação, manutenção e reparação de sistemas informáticos.

5.2 RESPONSABILIDADES

O Laboratório deve nomear uma pessoa ou pessoas responsáveis pela gestão e supervisão dos computadores ou sistemas informáticos. Estas pessoas devem ter autoridade para tomar decisões relativas ao sistema em questão e possuírem pelo menos as seguintes qualificações:

- conhecimentos específicos necessários para utilizar o sistema sem ameaçar a integridade ou segurança dos resultados das calibrações ou dos ensaios

- experiência necessária para determinar se os procedimentos documentados utilizados no sistema são adequados ao seu objectivo
- conhecimento e experiência para avaliar se uma alteração a ser introduzida poderá causar danos ao sistema ou modificar a qualidade do trabalho do Laboratório

É inevitável que em pequenos Laboratórios a responsabilidade de todo o sistema recaia numa só pessoa. Contudo, para sistemas críticos, pode ser necessário separar os elementos de autorização, segurança, funções de administração do sistema, entrada de dados e respectiva possibilidade de modificação. Em particular, as responsabilidades de autorização e execução devem ser separadas para evitar o risco de actividade fraudulenta. Nas tecnologias de informação, os erros são mais prováveis quando uma alteração é sugerida, especificada, aprovada, implementada e autorizada por um só indivíduo, embora tal possa ser necessário na prática.

O Laboratório deve definir as seguintes áreas de responsabilidades:

Especificação, concepção, aquisição, instalação, modificação, teste, aceitação, manutenção, administração, segurança, formação, suporte ao utilizador, entrada de dados, saída de dados, backup, abate[1].

É importante a existência de descritivos de funções para todos os elementos cuja actividade esteja relacionada com os sistemas de informação. É indispensável que o pessoal tenha formação, qualificação e experiência adequadas às funções que desempenha.

6. PESSOAL

Um Laboratório tem de dispor de pessoal devidamente qualificado e com experiência e implementar programas de formação devidamente documentados que podem incluir quer a formação em exercício, quer a frequência de cursos de formação.

Devem existir registos de todas essas Acções de Formação.

[1] Saída do activo

As disposições acima referidas devem ser aplicadas a todas as pessoas envolvidas nos sistemas informáticos.

O Laboratório deve ter procedimentos documentados para a formação e autorização do pessoal que execute qualquer actividade com a utilização do sistema informático. Estes procedimentos devem prever a informação e formação prática pelo menos no seguinte:

- Todas as instruções técnicas e administrativas e, informações necessárias para uma correcta e segura operação do sistema;

- Todos os procedimentos técnicos e administrativos a serem seguidos em caso de falha do sistema ou de outras anomalias que possam surgir durante a operação diária;

- A extensão e limites das responsabilidades de cada pessoa qualificada e autorizada a trabalhar com o sistema, a mantê-lo e modificá-lo.

7. INSTALAÇÃO E CONDIÇÕES AMBIENTAIS

Todos os componentes do sistema informático devem ser mantidos num ambiente que assegure o seu correcto funcionamento e a sua segurança.

Deverá ser objecto da devida atenção:

- a localização física do sistema (computador, periféricos, equipamentos de comunicações e meios electrónicos de armazenamento)
- a garantia do fornecimento ininterrupto de energia (durante o tempo necessário para se realizar o backup e outras operações).

Sempre que necessário o Laboratório deverá monitorizar e controlar os parâmetros ambientais que afectem a segurança e o correcto funcionamento de cada parte do sistema incluindo a área onde os registos são armazenados electronicamente (condições extremas de temperatura e de humidade, de poeira, de certos reagentes como por exemplo solventes orgânicos e amónia, de interferência

electromagnética e a proximidade aos cabos de alta tensão devem ser evitados a menos que o equipamento seja projectado especificamente para operar sob tais condições).

8. DESCRIÇÃO DO SISTEMA

O Laboratório deve descrever o sistema, nomeadamente através dos seguintes elementos:

- lista de todos os componentes do sistema univocamente identificados, por exemplo, a marca, o modelo e o n.º de série
- registos das alterações à configuração original (hardware, versões do software e do firmware)
- manual de utilização (hardware, software e firmware)
- fluxograma das aplicações, quando apropriado
- descrição sumária das aplicações (textual e/ou esquemática)
- descrição dos procedimentos de processamento de dados no sistema, incluindo fórmulas, algoritmos, factores de correcção utilizados, etc..
- estimativa da incerteza da medição introduzida pelo sistema no resultado final

A configuração actual do sistema pode ser dependente de parâmetros controlados pelo utilizador. É essencial que estes sejam registados, de forma a que se possa restabelecer a configuração em caso de falha.

9. MANUTENÇÃO

Todos os sistemas informáticos devem ser instalados e mantidos de forma a assegurar a continuidade do seu funcionamento de acordo com as especificações. Isto pode envolver a gestão do sistema, treino (formação), manutenção, suporte técnico, auditorias e ou avaliação do desempenho.

A avaliação do desempenho é a revisão periódica do sistema de forma a assegurar que continua a satisfazer os critérios de desempenho pré-estabelecidos como por exemplo a fiabilidade e a capacidade de resposta.

Devem existir procedimentos de manutenção preventiva de rotina e reparação de avarias. Estes procedimentos devem especificar claramente as funções e responsabilidades do pessoal envolvido. Se o Laboratório subcontrata estas actividades, deve assegurar que as actividades subcontratadas estão de acordo com os requisitos de qualidade do Laboratório.

A manutenção do sistema informático deve incluir verificações periódicas equivalentes a alguns dos procedimentos utilizados na verificação inicial do sistema. Sempre que na manutenção exista necessidade de se proceder a alterações do hardware e / ou software , é necessário validar o sistema de novo. Durante o funcionamento diário do sistema, devem ser mantidos registos de quaisquer problemas e/ou incompatibilidades detectadas, devendo ser tomadas as medidas correctivas necessárias.

Os procedimentos devem encontrar-se no local e descrever as medidas a tomar no caso de uma falha total ou parcial do sistema informático.

10. VALIDAÇÃO DE SISTEMAS INFORMÁTICOS

10.1 ACEITAÇÃO

Os sistemas informáticos devem ser concebidos de modo a satisfazer os princípios da Garantia da Qualidade e introduzidos de forma devidamente planeada. Deve existir documentação que evidencie que o sistema foi desenvolvido de forma planeada e que está de acordo com os requisitos técnicos e da qualidade. Exemplo: NP EN ISO 9001. A verificação inicial do sistema deve evidenciar que o mesmo está em conformidade com o critério de aceitação estabelecido.

O sistema pode ser verificado e documentado através da utilização de um ou mais dos seguintes procedimentos ou outros relevantes:

- utilitários de teste, quando disponíveis
- testes de simulação através da introdução de valores teóricos
- medições em padrões com resultados conhecidos
- conjunto de dados certificados, quando apropriado e disponíveis

A aceitação formal deve ser evidenciada através dum documento e requer que os ensaios sejam realizados de acordo com um plano pré-definido, que sejam guardados os registos dos procedimentos, dos dados e dos resultados dos ensaios.

Para sistemas informáticos adquiridos é provável que parte da documentação criada durante o desenvolvimento não seja disponibilizada ao Laboratório. Neste caso a evidência da aceitação formal deve estar disponível nas instalações.

10.2 AVALIAÇÃO RETROSPECTIVA

É provável que existam sistemas informáticos para os quais a necessidade de verificação dos princípios da Garantia da Qualidade não foi planeada ou pedida. Nestes casos deve haver documentação a justificar a utilização desses sistemas e deve ser realizada uma avaliação retrospectiva para avaliar a respectiva adequabilidade.

A avaliação retrospectiva começa pela reunião de todos os registos históricos relacionados com os sistemas. Esses registos devem ser analisados e sumarizados. Este resumo deve indicar quais os registos existentes e o que falta para assegurar a validação deste sistema.

10.3 CONTROLO DE ALTERAÇÕES

Do controlo de alterações devem constar os respectivos registos e a sua aprovação formal.

O controlo de alterações é necessário quando uma alteração possa afectar o estado de validação do sistema informático.

O procedimento de controlo de alterações deve descrever o método de avaliação para determinar quais os testes necessários para manter o sistema válido.

Independentemente da origem da alteração (fornecedor ou sistema desenvolvido internamente), a informação apropriada deve ser fornecida como parte do processo de controlo de alterações. Os procedimentos de controlo de alterações devem manter a integridade dos dados.

Considera-se uma alteração ao sistema quando qualquer uma das seguintes actividades ou outras equivalentes forem efectuadas:

- reparação de componentes do hardware;
- instalação de novo hardware;
- instalação de nova versão do software ou firmware;
- instalação de novo software;
- instalação de novo equipamento auxiliar;
- outras alterações ao sistema devido a novos requisitos no sistema;
- alterações nos parâmetros de configuração (como por exemplo, velocidade de transmissão de dados, alterações resultantes de calibração, etc.);
- adição ou modificação do software, incluindo rotinas introduzidas pelo utilizador.

O Laboratório deve garantir que o software inválido ou obsoleto não é utilizado indevidamente e que está claramente identificado como tal.

11. MÉTODOS DE ENSAIO E/OU CALIBRAÇÃO

Todos os documentos relevantes, tais como, manuais, instruções de funcionamento e outros procedimentos necessários para o uso e manutenção do sistema, devem estar escritos numa linguagem compreensível e facilmente acessíveis.

O Laboratório deverá ter procedimentos escritos que descrevam os ensaios que são realizados utilizando o sistema informático. Os procedimentos devem para além de uma descrição do ensaio a ser realizado, conter pelo menos as seguintes informações:

- Lista dos dados brutos a serem registados.
- Formas de aquisição de dados
- Interpretação dos erros e alarmes produzidos pelo software e procedimentos das respectivas acções correctivas.

Quando os Laboratórios de ensaio e/ou calibração calcularem a estimativa da incerteza da medição devem incluir as contribuições provenientes do sistema informático, como por exemplo, os erros de arredondamento, etc..

12. SEGURANÇA

O Laboratório deve ter políticas e procedimentos documentados para assegurar a integridade do sistema, (*hardware, software*, *firmware*) e qualquer registo produzido e/ou armazenado no sistema. As políticas e procedimentos devem necessariamente cobrir a especificação, a aquisição, o teste, a aceitação, o controlo de acessos, o controlo de configuração, a protecção contra intervenções maliciosas (por exemplo, vírus) e outras políticas que sejam consideradas necessárias.

O sistema deve ser protegido através de medidas de segurança apropriadas dependendo a solução a adoptar das possibilidades disponíveis e do resultado das análises de risco efectuadas. Podem ser implementadas medidas de segurança física e/ou lógica.

A segurança física pode consistir simplesmente no bloqueamento físico do teclado ou no controlo do acesso físico aos utilizadores autorizados no caso de estações de trabalho não conectadas à rede. No entanto quando forem utilizados, por exemplo, computadores portáteis ligados por modem em locais remotos são necessárias medidas de segurança adicionais.

A segurança lógica pode incluir a obrigatoriedade de identificação única dos utilizadores associada a uma *password*. Pode também definir um sistema de segurança duplo, o primeiro nível permite ao utilizador a entrada no sistema e o segundo nível permite apenas o acesso aos ficheiros autorizados.

O acesso ao sistema não pode ser condicionado pela perda da password. As passwords necessárias para garantir a total operacionalidade do sistema devem ser registadas e no caso de serem consultadas essa operação deverá ser claramente detectável.

O Laboratório deve ter procedimentos documentados para assegurar a integridade dos dados, na eventualidade de falha do sistema, nomeadamente descrevendo a metodologia para a execução de backups dos dados e armazenamento seguro dos mesmos. Devem ser efectuados backups de todos os

"dados brutos" e não apenas dos resultados. Deve ser avaliada a necessidade e capacidade de fontes de alimentação alternativas, que permitam assegurar a integridade do sistema em caso de falha de energia (durante uma operação no sistema informático, a existência de fontes de alimentação alternativas, evitam a introdução de possíveis erros nos ficheiros).

Qualquer introdução de dados ou software proveniente de fontes externas deve ser controlada. Este controlo pode ser assegurado pelo sistema operativo, por rotinas de segurança específicas, por rotinas incluídas nas aplicações ou por uma combinação dos três métodos anteriores. O Laboratório deve ter procedimentos escritos descrevendo a sua política de protecção contra vírus e como é posta em prática.

13. DOCUMENTAÇÃO

A lista de documentação a seguir referida é exemplificativa dos documentos base que devem existir para o desenvolvimento, validação, funcionamento e manutenção de sistemas informáticos.

a) Política de Gestão

Deve ser descrita a política de gestão abrangendo as seguintes áreas: os requisitos, a aquisição, a instalação, os testes, a validação, o funcionamento, a manutenção, a monitorização, a auditoria, a substituição e a retirada de sistemas informáticos.

b) Descrição da aplicação

Para cada aplicação deverá haver uma documentação que descreva completamente:

- o nome da aplicação ou código de identificação e uma clara descrição da finalidade da aplicação
- o hardware (marca, modelo e números de série) na qual a aplicação opera
- o sistema operativo e outro software (por exemplo, processador de texto) usados conjuntamente com a aplicação
- a linguagem de programação da aplicação e/ou base de dados usada
- as funções principais executadas pela aplicação
- o fluxograma de dados

- a estrutura dos ficheiros, mensagens de erro e de alarme, e algoritmo associado com a aplicação
- a versão da aplicação
- a configuração e a transmissão de dados entre os módulos da aplicação e o equipamento e outro sistemas

c) Procedimentos

Exemplos de possíveis procedimentos:

- procedimento para o funcionamento de sistemas informáticos (hardware-software), e responsabilidade do pessoal envolvido;
- procedimento para medidas de segurança utilizadas na detecção e prevenção de acesso não autorizado e alteração de programas;
- procedimento e autorização para alterações de programa e registo das alterações;
- procedimento e autorização para alterações de equipamentos (hardward-software) incluindo testes antes de utilização, se aplicável;
- procedimento para testes periódicos para o funcionamento correcto do sistema ou dos seus componentes e registo destes testes;
- procedimentos para a manutenção dos sistemas informáticos e de algum equipamento associado;
- procedimentos para o desenvolvimento de software e testes de aceitação assim como dos respectivos registos;
- procedimentos de backup para todos os dados armazenados e planos de acções correctivas no caso de uma avaria;
- procedimentos para arquivo e recuperação de todos os documentos originais, software e dados;
- procedimentos para a monitorização e auditoria de sistemas informáticos.

14. REGISTOS

Deve haver registos de:

- Especificações para a compra do sistema.
- Todas as calibrações, verificações e actividades de manutenção realizadas e de todas as alterações incorporadas no sistema.
- Resultados de todas as actividades de calibração e verificação.
- Falhas do sistema e recuperação.
- Detalhes da configuração do hardware e software no momento de cada calibração e ensaio ou em cada etapa do processo de calibração ou ensaio.

Como resultado do procedimento de instalação, devem ser mantidos registos de pelo menos os seguintes pontos:

- identificação inequívoca do sistema em todos os seus componentes;
- procedimento de instalação;
- procedimento de verificação adoptado;
- dados e outros resultados provenientes dos procedimentos de instalação e verificação;
- integração do sistema no actual sistema informático do Laboratório;
- verificação final da instalação.

Os registos de verificação do software deve conter, pelo menos:

- identificação inequívoca do software verificado;
- dados e outros resultados provenientes do processo de verificação;
- identificação e assinatura dos responsáveis pela verificação e pela validação dos resultados.

Os dados devem ser registados de maneira a prevenir a sua modificação após a sua aprovação final. Se for permitida qualquer alteração dos dados devem existir procedimentos que mantenham a rastreabilidade total da modificação incluindo a sua justificação (quando e porquê).

Recomenda-se a tomada de medidas que assegurem a manutenção da integridade dos dados brutos. Todos os dados brutos bem como a documentação necessária à sua interpretação e análise devem ser registados e mantidos durante um período de tempo definido pelo Laboratório e o conhecimento desse facto deve ser dado ao cliente.

Sempre que alterações significativas sejam realizadas no sistema informático o Laboratório deve assegurar que a informação registada e armazenada permaneça acessível.

Observações originais, cálculos e valores transformados, registos de calibrações e relatórios finais de ensaio, armazenados em meios electrónicos devem ser identificados inequivocamente de modo a

serem rastreáveis ao item ensaiado, ao ensaio e ao cliente em questão. Se os dados armazenados em suporte electrónico são apenas parte do registo total que diz respeito ao ensaio específico, os registos não mantidos sob forma electrónica devem ser identificados de forma a estabelecer a rastreabilidade de todos os registos relacionados com o ensaio específico. Esta rastreabilidade deve ser conseguida de forma a estabelecer sem quaisquer dúvidas qual o item ensaiado, o ensaio, o cliente a que os registos dizem respeito.

Se os backups são usados como arquivo de registos ou se forem utilizados para repor o sistema num estádio prévio, isto é, para gerar resultados, é importante que exista o procedimento e que este seja aplicado. O Laboratório deve ser capaz de evidenciar através de registos que o sistema de backup referido nos seus procedimentos é cumprido.

A integridade dos dados ou informação é mais vulnerável no momento de aquisição quer esta seja realizada de forma manual quer pelo sistema informático. O Laboratório deve garantir que:

- a pessoa responsável pela entrada directa de dados seja identificada no momento da aquisição de dados;
- o dispositivo utilizado para a transferência de dados e a data da sua transmissão devem ser registados;
- a transferência de dados deve ser sujeita a verificação adequada de forma sistemática.

Deve tomar-se especial atenção para proteger os registos armazenados electronicamente, de interferências electromagnéticas e de outros danos. As partes do sistema informático ou a área física onde os registos são mantidos não devem ser acessíveis a pessoas não autorizadas e devem cumprir todos os requisitos de protecção, segurança, confidencialidade para o cliente.

Os dados em suporte electrónico devem ser arquivados com os mesmos níveis de controlo de acesso, indexação, acessibilidade e prazo de arquivo como os outros tipos de dados.

É necessário implementar procedimentos para assegurar que durante o prazo estabelecido para o arquivo, a integridade e o acesso dos dados armazenados electronicamente não são comprometidos. Para se prevenir eventuais problemas com o acesso aos dados arquivados ou quando os sistemas informáticos forem substituídos, devem ser estabelecidos procedimentos para assegurar a continuação

da possibilidade de leitura dos dados. Isto pode, por exemplo, incluir a produção de cópias em papel ou a transferência dos dados para outro sistema. Em relação ao hardware, a substituição tem de ter em consideração a confidencialidade dos registos existentes no disco.

15. RELATÓRIOS DE ENSAIO E CERTIFICADOS DE CALIBRAÇÃO

Os relatórios de ensaio e/ou certificados de calibração devem estar de acordo com a norma ISO/IEC 17025[3].

Estes documentos originais quando são elaborados e distribuídos por meios electrónicos devem conter um código ou assinatura electrónica que inequivocamente identifique a(s) pessoa(s) que tenha(m) a responsabilidade técnica pelo documento. Deve conter também um código que identifique inequivocamente o Laboratório que emite o relatório.

Em Portugal, o regime jurídico dos documentos electrónicos e da assinatura digital está legislado pelo Decreto Lei 290-D/99 de 2 de Agosto[4].

O Laboratório deve dispor de procedimentos documentados para verificar a correcta transmissão para o cliente e deve, se requerido, ter possibilidade de enviar por correio ou por outros meios o mesmo relatório.

Se o relatório de ensaio contiver informação ou anexos que não seja possível transmitir por meios electrónicos, deve ser enviado ao cliente uma versão em papel do relatório completo conjuntamente com os anexos.

Qualquer correcção a um relatório produzido por meios electrónicos deve ser efectuada de acordo com os princípios utilizados para os relatórios emitidos em papel.

Os relatórios produzidos por meios electrónicos devem estar sob controlo de acesso (escrita e leitura), na fase da elaboração e uma vez aprovados e assinados, deve ser garantida a impossibilidade de alterações posteriores.

Quando são introduzidas alterações no sistema ou quando são instalados novos sistemas, o Laboratório deve assegurar-se que os relatórios emitidos no anterior sistema continuam a poder ser lidos e enviados até ao fim do seu período de retenção, tal como definido no sistema da qualidade.

16. BIBLIOGRAFIA

ASTM E 1579 - 93 : Standard Guide for Ensuring Data Integrity in Highly Computerized Laboratory Operations.

EA Guidelines for the use of computers and computer systems in accredited laboratories, version 4, May 1998.

OECD Series on Principles of Good Laboratory Practice and Compliance monitoring, Number 10, GLP Consensus Document - The Application of the principles of GLP to computerised Systems, Environment Monograph No. 116.

NP 3003-04: 1993 - Computadores e tratamento da informação. Vocabulário. Parte 04: Organização de dados.

NP 3003-14: 1995 - Computadores e tratamento da informação. Vocabulário. Parte 14 Fiabilidade, Manutenção e Disponibilidade.

L. Huber, Validation of computerized analytical systems, Buffalo Grove, IL, Interpharm, May 1995.

Últimos guias publicados

1 CALIBRAÇÃO DE MATERIAL VOLUMÉTRICO

1995; ISBN 972 - 96727 - 0 - 9

2 AUDITORIAS INTERNAS DE LABORATÓRIOS QUÍMICOS

1995; ISBN 972 - 96727 - 1 - 7

3 VALIDAÇÃO DE RESULTADOS EM LABORATÓRIOS QUÍMICOS

1996; ISBN 972 - 96727 - 2 - 5

4 DETERMINAÇÃO DA MELHOR INCERTEZA DE MEDIÇÃO DE UM LABORATÓRIO DE CALIBRAÇÃO DE FORÇAS

1996; ISBN 972 - 96727 - 3 - 3

5 DETERMINAÇÃO DA INCERTEZA DOS RESULTADOS DA CALIBRAÇÃO DE INSTRUMENTOS DE MEDIÇÃO DE FORÇAS

1996; ISBN 972 - 96727 - 4 - 1

6 ACREDITAÇÃO DE LABORATÓRIOS DE ENSAIOS MICROBIOLÓGICOS

1996; ISBN 972 - 96727 - 5 - x

7 ENSAIOS INTERLABORATORIAIS EM QUÍMICA

1996; ISBN 972 - 96727 - 6 - 8

8 DETERMINAÇÃO DA INCERTEZA DA CALIBRAÇÃO DE MASSAS

1997; ISBN 972 - 96727 - 7 - 6

9 ALGUNS EXEMPLOS DE CARTAS DE CONTROLO EM LABORATÓRIOS DE ANÁLISE QUÍMICA

1998; ISBN 972 - 96727 - 8 – 4

10 DETERMINAÇÃO DA INCERTEZA DOS RESULTADOS DE MEDIÇÃO NA CALIBRAÇÃO DE INSTRUMENTOS DE MEDIÇÃO NA ÁREA ELÉCTRICA

1999; ISBN 972 - 96727 - 9 - 2

11 ELABORAÇÃO DO MANUAL DA QUALIDADE DE LABORATÓRIOS

1999; ISBN 972 - 8574 - 00 - 2

12 DETERMINAÇÃO DA INCERTEZA DOS RESULTADOS DE VERIFICAÇÃO DE MÁQUINAS DE ENSAIO DE TRACÇÃO OU COMPRESSÃO

1999; ISBN 972 - 8574 - 01 - 0

13 VALIDAÇÃO DE MÉTODOS INTERNOS DE ENSIAO EM ANÁLISE QUÍMICA

2000; ISBN 972 - 8574 - 02 - 9

14 QUESTIONÁRIO DE AVALIAÇÃO DA SITUAÇÃO DOS LABORATÓRIOS DE ANÁLISES CLÍNICAS FACE À NOVA NORMA EN ISO/IEC 17025

2000; ISBN 972 - 8574 - 03 - 7

15 GARANTIA DA QUALIDADE DE SISTEMAS INFORMÁTICOS EM LABORATÓRIOS

2000; ISBN 972 - 8574 - 04- 5

RELACRE

Associação de Laboratórios Acreditados de Portugal

Rua Filipe Folque, 2, 6º Dto
1050-113 LISBOA
Telef. 21 313 98 40
Fax 21 313 98 41
relacre@mail.telepac.pt
www.relacre.pt

DESIGN: ALDA ROSA