Cássia Watanabe Kock

Avaliação da aplicação dos requisitos dos sistemas de gestão da qualidade relacionados a sistemas computacionais em laboratórios por parte de avaliadores e a respectiva aplicação por laboratórios acreditados

Dissertação apresentada ao Instituto de Química de São Carlos da Universidade de São Paulo como parte dos requisitos para a obtenção do título de mestre em ciências.

Área de concentração: Química Analítica

Orientador: Prof. Dr. Vitor Hugo Polisél Pacces

São Carlos

2023

Assinatura:
Data:

Ficha Catalográfica elaborada pela Seção de Referência e Atendimento ao Usuário do SBI/IQSC

Kock, Cássia Watanabe
Avaliação da aplicação dos requisitos dos sistemas de gestão da qualidade relacionados a sistemas computacionais em laboratórios por parte de avaliadores e a respectiva aplicação por laboratórios acreditados / Cássia Watanabe Kock. — São Carlos, 2023.
92 f.

Dissertação (Mestrado em Química Analítica e Inorgânica) — Instituto de Química de São Carlos / Universidade de São Paulo, 2023.

Orientador: Prof. Dr. Vitor Hugo Polisél Pacces

1. Garantia da qualidade. 2. Sistemas computadorizados. 3. Certificação ISO. 4. Boas práticas de laboratório. I. Título.

Sonia Alves - CRB: 4280/8

AGRADECIMENTOS

Aos meus pais, Guilherme e Irene, por me ampararem e nunca me deixarem desistir. Acho que chegou o momento de soltarmos rojões.

Ao Prof. Dr. Vitor Hugo Polisél Pacces, pela orientação e principalmente por toda a paciência, compreensão e confiança em mim.

A todos os meus amigos, por terem deixado meus dias mais leves e me ouvido nos momentos de crise.

O presente trabalho foi realizado com apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq

RESUMO

Considerando o fato de que na atualidade é praticamente impossível realizar ensaios laboratoriais sem recorrer a algum tipo de computador e que estes podem introduzir erros às etapas analíticas, as normas que regem as atividades de laboratórios precisaram incorporar diretrizes sobre o uso destes em sistemas de gestão da qualidade.

Contudo, não é raro que os laboratórios não consigam ou não saibam como aplicar tais regras integralmente, seja por falta de clareza das normas, por negligência às suas cobranças ou por desconhecimento mais profundo da área computacional. Somado a isso, a avaliação do cumprimento de requisitos relacionados a sistemas informatizados depende do nível de conhecimento dos próprios auditores sobre o tema.

Dessa forma, o trabalho compara a percepção dos laboratórios sobre a cobrança dos avaliadores em relação às exigências das normas e a execução por parte dos laboratórios, além de aquilatar o nível de conhecimento de auditores sobre sistemas informatizados aplicados a Sistemas de Gestão da Qualidade se utilizando de questionário *online*. Ainda, é feita a confirmação de quais itens nas normas geram as maiores dificuldades para aplicação pelos laboratórios e qual seu nível de implantação, na visão dos auditores.

ABSTRACT

Considering the fact that it is currently nearly impossible to carry out laboratory tests without resorting to some kind of computer and that computers can introduce errors into analytical procedures, the standards governing laboratory activities have had to incorporate guidelines on the use of computers in quality management systems.

However, it is not uncommon for laboratories not to be able to or not to know how to apply these rules in their entirety, either due to a lack of clarity about the standards, neglect of their requirements or a lack of in-depth knowledge of the computer area. In addition, the assessment of compliance with requirements related to computerized systems depends on the level of knowledge of the auditors themselves on the subject.

Therefore, this study compares the laboratories' perception of the evaluators' demands in regards to the standards and the laboratories' implementation, as well as gauging the auditors' level of knowledge about computerized systems applied to Quality Management Systems using an online questionnaire. It also confirms which items of the standards are the most difficult for laboratories to apply and what their level of implementation is, according to the auditors.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

1.1 Sistemas de Gestão da Qualidade em Laboratórios

A oferta crescente de produtos e serviços inundou o mercado com as mais variadas opções de tudo que se possa precisar ou querer, e isso levanta uma questão para o consumidor: qual escolher? Como escolher? A resposta parece óbvia: pela qualidade. E aqui outra questão é levantada: o que é qualidade?

Ainda que seja um termo muito difundido no meio empresarial e mesmo em nosso cotidiano, “qualidade” pode ter um caráter bastante subjetivo e genérico. Sua interpretação pode estar atrelada a atributos intrínsecos do bem adquirido, ao quanto ele atende determinadas especificações, à satisfação que ele gera no consumidor ou à relação desempenho x preço. Essa variedade de termos deve-se à mutação ao longo dos anos daquilo que é entendido como qualidade. Atualmente, um bem ou serviço de qualidade é entendido como algo que satisfaça os clientes – e a tendência é que esse conceito se mantenha no futuro. [1]

Assim, a maior oferta de produtos e serviços tornou necessária não somente uma forma de padronização desses como a implementação de requisitos mínimos para garantir que o cliente possa ter certeza de que está consumindo algo confiável. Dessa forma, inicia-se o conceito de Gestão da Qualidade.

Atualmente, a conformidade de empresas com normas técnicas e a implementação de Sistemas de Gestão da Qualidade (SGQs) não são mais vistas como diferenciais, e sim como exigências para ter competitividade no mercado. [1] Seguindo essa tendência, os laboratórios também precisaram escolher um caminho a seguir: adotar Sistemas de Gestão da Qualidade ou ter uma redução no seu número de potenciais clientes.

Os procedimentos realizados em laboratórios podem causar impactos imensos caso apresentem resultados errôneos ou duvidosos, de forma que se torna necessário haver confiabilidade e rastreabilidade desses. Considerando que são vários os fatores que podem afetar a qualidade dos ensaios – armazenamento da amostra, método utilizado, qualificação dos analistas – a criação de normas para reger o funcionamento das instituições foi, de certa forma, natural. Com elas, as atividades tornam-se sistematizadas, mais organizadas e os trabalhos realizados ficam mais eficientes,

fazendo com que a geração de resultados duvidosos seja bastante reduzida ou eliminada. [2]

Além desses fatores, a implantação de Sistemas de Gestão de Qualidade em um laboratório gera outros benefícios, como ganho de visibilidade no mercado, possibilidade de atender maior número de clientes (com a inclusão de outras empresas acreditadas e órgãos federais) e remoção de barreiras ao comércio internacional, visto que a acreditação é uma atestação formal de terceira parte de sua capacidade para realizar determinados ensaios. [3]

Dentre as normas mais extensamente implementadas nos laboratórios, há a NBR ISO/IEC 17025, NBR ISO 15189 e Boas Práticas Laboratoriais (BPL).

A história da NBR ISO/IEC 17025 inicia-se no final da década de 1970, com o início das atividades do *International Laboratory Accreditation Conference – ILAC*. O grupo buscava uma forma de agilizar a aceitação de resultados de ensaios e calibrações, de forma que em 1978 os laboratórios que proviam esse tipo de serviços começaram a passar por um processo de padronização que culminou na criação da ISO/IEC Guia 25. [3] A NBR ISO/IEC 17025 foi publicada pela primeira vez em 2000, chegando em 2001 ao Brasil. Em 2005, recebeu sua segunda edição e atualmente é a terceira edição que vigora, publicada em dezembro de 2017.

Também na década de 1970, a BPL foi introduzida na Nova Zelândia e na Dinamarca; anos mais tarde, o *Food and Drug Administration – FDA*, também propôs um texto a ser aplicado nos EUA, em resposta a atividades verificadas em companhias farmacêuticas, como execução incompetente de estudos, documentação insuficiente relativa a resultados e até mesmo fraude. [4] No Brasil, a implementação da norma se deu em 1994, quando da condução de estudos sobre a periculosidade de agrotóxicos. O Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis – IBAMA, exigia o cumprimento da norma como requisito para aceitação dos laudos emitidos pelos laboratórios envolvidos. [5]

1.2 Exigências para sistemas computadorizados de acordo com os sistemas ISO e BPL

Com a popularização dos computadores pessoais no início da década de 1980, o universo empresarial também passou por uma enorme informatização de suas atividades. [6] Além de sua disponibilidade, que motivou o emprego de tecnologias de informação no processo produtivo, foi a transição, na década de 1970, dos “30 anos dourados do capitalismo” para o “capitalismo financeirizado”, intrinsecamente instável.[7] Essa mudança fez com que surgissem novas exigências do mercado para serem atendidas, levando a uma consequente necessidade de reformular o método de acordo com o qual o trabalho era organizado. [6] Foi assim que os Programas de Qualidade Total passaram a ser largamente aplicados em todos os ramos empresariais. E visto que tais Programas têm como objetivo, acima de tudo, tornar as pessoas aptas a empregar da melhor forma possível os recursos a sua disposição, o desenvolvimento de normas para assegurar o bom uso dos sistemas informatizados foi espontâneo.

Os sistemas de gestão supracitados neste trabalho ou mencionam em seu texto como se empregar sistemas informatizados (*software* e *hardware*) para coleta e controle de dados (NBR ISO/IEC 17025, NBR ISO 15189 e NBR ISO/IEC 17043 e NBR ISO 15189) ou apresentam documentos inteiros discorrendo sobre a aplicação de seus princípios aos sistemas informatizados (NIT-DICLA-038).

A NBR ISO/IEC 17025 e a NBR ISO 15189 tratam tanto o *hardware* quanto o *software* como equipamentos e, por serem responsáveis por aquisição e processamento de dados que influenciam na qualidade dos resultados analíticos, são requeridos os seguintes pontos: [8, 9]

- Assegurar que estes, quando fora do controle permanente do laboratório, continuem seguindo os requisitos da norma;
- Garantir a existência de procedimentos para seu manuseio, transporte, armazenamento, uso e manutenção;
- Verificar se estão em conformidade com a norma antes de serem colocados ou recolocados para uso;
- Retirar os equipamentos de serviço quando mostrarem indícios de que tenham defeitos ou produzam resultados questionáveis;

- Manter registros que incluam identificação unívoca, evidência de verificação de que seguem os requisitos da norma, plano de manutenções, manutenções realizadas até o momento e detalhes de qualquer dano, mau funcionamento, modificações ou reparos;
- Validação realizada quanto à funcionalidade;
- Serem protegidos contra o acesso não autorizado;
- Serem protegidos contra adulteração ou perda;
- Serem mantidos de forma a assegurar a integridade dos dados e informações.

A NBR ISO/IEC 17043 faz em seu texto apenas duas menções a *software*, sendo elas: [10]

- Todos os equipamentos e *software* de processamento de dados devem ser validados de acordo com procedimentos antes de serem utilizados. A manutenção do sistema de computação deve incluir um processo de cópias de segurança e um plano de recuperação do sistema. Os resultados de tais manutenções e verificações operacionais devem ser registrados;
- O provedor de ensaio de proficiência deve estabelecer e manter procedimentos para controlar todos os documentos que fazem parte de seu sistema de gestão (gerados internamente ou obtidos de fontes externas), como [...] especificações de *software*.

No caso da NIT-DICLA-038, os requisitos existem em maior número e com mais especificidade para os sistemas informatizados. O exemplo de quão mais minuciosa é essa norma está relacionado com a necessidade de pessoal, contratado ou terceirizado, encarregado especificamente do desenvolvimento, validação, operação e manutenção dos sistemas informatizados. Também, o pessoal encarregado da garantia da qualidade deve ter acesso somente à leitura aos dados armazenados nos sistemas informatizados para seu controle, evitando assim possíveis modificações não intencionais. Outros requisitos da norma, em linhas gerais, estão dispostos a seguir. [11]

- Devem existir programas de treinamento documentados para o pessoal do laboratório;

- Deve-se considerar o local onde o hardware ficará localizado, evitando fortes variações de temperatura e de umidade, o pó, as interferências eletromagnéticas e a proximidade de cabos de alta tensão, exceto se o equipamento estiver especialmente projetado para funcionar em tais condições;
- Considerar que os sistemas de intercomunicação dos computadores podem ser uma fonte de erro e acarretarem perda ou alteração de dados;
- Existência de procedimentos, por escrito e em linguagem clara, descrevendo a manutenção rotineira e não rotineira;
- Revalidação do sistema informatizado quando alguma manutenção modificar o hardware ou *software*;
- Problemas, anomalias e as medidas corretivas aplicadas devem ser registradas;
- Existência de procedimentos, suficientemente detalhados e validados, que descrevam as medidas a serem tomadas em caso de falha parcial ou completa do sistema informatizado;
- No caso de sistemas informatizados que adquiram, processem, relatem ou armazenem dados brutos, os dados iniciais devem ser sempre recuperáveis, assim como todas as modificações realizadas;
- Ao trocar um sistema obsoleto por um novo, a transferência de dados brutos deve ser feita por método cuja integridade tenha sido previamente checada;
- Deve-se prevenir o acesso não autorizado aos sistemas informatizados e aos dados nele contido;
- Existência de *backup* de todos os *software* e dados;
- Devem ser feitos testes de aprovação documentados comprovando que os sistemas informatizados estão em conformidade com os princípios de BPL;
- Quaisquer modificações devem ser documentadas e justificadas;
- É recomendável que se tenha acesso ao código fonte do *software*;
- Existência de documentação completa para os sistemas informatizados, com o máximo de detalhamento possível;

- Existência de procedimentos operacionais padrão relativos à utilização dos sistemas informatizados.

Para os dois últimos itens, é possível encontrar mais particularidades no texto da norma, que por motivos de brevidade não serão expostos neste texto.

É importante mencionar que há uma norma específica para qualidade de *software* (ISO/IEC 25010:2011). Contudo, os programas utilizados pelos laboratórios podem ser considerados como “de qualidade” pelos padrões desta, não implicando em atendimento aos requisitos das normas técnicas desenvolvidas para laboratórios ou mesmo em adequação ao fim pretendido pelo laboratório,[12] visto que esses não são objetivos da ISO/IEC 25010. Logo, as disposições sobre sistemas computadorizados das normas expostas acima destinadas a laboratórios são não apenas pertinentes como também necessárias para assegurar a aplicação correta e segura de tais tecnologias.

Como pode-se perceber, as disposições das normas são pontos um tanto quanto óbvios quando se reflete sobre o uso de sistemas que armazenam e processam algo tão valioso como os dados necessários para a realização de todo o serviço do laboratório. Contudo, alguns fatores como confiança excessiva nos computadores, naturalização do uso da tecnologia e preocupação intensa acerca do seguimento dos requisitos para as atividades laboratoriais de bancada podem fazer com que os requisitos para sistemas informatizados sejam deixados em segundo plano. Em pesquisa realizada anteriormente, constatou-se que os laboratórios reconhecem a importância de tais requisitos, mas ainda ocorrem algumas práticas alarmantes, como o uso de versões não originais de sistemas operacionais nos computadores. [13] Além disso, o nível de cobrança dos auditores percebido pelos laboratórios em itens relacionados a sistemas informatizados também se mostrou inferior ao desejável, o que levanta o questionamento sobre o motivo disso.

2 OBJETIVOS

O presente trabalho tem o intuito de mapear a aplicação dos requisitos referentes a sistemas informatizados das normas técnicas em que os laboratórios possuem acreditação. Complementarmente, se realizará a confirmação de quais itens das normas geram as maiores dificuldades para implantação pelos laboratórios. Também será aquilatado o conhecimento de auditores sobre os requisitos previamente mencionados e comparados os dados obtidos a partir desta pesquisa com a percepção dos laboratórios sobre a cobrança dos avaliadores em relação às exigências das normas.

3 DESENVOLVIMENTO

3.1 Elaboração dos formulários

Os dados foram coletados por meio de formulários eletrônicos criados na plataforma Formulários Google, dada a sua simplicidade de uso com a qual usuários de internet são familiarizados, tornando seu preenchimento mais intuitivo e menos propenso a falhas causadas por equívocos acerca de sua utilização. Os formulários se encontram ao final deste trabalho, constando como Apêndice I e Apêndice II.

Foram criados dois formulários para colher respostas de auditores e de laboratórios. O formulário de auditores contava com três seções:

I. Caracterização do participante
   Foram solicitadas informações para classificar os auditores por tipo de auditoria realizada (interna, segunda ou terceira parte), estado e cidade de atuação, tipo da entidade pela qual o auditor era contratado (particular, pública ou de capital misto), em quais sistemas de gestão e em qual principal classe de ensaio se baseia a atuação do participante.
II. Conhecimentos sobre informática
   Considerando que, para uma auditoria ser efetiva, é necessário que o avaliador tenha um bom entendimento sobre a área a ser auditada, foram formuladas 14 situações possíveis de serem encontradas em sistemas computadorizados em sistemas de gestão da qualidade aplicados a laboratórios e que poderiam ou

não configurar uma não conformidade. Por meio de opções apresentadas como múltipla escolha, o participante deveria classificar cada uma das situações.

III. Situação da implantação dos sistemas computadorizados nos laboratórios

Foi solicitado ao participante que classificasse o nível de implantação de diversos itens relacionados a sistemas computadorizados - tais como proteção de planilhas e acesso controlado a computadores - nos laboratórios, seguindo uma escala de zero (0) a cinco (5).

O formulário de laboratórios contava com duas seções:

I. Caracterização da empresa/instituição

Assim como para os auditores, foram solicitadas informações que possibilitassem a categorização dos laboratórios:

- estado e cidade em que a instalação está localizada;
- quantidade de funcionários;
- sistemas de gestão nos quais a instituição é acreditada, reconhecida ou certificada;
- principal classe de ensaio do laboratório;
- há quanto tempo a instituição é acreditada, reconhecida ou certificada;
- caráter da instituição (pública, particular, capital misto ou educacional).

II. Sobre as não conformidades

Foi solicitado ao participante que indicasse se, durante a última auditoria externa, os tópicos descritos relacionados a sistemas computadorizados haviam sido verificados pelos avaliadores e se a instituição havia recebido alguma não conformidade (NC). Em caso afirmativo, era pedido que a não-conformidade fosse relatada. Também nessa seção, foi adicionada uma questão solicitando que o participante avaliasse a dificuldade de implantar os itens descritos.

Para determinar quais situações e questionamentos seriam apresentados aos participantes, foi levada em consideração a experiência do orientador desta pesquisa, que atua na área de Gestão de Qualidade desde 2008.

3.2 Contato com os participantes

Inicialmente, o *link* para os formulários foi enviado aos participantes via *e-mail*, juntamente com um texto de apresentação dos idealizadores da pesquisa e seus objetivos, além do endereço do *site* criado na plataforma Wix para divulgar a pesquisa, contendo informações mais detalhadas sobre essa. Os endereços de *e-mail* para contato com os laboratórios foram obtidos no site do Inmetro, em seu catálogo de laboratórios pertencentes à Rede Brasileira de Laboratórios de Ensaio (RBLE). Adicionalmente, a pesquisa foi divulgada no site de notícias do IQSC-USP e em grupos de redes sociais relacionados a auditores e laboratórios com sistemas de gestão implementados.

3.3 Análise dos dados

As respostas recebidas foram compiladas em planilhas do Excel e analisadas com o auxílio da função *cont.se*.

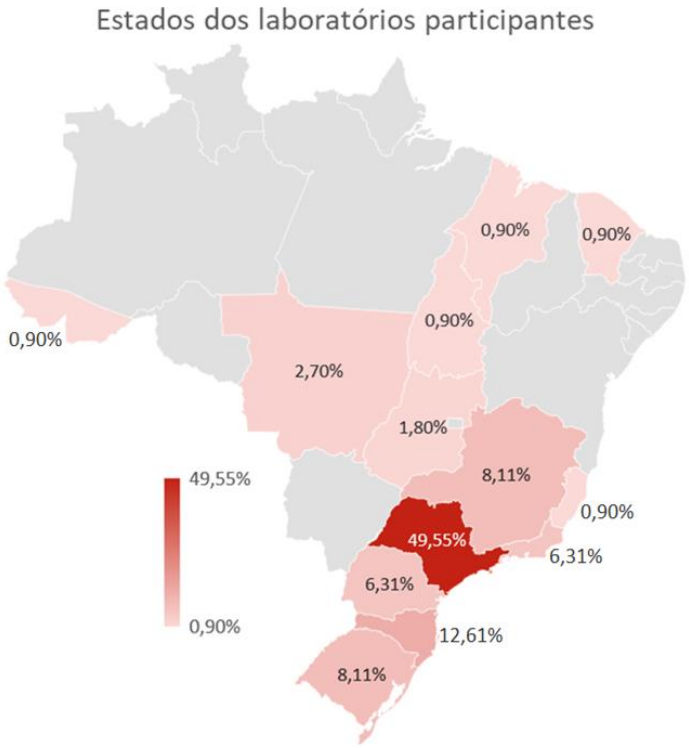
4 RESULTADOS E DISCUSSÃO

4.1 Laboratórios

4.1.1 Caracterização dos laboratórios

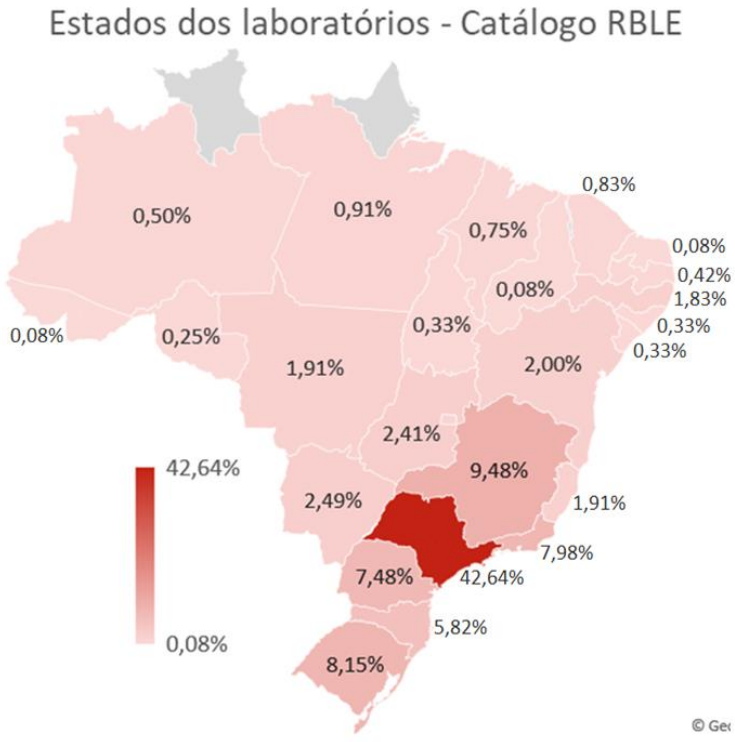
Houve a participação de 111 laboratórios, localizados em treze diferentes estados, como mostra a Figura 1. São Paulo e Santa Catarina foram as unidades federativas com maior número de participantes, seguidos por Minas Gerais, Rio Grande do Sul, Paraná e Rio de Janeiro. Analisando a listagem de laboratórios da RBLE, esta mesma ordem é seguida, com a exceção de Santa Catarina, que figura como o sexto estado com mais laboratórios acreditados. No caso dos dados coletados, esses seis estados correspondem a 90,99% das respostas recebidas, enquanto no catálogo da RBLE eles representam 82,48% do total, mostrando que a pesquisa feita possui uma boa aproximação da realidade.

Figura 1 Localização dos laboratórios participantes por estado



Fonte: Autoria própria

Figura 2 Localização dos laboratórios cadastrados no catálogo da RBLE por estado

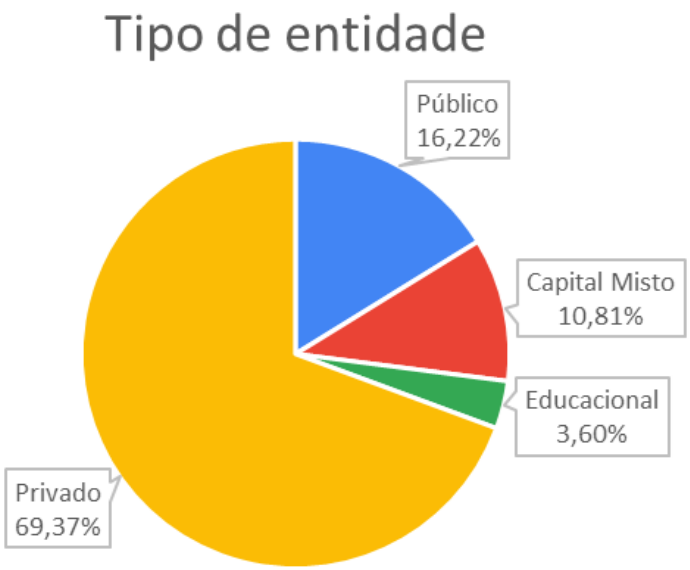


Fonte: Autoria própria

Era dada aos participantes a opção de informar qual cargo ocupavam na empresa, porém, por não se tratar de uma pergunta obrigatória, há vários casos em que não se obteve um retorno. Não obstante, constatou-se que predominaram respostas de gerentes da qualidade, gerentes técnicos e membros da diretoria dos laboratórios. Tal fato é importante por serem cargos cujo escopo de atribuições segundo as normas de interesse inclui ter expressivo conhecimento sobre o sistema de qualidade implantado no laboratório e nível de aderência a ele por parte dos funcionários.

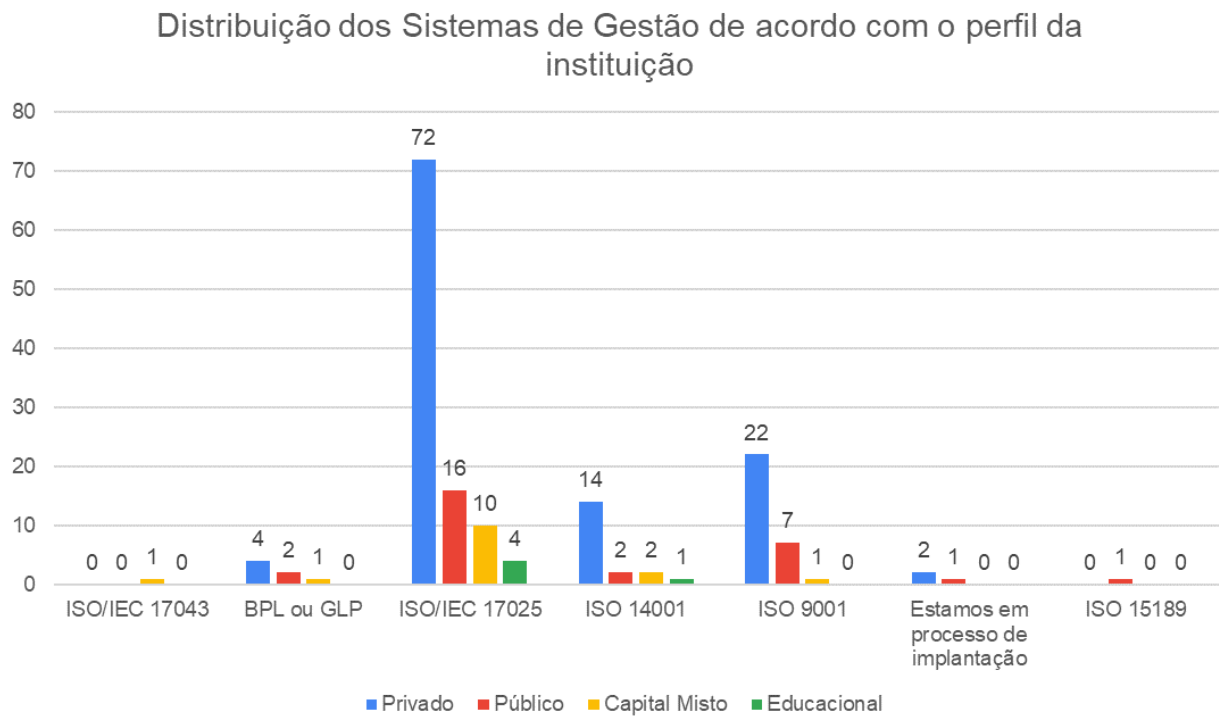
Grande parte das instituições participantes – 69,37% – declarou ser de caráter particular (Figura 3). Neste grupo, apenas 3,90% não são acreditados na ISO/IEC 17025 e 2,60% estão em processo de acreditação. É apresentada uma relação entre o perfil das instituições e seus Sistemas de Gestão na Figura 4. Tratando-se da quantidade de funcionários, a participação de instituições de todos os tamanhos foi razoavelmente homogênea, com pequeno predomínio de empresas com mais de 100 funcionários, como mostra a Figura 5. Entre tais empresas, o tempo de certificação superior a cinco anos representa 79,49% das respostas, e apenas 2,56% ainda está em processo de implantação de um sistema de gestão da qualidade.

Figura 3 Quantidade de instituições públicas, privadas, educacionais ou de capital misto



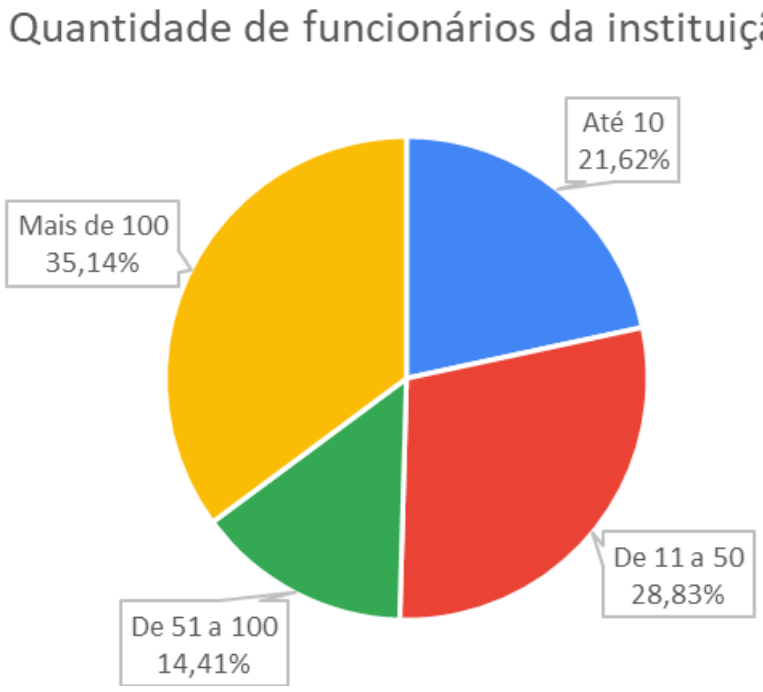
Fonte: Autoria própria

Figura 4 Distribuição dos Sistemas de Gestão de acordo com o perfil de instituição



Fonte: Autoria própria

Figura 5 Quantidade de funcionários nas instituições



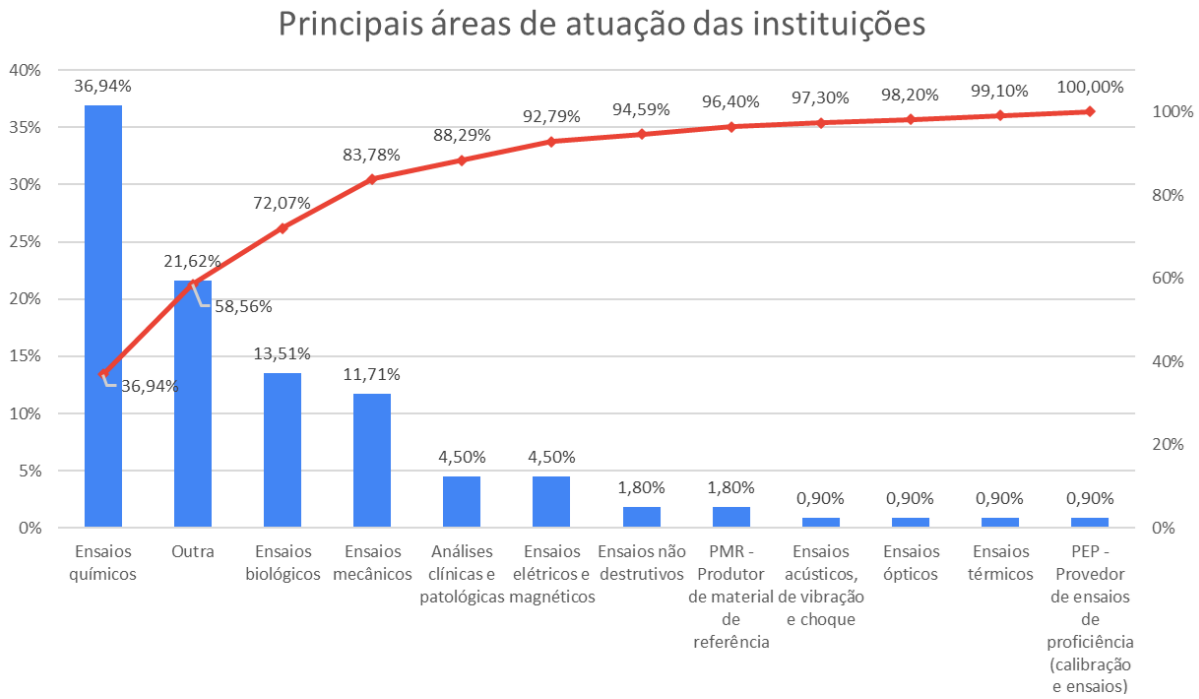
Fonte: Autoria própria

Quanto às classes de ensaio, 36,94% dos laboratórios trabalham com ensaios químicos (Figura 6), outro grupo no qual predomina a acreditação na ISO/IEC 17025: 87,80% são acreditados nessa norma, e nos casos de exceção, os laboratórios estão em processo de implantação de um SGQ (7,32%) ou a única certificação é em BPL ou ISO 9001 (2,44% cada).

Como era esperado, a maior parte dos laboratórios é acreditada na ISO/IEC 17025 (Figura 7); 59,46% dos laboratórios são acreditados unicamente nessa norma, 12,61% também possuem acreditação na ISO 9001, 9,01% têm uma terceira acreditação (na ISO 14001) e 6,31% dos laboratórios são acreditados na ISO/IEC 17025 e na ISO 14001.

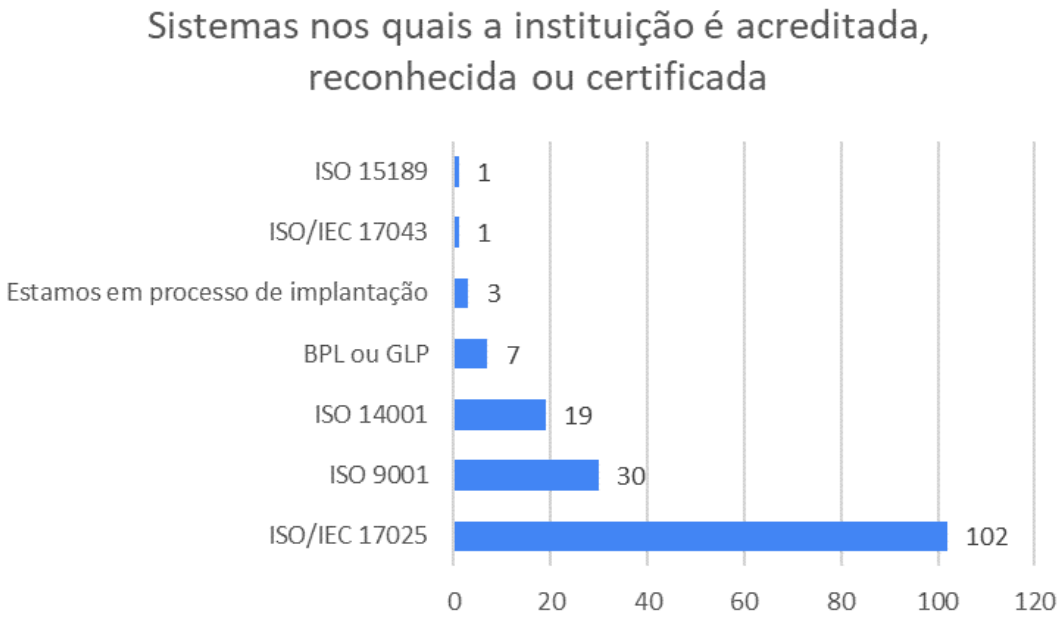
Tratando do tempo de acreditação, a grande maioria dos laboratórios tem Sistemas de Gestão da Qualidade já com certa maturidade: 22,52% possuem acreditação há três ou quatro anos e 66,67% são acreditados há pelo menos cinco anos (Figura 8). Em teoria, isso permite inferir que nesses casos houve tempo suficiente para a instituição se ajustar aos requisitos e o SGQ já está bem fundamentado e adaptado à rotina da empresa, com os funcionários familiarizados com suas exigências.

Figura 6 Principais áreas de atuação das instituições



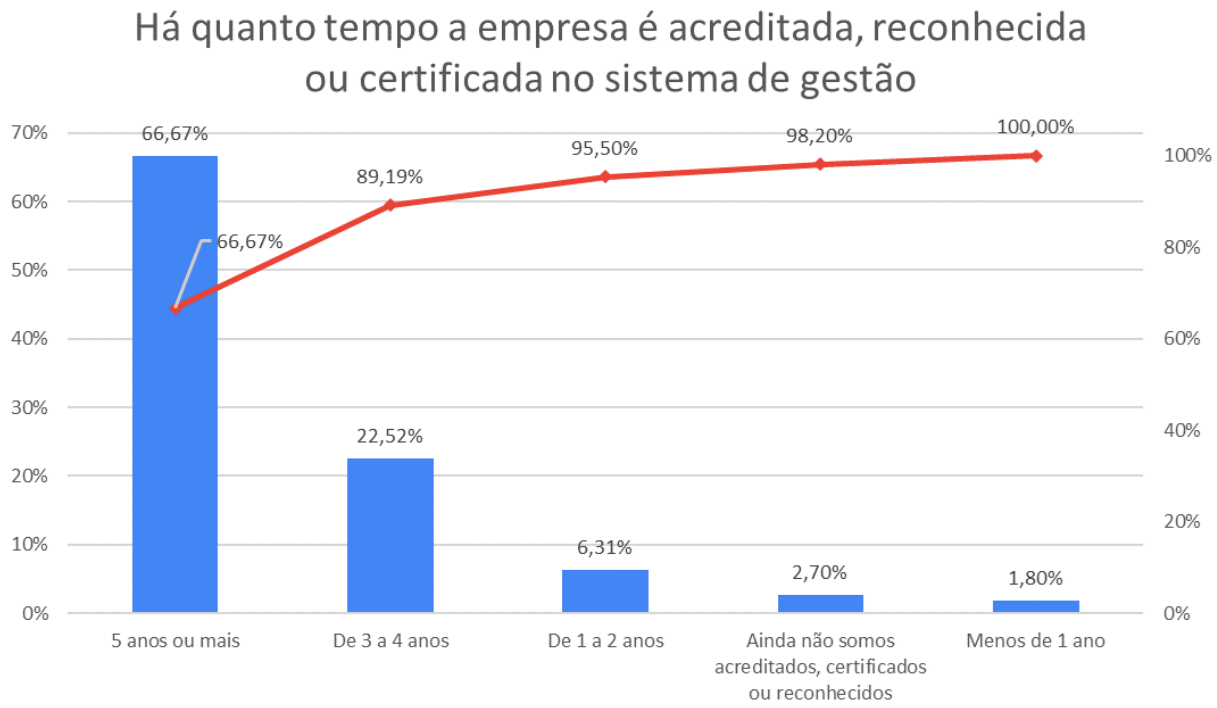
Fonte: Autoria própria

Figura 7 Sistemas de Gestão da Qualidade nos quais as instituições são acreditadas, reconhecidas ou certificadas (em número de laboratórios)



Fonte: Autoria própria

Figura 8 Há quanto tempo a empresa é acreditada, reconhecida ou certificada no SGQ

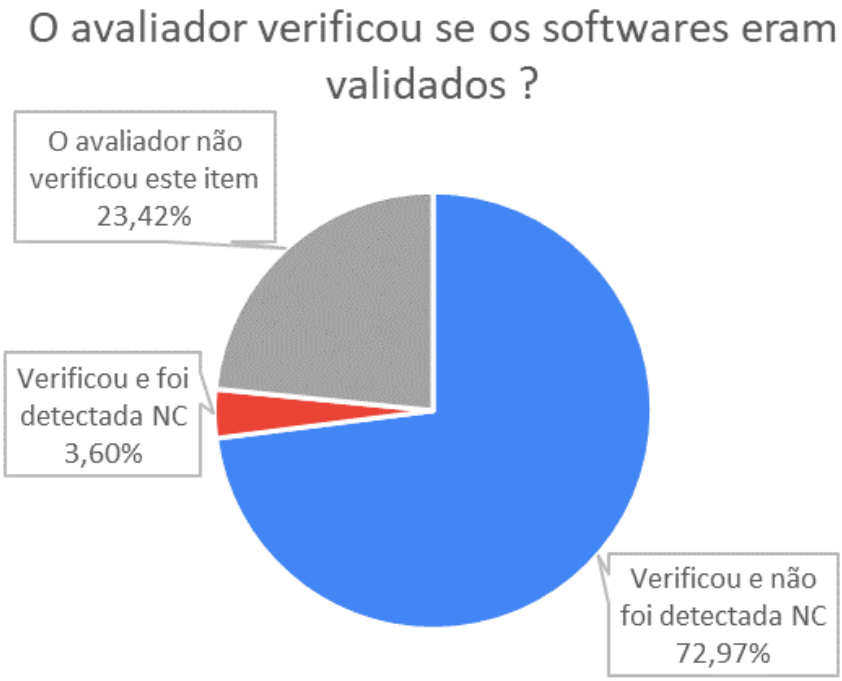


Fonte: Autoria própria

4.1.2 Sobre os itens avaliados e conformidades com os requisitos

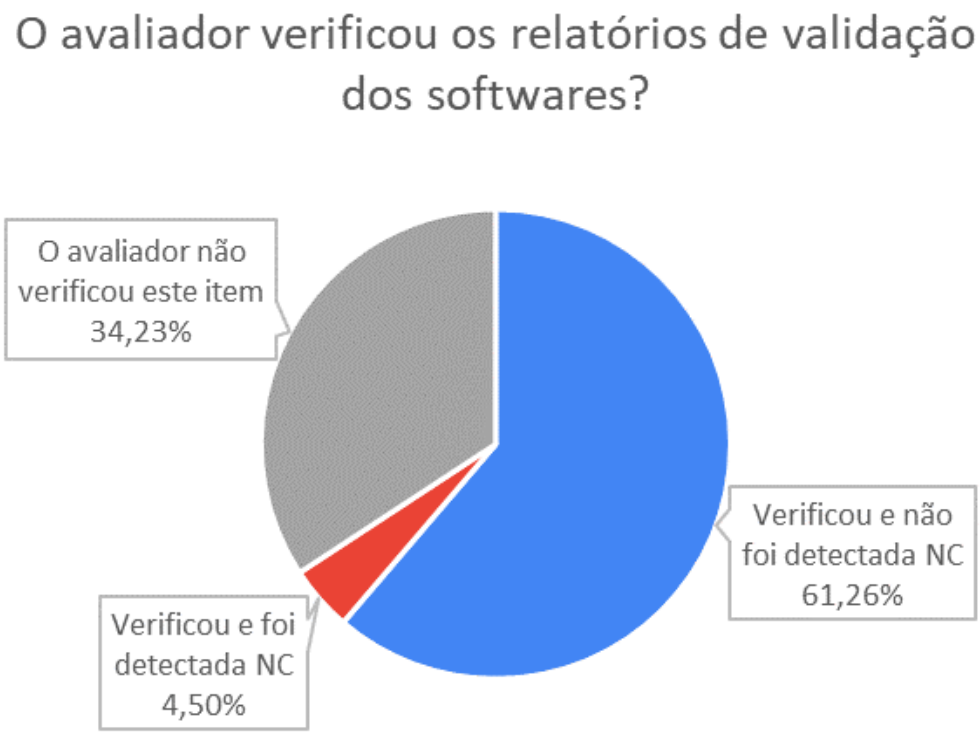
O propósito de avaliar as não conformidades recebidas pelos laboratórios durante sua última auditoria externa era não apenas identificar os itens relacionados a sistemas computadorizados com maior incidência de NCs, mas também averiguar a taxa de verificação dos avaliadores de cada item. Iniciando as perguntas, os laboratórios foram questionados sobre a validação dos *software* utilizados e seus relatórios de validação (Figuras 9 e 10). 76,57% disseram que a validação foi verificada pelo avaliador, porém em apenas 65,76% dos casos o relatório que comprovaria tal validação foi solicitado. Ambos os itens são requisitos de quatro das seis normas citadas na pesquisa (requisito 7.11.2 da ISO/IEC 17025, 4.7.1.1 da ISO/IEC 17043, 5.10.3 da ISO 15189 e item 7 da NIT-DICLA-038), de forma que só 2,70% dos laboratórios não são de fato cobrados por tais itens. Isso torna ainda mais inquietante a constatação de que quase 25% dos avaliadores não verificaram a validação de *software* e mais de 33% não verificaram os relatórios de tal validação. A diferença entre esses valores ainda permite levantar o questionamento sobre qual foi a forma utilizada pelo avaliador para verificar a validação dos programas quando os relatórios não foram solicitados, sendo que estes são os documentos que comprovam a realização do procedimento.

Figura 9 "O avaliador verificou se os softwares eram validados?"



Fonte: Autoria própria

Figura 10 "O avaliador verificou os relatórios de validação dos softwares?"



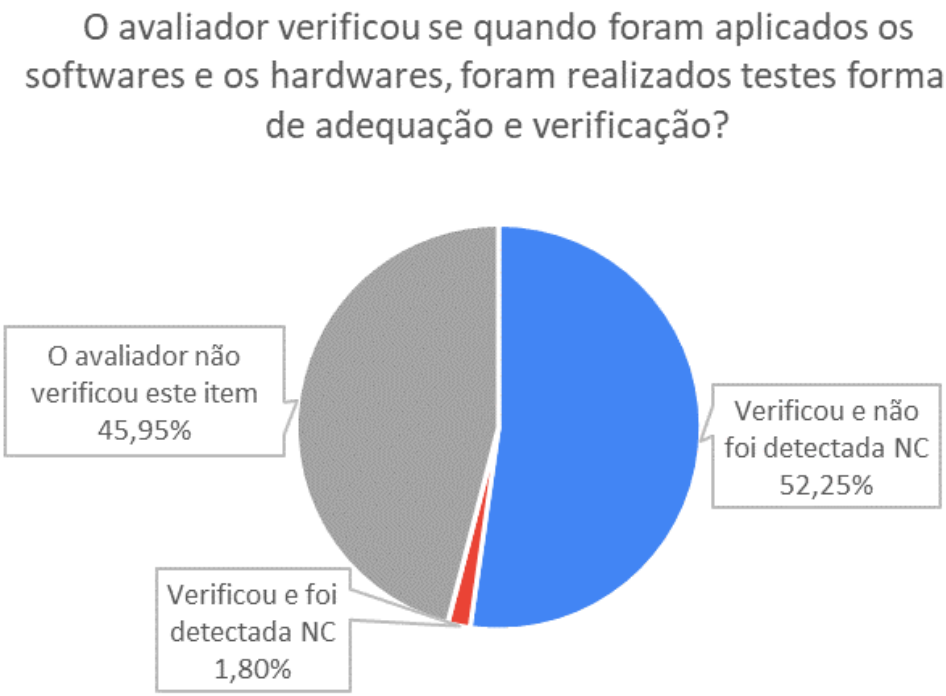
Fonte: Autoria própria

Em casos de aquisição de *software* já validado, o processo que comprova sua pertinência ao fim pretendido é o teste formal de adequação e verificação. Sua definição pela BPL é:

> Teste formal de um sistema informatizado no contexto operacional projetado para verificar se todos os critérios da Unidade Operacional foram devidamente respeitados e se o sistema pode ser aceito para funcionar no modo operacional. [11]

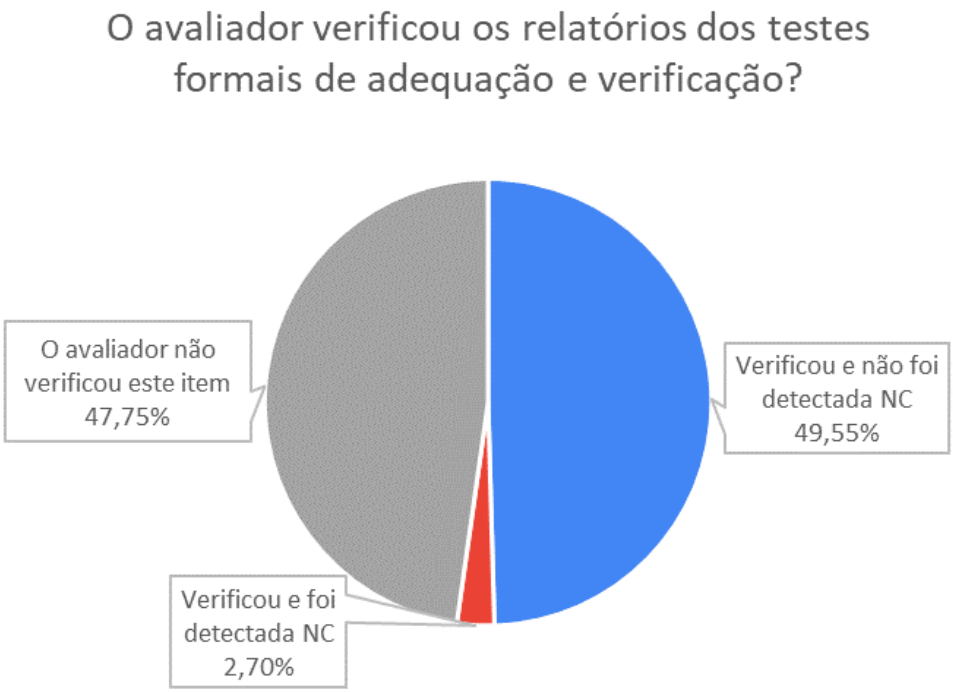
Com ele, garante-se não apenas que o *software* está em conformidade com os requisitos necessários, como também que não ocorrerão erros em decorrência de uma possível insuficiência de desempenho (por exemplo, um *software* de planilhas eletrônicas adquirido com a finalidade de processar dados analíticos que, no entanto, retorna resultados com o máximo de duas casas decimais). Assim como para a validação feita pelo próprio laboratório, é necessário elaborar um relatório dos testes para evidenciar tanto sua realização quanto sua efetividade. Ainda que seja um processo importante, quase metade dos avaliadores não chegou a conferir os testes (45,95%) nem os relatórios (47,75%), como mostram as Figuras 11 e 12.

Figura 11 "O avaliador verificou se quando foram aplicados os softwares e hardwares, foram realizados testes formais de adequação e verificação?"



Fonte: Autoria própria

Figura 12 "O avaliador verificou os relatórios dos testes formais de adequação e verificação?"



Fonte: Autoria própria

Um ponto que não é explicitamente abordado por nenhuma norma, porém se enquadra em requisitos que tratam de segurança dos dados e de correto funcionamento dos equipamentos para prevenir sua deterioração, é a versão do sistema operacional (SO) instalado nos computadores. É o SO que controla todos os programas executados pelo computador e gerencia a distribuição de sua capacidade entre os processos sendo executados,[14] portanto influencia na estabilidade destes e em falhas causadas por travamentos, por exemplo.

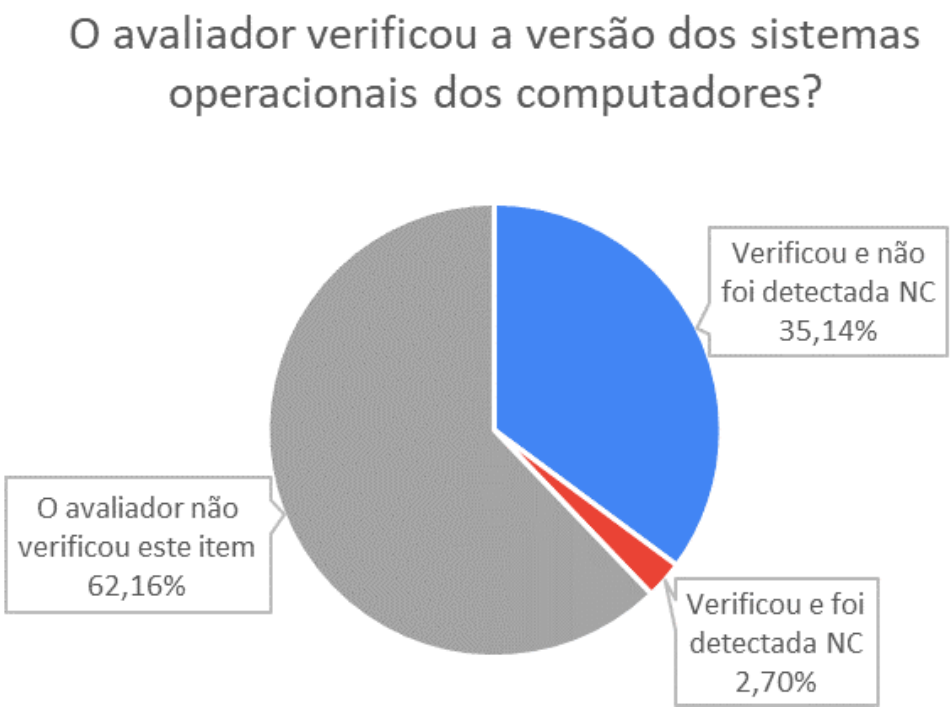
Em um panorama mundial, os SOs Windows são a escolha de 87,62% dos usuários, seguido por Mac OS com 9,51% e Linux com 2,30%. [15] Dentro dessa parcela do SO da Microsoft, a versão mais difundida é o mais recente Windows 10, utilizado em 77,31% das máquinas. [16] Seus antecessores mais famosos, Windows 8.1, 8, 7 e XP, representam, respectivamente, 3,79%, 1,00%, 16,8% e 0,71% dos computadores mundiais. [16] No Brasil, a porcentagem de usuários do Windows 10 sobe para 82,85%, enquanto seus antecessores diminuem para 3,03% (Windows 8.1), 0,54% (Windows 8), 13,29% (Windows 7) e 0,26% (Windows XP). [17]

De forma geral, SOs mais recentes têm melhor performance e é importante mantê-los em dia com as atualizações fornecidas pelo desenvolvedor, visto que estas trazem correções de *bugs* e segurança (atualização de qualidade), podem otimizar a produtividade – pois um computador mais rápido permite que mais trabalho seja realizado em menor tempo e com menos falhas – e podem oferecer novas funcionalidades para o usuário (atualização de recursos). Dito isso, é importante ressaltar que SOs como Windows XP, Windows 7 e Windows 8, ainda populares entre laboratórios brasileiros,[13] já estão fora da Política de Ciclo de Vida Fixa da Microsoft (produtos com a data de término do suporte já determinada no momento de seu lançamento). [18-20] Esse encerramento do suporte acarreta possível desempenho reduzido de softwares mais recentes, que são projetados para SOs modernos, e na inexistência de novas atualizações, tanto de recursos quanto de qualidade, para o SO,[21] o que torna os três mencionados desaconselháveis para uso. Na época da pesquisa, os únicos SOs da Microsoft ainda com suporte eram Windows 8.1 (com encerramento em 01/2023) [22] e Windows 10.

Apesar da influência da versão dos SOs e de suas atualizações sobre os sistemas computadorizados, esses não são aspectos muito observados em auditorias: 62,16% dos avaliadores não verificaram quais eram as versões dos SOs utilizados em

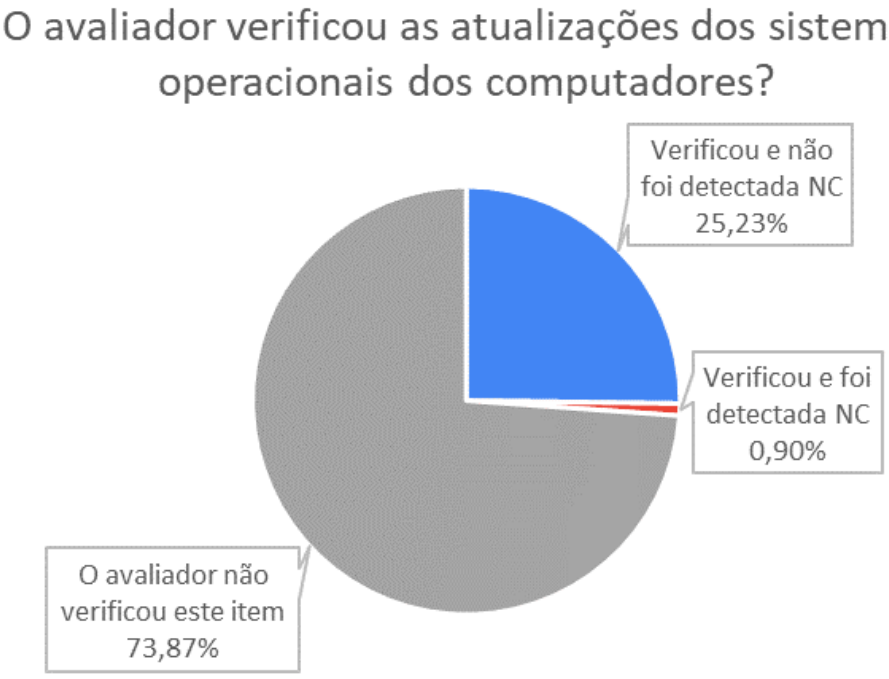
computadores laboratoriais e 73,87% não verificou se os SOs eram mantidos atualizados (Figuras 13 e 14).

Figura 13 "O avaliador verificou a versão dos sistemas operacionais dos computadores?"



Fonte: Autoria própria

Figura 14 "O avaliador verificou as atualizações dos sistemas operacionais dos computadores?"

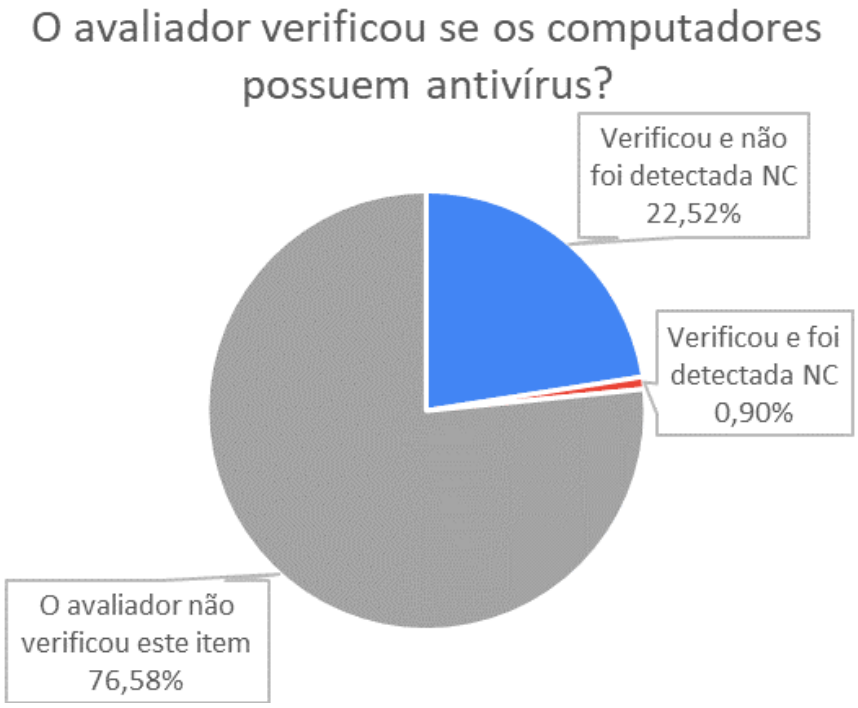


Fonte: Autoria própria

A utilização de antivírus – que atualmente recebe o nome mais apropriado de *antimalware* – também não é um requisito explícito, mas englobado por requisitos que mencionam a necessidade de segurança dos dados e arquivos. Sua importância, porém, é muito mais evidente; os computadores estão constantemente expostos a situações em que podem ser contaminados por algum *malware*, seja a partir de uma conexão com a internet ou mesmo de um *pendrive* inserido para transportar dados entre computadores. *Malware*, como explica seu próprio nome em inglês – *malicious software* – engloba softwares maliciosos, como *trojans*, *spyware* e *ransomware*, além dos conhecidos vírus digitais. Por isso, é indicado que se utilizem *antimalware* apropriados para empresas, sendo executados e atualizados na maior frequência possível, visto que novos programas maliciosos são criados diariamente. [23]

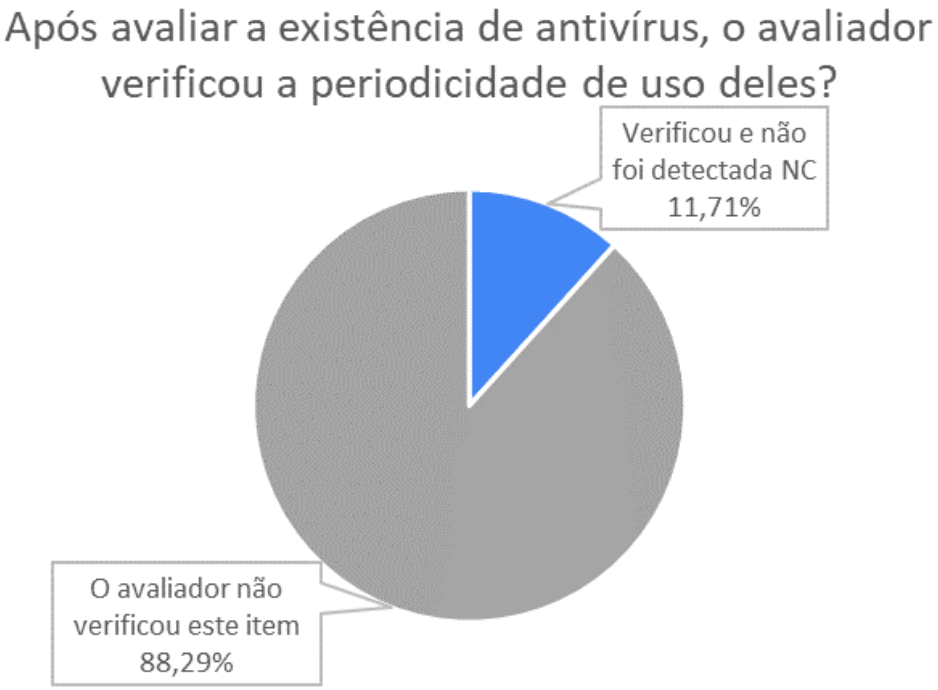
Entretanto, talvez pela obviedade de quão indispensável o *antimalware* é, este foi o item menos avaliado durante auditorias. Em 76,58% dos laboratórios, a existência de um *antimalware* nos computadores não foi investigada; em 88,29%, não foi verificada a periodicidade de uso deste tipo de programa e em 89,19%, não se verificou sua periodicidade de atualização (Figuras 15, 16 e 17).

Figura 15 "O avaliador verificou se os computadores possuem antivírus?"



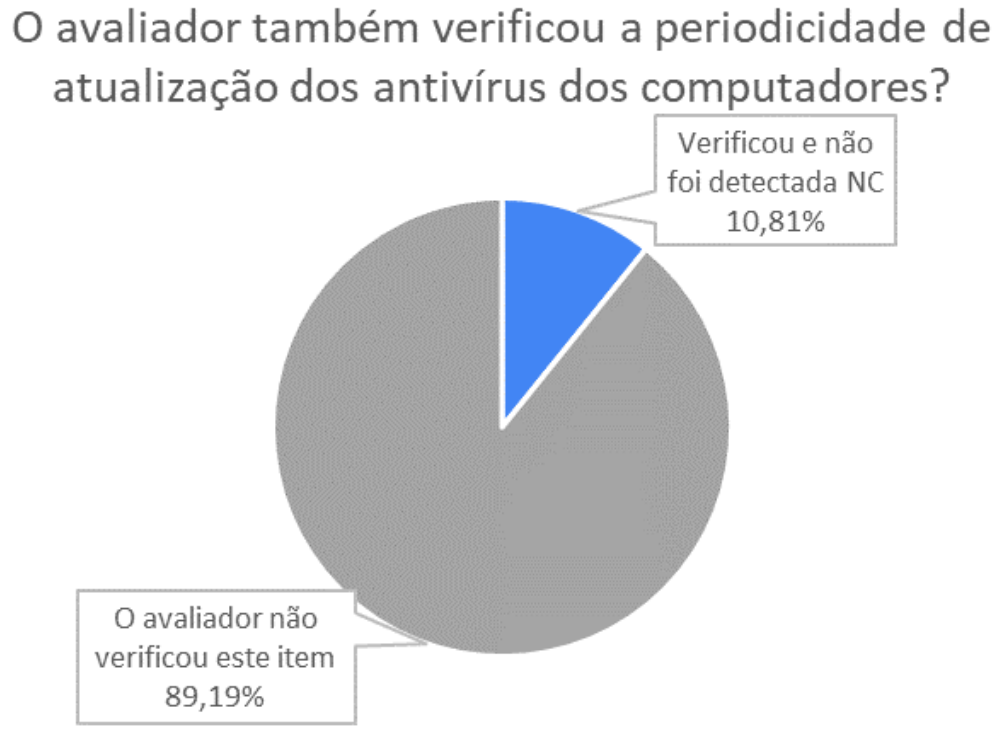
Fonte: Autoria própria

Figura 16 - "Após avaliar a existência de antivírus, o avaliador verificou sua periodicidade de uso?"



Fonte: Autoria própria

Figura 17 - "O avaliador também verificou a periodicidade de atualização dos antivírus dos computadores?"



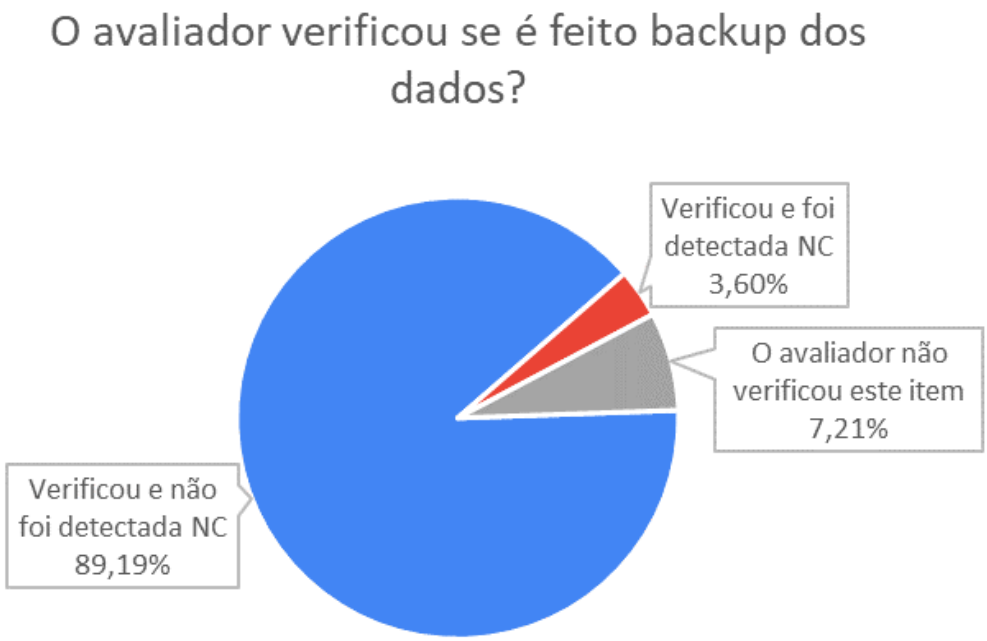
Fonte: Autoria própria

Outro item que também é sabidamente indispensável, é o *backup* dos dados e documentos gerados na rotina do laboratório. As normas ISO/IEC 17025 (requisito 7.11.3), ISO/IEC 17043 (requisito 5.13.1.4), ISO 15189 (requisito 5.10.3) e NIT-DICLA-038 (item 6) mencionam em seus textos a exigência de "*backup*", "cópias de segurança" ou, pelo menos, cópias de diferentes tipos de documentos e registros, a serem mantidas impressas ou em meio digital. Tais medidas são necessárias para garantir a rastreabilidade de informações, integridade de dados brutos e facilitar a recuperação do sistema informatizado em caso de falha total ou parcial desse, por exemplo. Adicionalmente, quanto maior a frequência com que o *backup* é feito, menor é a probabilidade de que qualquer quantidade de informação, ainda que pequena, possa se perder.

Contrariamente ao *antimalware*, as perguntas relacionadas ao *backup* dos dados tiveram as maiores porcentagens referentes a uma verificação realizada pelo avaliador. 92,79% das auditorias contaram com a apuração acerca da existência de *backup* e 90,99%, com sua frequência de realização. Na grande maioria dos casos, não foi detectada não conformidade, mas não é possível afirmar se isso se deve a uma boa implementação por parte dos laboratórios ou por carência de avaliação, visto que os auditores demonstraram possuir a fundamentação necessária para realizá-la, como será discutido no item 4.2.2. Além disso, há casos em que não se configura uma não conformidade, porém a forma escolhida para o *backup* não é aconselhável, como as mídias externas (CDs, *pen drives* e HDs externos) utilizadas por cerca de 35% dos laboratórios. [11]

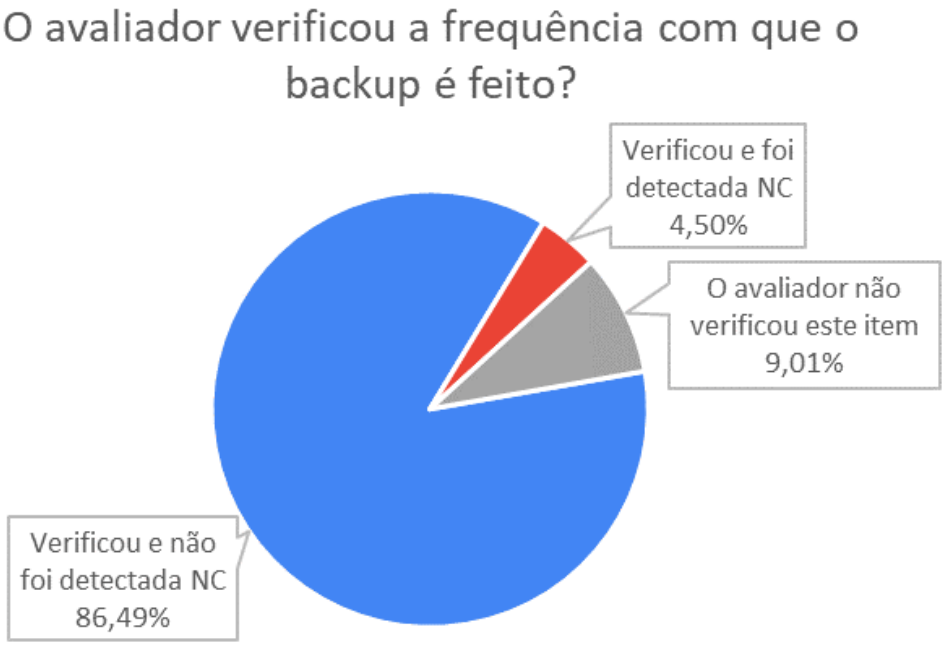
Também é possível que, apesar de relacionada ao *backup*, a não conformidade seja observada em outro item, como o contrato de confidencialidade. Por exemplo, aproximadamente um terço das instituições utilizam o servidor em nuvem para a segurança de seus dados,[11] portanto todas devem apresentar tal contrato (o que será discutido mais à frente neste texto).

Figura 18 - "O avaliador verificou se é feito *backup* dos dados?"



Fonte: Autoria própria

Figura 19 - "O avaliador verificou a frequência com que o *backup* é feito?"

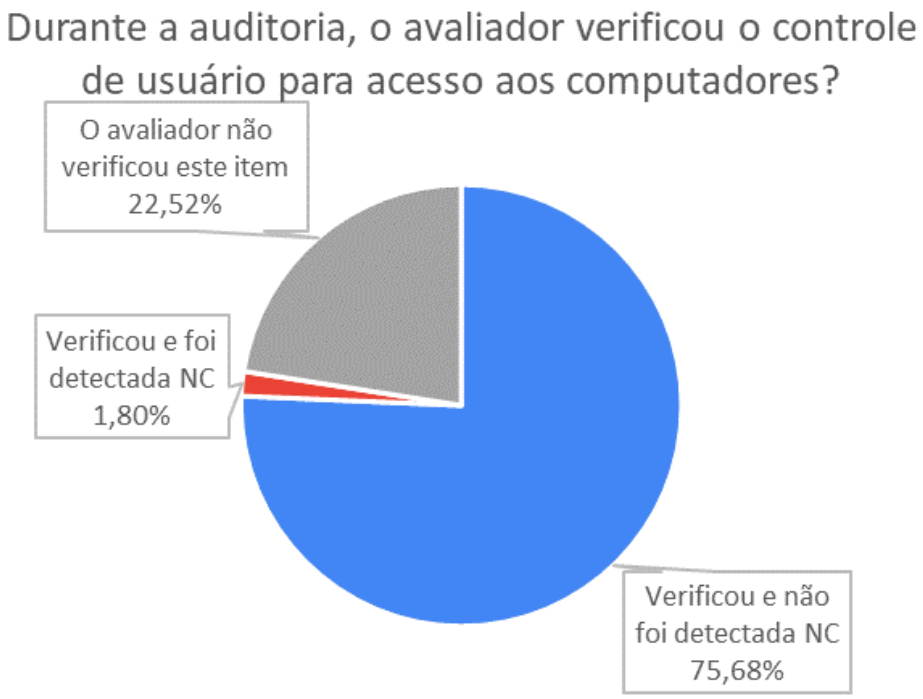


Fonte: Autoria própria

O acesso controlado às informações laboratoriais é necessário para evitar que dados dos estudos conduzidos pelo laboratório sejam alterados indevidamente por pessoas não autorizadas ou mesmo divulgados, o que acarretaria quebra de contrato com clientes. Além disso, o controle permite monitorar quem acessou os dados e quando isso foi feito, o que auxilia na rastreabilidade de informações, sensíveis ou não. A proteção contra acesso não autorizado também é um requisito das normas ISO/IEC 17025 (requisito 7.11.3), ISO/IEC 17043 (requisito 5.13.1.4), ISO 15189 (requisito 5.10.3) e NIT-DICLA-038 (item 6) e ainda é mencionada na ISO 9001 (requisito 7.5.3.2), portanto, é necessária a todos os laboratórios participantes. Dessa forma, ainda que o controle de usuário tenha sido verificado em mais de três quartos dos casos, a porcentagem de 22,52% de avaliadores que ignoraram este ponto (Figura 20) é alarmante.

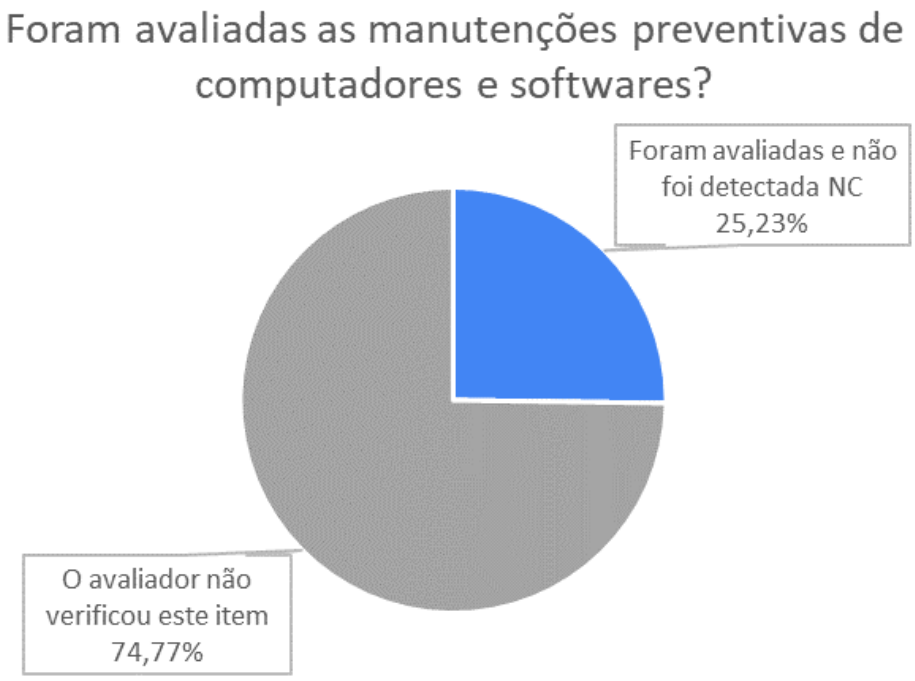
Manutenções preventivas e corretivas são processos para manter a integridade dos equipamentos e informações nele contidas. As manutenções preventivas reduzem a necessidade de execução das corretivas, podendo evitar perdas relacionadas ao tempo de permanência de um equipamento em reparo e falhas cometidas em decorrência de decisões tomadas em caráter de urgência, por exemplo. A existência de procedimentos documentados para manutenções preventivas e corretivas também é exigida por todas as normas (requisito 6.4.3 da ISO/IEC 17025, 5.10 da ISO/IEC 17043, 5.3.1.5 da ISO 15189, 7.1.1 da ISO 9001 e itens 4.a e 4.b da NIT-DICLA-038), mas 74,77% dos auditores não verificaram se os laboratórios possuíam manutenções preventivas de computadores e softwares e 82,88% não verificaram as manutenções corretivas (Figuras 21 e 22).

Figura 20 - "Durante a auditoria, o avaliador verificou o controle de usuário para acesso aos computadores?"



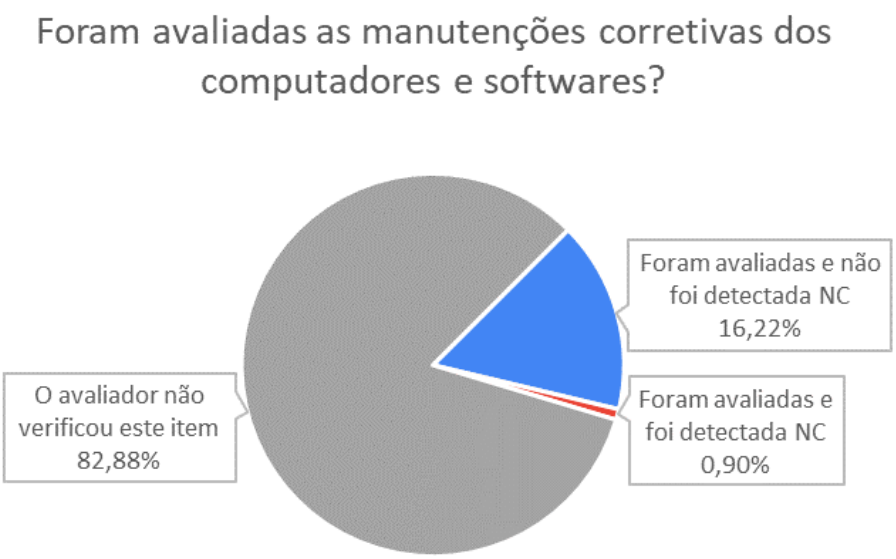
Fonte: Autoria própria

Figura 21 - "Foram avaliadas as manutenções preventivas de computadores e softwares?"



Fonte: Autoria própria

Figura 22 – “Foram avaliadas as manutenções corretivas dos computadores e softwares?"

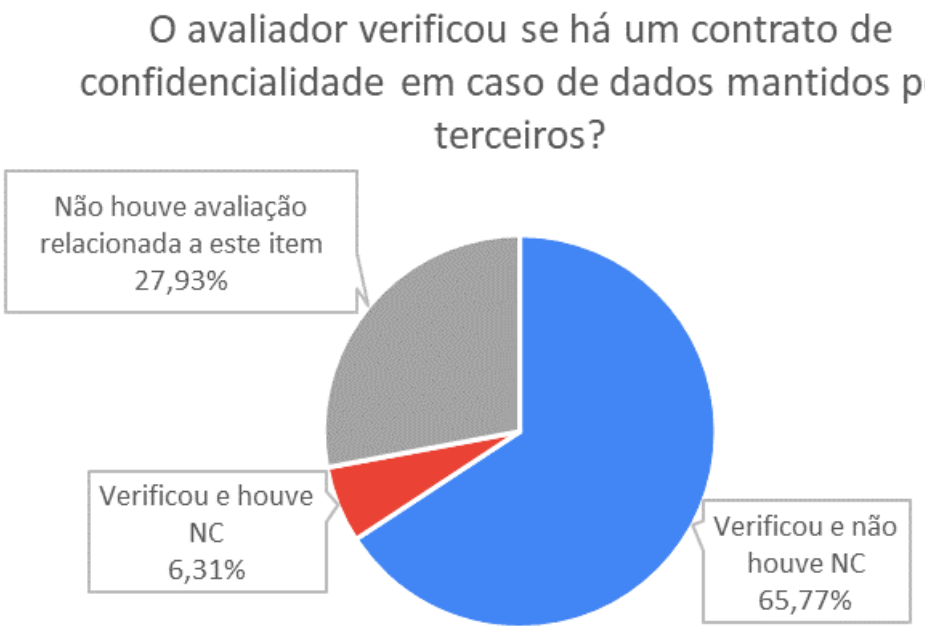


Fonte: Autoria própria

Quando os dados referentes aos ensaios realizados não são mantidos nas instalações dos laboratórios ou estão em servidores externos, é preciso assegurar que o provedor do serviço esteja em conformidade com os requisitos da norma seguida pelo laboratório, o que inclui a confidencialidade (requisito 7.11.4 da ISO/IEC 17025, 5.13.1.3 da ISO/IEC 17043, 5.10.3 da ISO 15189, 7.5.3.1 da ISO 9001 e item 9 da NIT-DICLA-038). Assim, o mais indicado é que exista um contrato entre as partes envolvidas assegurando o sigilo das informações armazenadas. 72,08% dos avaliadores verificaram a existência de tal contrato e em 6,31% dos casos foi observada alguma não conformidade. Em uma delas, tendo em vista que os dados são mantidos na plataforma da Microsoft de serviços de computação em nuvem, o avaliador citou a necessidade de um contrato com a empresa, dizendo "Não foram evidenciados os acordos de confidencialidade relativos ao fornecedor de informática que gere os servidores utilizados pelo laboratório (nome da instituição), nem à Microsoft, onde são alojados os Backups na “nuvem” Azure".

No entanto, isso evidencia um provável desconhecimento tanto da parte do avaliador quanto do laboratório, pois tal contrato é padrão da Microsoft para todos os seus sistemas e é firmado no momento em que o revendedor fornece a assinatura do produto ao cliente – no caso, o laboratório.

Figura 23 - "O avaliador verificou se há um contrato de confidencialidade em caso de dados mantidos por terceiros?"

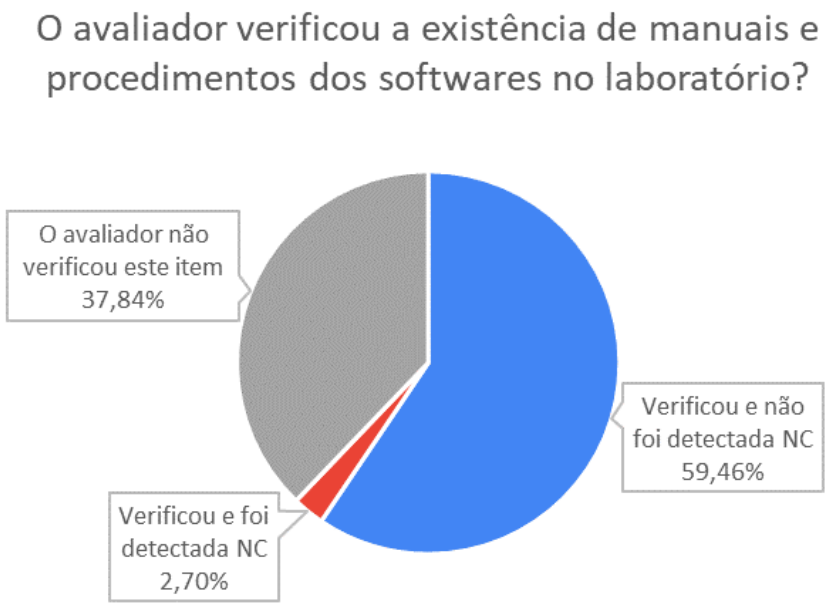


Fonte: Autoria própria

Outro item apresentado como requisito de todas as normas é a existência de manuais e instruções referentes a equipamentos, e que estes estejam prontamente disponíveis (requisito 7.11.5 da ISO/IEC 17025, 5.2.2 da ISO/IEC 17043, 5.3.1.3 da ISO 15189, 7.5.3.1 da ISO 9001, 7.5.3 da ISO 14001 e item 8 da NIT-DICLA-038). Mesmo que os funcionários recebam treinamento sobre o sistema de gestão, *software* e equipamentos pertinentes à sua rotina de trabalho, a presença dos manuais pode sanar dúvidas que gerariam erros de manuseio e, consequentemente, erros no ensaio. No entanto, para 37,84% dos laboratórios não foi feita a verificação dos manuais (Figura 24).

Um fato interessante a ser mencionado é que as instruções disponíveis também devem passar por retificações quando necessário, e tal item deve ser igualmente verificado, assim como feito por um avaliador que detectou uma não conformidade em um dos laboratórios.

Figura 24 - "O avaliador verificou a existência de manuais e procedimentos dos softwares no laboratório?"



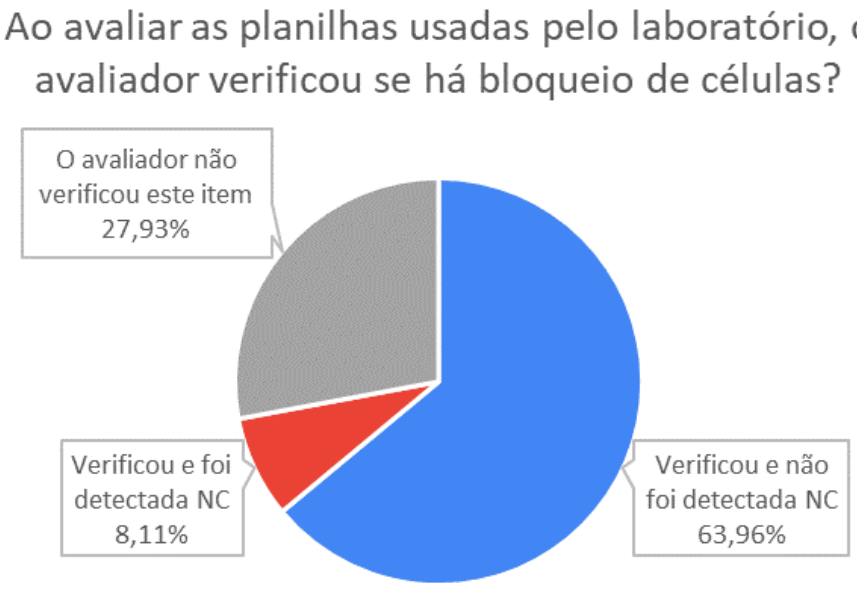
Fonte: Autoria própria

O último ponto abordado com relação às não conformidades foi o uso de planilhas. Pelo fato de serem o produto de um *software* que é adquirido e considerado validado, é possível que se acredite que somente os testes de adequação e verificação sejam abrangentemente suficientes. Porém, é necessário que as próprias planilhas criadas nestes softwares sejam validadas. Esse processo é necessário para averiguar a confiabilidade dos resultados gerados por elas, visto que ao preenchê-las é possível que haja fórmulas buscando dados de células com endereçamento errado, fórmulas digitadas incorretamente ou a inserção de dados inválidos. Para garantir que não sejam feitas modificações indesejadas após a validação da planilha, é indicado que as células contendo fórmulas sejam bloqueadas, permitindo alterações somente por pessoal e em campos autorizados, o que deveria resultar em uma nova validação da planilha no que diz respeito a estas modificações.

As verificações de bloqueio de células e validação de planilhas foram os itens pesquisados que mais apresentaram não conformidades entres os laboratórios, juntamente com os contratos de confidencialidade. Em 5,41% dos laboratórios foi identificada alguma não conformidade relacionada à validação de planilhas e em 8,11%, ao bloqueio de células (Figuras 25 e 26). Em referência ao último, um dos laboratórios comentou:

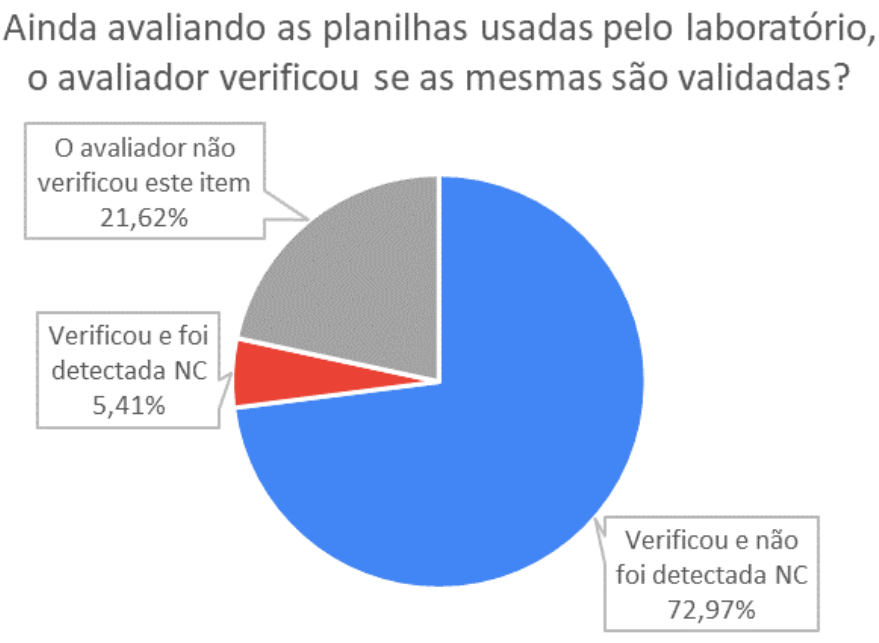
“Nesse item sempre ocorre NC (não conformidade), por falta de atenção, às vezes esquecemos de bloquear. Alguns consideram o acesso a planilha como bloqueio e outros solicitam o bloqueio do acesso e o bloqueio das células.”

Figura 25 - "Ao avaliar as planilhas usadas pelo laboratório, o avaliador verificou se há bloqueio de células?"



Fonte: Autoria própria

Figura 26 - "Ainda avaliando as planilhas usadas pelo laboratório, o avaliador verificou se as mesmas são validadas?"



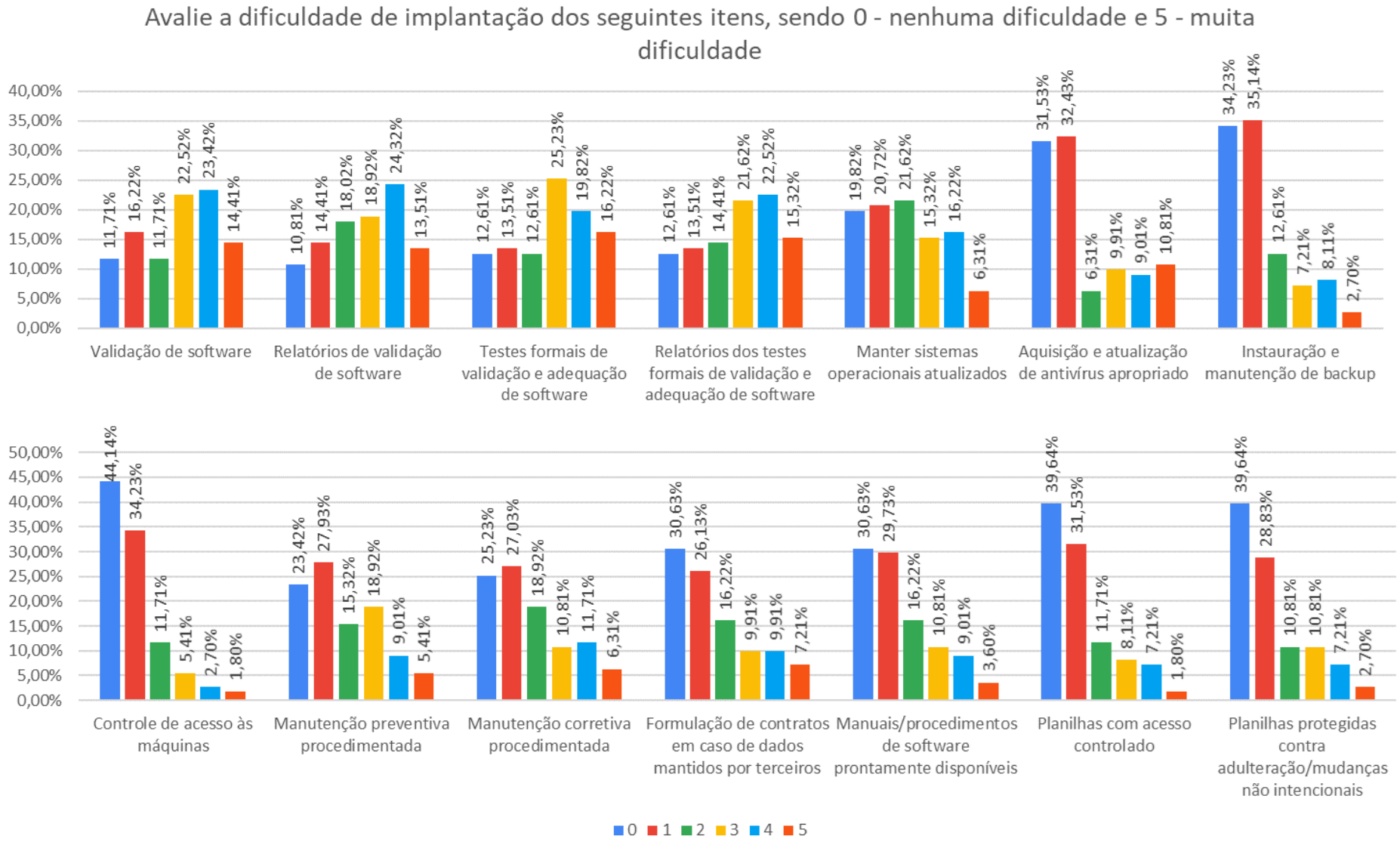
Fonte: Autoria própria

4.1.3 Avaliação de dificuldade para implantação dos itens mencionados

Por fim, solicitou-se aos laboratórios que avaliassem a dificuldade encontrada para implantar os itens presentes na pesquisa. Os que receberam mais votos de “muita dificuldade para implantar” foram validação de *software* e seus relatórios e testes formais de adequação e seus relatórios. Em pesquisa realizada anteriormente[13], os laboratórios também foram questionados sobre a dificuldade encontrada ao validar *software* e o perfil de votos observado é consonante com o obtido pela atual pesquisa. É provável que tal dificuldade exista por ser uma atividade a ser realizada por funcionários do laboratório, sem grandes conhecimentos ou experiência com a área de informática, o que é agravado pela ausência de um documento orientativo sobre como proceder com a validação e testes de adequação. Tal ausência também afeta a criação dos relatórios; é razoável que uma pessoa sem orientação para realizar o processo tenha dificuldades para relatá-lo, evidenciando de forma completa e satisfatória aquilo que foi observado.

Com exceção do item “manter sistemas operacionais atualizados”, os restantes apresentaram perfis que indicam uma percepção de pouca dificuldade para serem implementados, como pode ser visto na Figura 27. Quanto à atualização dos sistemas operacionais, os votos foram homogeneamente distribuídos entres os níveis de dificuldade, provavelmente por não ser uma tarefa de fato difícil, mas sim financeiramente dificultosa. No entanto, a aplicação da atualização das versões do sistema operacional dentro de uma mesma grande distribuição do SO (Windows 10, Windows 8, Windows 7, Mac OS 11 etc.) geralmente não envolve custos adicionais e traz um certo nível de melhoria (que é o não ideal caso o SO esteja fora do ciclo de vida definido).

Figura 27 - "Avalie a dificuldade de implantação dos seguintes itens, sendo 0 - nenhuma dificuldade e 5 - muita dificuldade”



Fonte: Autoria própria

4.2 Auditores

4.2.1 Caracterização dos auditores

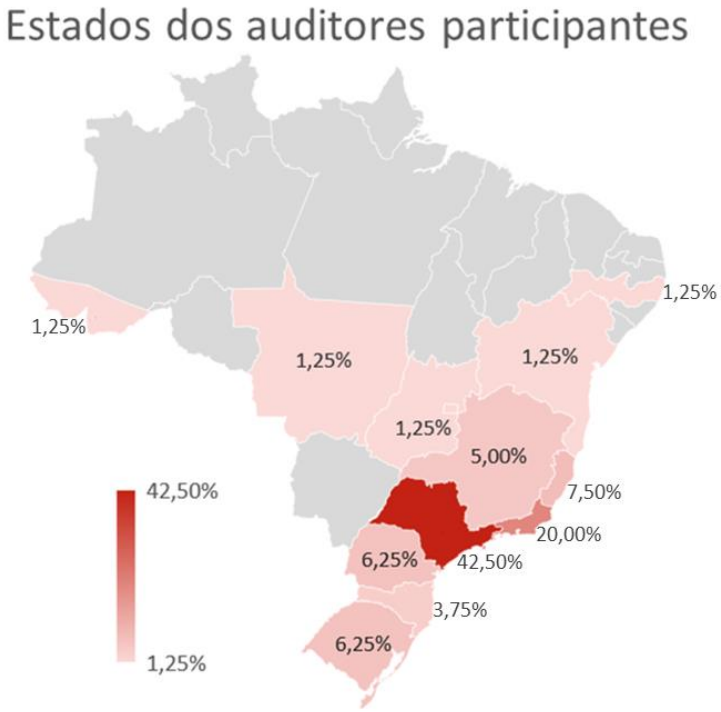
Participaram desta pesquisa 80 auditores de 14 estados brasileiros (Figura 28). Há três possibilidades quanto ao tipo de atuação do auditor:

- Auditor de primeira parte: é um integrante da própria empresa que realiza auditorias internas, a fim de acompanhar o andamento dos métodos, processos e atividades da instituição. Tal prática é importante para avaliar se o SGQ está de acordo com os resultados inicialmente esperados e para implantar medidas necessárias para a melhoria contínua;
- Auditor de segunda parte: é um indivíduo externo ao quadro da empresa auditada, representando uma segunda empresa, contratante da primeira. A auditoria no fornecedor tem como objetivo verificar se este está operando em conformidade com o sistema e com requisitos legais e contratuais;
- Auditor de terceira parte: é um auditor independente, indicado por um organismo de certificação e acreditação. Sua função é determinar se a organização implantou corretamente o SGQ no qual deseja ser acreditada.[24]

É importante ressaltar que um auditor pode atuar em mais de um tipo de categoria. Como exemplo, é possível que um membro da Garantia da Qualidade de uma empresa seja responsável pela condução das auditorias internas de sua empresa – sendo neste caso um auditor interno, de primeira parte – e também seja enviado para realizar auditorias em prestadores de serviços, assumindo nessa ocasião o papel de auditor de segunda parte. Ao questionar os participantes sobre sua atuação, as respostas recebidas contemplaram todas as possibilidades de combinações, desde aqueles que desempenham a função de apenas um tipo de auditor, passando pelos que realizam dois tipos de auditoria distintos até aqueles que acumulam as funções dos três tipos de auditores. Assim sendo, dos 80 participantes, 56 atuam como auditores de primeira parte (70,00%); 37, como auditores de segunda parte (46,25%) e 23, como auditores de terceira parte (28,75%). A distribuição das respostas quanto ao tipo de atuação está apresentada na

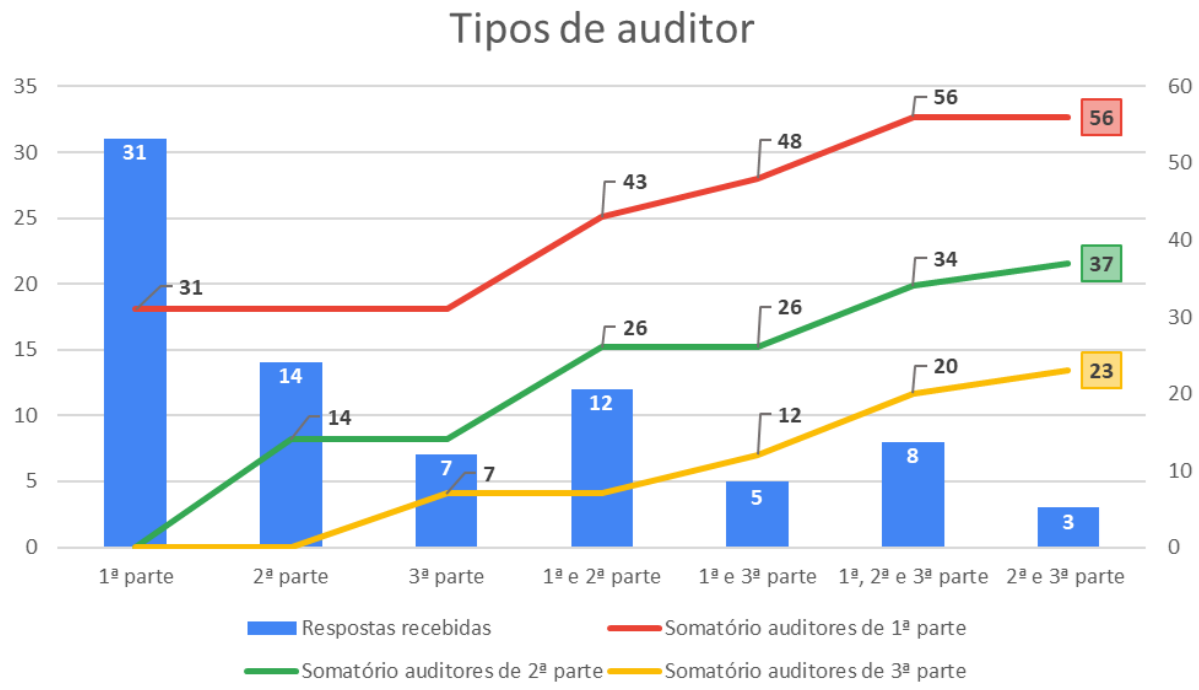
Figura ***29***.

Figura 28 Porcentagem de participação dos auditores por estados brasileiros



Fonte: Autoria própria

Figura 29 Quantidade de auditores de primeira, segunda e/ou terceira parte participantes na pesquisa (mais de uma resposta permitida)

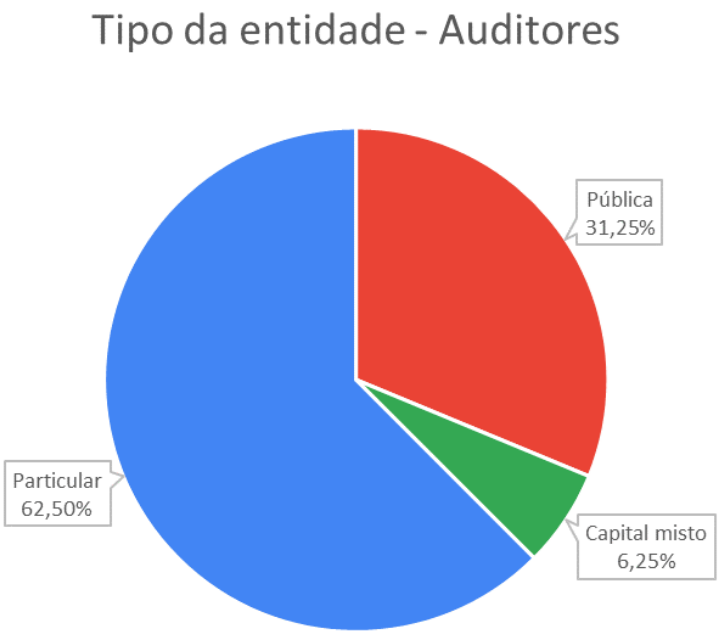


Fonte: Autoria própria

A maioria dos auditores atua em instituições privadas (Figura 30). Nessa categoria, 54,00% atuam como auditor interno, 60,00%, como auditor de segunda parte e 30,00%, como auditor de terceira parte; 82,00% realizam auditorias da norma NBR ISO/IEC 17025 e 74,00%, da ISO 9001. No caso de auditores contratados por instituições públicas, todos atuam como auditores internos e 28,00% realizam auditoria de segunda parte. A mesma porcentagem é observada para aqueles que também ocupam a função de auditor de terceira parte. Novamente, as normas NBR ISO/IEC 17025 e ISO 9001 figuraram como as mais auditadas, com 88,00% e 28,00%, respectivamente.

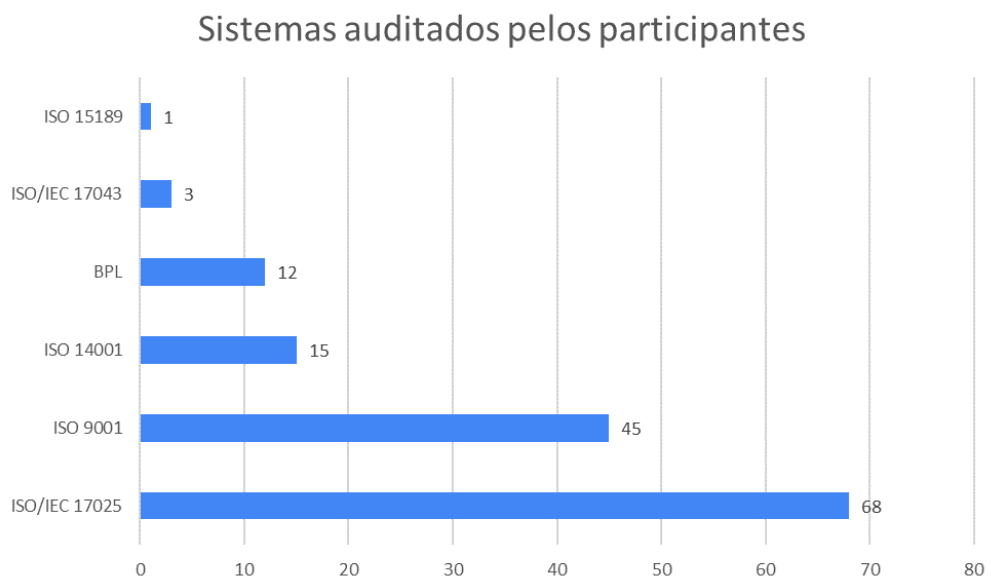
Tais normas foram as mais citadas pelos participantes no geral (Figura 31), sendo que 42,50% trabalham com as duas normas em sua rotina, 22,50% auditam exclusivamente as duas e apenas 1,25% não audita nenhuma delas.

Figura 30 Quantidade de auditores empregados em instituições públicas, particulares ou de capital misto



Fonte: Autoria própria

Figura 31 Sistemas auditados pelos participantes

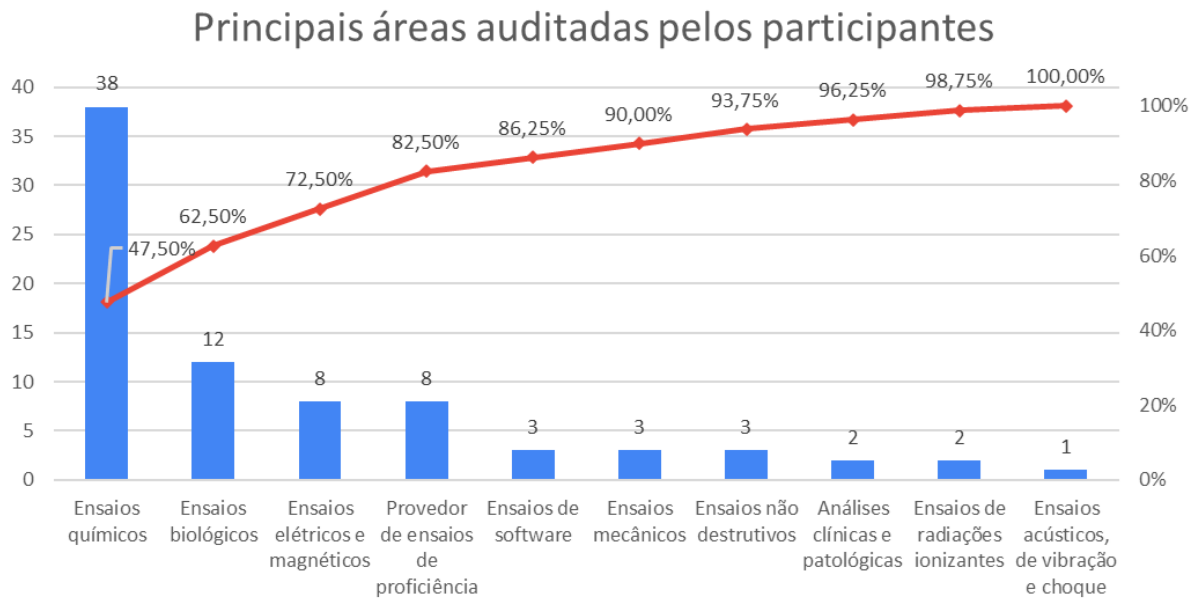


Fonte: Autoria própria

A constatação desses fatos é coerente com as áreas mais comumente auditadas (Figura 32) e também com os dados obtidos em relação às normas mais amplamente adotadas pelos laboratórios – os quais são apresentados na seção 4.1.1, Figura 4.

A certificação na ISO 9001 tem sido buscada por muitas empresas por se tratar de uma norma de nível mundial, aplicável às mais diversas áreas, que proporciona padronização de processos e garante a qualidade dos produtos e serviços oferecidos, facilitando o diálogo e consenso entre prestadores e contratantes. [25, 26] Já a NBR ISO/IEC 17025 pode ser vista como uma norma coincidente com a ISO 9001, porém expandida para abranger requisitos específicos em ensaios de laboratórios de ensaio e calibração,[27] os alvos deste estudo. Ambas discorrem sobre itens como auditorias internas, documentação do sistema de gestão e seu controle, gestão de riscos e oportunidades, ações corretivas e melhorias, todos muito discutidos e necessários para qualquer SGQ. E para garantir a qualidade dos resultados laboratoriais, a NBR ISO/IEC 17025 ainda abrange a rastreabilidade metrológica, análise crítica de contratos, seleção, verificação e validação de métodos, processo de amostragem e elaboração de relatórios.

Figura 32 Principais áreas auditadas pelos participantes



Fonte: Autoria própria

4.2.2 Levantamento sobre os conhecimentos em informática

São apresentadas a seguir as 14 situações expostas aos auditores participantes e as respostas recebidas.

Situação 1

Na primeira situação apresentada, o participante era questionado se computadores utilizando Windows 8 como sistema operacional (SO) estão seguros e dentro das conformidades. Como discutido no item 4.1.2, na época em que a pesquisa foi realizada, tal SO já se encontrava fora da Política de Ciclo de Vida Fixa da Microsoft e não recebia atualizações de qualidade – ou seja, seus problemas de segurança já não eram mais investigados e reparados –, o que compromete a proteção da máquina e dos dados nela armazenados. No entanto, 57,50% dos auditores não julgaram o sistema como vulnerável (Figura 33) e considerou seu uso pertinente. Apesar de não parecer ser uma falha grosseira, a ausência de atualização do SO é uma das brechas mais exploradas por *hackers*. Em um estudo realizado pelo Ponemon Institute com profissionais da área de tecnologia da informação, 48% dos entrevistados disseram que suas empresas passaram por situações de violação de dados nos dois anos anteriores à pesquisa e 60% desses afirmaram que possivelmente a violação havia ocorrido por existir uma atualização disponível para uma vulnerabilidade conhecida,

mas tal atualização não havia sido aplicada. [28] Somado a isso, as falhas de segurança corrigidas pelas atualizações não são abrangidas pela segurança propiciada por programas *antimalware*.

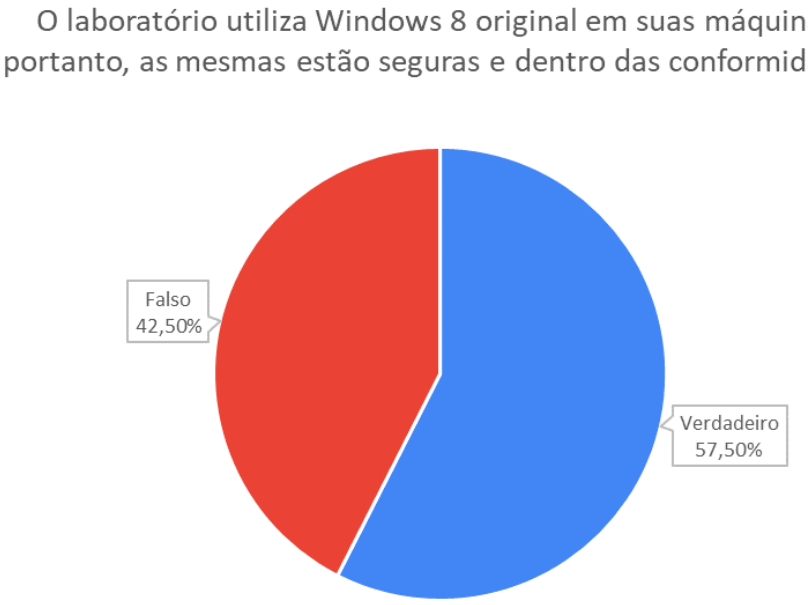
Em diversos casos, alega-se ser necessário manter um SO mais antigo para garantir o funcionamento de alguns *software* legados cuja migração para uma tecnologia mais recente ainda não se faça vantajosa, seja por incompatibilidade com SOs recentes ou por se tratar de programas já profundamente assimilados na rotina do laboratório. Nessas situações, é necessário ponderar sobre alguns aspectos:

- as funcionalidades providas por *software* mais recentes são, de forma geral, mais convenientes e facilmente integráveis a diferentes plataformas e programas;
- é comum que *software* antigos usem linguagens de programação já em desuso, o que torna necessário mão de obra mais especializada nos casos de reparo;
- como já mencionado, programas e SOs antigos têm, de forma geral, nível menor de segurança por não receberem mais atualizações. Somado a isso, seu tempo no mercado torna possível que seus códigos já tenham sido profundamente explorados em busca de brechas para ataques cibernéticos.

Em contraste com tais *software* e SOs desatualizados, o Windows 11, por exemplo, utiliza o TPM 2.0 como uma camada extra de proteção. O TPM (*trusted platform module,* módulo de plataforma confiável, em português) é um componente localizado na placa mãe com a função de criar e armazenar chaves criptográficas no processo de inicialização do sistema, garantindo que o computador não tenha sido adulterado enquanto não estava conectado. [29] Ele foi criado por engenheiros de computação do *Trusted Computing Group* na década de 1990 com o intuito de ser um alicerce sobre o qual sistemas seguros pudessem ser construídos[30] – um pensamento inovador em uma época durante a qual a relação do consumidor doméstico com a tecnologia e internet dava seus primeiros passos rumo à intimidade existente hoje. Cada inicialização gera um novo conjunto de chaves e este conjunto é adicionado aos dados previamente existentes, com uma criptografia que pode ser quebrada apenas

pelo módulo daquele computador e à qual nem mesmo o SO tem acesso, de forma que a segurança da máquina aumenta progressivamente. [30]

Figura 33 "O laboratório utiliza Windows 8 original em suas máquinas, portanto, estas estão seguras e dentro das conformidades."



Fonte: Autoria própria

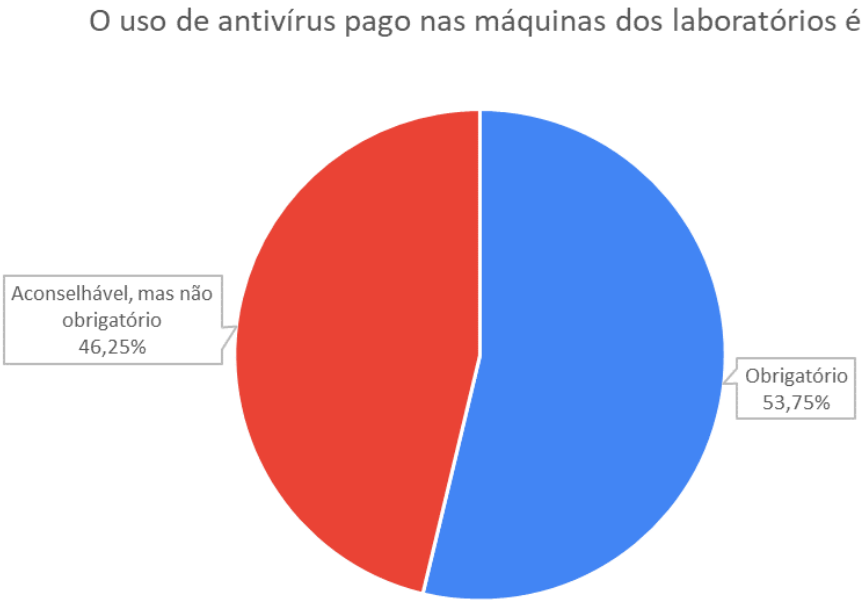
Situação 2

Em seguida, o questionamento colocado era referente ao uso de *antimalware* de licença paga. Eram oferecidas três possibilidades de resposta: “uso obrigatório”, “uso aconselhável, mas não obrigatório” e “uso desnecessário”; a última opção não foi selecionada por nenhum participante (Figura 34). Isso reforça a suposição feita no item 4.1.2, de que itens relativos a “antivírus” eram os menos avaliados por causa de sua indispensabilidade incontestável, o que provavelmente faria os auditores suporem que o recurso estaria sendo usado corretamente e não haveria necessidade de avaliá-lo. Todavia, considerar a licença paga de *antimalware* como “não obrigatória” – o caso de 46,25% dos participantes – é um equívoco.

Uma pesquisa realizada pela Check Point Research concluiu que, comparando os anos de 2020 e 2021, houve um aumento de 50% nos ataques cibernéticos direcionados a organizações de todos os tipos, globalmente, e tendo o setor de educação e pesquisa como o alvo mais comum. No território brasileiro, esse aumento chegou aos 77%, com média de 1046 ataques semanais às organizações. [31]

Além do fato de geralmente as licenças gratuitas fornecidas por empresas de *software* serem liberadas apenas para uso doméstico – o que implica em ato ilegal por parte de instituições que as utilizem em seus computadores[32] – as suítes de segurança corporativa contam com recursos adicionais, como gestão dos sistemas usados, e têm arquitetura pensada para lidar com um grande volume de dados. Ou seja, o uso de licenças gratuitas pode comprometer a segurança do ambiente virtual da empresa.

Figura 34 "O uso de antivírus pago nas máquinas dos laboratórios é:"



Fonte: Autoria própria

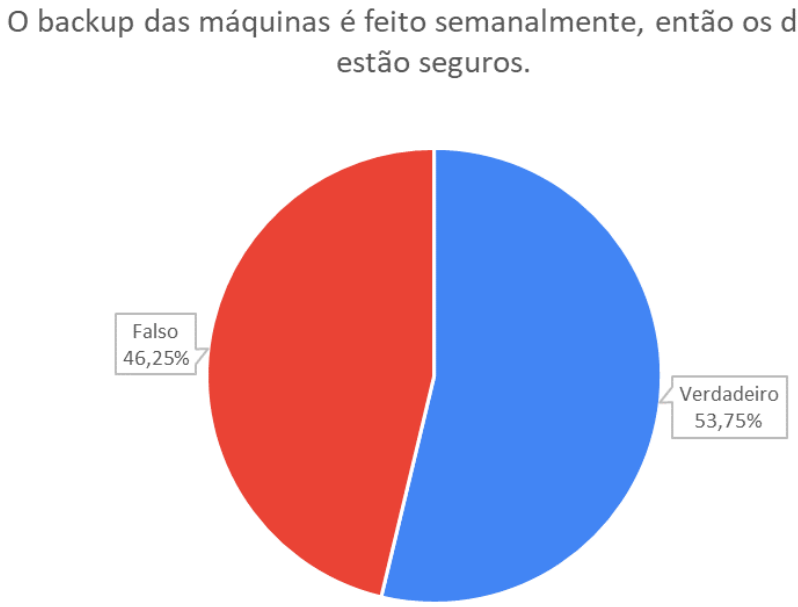
Situação 3

O item subsequente tratou de *backups* e admitia a hipótese de os dados da empresa estarem seguros no caso de a cópia de segurança ser feita semanalmente, cenário com o qual 53,75% dos avaliadores concordou (Figura 35).

É importante ressaltar que não há nas normas uma periodicidade recomendada para essa ação, é apenas requerido que ela seja feita e mantida de forma eficiente. Assim, indica-se o *backup* diferencial, que deve ser realizado diariamente, quando se trata de dados cruciais para a rotina da empresa,[33] como os resultados de análises, verificações diárias de instrumentos, planilhas de cálculos, entre outros arquivos gerados e alimentados com novas informações com uma alta frequência. Portanto,

um *backup* semanal é mais apropriado para documentos que são modificados em intervalos de tempo mais esparsos e que têm menor urgência ou importância [33] e, portanto, demonstrando o desconhecimento da importância dos dados armazenados.

Figura 35 "O *backup* das máquinas é feito semanalmente, então os dados estão seguros."

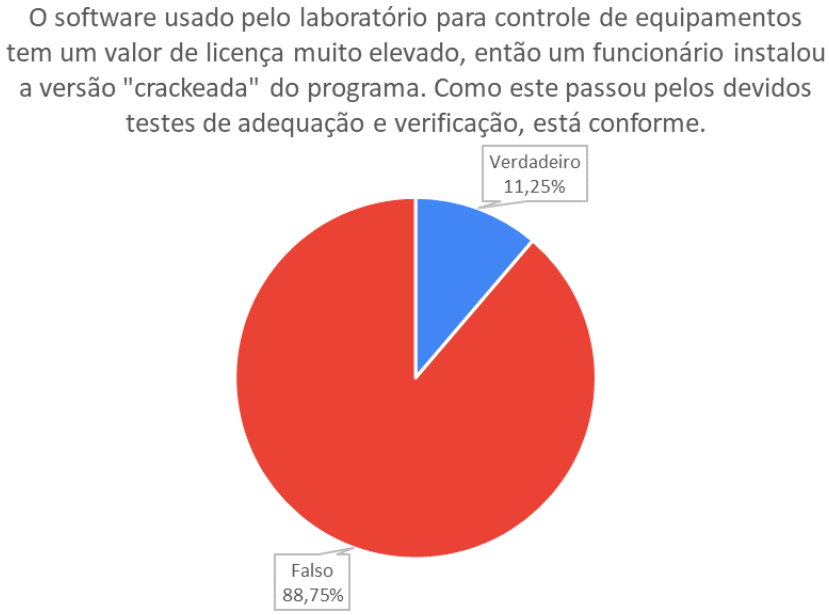


Fonte: Autoria própria

Situação 4

A quarta situação tratava do uso de um *software* "crackeado" que tivesse sido aprovado nos testes de adequação e verificação. Mesmo no caso em que essa aprovação pudesse indicar aptidão do programa para os fins aos quais se destinaria na rotina do laboratório, o processo de *cracking* se baseia em realizar modificações em partes do *software* para que o usuário tenha acesso a recursos pagos – sem efetivamente pagar por eles – ou que exigem uma senha não disponível a ele. Essas modificações automaticamente anulam quaisquer validações pelas quais o *software* tenha passado. Também é comum que, durante o *cracking*, arquivos e programas maliciosos sejam instalados no computador sem o conhecimento do usuário,[34] prejudicando o desempenho da máquina e segurança das informações nela contidas. Além disso, o fato de ser uma versão não original de um programa configura um ato ilegal por violar direitos autorais, tornando-o absolutamente inadequado. Dito isso, é inquietante constatar que 11,25% dos avaliadores julgaram o cenário proposto como uma situação conforme (Figura 36).

Figura 36 "O *software* utilizado pelo laboratório para controle de equipamentos tem um valor de licença muito elevado, então um funcionário instalou a versão "crackeada" do programa. Como este passou pelos devidos testes de adequação e verificação, está conforme."

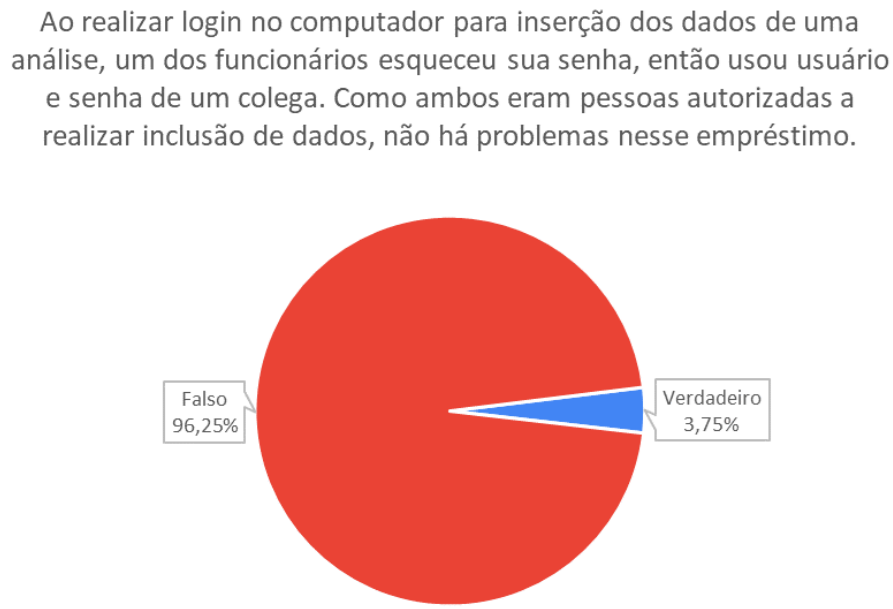


Fonte: Autoria própria

Situação 5

Esta situação abarca o empréstimo de credenciais para acesso a um computador com a finalidade de inserção de dados. Ainda que ambas as pessoas envolvidas nesse cenário tivessem autorização para a atividade, é importante que cada funcionário faça o *login* com seu próprio usuário e senha para garantir a rastreabilidade dos dados. Possivelmente por se tratar de um item explícito nas normas, a maioria dos participantes – 96,25% – reconheceu a não conformidade. Assim, conclui-se que em uma parcela apreciável dos 22,52% dos casos em que não foi verificado o controle de usuário para acesso aos computadores nos laboratórios (Figura 20) os avaliadores tinham conhecimento do requisito, mas este acabou sendo negligenciado.

Figura 37 "Ao realizar *login* no computador para inserção dos dados de uma análise, um dos funcionários esqueceu sua senha, então usou usuário e senha de um colega. Como ambos eram pessoas autorizadas a realizar inclusão de dados, não há problemas nesse empréstimo."



Fonte: Autoria própria

Situação 6

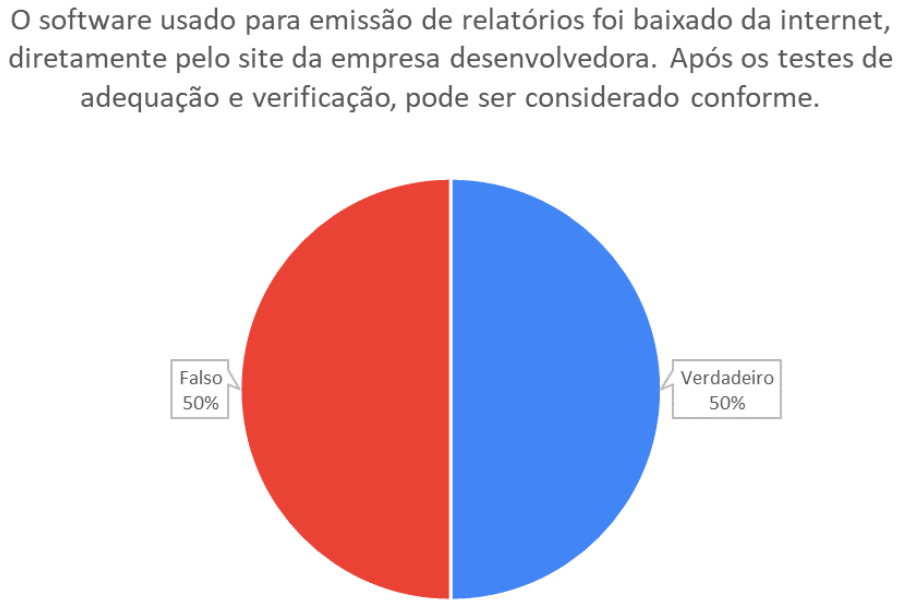
A sexta situação possui similaridade com a quarta: trata de um *software* que já havia passado por testes de adequação e verificação – indicando ser apropriado para o uso pretendido na rotina da empresa –, mas desta vez sua origem era o *site* da própria empresa desenvolvedora.

Não são raros os casos em que empresas desenvolvedoras disponibilizam seus produtos de forma gratuita em seus *sites*, seja como uma assinatura de avaliação ou como um programa "base" para o qual é necessário pagar para acessar mais recursos, por exemplo. [35] E em virtude dos inúmeros alertas que são dados em relação aos riscos envolvendo arquivos e programas obtidos na internet, é legítimo e conveniente o receio demonstrado por metade dos participantes, que entenderam a situação descrita na pesquisa como "falsa" (Figura 38). No entanto, se o *download* for feito a partir de fontes confiáveis, o *software* pode ser considerado seguro[23].

Para garantir que o *site* da empresa desenvolvedora se enquadra nessa condição, indica-se averiguar alguns pontos, tais como a existência de um contrato de licença para uso do programa e se a empresa tem uma boa reputação. [35]

Ainda assim, é possível verificar que a dúvida persiste entre os avaliadores dessa prática.

Figura 38 "O *software* usado para emissão de relatórios foi baixado da internet, diretamente pelo *site* da empresa desenvolvedora. Após os testes de adequação e verificação, pode ser considerado conforme."

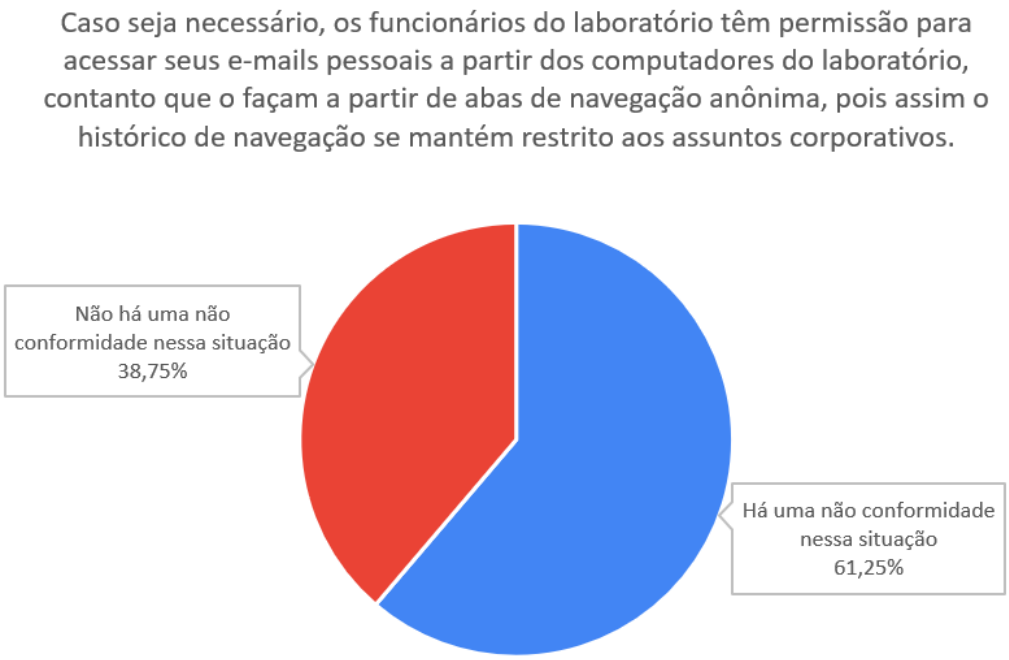


Fonte: Autoria própria

Situação 7

O questionamento levantado na sétima situação era referente ao uso de *e-mail* pessoal nos computadores do laboratório, utilizando abas de navegação anônima (Figura 39). Visto que o computador disponibilizado pela empresa é uma ferramenta de trabalho, seu uso deveria ser restrito a tarefas pertinentes ao ofício do funcionário.[36] Além disso, com a disseminação do uso de *desktops* virtuais, nos quais toda a empresa compartilha os mesmos recursos de rede, utilizar uma máquina para fins pessoais consumiria capacidade de processamento desnecessariamente[23]. Assim, o cenário exposto representa algo desaconselhável – como considerado por 61,25% dos auditores –, mas não se enquadraria como um descumprimento de regras.

Figura 39 “Caso seja necessário, os funcionários do laboratório têm permissão para acessar seus *e-mails* pessoais a partir dos computadores do laboratório, contanto que o façam a partir de abas de navegação anônima, pois assim o histórico de navegação se mantém restrito a assuntos corporativos.”



Fonte: Autoria própria

Situação 8

A oitava situação tratava da localização e acesso ao servidor no qual o *backup* de dados é armazenado. Como mencionado no item 4.1.2 deste texto, a proteção contra acesso não autorizado é um requisito de todas as normas mencionadas neste trabalho. Na NIT-DICLA-038 há ainda recomendações mais detalhadas:

> Métodos de controle adequados para impedir o acesso físico não autorizado ao sistema (por exemplo, hardware, equipamentos de comunicação, componentes periféricos e mídia de armazenamento eletrônico) podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria ou acesso restrito a equipamento informático (por exemplo, áreas de armazenamento de dados, interfaces, computadores, salas de servidores, etc.).[11]

Com relação à segurança e recuperação dos dados, as recomendações das normas da série ISO seguem, em linhas gerais, o texto exposto no item 5.13.1.2 da ISO/IEC 17043:

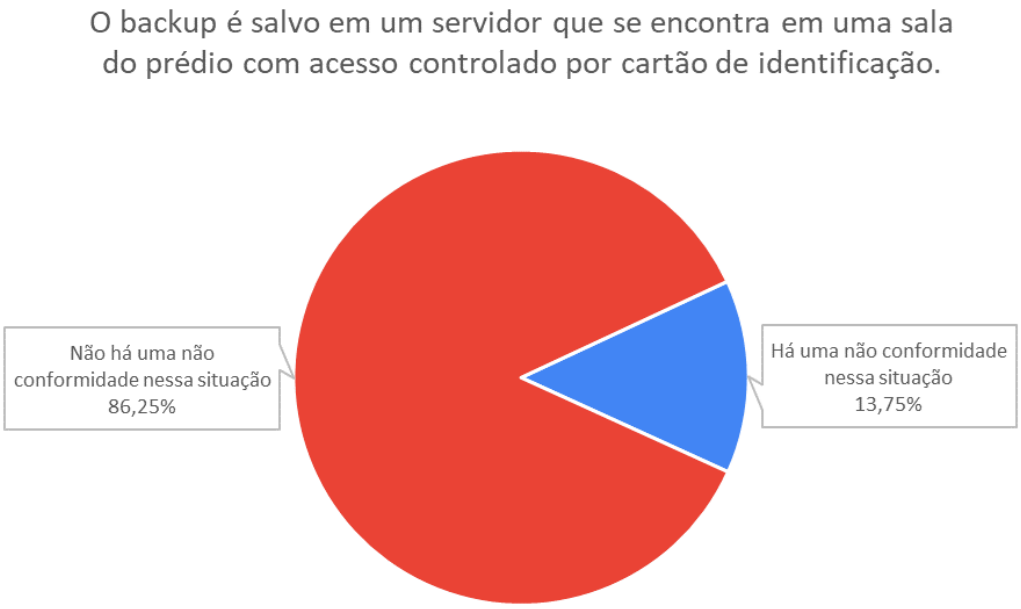
> Todos os registros devem ser legíveis e armazenados e preservados de tal forma que possam ser prontamente recuperados, em instalações que ofereçam ambiente adequado, de forma a prevenir danos, deterioração ou perda. O tempo de retenção dos registros deve ser estabelecido. [10]

Já a BPL tem páginas inteiras em mais de um documento dissertando sobre o assunto, o que impede a transcrição de todas as suas recomendações. Assim, será mencionado apenas um ponto relevante para a discussão neste trabalho: no item 3.2 da NIT-DICLA-038, a norma traz o requisito de que haja descrição de como os registros eletrônicos são armazenados, incluindo “proteção física dos meios de armazenamento contra perda ou destruição (por exemplo, incêndio, umidade, falhas elétricas destrutivas ou anomalias, roubo etc.” [11]

Assim, a situação apresentada para os auditores possui mais de uma camada a ser avaliada. O fato de o acesso à sala do servidor ser controlado por cartão de identificação está dentro da conformidade de todas as normas, como 86,25% dos participantes julgaram. No entanto, a localização do *backup* poderia ser considerada inadequada.

No tocante à Segurança da Informação e Continuidade dos Processos, é importante que as empresas tenham algum tipo de planejamento para impedir que suas atividades sejam prejudicadas ou mesmo interrompidas no caso de ocorrência de situações inesperadas que inviabilizem o acesso às informações armazenadas em meio eletrônico ou comprometam a disponibilidade e capacidade de processamento dos computadores usados na rotina de trabalho. [37,38] Como descrito na NIT-DICLA-038, é necessário proteger fisicamente a mídia em que o *backup* se encontra. Para fins ilustrativos, no caso de o prédio da empresa em questão ser acometido por um incêndio, todos os dados – brutos e de recuperação – seriam perdidos se o servidor mencionado estivesse localizado em uma sala comum dentro do prédio, sem isolamento adequado contra fogo ou umidade. Uma opção para evitar a perda de todos os dados seria manter um local redundante, fora do prédio sede, com uma cópia total do *backup* ou parcial, apenas com os dados críticos. [37]

Figura 40 "O *backup* é salvo em um servidor que se encontra em uma sala do prédio com acesso controlado por cartão de identificação."

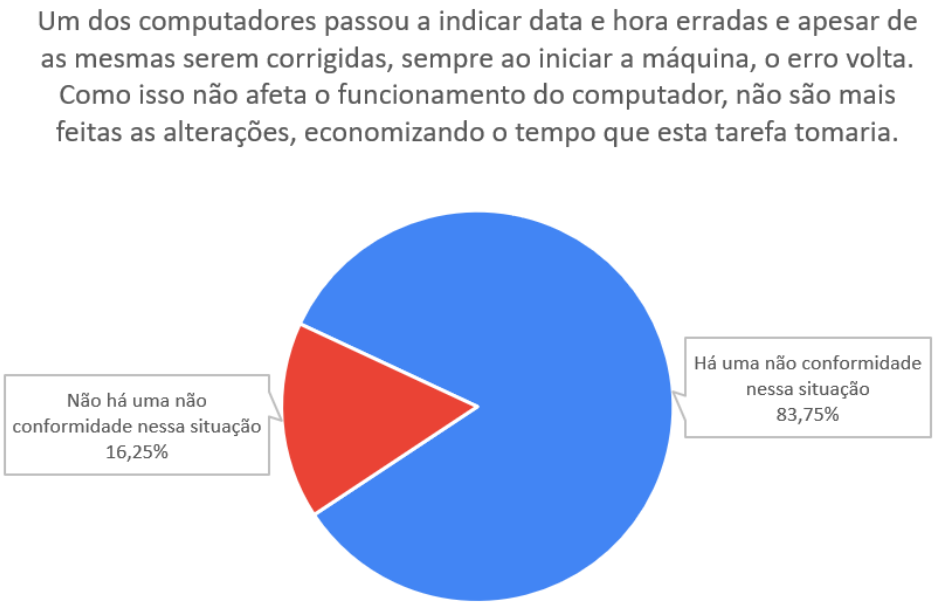


Fonte: Autoria própria

Situação 9

A seguir, foi apresentada uma situação na qual um computador passou a indicar data e hora erradas e a correção parou de ser feita pelos funcionários, visto que o erro aparentemente não afetava o funcionamento da máquina. Esta, assim como a Situação 5, é uma circunstância que envolve a rastreabilidade dos dados. Ao fazer quaisquer alterações em documentos ou acessar programas no computador, são criados arquivos de *log* que registram a ação efetuada, o usuário responsável por ela e o momento em que aconteceu. Todas essas informações podem ser valiosas em auditorias futuras. [37,39] Além disso, alguns programas funcionam com permissões baseadas em data e horário – e assim o acesso a eles seria prejudicado – ou necessitam dessas informações para gerar arquivos, havendo então a possibilidade de um eventual conflito de informações e mal funcionamento do programa. [39] Portanto, o uso do computador que indique data e hora incorretas é desaconselhado – como 83,75% dos participantes apontou (Figura 41). Ainda, a ação mais adequada seria buscar uma correção definitiva, evitando que se faça necessária a retificação sempre que a máquina é reiniciada, visto que isso é uma oportunidade para falha que deve ser minimizada.

Figura 41 "Um dos computadores passou a indicar data e hora erradas e apesar de as mesmas serem corrigidas, sempre ao iniciar a máquina, o erro volta. Como isso não afeta o funcionamento do computador, não são mais feitas as alterações, economizando o tempo que esta tarefa tomaria."

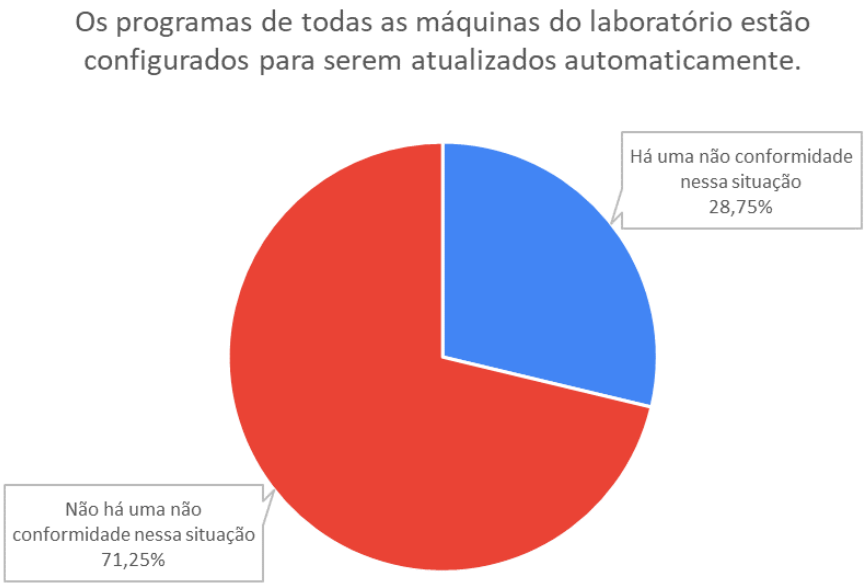


Fonte: Autoria própria

Situação 10

Na décima situação era apresentado aos participantes um cenário em que os *software* de todos os computadores do laboratório eram configurados para serem atualizados automaticamente. Assim como para os SOs, é importante que os programas sejam atualizados sempre que possível, pois *hackers* estão sempre estudando suas arquiteturas em busca de brechas que permitam uma invasão e roubo ou sequestro de dados, por exemplo. [40] Então, quando as empresas desenvolvedoras descobrem tais brechas, lançam atualizações para corrigi-las. Além do reforço na segurança, as atualizações trazem novos recursos e correção de *bugs*, garantindo melhor desempenho do *software*, o que torna a atualização automática altamente indicada[23] e não configura uma não conformidade, como 71,25% dos auditores observou corretamente (Figura 42). É importante ressaltar que, além de configurar os programas para baixar atualizações sempre que estas estiverem disponíveis, aconselha-se verificar com alguma frequência se tal configuração permanece ativa, pois há alguns tipos de *malware* que a desabilitam exatamente para depois explorar a vulnerabilidade gerada. [40] Isto posto, surge a dúvida sobre qual é a interpretação de quase um terço dos auditores que encontraram uma não conformidade nesta situação.

Figura 42 "Os programas de todas as máquinas do laboratório estão configurados para serem atualizados automaticamente."

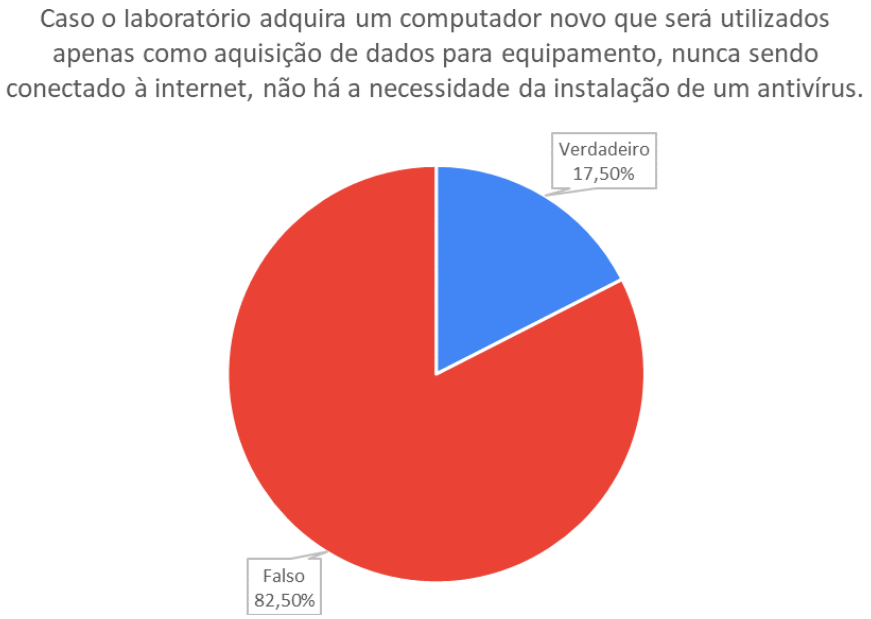


Fonte: Autoria própria

Situação 11

Na sequência, a situação exposta era a de um computador novo, adquirido com a finalidade de ser a interface para aquisição de dados de um equipamento, sem a pretensão de conectá-lo à internet. A hipótese então era de que a instalação de um antivírus seria desnecessária. 82,50% dos auditores discordaram de tal hipótese (Figura 43), evidenciando um bom conhecimento e avaliação do caso, pois ainda que a maior fonte de *malware* seja a internet, não há nenhuma garantia de que eventualmente não será necessário conectar uma mídia externa (*pen drive*, HD externo, celular) ao computador e que está não estará infectada com programas maliciosos que possam comprometer a máquina e os dados nela contidos.

Figura 43 "Caso o laboratório adquira um computador novo que será utilizado apenas como aquisição de dados para equipamento, nunca sendo conectado à internet, não há necessidade da instalação de um antivírus."

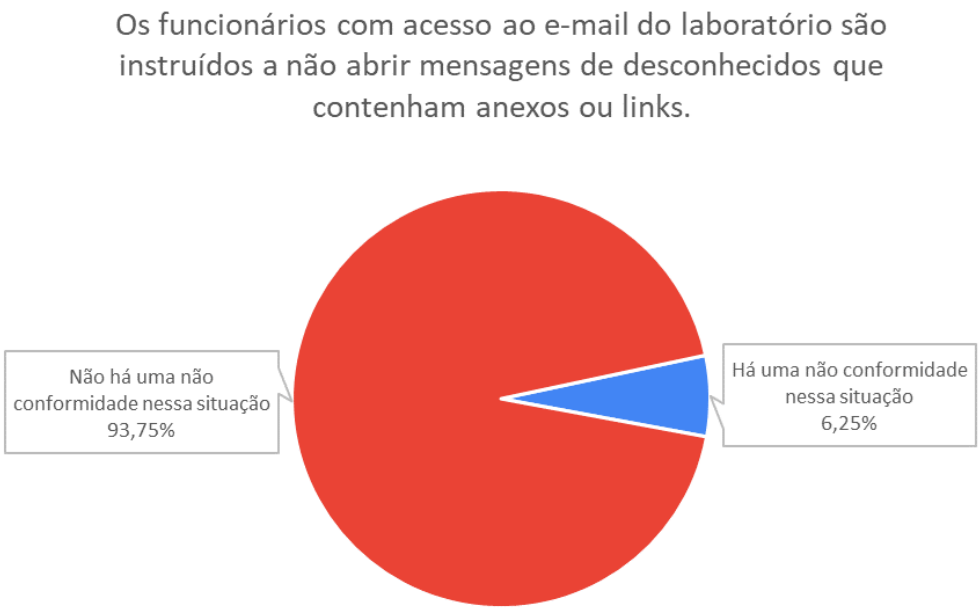


Fonte: Autoria própria

Situação 12

A Situação 12 também abordava o assunto de *antimalware*: era apresentado um cenário no qual funcionários com acesso ao *e-mail* do laboratório eram instruídos a não abrir mensagens de desconhecidos que contivessem anexos ou *links*. Como 93,75% dos participantes foi capaz de identificar (Figura 44), essa é a ação adequada a ser tomada nessas circunstâncias, visto que a situação representa um risco potencial de contaminação da máquina por *malware*. Ademais, é aconselhável que mesmo em casos de remetentes conhecidos não se abra anexos ou *links* sem conhecimento do que se trata e sem um programa *antimalware* ativo, pois eles próprios podem ter sido alvos de programas maliciosos que passaram a se disseminar por suas contas sem seu conhecimento[23].

Figura 44 "Os funcionários com acesso ao *e-mail* do laboratório são instruídos a não abrir mensagens de desconhecidos que contenham anexos ou *links*."



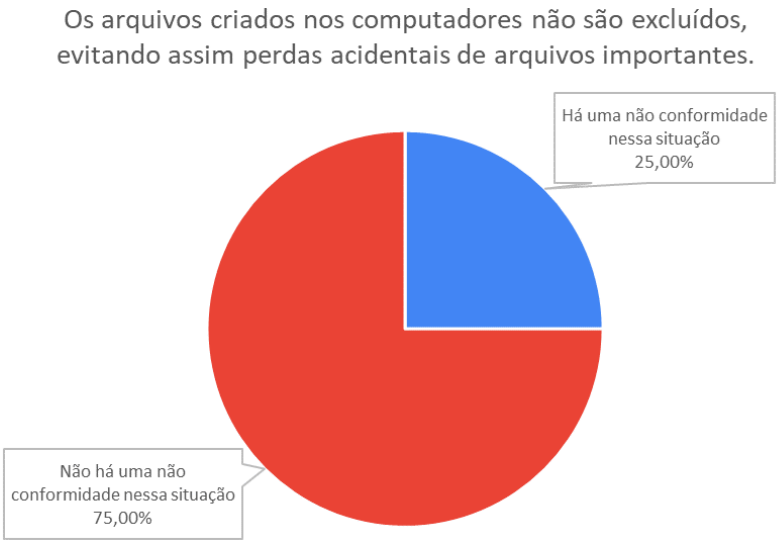
Fonte: Autoria própria

Situação 13

A penúltima situação era referente à exclusão de arquivos, mencionando que aqueles criados nos computadores não eram excluídos a fim de evitar perdas acidentais de documentos importantes.

Nas normas NBR ISO 9001 e 14001, os documentos do sistema de gestão e registros são englobados em uma só categoria, “informação documentada”. Para esta, segundo os requisitos, deve haver procedimentos abordando o armazenamento e preservação adequados, mas também a disposição final, como descrito nos itens 7.5.3.2 da 9001 e 7.5.3 da 14001. Para a NBR ISO 15189, há itens separados tratando de documentos e registros, mas em ambos os casos a disposição também é prevista; para documentos, é definido que sejam mantidos apenas durante um período de tempo específico (item 4.3) e para registros é explícito que é necessário haver procedimentos definidos para seu descarte seguro (item 4.13). Nos casos das NBR ISO/IEC 17025 e 17043, é estabelecido nos itens 8.4.2 e 5.13.2.1, respectivamente, que os registros devem ser mantidos por um período de tempo definido e que devem ser implementados os controles necessários para sua disposição.

Figura 45 "Os arquivos criados nos computadores não são excluídos, evitando assim perdas acidentais de arquivos importantes."



Fonte: Autoria própria

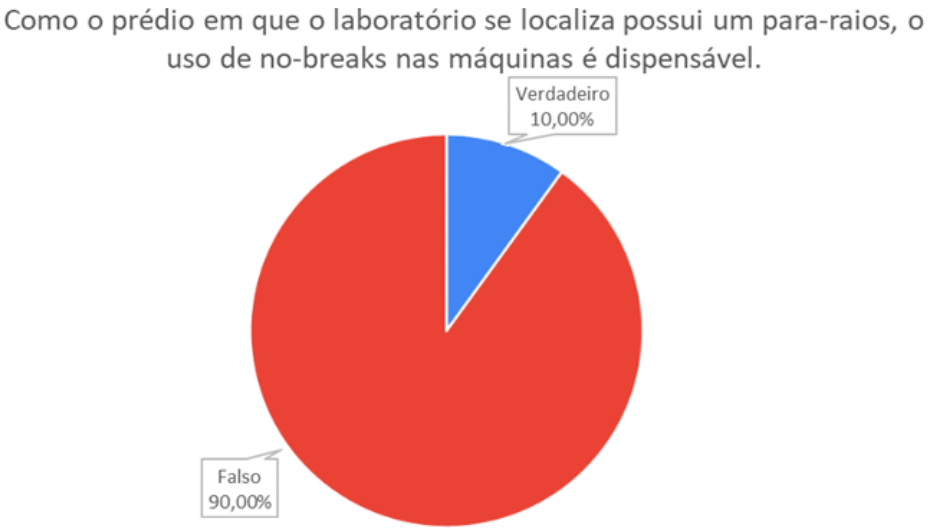
Isto significa que, contanto que estejam bem definidos os mecanismos para proteção de arquivos que não devem ser excluídos, não há por que manter todos os arquivos já criados. Eliminar aqueles que não são mais necessários é importante para cortar gastos e capacidade de armazenamento e processamento. [41] Porém, tendo em vista o destaque que é dado à preservação de documentos e informações nos sistemas de gestão, é compreensível que 75,00% dos participantes tenham considerado esta situação como adequada (Figura 45)

Situação 14

Por fim, apresentou-se a hipótese de o uso de *no-breaks* nas máquinas ser dispensável, já que o prédio em que o laboratório se localiza conta com um para-raios. De acordo com todas as normas, é necessário que os equipamentos sejam alocados e armazenados de forma a garantir seu funcionamento correto (item 6.4.3 da NBR ISO/IEC 17025, item 4.1 da NIT-Dicla-035, item 4.3.6 da NBR ISO/IEC 17043, item 5.3.1.5 da NBR ISO 15189 e item 7.1.3 da NBR ISO 9001).

O funcionamento do para-raios baseia-se em desviar de um possível alvo a descarga elétrica que poderia causar danos, mas ele não garante uma proteção total.[42] Além disso, para o bom funcionamento e preservação de computadores, é indicado que estes sejam alimentados com energia “limpa”, ou seja, sem picos e sem quedas. Portanto, o uso de *no-breaks* é altamente recomendado, para filtrarem a corrente de alimentação e fornecer energia em casos de interrupção em seu fornecimento. [41]

Figura 46 Como o prédio em que o laboratório se localiza possui um para-raios, o uso de *no-breaks* nas máquinas é dispensável."



Fonte: Autoria própria

4.2.3 Percepção sobre a implantação dos itens mencionados

Na última seção do formulário, foi solicitado aos participantes que indicassem qual era sua percepção sobre o nível de implantação de diversos itens nos laboratórios em que tivessem executado auditorias. Tais itens eram essencialmente os mesmos que foram avaliados pelos laboratórios em termos da dificuldade encontrada para implantá-los.

Como discutido no item 4.1.3, a validação de software e seus relatórios e testes formais de adequação e seus relatórios foram tópicos em que os laboratórios alegaram ter maiores dificuldades. Ainda assim, como visto na Figura 47, os auditores dizem tê-los encontrado na maioria de suas avaliações – principalmente os *softwares* validados. Isso provavelmente se deve ao fato de os laboratórios compreenderem a importância dessa atividade[13]; sendo assim, a colocam em prática apesar de sua complexidade. No entanto, é importante ressaltar que, assim como discutido no item 4.1.2, há dúvidas quanto ao critério aplicado pelos avaliadores ao auditar a validação de *software*. Nos casos em que o relatório de validação não foi solicitado, por exemplo, a auditoria se baseia unicamente na percepção do avaliador, tornando necessária a apreciação de seus conhecimentos sobre o tema e a profundidade da validação.

O nível de dificuldade declarado pelos laboratórios em manter os SOs atualizados é compatível com a percepção dos auditores, posto que 6,31% dos

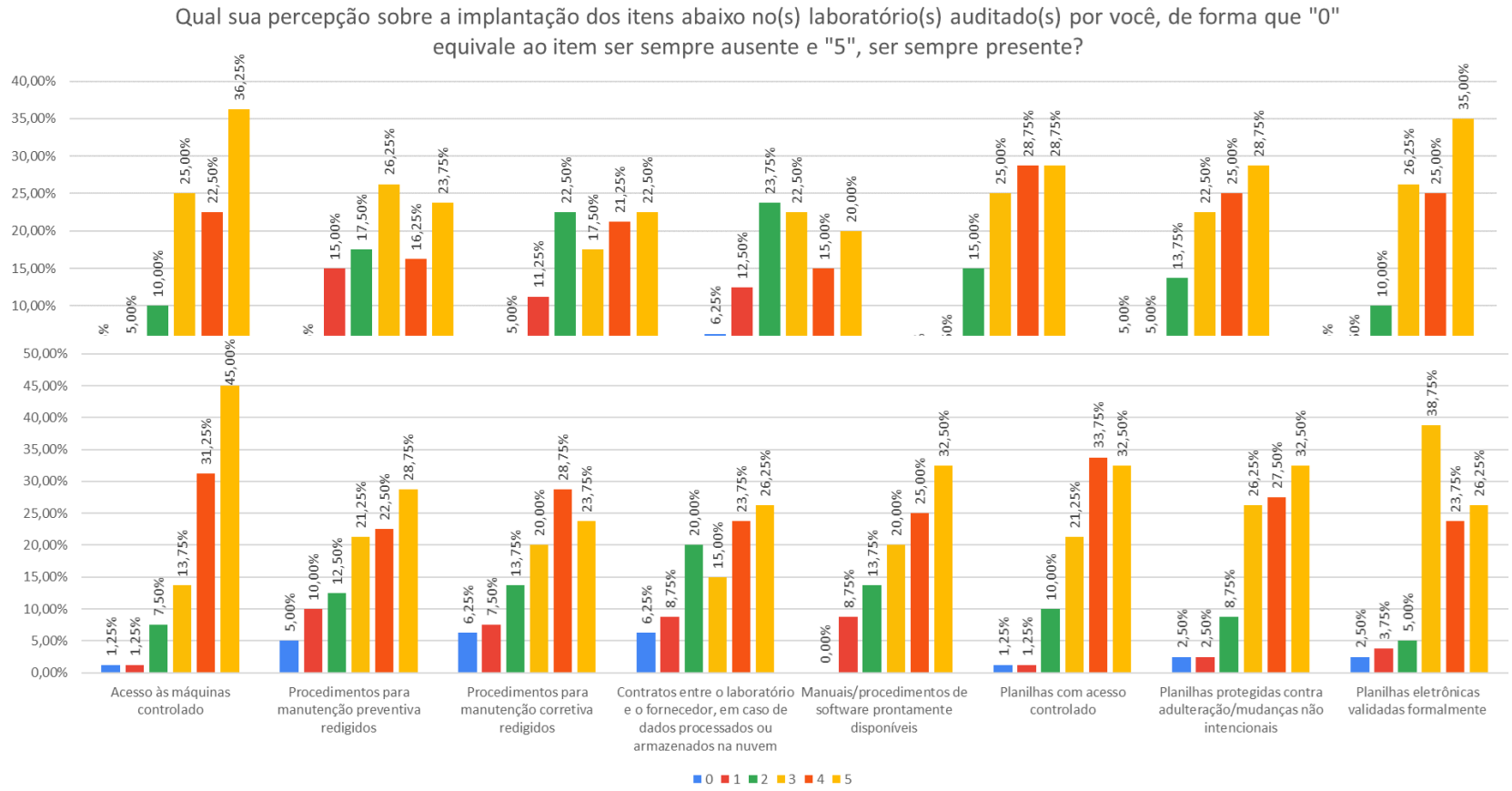
laboratórios a julgou como uma tarefa muito difícil (Figura 27) e apenas 2,50% dos auditores disse ser raro encontrar sistemas operacionais atualizados em suas auditorias (Figura 47). Todavia, como apresentado na Situação 1, mais de 40% dos auditores não conseguiram reconhecer um SO cujo uso é desaconselhado, então existe a possibilidade de sua percepção não condizer com a realidade. Ressalte-se aqui que, em pesquisa anterior, foi detectado que cerca de 53% dos laboratórios utilizavam em suas máquinas sistemas operacionais que já não recebiam atualizações de recursos e de qualidade. [13]

Para a aquisição e manutenção de programas *antimalware* apropriados, a maioria dos laboratórios manifestou ter pouca ou nenhuma dificuldade e 76,25% dos auditores constatou a presença de tais programas em todas ou quase todas as auditorias que realizou. É importante salientar que neste item foi antevisto o desconhecimento de muitos sobre a obrigatoriedade da aquisição de uma licença paga, então o seguinte esclarecimento foi adicionado à questão no formulário: “versões disponíveis gratuitamente são voltadas para o uso doméstico. Para fins corporativos, é indicado a compra de uma licença de antivírus”. É interessante notar que 23,75% dos auditores declararam ser raro encontrar *antimalware* apropriados nos laboratórios e, na mesma pesquisa mencionada no parágrafo anterior, cerca de 30% dos laboratórios informou utilizar *antimalware* inadequados. [13]

A instauração e manutenção de *backup* também foi um item considerado de pouca ou nenhuma dificuldade pelos laboratórios, assim como controle de acesso às máquinas e planilhas e proteção de planilhas contra adulteração/mudanças não intencionais. Todos estes itens estavam sempre ou quase sempre presentes nas auditorias, segundo os avaliadores. É provável que essa facilidade se deva ao fato de, em todas as normas abrangidas por este trabalho, o *backup* ser um item explícito, fato que também ocorre com o acesso controlado na BPL, ISO/IEC 17025 e ISO 15189.

No tocante à elaboração de procedimentos para manutenção preventiva e corretiva e formulação de contratos em caso de dados mantidos por terceiros, os laboratórios não declararam ter grandes dificuldades. Porém, foram os itens com os maiores índices de percepção “0 – sempre ausente” por parte dos auditores (ainda que fossem porcentagens baixas se comparadas com os casos em que os itens estavam presentes em todos os laboratórios, como mostrado na Figura 47).

Figura 47 “Qual sua percepção sobre a implantação dos itens abaixo no(s) laboratório(s) auditado(s) por você, de forma que “0” equivale ao item ser sempre ausente e “5”, ser sempre presente?”



Fonte: Autoria própria

5 CONCLUSÃO

Percebe-se que um elevado número de auditores deixa de avaliar diversos itens relacionados a sistemas computadorizados, mesmo quando há a possibilidade de a segurança dos dados ser afetada. Como mostrado na Figura 48, os quatro itens mais negligenciados foram a periodicidade de atualização de *antimalware*, a manutenção corretiva dos computadores e softwares, a existência de *antimalware* e a manutenção preventiva dos computadores e softwares. Em um caso hipotético no qual houvesse não conformidades em tais itens, não seria difícil que um *software* malicioso se infiltrasse nos computadores e gerasse danos que forçariam a pausa nas atividades laboratoriais, por exemplo.

Com exceção dos itens relacionados a *backups*, mesmo aqueles com valores mais elevados de verificação realizada apresentaram respostas correspondentes a “o avaliador não verificou este item” na faixa de 20 a 25%. Isso abre brechas para falhas que podem provocar desde a perda de documentos com pouca ou nenhuma importância (os quais podem ser refeitos, como modelos de formulários) até a geração de resultados errôneos para os ensaios ou perda de documentos de observações únicas que não podem ser refeitos por falta de amostra, ou por outro motivo impeditivo. Ao considerar que 54,95% dos laboratórios participantes efetuam ensaios químicos, biológicos e análises clínicas, o impacto dessas consequências torna-se mais claro.

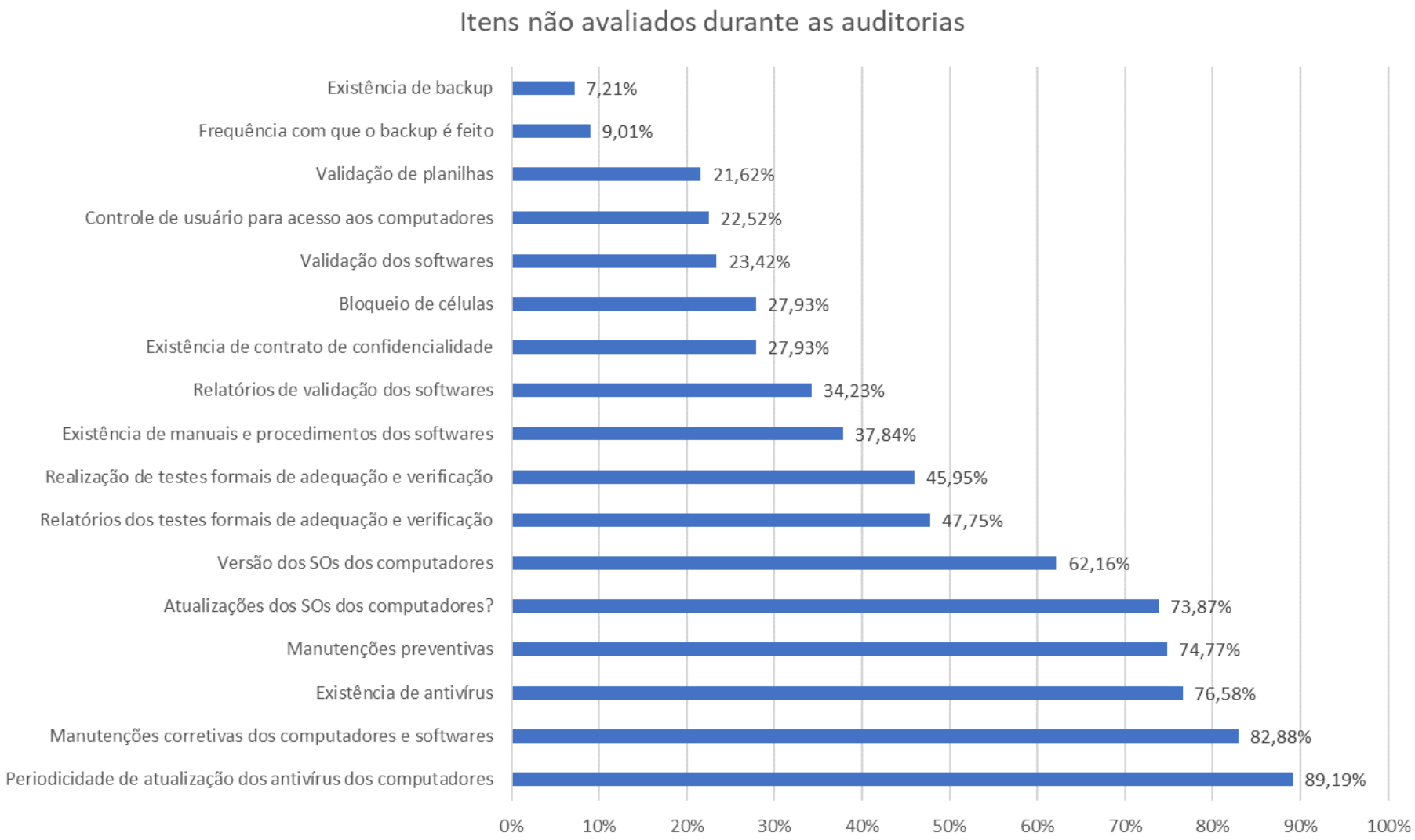
A Figura 49 mostra que a porcentagem de não-conformidades detectadas é baixa - sendo que a maior de todas foi o bloqueio de células, com 8,11% - e os cinco itens com mais NCs são simples de serem corrigidos pelos laboratórios, pois consistem em bloqueio de células das planilhas utilizadas, contrato de confidencialidade quando dados são mantidos por terceiros, validação das planilhas utilizadas, redação de relatórios de validação dos softwares e frequência de realização de backups.

É interessante se atentar ao fato de que os itens com menos não-conformidades detectadas são também os menos avaliados durante auditorias (Figuras 48 e 49), o que levanta a dúvida: há realmente menos não conformidades nesses itens ou elas apenas não foram identificadas pelos auditores? Além disso, a existência de procedimentos documentados para manutenções preventivas e corretivas figuram entre os itens com nenhuma ou pouquíssima detecção de não

conformidades, mas também estão entre os itens que mais frequentemente estão ausentes nos laboratórios, segundo os auditores. Neste caso, o questionamento é sobre o motivo de não serem aplicadas não conformidades ainda que os auditores as tenham identificado.

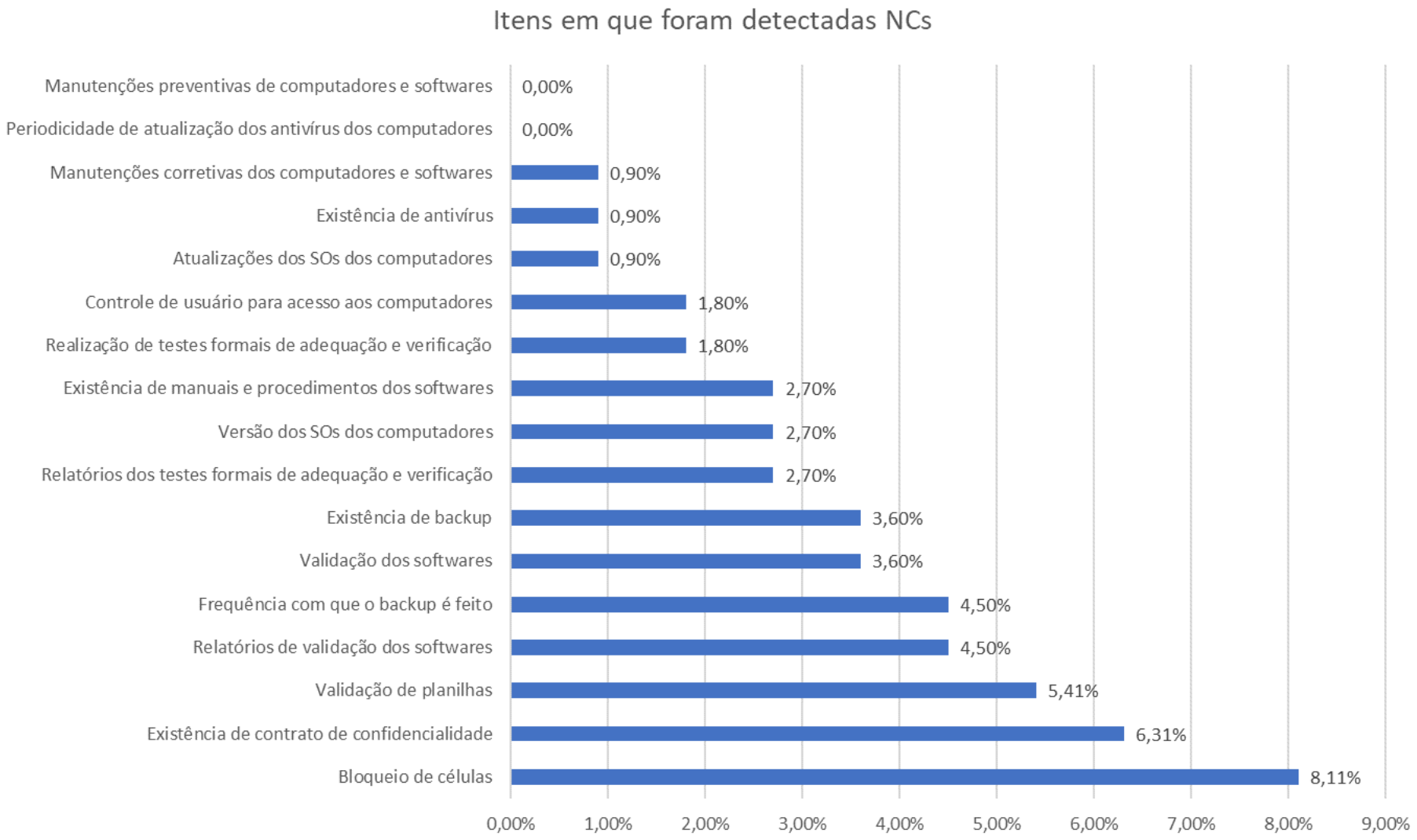
Com relação à aquilatação dos conhecimentos dos auditores, os temas que geraram mais respostas equivocadas por parte dos auditores foram a segurança de um software baixado do site de sua desenvolvedora (50%), adequabilidade de programas *antimalware* (46,25%) e de sistemas operacionais (42,50%) e frequência aconselhada de realização de *backup* (46,25%). Isto posto, fica claro que os auditores têm boa fundamentação nas normas, mas nos casos em que lhes é exigido um conhecimento mais aprofundado sobre sistemas informatizados para identificar uma não conformidade, é possível que esta não seja devidamente avaliada. Considerando que na atualidade já é virtualmente impossível que algum laboratório não utilize computadores em sua rotina, principalmente no tratamento de dados, o descuido com não conformidades nesse âmbito se torna bastante perturbador. Para que as auditorias em sistemas computadorizados fossem mais efetivas, o ideal seria que pessoal com maior experiência e conhecimento nesta área a avaliasse em conjunto com os auditores principais. Ou, como outra solução, poderiam ser disponibilizados guias aos auditores para que conduzissem as avaliações desse setor com maior eficiência e resultados mais fundamentados.

Figura 48 - Itens não avaliados durante as auditorias



Fonte: Autoria própria

Figura 49 - Itens em que foram detectadas não-conformidades



Fonte: Autoria própria

REFERÊNCIAS

[1] CARPINETTI, L. C. R. A evolução do conceito e da prática da gestão de qualidade. *In*: CARPINETTI, L. C. R. **Gestão de qualidade:** conceitos e técnicas. 3. ed. São Paulo: Atlas, 2017. 248 p.

[2] LEITE, D. M.; GASPAR, A.; CHAGAS, V. R. S.; COSTA, S. R. R. Avaliação da aplicação de sistema de gestão da qualidade em laboratório de pesquisa e análise de alimentos. **Sistemas & Gestão**, Niterói, v. 4, n. 3, p. 205-220. 2010.

[3] NETTO, D. A. M. **A busca pela excelência laboratorial:** acreditação de ensaios do laboratório de análise de sementes da Embrapa Milho e Sorgo pela ISO/IEC 17025:2005. 2008. 26 f. Especialização (Monografia apresentada ao curso de Pós-graduação Lato sensu em produção e tecnologia de sementes) - Departamento de Agricultura, Universidade Federal de Lavras, Lavras. 2008.

[4] GALACHO, C. **Boas práticas de laboratório:** Como sugiram? O que são? A que se aplicam? Évora: Universidade de Évora: 2013. 16p. Disponível em: https://dspace.uevora.pt/rdpc/ bitstream/10174/9866/1/CGalacho-BPL_SPQ_nv_final.pdf. Acesso em: 05 out. 2018.

[5] RODRIGUES, N. R.; SOUZA, A. P. F.; WATANABE, M. Implantação e implementação das normas das Boas Práticas Laboratoriais (BPL) no laboratório de análises de resíduos da Universidade Estadual de Campinas. **Química Nova**, São Paulo, v. 35, n. 6, p. 1276-1280. 2012.

[6] WOLFF, S. **Informatização do trabalho e reificação:** uma análise à luz dos Programas de Qualidade Total. 1998. 211 f. Dissertação (Mestrado) – Departamento de Sociologia, Instituto de Filosofia e Ciências Humanas, Universidade Estadual de Campinas, Campinas. 1998.

[7] BRESSER-PEREIRA, L. C. **A crise financeira global e depois:** um novo capitalismo? **Novos estudos-CEBRAP**, São Paulo, n. 86, p. 51-72. 2010.

[8] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17025:2017**: requisitos gerais para a competência de laboratórios de ensaio e calibração. 3. ed. Rio de Janeiro: ABNT, 2017.

[9] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 15189:2015**: laboratórios clínicos – requisitos de qualidade e competência. Rio de Janeiro: ABNT, 2015.

[10] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17043:2011**: avaliação da conformidade – requisitos gerais para ensaios de proficiência. Rio de Janeiro: ABNT, 2017.

[11]INMETRO. **NIT-DICLA-038, Revisão 02**: a aplicação dos princípios BPL aos sistemas informatizados. Aprovada em setembro de 2008. Brasília: INMETRO, [2008?].

[12]LIRA, L .S. **Validação de software para laboratórios:** o atendimento aos requisitos da qualidade do software (ISO/IEC 25010:2011) não acolhe a completeza dos requisitos dos sistemas de gestão da qualidade com relação ao uso de programas em laboratórios. 2016. 44 f. Monografia (Bacharelado em Química) – Instituto de Química de São Carlos, Universidade de São Paulo, São Carlos, 2016.

[13]KOCK, C. W. **Investigação sobre o uso de softwares em entidades certificadas, reconhecidas ou acreditadas pela ISO/IEC 17025, BPL ou ISO 15189**. 2018. 55 f. Monografia (Bacharelado em Química) – Instituto de Química de São Carlos, Universidade de São Paulo, São Carlos, 2018.

[14]STALLINGS, W.; BROWN, L. Segurança de software. *In*: STALLINGS, W.; BROWN, L. **Segurança de computadores**. 2. ed. Rio de Janeiro: Elsevier, 2014. 726 p.

[15]NET MARKETSHARE. **Operating system market share**. Aliso Viejo, 2020. Disponível em: https://netmarketshare.com/operating-system-market-share.aspx?options=%7B%22filter%22%3A%7B%22%24and%22%3A%5B%7B%22deviceType%22%3A%7B%22%24in%22%3A%5B%22Desktop%2Flaptop%22%5D%7D%7D%5D%7D%2C%22dateLabel%22%3A%22Custom%22%2C%22attributes%22%3A%22share%22%2C%22group%22%3A%22platform%22%2C%22sort%22%3A%7B%22share%22%3A-1%7D%2C%22id%22%3A%22platforms Desktop%22%2C%22dateInterval%22%3A%22Monthly%22%2C%22dateStart%22%3A%222019-10%22%2C%22dateEnd%22%3A%222020-10%22%2C%22segments%22%3A%22-1000%22%2C%22plotKeys%22%3A%5B%7B%22platform%22%3A%22Windows%22%7D%5D%7D. Acesso em: 10 nov. 2020.

[16]STATCOUNTER. **Desktop Windows version market share worldwide**. Dublin, 2020. Disponível em: https://gs. statcounter.com/windows-version-market-share/desktop/worldwide#monthly-201910-202010. Acesso em:10 nov. 2020.

[17]STATCOUNTER. **Desktop Windows version market share in Brazil**. Dublin: 2020. Disponível em: https://gs.statcounter. com/windows-version-market-share/desktop/brazil/#monthly-201910-202010. Acesso em: 10 nov. 2020.

[18]MICROSOFT. **Windows XP**. Albuquerque, 2020. Disponível em: https://docs.microsoft.com/pt-br/lifecycle/products/windows-xp. Acesso em: 10 nov. 2020.

[19]MICROSOFT. **Windows 7**. Albuquerque, 2020. Disponível em: https://docs.microsoft.com/pt-br/lifecycle/products/windows-7. Acesso em: 10 nov. 2020.

[20]MICROSOFT. **Windows 8**. Albuquerque, 2020. Disponível em: https://docs.microsoft.com/pt-br/lifecycle/products/windows-8. Acesso em: 10 nov. 2020.

[21]MICROSOFT. **Perguntas frequentes sobre ciclo de vida - geral**. Albuquerque, 2020. Disponível em: https://docs.microsoft.com/pt-br/lifecycle/faq/general-lifecycle. Acesso em: 10 nov. 2020.

[22]MICROSOFT. **Windows 8**.**1**. Albuquerque, 2020. Disponível em: https://docs.microsoft.com/pt-br/lifecycle/products/windows-81. Acesso em: 10 nov. 2020.

[23]CENTRO DE TECNOLOGIA DA INFORMAÇÃO DE RIBEIRÃO PRETO. **Boas práticas de segurança para usuários de informática**. Ribeirão Preto, 2017. *E-book*. Disponível em: https://cetirp.sti.usp.br/wp-content/uploads/sites/47/2019/10/Cartilha-Seguranca-2019.pdf. Acesso em: 06 ago. 2019.

[24]CONSULTORIAISO. **Conheça os tipos de auditorias de sistema de gestão e para que servem**. Belo Horizonte: Ambipar, 2021. Disponível em: https://www.consultoriaiso.org/tipos-de-auditorias-sistema-de-gestao. Acesso em: 26 jul. 2021.

[25]CONSULTORIAISO. **O que é o selo ISO 9001 e para que serve**. Belo Horizonte: Ambipar, 2021. Disponível em: https://www.consultoriaiso.org/o-que-e-o-selo-iso-9001-e-para-que-serve/. Acesso em: 27 ago. 2021.

[26]LOPES, J.C.C. **Gestão da qualidade:** decisão ou constrangimento estratégico. 2014. 76 f. Dissertação (Mestrado em Estratégia Empresarial) - Universidade Europeia, Lisboa, 2014.

[27]AFINKO SOLUÇÕES EM POLÍMEROS. **ISO 17025**: a importância dessa norma para um laboratório. São Carlos, 2021. Disponível em: https://afinkopolimeros.com.br/iso-17025/. Acesso em: 28 ago. 2021.

[28]PONEMON INSTITUTE. **Costs and consequences of gaps in vulnerability response**. Traverse City, 2019. 46p.

[29]AARAJ, N.; RAGHUNATHAN, A.; JHA, N. K. Analysis and design of a hardware/software trusted platform module for embedded systems. **ACM Transactions on Embedded Computing Systems**, New York, v. 8, n. 1, p. 1-31, dez. 2008.

[30]ARTHUR, W.; CHALLENER, D.; GOLDMAN, K. **A practical guide to TPM 2.0:** using the new trusted platform module in the new age of security. Berkeley: Apress, 2015.

[31]CISO ADVISOR. **Brasil tem 77% mais ataques em 2021 do que em 2020.** [S. l.: s.n], [200-]. Disponível em: /www.cisoadvisor.com.br/brasil-tem-77-mais-ataques-em-2021-do-que-em-2020/>. Acesso em: 08 nov. 2023.

[32]DATAUNIQUE. **Por que utilizar um antivírus corporativo?** Goiânia: Data Unique Tecnologia, 2021. Disponível em https://dataunique.com.br/blog/por-que-utilizar-um-antivirus-corporativo/. Acesso em: 28 ago. 2021.

[33]MICROSERVICEIT. **Gestão de backup**: como fazer e garantir a eficácia do processo? Blumenau: Microservice 2021. Disponível em https://www.microserviceit.com.br/gestao-de-backup/. Acesso em: 28 ago. 2021.

[34]WELIVESECURITY. **Casos recentes mostram como um crack pode propagar ameaças.** Bratislava, 2021. Disponível em https://www.welivesecurity.com/br/2021/09/01/casos-recentes-mostra m-como-um-crack-pode-propagar-ameacas/. Acesso em: 03 set. 2021.

[35]IDEAGRI. P**or que nem sempre é seguro fazer o download de um software gratuito?** Belo Horizonte: Ideagri, 2021. Disponível em: https://ideagri. com.br/posts/por-que-nem-sempre-e-seguro-fazer-o-download-de-um-software-gratuito. Acesso em: 03 set. 2021.

[36]PERITUM CONSULTORIA E TREINAMENTO**. A empresa pode monitorar os e-mails dos seus colaboradores?** Harmonia, 2021. Disponível em: https://periciacomputacional.com/a-empresa-pode-monitorar-os-e-mails-dos-seus-colaboradores/. Acesso em: 03 set. 2021.

[37]BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. Brasília: TCU, 2012. *E-book*. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDow nload.jsp?fileId=8A8182A24F0A728E014F0B226095120B. Acesso em: 18 out. 2021.

[38]HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. **Fundamentos de segurança da informação com base na ISO 27001 e na ISO 27002**. 3. ed. Rio de Janeiro: BRASPORT Livros e Multimídia Ltda, 2018.

[39]CHRON. **Importance of correct computer date & time**. São Francisco: Hearst Communications, 2021. Disponível em: https://smallbusiness.chron.com/importance-correct-computer-date-time-67593.html. Acesso em: 18 out. 2021.

[40]INFONET. **Entenda a importância de atualizar sistemas operacionais e apps.** Aracaju: Infonet 2021. Disponível em: https://info net.com.br/noticias/cidade/entenda-a-importancia-de-atualizar-sistemas-operacionais -e-apps/. Acesso em: 03 set. 2021.

[41]UNIVERSIDADE DE BRASÍLIA. **Manual de gestão de documentos**. Brasília: UNB, 2015. *E-book.* Disponível em: https://www.arquivocentral.unb.br/images/documentos/Manual_ de_Gesto_de_Documentos_da_UnB.pdf. Acesso em: 18 out. 2021.

[42]UNIVERSIDADE FEDERAL DO RECÔNCAVO BAIANO. Centro de Formação de Professores. **O funcionamento do pára-raios**. Amargosa: UFRB, 2021. Disponível em: https://www.ufrb.edu.br/bibliotecacfp/noticias/316-o-funcionam ento-do-para-raios. Acesso em: 18 out. 2021.

APÊNDICES

Apêndice 1 – Questionário enviado aos avaliadores

Pesquisa Acadêmica da Universidade de São Paulo (USP) sobre Sistemas Computadorizados em laboratórios

O presente questionário foi elaborado para que você possa contribuir com uma pesquisa de mestrado da Universidade de São Paulo - IQSC/USP.

Em pesquisa anterior, realizada no segundo semestre de 2018, percebeu-se que laboratórios acreditados, reconhecidos e/ou certificados em diversas normas concordam que os conceitos dos Sistemas de Gestão da Qualidade referentes a Sistemas Computadorizados são de grande importância para seu bom funcionamento. Porém, as medidas nem sempre são aplicadas corretamente e, em alguns casos, nem mesmo cobradas. A fim de obter um conhecimento mais profundo sobre o atual cenário do uso de Sistemas Computadorizados em Laboratórios, a aluna Cássia Watanabe Kock, sob orientação do Prof. Dr. Vitor Hugo Polisél Pacces, está realizando esta pesquisa.

Informações:
- Os dados coletados nesta pesquisa são sigilosos e restritos aos organizadores. Não serão divulgados nomes de empresas ou participantes;
- O participante pode se recusar a continuar com o questionário a qualquer momento, sem penalização alguma e sem prejuízo ao seu cuidado;
- Caso seja do interesse do participante, será enviado o trabalho final para seu e-mail.

Pesquisador responsável: Cássia Watanabe Kock – IQSC/USP
Contato: cassia.kock@usp.br
Instituto de Química de São Carlos da Universidade de São Paulo - IQSC/USP. Avenida Trabalhador São-carlense, 400
CEP 13566-590 - São Carlos - SP - Brasil

*Obrigatório

Li e entendi as informações acima e concordo em participar da pesquisa *

Sim

Não

Próxima

Nunca envie senhas pelo Formulários Google.

Este conteúdo não foi criado nem aprovado pelo Google. Denunciar abuso - Termos de Serviço - Política de Privacidade

Google Formulários

Pesquisa Acadêmica da Universidade de São Paulo (USP) sobre Sistemas Computadorizados em laboratórios

*Obrigatório

CARACTERIZAÇÃO DO PARTICIPANTE

A fim de conhecer melhor os participantes da pesquisa e agrupar respostas, precisamos realizar uma rápida caracterização.

Em qual(is) tipo(s) de auditor o(a) senhor(a) se enquadra? *

- [ ] Auditor interno
- [ ] Auditor contratado, autônomo, terceirizado (segunda parte)
- [ ] Auditor de órgãos reguladores ou regulamentadores (terceira parte)

Estado *

Escolher

Cidade

Sua resposta

Qual o caráter de sua instituição? *

- ◯ Particular
- ◯ Pública
- ◯ Capital misto

Qual o nome de sua instituição? (Opcional)

Sua resposta

Quais sistemas são auditados pelo senhor(a)? *

- ☐ BPL ou GLP
- ☐ ISO 9001
- ☐ ISO/IEC 17025
- ☐ ISO/IEC 17043
- ☐ ISO 15189
- ☐ ISO 14001

Qual a principal área auditada pelo senhor(a)? *

Escolher

Voltar Próxima

Pesquisa Acadêmica da Universidade de São Paulo (USP) sobre Sistemas Computadorizados em laboratórios

*Obrigatório

CONHECIMENTOS SOBRE INFORMÁTICA

Esta seção foi desenvolvida para que tenhamos melhor entendimento do nível de conhecimentos dos auditores em questões de informática relacionadas às normas que este estudo abrange. Por favor, leia as situações apresentadas e escolha a alternativa que considerar correta.
Reforçamos que os dados aqui colhidos serão apresentados como um todo na dissertação de mestrado, sem a divulgação de nomes.

O laboratório utiliza Windows 8 original em suas máquinas, portanto, as mesmas estão seguras e dentro das conformidades *

- ◯ Verdadeiro
- ◯ Falso

O uso de antivírus pago nas máquinas dos laboratórios é *

- ◯ Desnecessário
- ◯ Aconselhável, mas não obrigatório
- ◯ Obrigatório

O backup das máquinas é feito semanalmente, então os dados estão seguros. *

- ◯ Verdadeiro
- ◯ Falso

O software usado pelo laboratório para controle de equipamentos tem um valor de licença muito elevado, então um funcionário instalou a versão "crackeada" do programa. Como este passou pelos devidos testes de adequação e verificação, está conforme. *

- ◯ Verdadeiro
- ◯ Falso

Ao realizar login no computador para inserção dos dados de uma análise, um dos funcionários esqueceu sua senha, então usou usuário e senha de um colega. Como ambos eram pessoas autorizadas a realizar inclusão de dados, não há problemas nesse empréstimo. *

- ◯ Verdadeiro
- ◯ Falso

O software usado para emissão de relatórios foi baixado da internet, diretamente pelo site da empresa desenvolvedora. Após os testes de adequação e verificação, pode ser considerado conforme. *

- ◯ Verdadeiro
- ◯ Falso

Caso seja necessário, os funcionários do laboratório têm permissão para acessar seus e-mails pessoais a partir dos computadores do laboratório, contanto que o façam a partir de abas de navegação anônima, pois assim o histórico de navegação se mantém restrito aos assuntos corporativos. *

- ◯ Não há uma não conformidade nessa situação
- ◯ Há uma não conformidade nessa situação

O backup é salvo em um servidor que se encontra em uma sala do prédio com acesso controlado por cartão de identificação. *

- ◯ Não há uma não conformidade nessa situação
- ◯ Há uma não conformidade nessa situação

Um dos computadores passou a indicar data e hora erradas e apesar de as mesmas serem corrigidas, sempre ao iniciar a máquina, o erro volta. Como isso não afeta o funcionamento do computador, não são mais feitas as alterações, economizando o tempo que esta tarefa tomaria. *

- ◯ Não há uma não conformidade nessa situação
- ◯ Há uma não conformidade nessa situação

Os programas de todas as máquinas do laboratório estão configurados para serem atualizados automaticamente. *

- ◯ Não há uma não conformidade nessa situação
- ◯ Há uma não conformidade nessa situação

Caso o laboratório adquira um computador novo que será utilizados apenas como aquisição de dados para equipamento, nunca sendo conectado à internet, não há a necessidade da instalação de um antivírus. *

- ◯ Verdadeiro
- ◯ Falso

Os funcionários com acesso ao e-mail do laboratório são instruídos a não abrir mensagens de desconhecidos que contenham anexos ou links. *

- ◯ Não há uma não conformidade nessa situação
- ◯ Há uma não conformidade nessa situação

Os arquivos criados nos computados não são excluídos, evitando assim perdas acidentais de arquivos importantes. *

- ◯ Não há uma não conformidade nessa situação
- ◯ Há uma não conformidade nessa situação

Como o prédio em que o laboratório se localiza possui um para-raios, o uso de no-breaks nas máquinas é dispensável. *

- ◯ Verdadeiro
- ◯ Falso

Voltar Próxima

Nunca envie senhas pelo Formulários Google.

Pesquisa Acadêmica da Universidade de São Paulo (USP) sobre Sistemas Computadorizados em laboratórios

*Obrigatório

SITUAÇÃO DA IMPLANTAÇÃO DOS SISTEMAS COMPUTADORIZADOS NOS LABORATÓRIOS

Nesta seção, gostaríamos de saber sua percepção sobre a implantação dos itens abaixo no(s) laboratório(s) auditado(s) por você, de forma que "0" (zero) equivale ao item ser sempre ausente e "5" (cinco), ser sempre presente.

Uso de softwares validados *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	◯	◯	◯	◯	◯	◯	Presente em todos os laboratórios

Relatórios de validação dos software *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	◯	◯	◯	◯	◯	◯	Presente em todos os laboratórios

Testes formais de verificação e adequação dos software *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios

Relatórios dos testes formais de verificação e adequação dos software *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios

Sistemas Operacionais atualizados *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios

Antivírus apropriados (versões disponíveis gratuitamente são voltadas para o uso doméstico. Para fins corporativos, é indicado a compra de uma licença de antivírus) *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios

Formas eficientes de backup *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios

Acesso às máquinas controlado *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios

Procedimentos para manutenção preventiva redigidos *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios

Procedimentos para manutenção corretiva redigidos *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios

Contratos entre o laboratório e o fornecedor, em caso de dados processados ou armazenados por terceiros (nuvem) *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios

Manuais/procedimentos de software prontamente disponíveis *

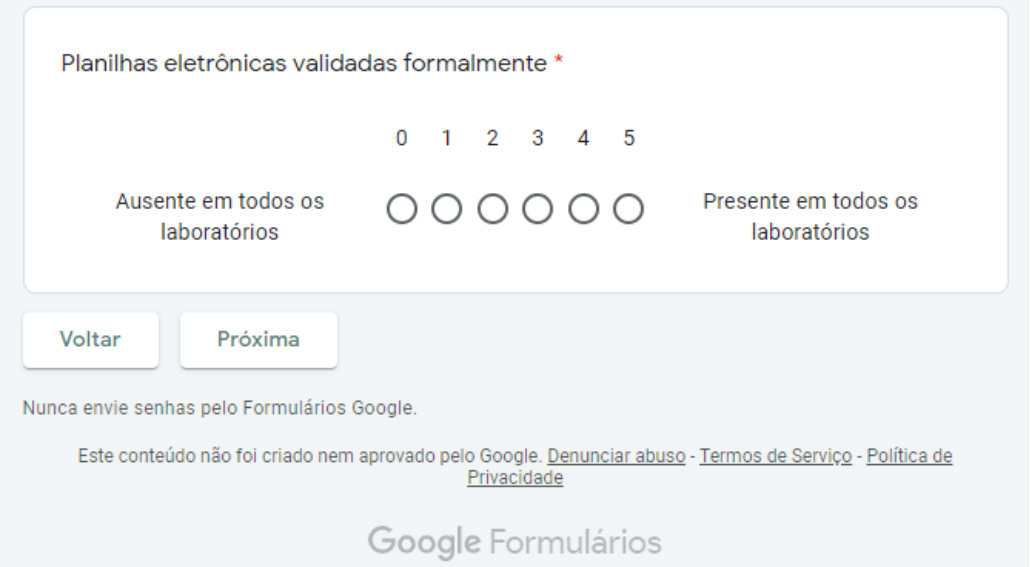
	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios

Planilhas com acesso controlado *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios

Planilhas protegidas contra adulteração/mudanças não intencionais *

	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios



Planilhas eletrônicas validadas formalmente *

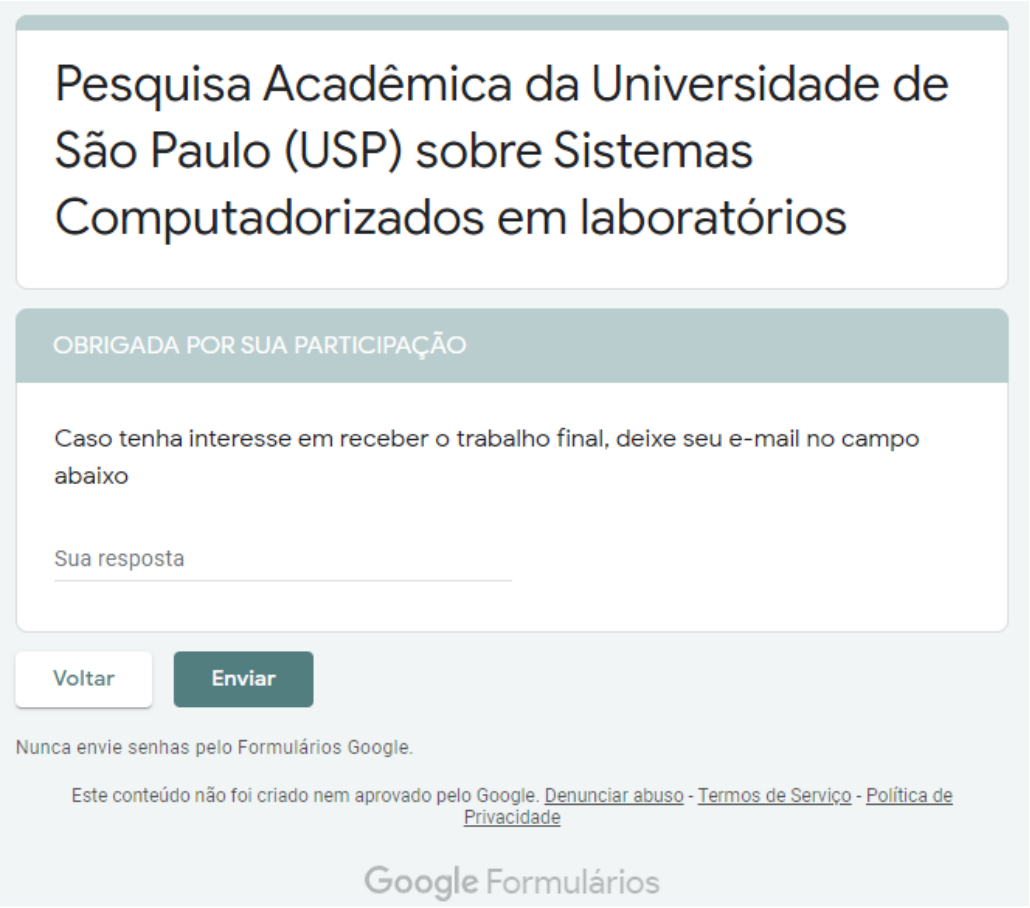
	0	1	2	3	4	5	
Ausente em todos os laboratórios	○	○	○	○	○	○	Presente em todos os laboratórios

Voltar Próxima

Nunca envie senhas pelo Formulários Google.

Este conteúdo não foi criado nem aprovado pelo Google. Denunciar abuso - Termos de Serviço - Política de Privacidade

Google Formulários



Pesquisa Acadêmica da Universidade de São Paulo (USP) sobre Sistemas Computadorizados em laboratórios

OBRIGADA POR SUA PARTICIPAÇÃO

Caso tenha interesse em receber o trabalho final, deixe seu e-mail no campo abaixo

Sua resposta

Voltar Enviar

Nunca envie senhas pelo Formulários Google.

Este conteúdo não foi criado nem aprovado pelo Google. Denunciar abuso - Termos de Serviço - Política de Privacidade

Google Formulários

Apêndice 2 – Questionário enviado aos laboratórios

Pesquisa Acadêmica da Universidade de São Paulo (USP) sobre Sistemas Computadorizados em laboratórios

O presente questionário foi elaborado para que você possa contribuir com uma pesquisa de mestrado da Universidade de São Paulo - IQSC/USP.

Em pesquisa anterior, realizada no segundo semestre de 2018, percebeu-se que laboratórios acreditados, reconhecidos e/ou certificados em diversas normas concordam que os conceitos dos Sistemas de Gestão da Qualidade referentes a Sistemas Computadorizados são de grande importância para seu bom funcionamento. Porém, as medidas nem sempre são aplicadas corretamente e, em alguns casos, nem mesmo cobradas. A fim de obter um conhecimento mais profundo sobre o atual cenário do uso de Sistemas Computadorizados em Laboratórios, a aluna Cássia Watanabe Kock, sob orientação do Prof. Dr. Vitor Hugo Polisél Pacces, está realizando esta pesquisa.

Informações:
- Os dados coletados nesta pesquisa são sigilosos e restritos aos organizadores. Não serão divulgados nomes de empresas ou participantes;
- O participante pode se recusar a continuar com o questionário a qualquer momento, sem penalização alguma e sem prejuízo ao seu cuidado;
- Caso seja do interesse do participante, será enviado o trabalho final para seu e-mail.

Pesquisador responsável: Cássia Watanabe Kock – IQSC/USP
Contato: cassia.kock@usp.br
Instituto de Química de São Carlos da Universidade de São Paulo - IQSC/USP. Avenida Trabalhador São-carlense, 400
CEP 13566-590 - São Carlos - SP - Brasil

*Obrigatório

Li e entendi as informações acima e concordo em participar da pesquisa *

- ◯ Sim
- ◯ Não

Próxima

Pesquisa Acadêmica da Universidade de São Paulo (USP) sobre Não Conformidades aplicadas aos Sistemas Computadorizados

*Obrigatório

CARACTERIZAÇÃO DA EMPRESA/INSTITUIÇÃO

Qual o nome da empresa/instituição? (Opcional)

Sua resposta

Cidade

Sua resposta

Estado *

Escolher

Qual seu cargo/função na empresa/instituição?

Sua resposta

Quantos funcionários há na empresa/instituição? *

- ◯ Até 10
- ◯ De 11 a 50
- ◯ De 51 a 100
- ◯ Mais de 100

Em qual/quais sistemas de gestão sua empresa possui certificação, reconhecimento ou acreditação? *

- [ ] BPL ou GLP
- [ ] ISO 9001
- [ ] ISO/IEC 17025
- [ ] ISO/IEC 17043
- [ ] ISO 15189
- [ ] ISO 14001
- [ ] Estamos em processo de implantação

Qual a principal área de atuação da sua empresa/instituição? *

Escolher

Há quanto tempo a empresa é acreditada, reconhecida ou certificada no Sistema de Gestão? *

- ( ) Ainda não somos acreditados, certificados ou reconhecidos
- ( ) Menos de 1 ano
- ( ) De 1 a 2 anos
- ( ) De 3 a 4 anos
- ( ) 5 anos ou mais

A empresa/instituição é de caráter *

- ◯ Público
- ◯ Privado
- ◯ Educacional
- ◯ Capital Misto

Voltar Próxima

Nunca envie senhas pelo Formulários Google.

Pesquisa Acadêmica da Universidade de São Paulo (USP) sobre Não Conformidades aplicadas aos Sistemas Computadorizados

*Obrigatório

SOBRE AS NÃO CONFORMIDADES

Em cada um dos itens abaixo, indique se na última auditoria externa sua empresa/instituição recebeu alguma não conformidade (NC) relacionada ao tópico. Se possível, relate/transcreva a(s) não conformidade(s) no espaço seguinte a cada pergunta.

O avaliador verificou se os softwares eram validados ? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

O avaliador verificou os relatórios de validação dos softwares? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

O avaliador verificou se quando foram aplicados os softwares e os hardwares, foram realizados testes formais de adequação e verificação? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

O avaliador verificou os relatórios dos testes formais de adequação e verificação? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

O avaliador verificou a versão do sistemas operacionais dos computadores? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

O avaliador verificou as atualizações dos sistema operacionais dos computadores? *

- ◯ Verificou e foi verificada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

O avaliador verificou se os computadores possuem antivírus? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

Após avaliar a existência de antivírus, o avaliador verificou a periodicidade de uso dos mesmos? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

O avaliador também verificou a periodicidade de atualização dos antivírus dos computadores? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

O avaliador verificou se é feito backup dos dados? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

O avaliador verificou a frequência com que o backup é feito? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

Durante a auditoria, o avaliador verificou o controle de usuário para acesso aos computadores? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

Foram avaliadas as manutenções preventivas de computadores e softwares? *

- ◯ Foram avaliadas e foi detectada NC
- ◯ Foram avaliadas e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

Foram avaliadas as manutenções corretivas dos computadores e softwares? *

- ◯ Foram avaliadas e foi detectada NC
- ◯ Foram avaliadas e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

O avaliador verificou se há um contrato de confidencialidade em caso de dados mantidos por terceiros? *

- ◯ Verificou e houve NC
- ◯ Verificou e não houve NC
- ◯ Não houve avaliação relacionada a este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

O avaliador verificou a existência de manuais e procedimentos dos softwares no laboratório? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

Ao avaliar as planilhas usadas pelo laboratório, o avaliador verificou se há bloqueio de células? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

Ainda avaliando as planilhas usadas pelo laboratório, o avaliador verificou se as mesmas são validadas? *

- ◯ Verificou e foi detectada NC
- ◯ Verificou e não foi detectada NC
- ◯ O avaliador não verificou este item

Caso tenha sido detectada uma NC relacionada à questão anterior, relate-a no espaço abaixo

Sua resposta

Avalie a dificuldade de implantação dos seguintes itens, sendo 0 - nenhuma dificuldade e 5 - muita dificuldade *

	0	1	2	3	4	5
Validação de software	◯	◯	◯	◯	◯	◯

Relatórios de validação de software	○	○	○	○	○	○
Testes formais de validação e adequação de software	○	○	○	○	○	○
Relatórios dos testes formais de validação e adequação de software	○	○	○	○	○	○
Manter sistemas operacionais atualizados	○	○	○	○	○	○
Aquisição e atualização de antivírus apropriado	○	○	○	○	○	○
Instauração e manutenção de backup	○	○	○	○	○	○
Controle de acesso às máquinas	○	○	○	○	○	○
Manutenção preventiva procedimentada	○	○	○	○	○	○
Manutenção corretiva procedimentada	○	○	○	○	○	○
Formulação de contratos em caso de dados mantidos por terceiros	○	○	○	○	○	○
Manuais/procedimentos de software prontamente disponíveis	○	○	○	○	○	○
Planilhas com acesso controlado	○	○	○	○	○	○
Planilhas protegidas contra adulteração/mudanças não intencionais	○	○	○	○	○	○

Voltar Próxima