

Ministério da Saúde

FIOCRUZ

Fundação Oswaldo Cruz



Bruno Bezerra Carvalho

Boas práticas de integridade de dados em registros eletrônicos gerados em sistemas computadorizados de equipamentos analíticos: uma proposta para os laboratórios de pesquisa científica experimental da Fiocruz

Rio de Janeiro

2021

Bruno Bezerra Carvalho

Boas práticas de integridade de dados em registros eletrônicos gerados em sistemas computadorizados de equipamentos analíticos: uma proposta para os laboratórios de pesquisa científica experimental da Fiocruz

Dissertação apresentada ao Programa de Pós-graduação em Saúde Pública, da Escola Nacional de Saúde Pública Sergio Arouca, na Fundação Oswaldo Cruz, como requisito parcial para obtenção do título de Mestre em Saúde Pública. Área de concentração: Políticas Públicas, Gestão e Cuidado em Saúde.

Orientador: Prof. Dr. José Manuel Santos de Varge Maldonado

Coorientadora: Prof.^a Dra. Renata Almeida de Souza

Rio de Janeiro

2021

Good data integrity practices in electronic records generated in computerized analytical equipment systems: a proposal for Fiocruz's experimental scientific research laboratories

Catálogo na fonte

Fundação Oswaldo Cruz

Instituto de Comunicação e Informação Científica e Tecnológica em Saúde

Biblioteca de Saúde Pública

C331b Carvalho, Bruno Bezerra.

Boas práticas de integridade de dados em registros eletrônicos gerados em sistemas computadorizados de equipamentos analíticos: uma proposta para os laboratórios de pesquisa científica experimental da Fiocruz / Bruno Bezerra Carvalho. -- 2021.

167 f. : il. ; tab.

Orientador: José Manuel Santos de Varge Maldonado.

Coorientadora: Renata Almeida de Souza.

Dissertação (mestrado) – Fundação Oswaldo Cruz, Escola Nacional de Saúde Pública Sergio Arouca, Rio de Janeiro, 2021.

1. Armazenamento e Recuperação da Informação. 2. Gerenciamento de Dados. 3. Segurança Computacional. 4. Pesquisa Científica e Desenvolvimento Tecnológico. 5. Reprodutibilidade. 6. Integridade de Dados. 7. Administração das Tecnologias da Informação. 8. Gestão da Qualidade. I. Título.

CDD – 23.ed. – 025.06

Bruno Bezerra Carvalho

Boas práticas de integridade de dados em registros eletrônicos gerados em sistemas computadorizados de equipamentos analíticos: uma proposta para os laboratórios de pesquisa científica experimental da Fiocruz

Dissertação apresentada ao Programa de Pós-graduação em Saúde Pública, da Escola Nacional de Saúde Pública Sergio Arouca, na Fundação Oswaldo Cruz, como requisito parcial para obtenção do título de Mestre em Saúde Pública. Área de concentração: Políticas Públicas, Gestão e Cuidado em Saúde.

Aprovada em: 12 de novembro de 2021.

Banca Examinadora

Prof.^a Dra. Vanessa de Arruda Jorge
Fundação Oswaldo Cruz - Vice-Presidência de Educação, Informação e Comunicação

Dra. Ivanete Milagres Presot
Fundação Oswaldo Cruz - Instituto René Rachou

Dra. Renata Almeida de Souza (Coorientadora)
Fundação Oswaldo Cruz - Vice-Presidência de Gestão e Desenvolvimento Institucional

Dr. José Manuel Santos de Varge Maldonado (Orientador)
Fundação Oswaldo Cruz - Escola Nacional de Saúde Pública Sergio Arouca

Rio de Janeiro

2021

Dedico este trabalho com imensurável agradecimento à minha amada esposa Anna Carolina e às minhas filhas Anna Clara Carvalho e Bruna Carvalho, bênçãos de Deus na minha vida.

Aos meus pais Maria Salete e Vilson Carvalho pelos ensinamentos e perseverança demonstrados, incentivo, dedicação, amor e por sempre valorizar a importância dos meus estudos.

AGRADECIMENTOS

À Deus, primeiramente, por sua benevolência e a quem devo a vida, o que tenho e o que sou. A Ele toda glória e honra, principalmente nestes últimos meses, pois me direcionou com paciência, sabedoria, perseverança e, sobretudo, com humildade para seguir a diante.

A concretização deste trabalho, de suma importância para minha vida profissional, é o produto da colaboração de diversas pessoas e por isso não poderia deixar de evidenciar meus sinceros agradecimentos e compartilhar um sentimento único no qual estou vivendo de vitória, superação, satisfação e de dever cumprido e que há um longo caminho ainda a percorrer.

À Fundação Oswaldo Cruz, à Escola Nacional de Saúde Pública Sergio Arouca e ao Programa de Pós-graduação em Saúde Pública (PPGSP) pela oportunidade.

Aos professores do Mestrado Profissional que promoveram de forma fenomenal uma transferência de conhecimento e proporcionaram um processo de aprendizagem inigualável.

Ao meu orientador, Prof. Dr. José Manuel Santos de Varge Maldonado, pela enorme disposição em contribuir com seus conhecimentos, pelos seus direcionamentos e pela cordialidade com que me orientou durante todo o trabalho, principalmente, pelo período tão difícil, doloroso e desafiador em que passa toda a humanidade.

À minha coorientadora, Profa. Dra. Renata Almeida de Souza, pelo acompanhamento, apoio, direcionamento e ensinamentos.

À minha mãe, Maria Salete, que apesar de todas as dificuldades que a vida lhe impôs, sempre me orientou com carinho, dedicação e amor, e que mesmo distante fisicamente nunca deixou de me apoiar nas escolhas e desafios.

Ao meu pai, Vilson Carvalho, que mesmo distante, nunca deixou de me orientar pelo caminho do bem e, principalmente, na dedicação aos estudos.

À minha amada esposa, Anna Carolina, que desde antes do início desta empreitada já estava me incentivando, apoiando e acreditando em mim mais do que eu mesmo acreditava. Todo o seu carinho, amor e paciência foram indispensáveis para o resultado desse trabalho.

Por fim, agradeço meus colegas de turma que de alguma forma contribuíram para a elevação de meu conhecimento e que findou nesse trabalho.

*A tarefa não é tanto ver aquilo que ninguém viu, mas pensar o que ninguém ainda pensou
sobre aquilo que todo mundo vê.*

SCHOPENHAUER, 1851.

RESUMO

A integridade de dados eletrônicos é um problema de alta relevância implícito em todo o processo decorrente da aquisição e utilização de equipamentos analíticos. A adoção de princípios e diretrizes em ações de integridade de dados eletrônicos nas diferentes esferas da Fundação Oswaldo Cruz (Fiocruz) faz-se necessário, assim como, a compreensão de práticas relacionadas à integridade de dados durante todo o seu ciclo de vida nas atividades em laboratório de pesquisa científica experimental, seja em caráter orientativo ou visando a promoção da melhoria contínua. Neste sentido, este trabalho objetivou realizar uma pesquisa quali-quantitativa e exploratória, visando a adoção de práticas de integridade de dados gerados eletronicamente por sistemas computadorizados de equipamentos analíticos. O trabalho versou em um estudo exploratório na população constituída de 13 unidades técnico-científicas e 03 escritórios técnicos da Fiocruz que possuem laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada. A coleta de dados foi realizada a partir de duas fontes de evidências: documentação e questionários semiestruturados. Práticas existentes de gerenciamento de dados em registros eletrônicos gerados por sistemas computadorizados de equipamentos analíticos foram comparadas às recomendadas pelo guia de boas práticas em gerenciamento de dados presente no anexo 5 do 50º relatório técnico da OMS. Verificou-se que a população estudada possui práticas que apoiam o processo de implementação de integridade de dados eletrônicos, mas com grau de adoção baixo em sua maioria, principalmente em medidas de controles técnicos. Ao final, propõe-se identificar um conjunto de ações que auxiliem a implementação de requisitos mínimos de integridade de dados em registros eletrônicos gerados por sistemas computadorizados de equipamentos analíticos.

Palavras-chave: Integridade de dados. Gerenciamento de dados. Reprodutibilidade. Segurança da Informação. Pesquisa Científica

ABSTRACT

The integrity of electronic data is a highly relevant issue implicit in the entire process arising from the acquisition and use of analytical equipment. The adoption of principles and guidelines in electronic data integrity actions in the different spheres of the Oswaldo Cruz Foundation (Fiocruz) is necessary, as well as the understanding of practices related to data integrity throughout its life cycle in an experimental scientific research laboratory, either for guidance purposes or aimed at promoting continuous improvement. In this sense, this work aimed to carry out qualitative-quantitative and exploratory research, aiming at the adoption of data integrity practices electronically generated by computerized analytical equipment systems. The work was based on an exploratory study in the population consisting of 13 technical-scientific units and 03 Fiocruz technical offices that have laboratories with testing activities, technological platforms, and/or basic or applied experimental research. Data collection was performed from two sources of evidence: documentation and semi-structured questionnaires. Existing data management practices in electronic records generated by computerized analytical equipment systems were compared to those recommended by the data management best practices guide in Annex 5 of the 50th WHO technical report. It was found that the population studied has practices that support the implementation process of electronic data integrity, but with a low level of adoption in most cases, especially in technical control measures. In the end, it is proposed to identify a set of actions that help the implementation of minimum data integrity requirements in electronic records generated by computerized analytical equipment systems.

Keywords: Data integrity. Data management. Reproducibility. Information security. Scientific research

LISTA DE ILUSTRAÇÕES

Figura 1: Fases e etapas envolvidos no ciclo de vida de dados científicos alcançados em trabalhos de pesquisa	44
Figura 2: Principais fatores que influenciam a integridade de dados	47
Figura 3: Número de cartas de advertência associadas à integridade de dados por país, emitidas pelo FDA USA, no período de 2015 a 2018 e seu total acumulado	53
Figura 4: Etapas da pesquisa e suas respectivas atividades	59
Quadro 1: Relacionamento do gerenciamento de dados com o ciclo de vida de um projeto de pesquisa.....	45

LISTA DE TABELAS

Tabela 1: Dados brutos <i>versus</i> metadados	35
Tabela 2: Definição de integridade de dados segundo várias fontes	37
Tabela 3: Lista cronológica de regulamentos	39
Tabela 4: Acrônimo ALCOA+ (<i>Plus</i>)	41
Tabela 5: Princípios básicos de integridade de dados (ALCOA+)	41
Tabela 6: Princípios de governança de dados	48
Tabela 7: Tipos de controles sobre o ciclo de vida dos dados	49
Tabela 8: Possíveis implicações por violações de Boas Práticas (BPx)	52
Tabela 9: Relacionamento entre objetivos específicos, metodologia e fontes de coletas de dados da pesquisa	60
Tabela 10: Relação de unidades técnico-científicas e escritórios técnicos do universo pesquisados	65
Tabela 11: Caracterização dos profissionais que responderam os questionários	65
Tabela 12: Relação dos gestores da área da Qualidade por código de identificação que participaram da pesquisa	68
Tabela 13: Relação dos gestores da área de TIC por código de identificação que participaram da pesquisa	90
Tabela 14: Grau de adoção de práticas de gerenciamento de dados eletrônicos, obtidos sob a percepção dos gestores da área da Qualidade	123
Tabela 15: Grau de adoção de práticas de gerenciamento de dados eletrônicos, obtidos sob a percepção dos gestores da área de TIC	124

LISTA DE ABREVIATURAS E SIGLAS

AI -	<i>Artificial Intelligence</i>
ABNT -	Associação Brasileira de Normas Técnicas
ALCOA -	Atribuíveis, Legíveis, Contemporâneos, Originais e Acurados
ALCOA-plus -	Atribuíveis, Legíveis, Contemporâneos, Originais e Acurados com ênfase adicional dos atributos de ser Completo, Consistente, Duradouro e Disponível
ANVISA -	Agência Nacional de Vigilância Sanitária
AR -	Agência Reguladora
BI -	<i>Business Intelligence</i>
Bio-Manguinhos -	Instituto de Tecnologia em Imunobiológicos
BPD -	Boas Práticas de Distribuição
BPDoc -	Boas Práticas de Documentação
BPF -	Boas Práticas de Fabricação
BPL -	Boas Práticas de Laboratório
BPx -	Boas Práticas em geral
CAPA -	<i>Corrective Action and Preventive Action</i>
CEP -	Comitê de Ética em Pesquisa
CHMP -	<i>Committee for Medicinal Products for Human Use</i>
Cgcre-Inmetro	Coordenação Geral de Acreditação do Inmetro
Cogetic -	Coordenação de Gestão da Tecnologia da Informação e Comunicação
CNQPS -	Comissão Nacional de Qualidade e Produtividade em Saúde
CQuali -	Coordenação da Qualidade
CT&I -	Ciência, Tecnologia e Inovação
EMA -	<i>European Medicines Agency</i>
ENSP -	Escola Nacional de Saúde Pública
EU -	<i>European Union</i>
Farmanguinhos -	Instituto de Tecnologia em Fármacos
FDA -	<i>Food and Drug Administration</i>
GRQ -	Gerenciamento de Risco da Qualidade
IAM -	Instituto Aggeu Magalhães
ICC -	Instituto Carlos Chagas
ICH -	<i>International Council for Harmonisation</i>
ICTB -	Instituto de Ciência e Tecnologia em Biomodelos
ID -	<i>Identity</i>

IEC -	<i>International Electrotechnical Commission</i>
IF -	Indústria Farmacêutica
IFA -	Ingrediente Farmacêutico Ativo
IFF -	Instituto Nacional de Saúde da Mulher, da Criança e do Adolescente Fernandes Figueira
IGM -	Instituto Gonçalo Moniz
ILMD -	Instituto Leônidas & Maria Deanne
IN -	Instrução Normativa
INCQS -	Instituto Nacional de Controle de Qualidade em Saúde
INI -	Instituto Nacional de Infectologia Evandro Chagas
IOC -	Instituto Oswaldo Cruz
IoT -	<i>Internet of Things</i>
IRR -	Instituto René Rachou
ISO -	<i>International Organization for Standardization</i>
ISPE -	<i>International Society for Pharmaceutical Engineering</i>
JCI -	<i>Joint Commission International</i>
MHRA -	<i>Medicines and Healthcare products Regulatory Agency</i>
MS -	Ministério da Saúde
NBR -	Norma Técnica Brasileira
NIH -	<i>National Institutes of Health</i>
NTIC -	Novas Tecnologias de Informação e Comunicação
OECD -	<i>Organization for Economic Co-operation and Development</i>
OMS -	Organização Mundial de Saúde
OPAS -	Organização Pan-Americana da Saúde
ORA	<i>Office of Regulatory Affairs</i>
PDCA -	<i>Plan-Do-Check-Act</i>
P&D -	Pesquisa e Desenvolvimento
PIC/S -	<i>Pharmaceutical Inspection Co-operation Scheme</i>
POP -	Procedimentos Operacionais Padrão
PU -	Procedimentos de Uso
RDC -	Resolução da Diretoria Colegiada
SBPC/ML -	Sociedade Brasileira de Patologia Clínica/Medicina Laboratorial
SGQ -	Sistema de Gestão da Qualidade
SO	Sistema Operacional
SI -	Segurança da Informação
SNI -	Sistema Nacional de Inovação

SNIS -	Sistema Nacional de Inovação em Saúde
SNS -	Sistema Nacional de Saúde
SUS -	Sistema Único de Saúde
SVS/MS -	Secretaria de Vigilância em Saúde do Ministério da Saúde
TC -	<i>Technical Committee</i>
TCLE -	Termo de Consentimento Livre e Esclarecido
TI -	Tecnologia da Informação
TIC -	Tecnologias da Informação e Comunicação
USA -	<i>United States of America</i>
WHO -	<i>World Health Organization</i>

SUMÁRIO

1	INTRODUÇÃO	15
2	OBJETIVOS	18
2.1	OBJETIVO GERAL	18
2.2	OBJETIVOS ESPECÍFICOS	18
3	JUSTIFICATIVA	19
4	REFERENCIAL TEÓRICO E NORMATIVO	23
4.1	GESTÃO DA QUALIDADE	23
4.1.1	Gestão da qualidade na saúde	24
4.1.2	Gestão da qualidade em laboratórios de pesquisa em saúde: a importância das boas práticas na pesquisa científica	25
4.1.3	Aspectos éticos na pesquisa em saúde	27
4.1.4	Reprodutibilidade da pesquisa em saúde	29
4.2	GESTÃO DA TECNOLOGIA DA INFORMAÇÃO	30
4.2.1	Segurança da informação	32
4.3	INTEGRIDADE DE DADOS	34
4.3.1	Governança de dados	43
4.3.2	Impactos da não adoção da prática de integridade de dados	51
5	METODOLOGIA	55
5.1	CARACTERIZAÇÃO DA PESQUISA	55
5.2	DESENHO DO ESTUDO	55
5.3	POPULAÇÃO E AMOSTRA DA PESQUISA	57
5.4	ETAPAS DO TRABALHO	57
5.5	COLETA DE DADOS	59
5.6	INSTRUMENTO PARA COLETA DE DADOS DA POPULAÇÃO ESTUDADA	60
6	RESULTADOS E DISCUSSÃO	64
6.1	PERFIL DA AMOSTRA	64
6.2	ANÁLISE DOS RESULTADOS E DISCUSSÃO	65
7	CONSIDERAÇÕES FINAIS	126
	REFERÊNCIAS	132
	APÊNDICE A - Questionário 1: QUESTIONÁRIO DE INTEGRIDADE DE DADOS EM REGISTROS ELETRÔNICOS – QUALIDADE	144

**APÊNDICE B - Questionário 2: QUESTIONÁRIO DE
INTEGRIDADE DE DADOS EM REGISTROS ELETRÔNICOS
– TIC**

1. INTRODUÇÃO

Presentes desde as civilizações mais antigas, o conhecimento e a inovação, segundo Burke & Ornsten (1998), têm sido os fatores fundamentais na sobrevivência da humanidade.

A Revolução Industrial ocorrida a partir da segunda metade do século XVIII promoveu significativos avanços na Ciência, Tecnologia e Inovação (CT&I), gerando impactos diretos e indiretos sobre todos os aspectos da economia (NELSON, 2001).

A Terceira Revolução Industrial, também conhecida como Revolução Informacional ou ainda Revolução Técnico-científica, promoveu novas e profundas articulações no âmbito de processos econômicos, políticos, sociais e culturais, formas de organização de poder, projetos de sociedade e de atores sociais, entre outros (CUOGO, 2012).

Tendo seu início no século passado, a partir da década de 1980, a Revolução Informacional, caracterizou-se pelos grandes avanços das tecnologias da informação e comunicação (TIC) e da incorporação da informatização em todas as esferas da vida econômica, para garantir produtos e serviços de melhor qualidade e maior competitividade no mercado (SOARES NETO, 2012).

A informação, no atual contexto, possui um efeito multiplicador e forma uma força capaz de propiciar o desenvolvimento econômico, político, social, cultural e tecnológico (SPINATO, 2010).

No início do século XXI, anuncia-se o prenúncio de uma 4ª Revolução Industrial ou Indústria 4.0, caracterizada pela fusão de diversas tecnologias interagindo e integrando os domínios físicos, digitais e biológicos, com avanços nas áreas de nanotecnologia, sequenciamento genético, computação quântica, energias renováveis, *big data*, inteligência artificial, internet das coisas, novas tecnologias da informação e comunicação (NTIC), entre outras (CINTRA et al., 2019).

A instituição das NTIC contribui para introduzir na sociedade, empresas e organizações novas transformações que permeiam toda a economia global devido à geração e difusão de uma massa de dados e informações sem precedentes na história da humanidade (MUELLER, 1994).

Nesta perspectiva, estes atores passam a enfrentar um grande problema com a enxurrada de dados e informações que são gerados e que chegam em tempo real em seus cotidianos.

Para Cianconi et al. (2013), o processo de informatização, tanto na vida das pessoas, quanto nas organizações, resulta na necessidade de implantar políticas e procedimentos com objetivo de gerir todo o ciclo da informação, desde a geração passando pela coleta, organização, processamento e chegando até a disseminação e uso.

O aumento exponencial na quantidade de dados a serem geridos tem criado obstáculos não só para o gerenciamento da informação, mas também, na quantidade de profissionais que controlam os processos e nas necessidades para acesso em tempo real (PINOCHET, et al., 2014).

A gestão dos dados, em qualquer segmento, passou a ser crítica para a sobrevivência das organizações contemporâneas, pois a informação representa um ativo intangível e de alta relevância para as tomadas de decisões, sendo necessário adotar processos para coleta, validação, armazenamento e garantia da segurança dos dados para serem, então, transformados em informações úteis (ASSOCIAÇÃO BRASILEIRA DE AUTOMAÇÃO, 2017)

A área da saúde, segundo Tenório et al. (2017), caracteriza-se por ser intensiva em CT&I, além de ser um campo de análise e de significativas atividades de ciência de dados, de pesquisa e desenvolvimento (P&D), e tem experimentado desafios devido ao crescimento exponencial das NTIC.

Portanto, as atividades de pesquisa científica precisam cada vez mais transparecer confiança para a sociedade, pois são crescentes os problemas relacionados à fabricação de dados, falsificação de dados e informações, procedimentos e resultados, adulteração de dados, plágio, além de outras formas de condutas inadequadas (SILVA et al., 2018).

Para Baker (2016), a ciência enfrenta outro grande problema com relação à integridade, caracterizando uma crise existencial de reprodutibilidade de dados científicos, o que contribui para um alto percentual de dados científicos publicados e não reprodutíveis e uma baixa reprodutibilidade em estudos sobre medicamentos.

A Fundação Oswaldo Cruz (FIOCRUZ) é uma instituição pública e estratégica de Estado do Brasil, responsável pelo desenvolvimento de pesquisas, desenvolvimento tecnológico e educação no campo da saúde, além da produção de insumos estratégicos para o Sistema Único de Saúde (SUS) (LIMA et al., 2018).

Localizada em todas as regiões do Brasil, a instituição é vinculada ao Ministério da Saúde (MS) e é constituída por 16 institutos técnico-científicos, cujas atividades desenvolvidas compreendem especialmente ações de pesquisa e inovação; produção de medicamentos, imunobiológicos e reagentes diagnósticos; vigilância em saúde; educação; prestação de serviços de referência e assistência à saúde; informação, comunicação e divulgação científica em saúde; e preservação do patrimônio científico, histórico e cultural da saúde e das ciências (LIMA et al., 2018).

Com o advento das NTIC, a Fiocruz, ao longo dos últimos anos, vem adquirindo para seus laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas

experimentais básica ou aplicada, novos equipamentos analíticos com sistemas computadorizados para substituição de processos até então executados de forma manual nas atividades de análises laboratoriais (LIMA, 2020).

Não obstante, os sistemas computadorizados permitem a estes laboratórios a geração cada vez maior de dados eletrônicos decorrentes de análises e corridas realizadas nos equipamentos analíticos. Desse modo, cada vez mais processos manuais vão sendo substituídos por sistemas computadorizados nas atividades e processos analíticos, gerando dados importantes para tomada de decisão em todas as fases da cadeia de P&D de fármacos, medicamentos e kits de diagnósticos, além do controle de insumos (LIMA et al., 2018).

A integridade de dados eletrônicos é um problema de alta relevância e que está implícito em todo o processo decorrente desde a aquisição dos equipamentos analíticos e que perpassa pelas fases de instalação e configuração, além das fases do ciclo de vida dos dados (CALIXTO, 2017).

Muitos equipamentos analíticos são comprados e instalados pelas unidades técnico-científicas e escritórios técnicos da Fiocruz sem o estabelecimento mínimo de medidas de controles organizacionais, operacionais e técnicos, além da ausência de estratégias de controle e aplicação de gerenciamento de riscos. Estas ausências contribuem para que dados possam ser adulterados ou excluídos por questões de má prática ou má fé (ALISSON, 2014).

A FIOCRUZ estabeleceu em 2018, em atendimento ao Decreto nº 9.203/2017 e à Portaria CGU nº 1.089/2018, uma Unidade de Gestão de Integridade e aprovou o Programa de Integridade Pública, onde institui, em 06 de março de 2020 através da Portaria nº 5.318, o Guia de Integridade em Pesquisa da Fiocruz. O guia tem como finalidade orientar a atuação de profissionais que atuam na função de pesquisador, dos pesquisadores visitantes e dos estudantes, sobre as boas práticas em pesquisa nos projetos realizados e financiados pela Fiocruz e as complexas questões relacionadas com a pesquisa científica e a divulgação de seus resultados (LIMA, 2020). Todavia, no campo da integridade de dados e registros eletrônicos, constata-se a inexistência de qualquer orientação institucional.

Nesta perspectiva, definem-se a seguir os objetivos geral e específicos desta dissertação.

2. OBJETIVOS

2.1 OBJETIVO GERAL

Avaliar a adoção de princípios e diretrizes de integridade de dados gerados eletronicamente por sistemas computadorizados de equipamentos analíticos em laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada da Fiocruz segundo o guia de boas práticas em gerenciamento de dados da Organização Mundial da Saúde (OMS).

2.2 OBJETIVOS ESPECÍFICOS

Para alcançar o objetivo geral proposto, foram definidos os seguintes objetivos específicos:

- Analisar o grau de adoção de práticas de gerenciamento de dados em registros eletrônicos gerados por sistemas computadorizados de equipamentos analíticos em laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica ou aplicada da Fiocruz;
- Comparar as práticas existentes de gerenciamento de dados em registros eletrônicos gerados por sistemas computadorizados de equipamentos analíticos em laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica ou aplicada da Fiocruz com as do guia de boas práticas em gerenciamento de dados presente no anexo 5 do 50º relatório técnico da OMS;
- Propor um conjunto de ações que auxiliem a implementação de requisitos mínimos de integridade de dados em registros eletrônicos gerados por sistemas computadorizados de equipamentos analíticos em laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica ou aplicada da Fiocruz.

3. JUSTIFICATIVA

O campo da saúde possui, além de sua relevância social, significativa importância na geração, no uso e na difusão de inovação e é reconhecida como um campo estratégico da agenda de desenvolvimento e que constitui um elemento essencial na atual dinâmica do desenvolvimento e competitividade (GADELHA et al., 2012).

A informação, dentro do cenário atual, é considerada um dos bens mais valiosos para organizações e sociedade, sendo a todo instante criada, utilizada, armazenada, divulgada e compartilhada. Desta forma, garantir sua disponibilidade, integridade, confidencialidade e autenticidade é necessário na área da saúde (VIEIRA, 2014).

Cada vez mais processos manuais vão sendo substituídos por sistemas computadorizados nas atividades e processos analíticos na área da saúde, gerando dados importantes em todas as fases da cadeia de P&D de fármacos, medicamentos e kits de diagnósticos. Não implementar a adoção de práticas que assegurem uma gestão eficiente dos dados gerados é um risco eminente para as corretas tomadas de decisão que podem, inclusive, trazer impactos negativos para a saúde (WHO, 2016).

Segundo Carvalho (1976), um laboratório de saúde pública contribui, principalmente, para o estudo e a solução dos problemas importantes de saúde apresentados, além de gerar informação precisa e verdadeira para adoção de medidas adequadas por parte de profissionais médico-sanitaristas.

Um laboratório pode ser compreendido como sendo um ambiente equipado para estudo experimental em uma ciência ou para testes e análises e que promove oportunidade para experimentação, observação prática em um campo de estudo ou onde se cria, se transforma alguma coisa em outra (CARVALHO, 1976).

Dados eletrônicos, gerados em laboratórios através de sistemas computadorizados em equipamentos analíticos, vêm crescendo substancialmente em decorrência da substituição de processos manuais na indústria farmacêutica. Segundo Chatterjee (2016, apud Moschetta, 2017), 90% dos dados eletrônicos mundiais foram gerados nos últimos dois anos.

Portanto, o tema integridade de dados eletrônicos vem sendo uma área de crescente foco para agências reguladoras com objetivo de assegurar que boas práticas e diretrizes de gerenciamento de dados estejam sendo aplicadas para garantir integridade dos dados eletrônicos (WHO, 2016).

Em laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica e/ou aplicada, esse processo de transformação digital vem crescendo cada

vez mais em atividades laboratoriais e proporcionando a geração de dados eletrônicos de grande importância para toda a cadeia da pesquisa que possuem relação com as áreas de produção e controle de insumos (medicamentos, vacinas, kits de diagnósticos, entre outros).

Nesse ínterim, desenvolver e fortalecer boas estratégias de gerenciamento de dados eletrônicos em saúde é importante para garantir que os dados gerados são registrados, processados, retidos e usados para assegurar um registro completo, consistente e preciso ao longo do ciclo de vida dos dados.

Nos últimos anos agências de saúde e reguladores internacionais como o *Food and Drug Administration* (FDA) – agência dos EUA responsável por regular alimentos, medicamentos, produtos biológicos, dispositivos médicos, cosméticos, produtos veterinários entre outros (FDA, 2018), o *Medicines and Healthcare products Regulatory Agency* (MHRA) – agência reguladora de medicamentos, dispositivos médicos e hemocomponentes para transfusão de sangue no Reino Unido (MHRA, 2018) e a OMS – organização responsável por inspeções em laboratórios pré-qualificados e em indústrias no mundo todo (WHO, 2016), perceberam um número crescente de não conformidades relacionadas à integridade de dados, o que passou a chamar muita atenção e gerou um alerta por partes dos órgãos reguladores.

No campo científico, os cientistas têm como um dos seus maiores objetivos a publicação de artigos científicos, sendo imperativo nos avanços da ciência e da sociedade e para a soberania das nações. Neste contexto, segundo Mesquita (2017), nos últimos 20 anos o Brasil teve mais de 630 mil documentos citáveis na base de dados do SCImago entre 1996-2016, ocupando, em 2017, a 15ª posição no *ranking* de países do SCImago.

O ambiente do mundo acadêmico é dominado pela quantidade massiva de publicações científicas e tem, nesta métrica quantitativa, o aliado para conquistar contratações em universidades, promoções, premiações e obtenção de fomento financeiro (MESQUITA, 2017).

No entanto, como observado por Edwards e Roy (2016) *apud* Mesquita (2017), o ambiente de competição, estimulado por fundos de pesquisa e por recompensas financeiras e/ou acadêmicas, compromete o progresso científico e torna favorável o aumento de ações antiéticas e fraudes científicas.

Neste contexto, segundo Mesquita (2017), essas ações podem ser classificadas como:

- i) Fabricação – que é a criação de resultados na pesquisa;
- ii) Falsificação – que é a manipulação de materiais da pesquisa, equipamentos ou dos procedimentos da pesquisa, ou a omissão dos dados de forma que a pesquisa não represente acuradamente os achados reais; e

- iii) Plágio – que é a apropriação de ideias, processos, resultados ou palavras de outros, sem o devido crédito.

Entre 1992 e 2012, o *National Institutes of Health* (NIH) retratou um total de 291 artigos de pesquisas financiadas pelo instituto por causa de condutas antiéticas identificadas, com danos decorrentes da utilização de dados por pesquisadores e profissionais da área da saúde, com custo de financiamento em US\$ 58 milhões (EDWARDS E ROY, 2016 *apud* MESQUITA, 2017).

A ausência ou a não conformidade de integridade dos dados eletrônicos não está relacionada apenas às ações de má fé ou má conduta e sim, muitas vezes, por falhas encontradas por ações não intencionais, ou seja, quando não há a intenção de se violar ou fraudar dados (LEONARDI, 2018).

Existem muitos componentes que podem favorecer ações não intencionais e trazer riscos à integridade dos dados eletrônicos de uma organização, tais como: erro humano devido à ausência de conhecimento, erro de transferência de dados, equipamentos mal calibrados ou mantidos, sistemas computadorizados que foram ou são configurados em modo padrão, ausência de controles de acesso, hardwares antigos sem garantia dos fabricantes, sistemas operacionais e softwares sem atualização e suporte dos fabricantes, vírus, ataques cibernéticos, entre outros (GUERRA, 2020).

Instituições da área da saúde que utilizam sistemas computadorizados e realizam, dentro dos seus processos de trabalho, alguma atividade essencial dentro do ciclo de vida de medicamentos, vacinas e kits de diagnósticos, desde a área de pesquisa, passando por estudos pré-clínicos e clínicos, produção, controle de qualidade até a área de armazenamento e distribuição, precisam garantir a confiabilidade na qualidade e a integridade de dados eletrônicos gerados e a reprodutibilidade das atividades (BRASIL, 2010).

Neste sentido, a Fiocruz como uma instituição estratégica de Estado e com atuação importante no processo técnico-científico e produtivo, deve garantir a manutenção dos dados e registros eletrônicos íntegros (LIMA et al., 2018).

Erros graves na fabricação de medicamentos ou até mesmo falhas em pesquisas científicas, por exemplo, podem ocorrer devido a falhas no controle de gestão dos dados, colocando em risco o sistema por não desempenhar a função para qual foi criado, e conseqüentemente, gerar danos na cadeia produtiva e inovativa, com impacto na saúde e no bem-estar dos indivíduos (WHO, 2016).

Tais danos podem incluir desde medicamentos adulterados, ensaios clínicos com resultados não confiáveis, até falhas no processo de produção e controle de qualidade, além da possibilidade de fraudes e de sabotagem, quando dados importantes podem ser adulterados propositadamente (IVAMA, 2005).

A violação da integridade de dados deve ser seriamente considerada, pois apresenta grande risco podendo, inclusive, impactar na qualidade, eficácia e segurança de produtos ou a condução das pesquisas científicas (LEONARDI & MATOS, 2020).

Segundo PIC/S (2018), a integridade de dados é definida como a extensão em que todos os dados são completos, consistentes e precisos, durante todo o ciclo de vida dos dados e é fundamental em um sistema de gestão da qualidade.

A integridade da pesquisa deve ser um valor absoluto tanto para as instituições envolvidas com essas atividades nas pesquisas científicas como para os pesquisadores individuais (ACADEMIA BRASILEIRA DE CIÊNCIAS, 2013).

Neste contexto, a adoção de princípios e diretrizes em ações de integridade de dados eletrônicos nas diferentes esferas da Fiocruz, assim como, compreender práticas relacionadas à integridade de dados e registros gerados eletronicamente e mantidos durante todo o seu ciclo de vida nas atividades de laboratório de pesquisa científica experimental faz-se necessário e pertinente para que orientações institucionais sejam elaboradas no intuito de auxiliar e fomentar a participação dos laboratórios e ainda promover melhoria nas práticas já existentes.

4. REFERENCIAL TEÓRICO E NORMATIVO

4.1 GESTÃO DA QUALIDADE

O termo qualidade, dentre várias definições existentes, pode ser conceituado na era contemporânea como adequado ao uso, de modo a atender aos requisitos e percepções dos consumidores (PALADINI, 2019 & FERNANDES, 2011).

Durante a Primeira Guerra Mundial (1914-1918), a qualidade era fundamentada nas características físicas e na inspeção do produto com ênfase na detecção de defeitos. E desde então, a qualidade vem obtendo uma importância crescente no âmbito mundial (FERNANDES, 2011).

A partir da Segunda Guerra Mundial (1939-1945), técnicas estatísticas e de amostragem foram incorporadas ao processo de avaliação dos produtos, possibilitando assim o diagnóstico de defeitos aleatórios ou sistemáticos. Esse período com ênfase no processo ficou conhecido como a era do controle estatístico da qualidade (FERNANDES, 2011 & LOBO, 2020). Essa era foi impulsionada por Walter Shewhart com o desenvolvimento da carta de controle estatístico de processo (FERNANDES, 2011; SHEWHART, 1931).

Mais tarde, na década de 50, dois nomes tornaram-se notoriamente importantes para a qualidade. O primeiro, William Edwards Deming, estatístico especialista em qualidade com diversos trabalhos desenvolvidos nos Estados Unidos, revolucionou o processo da qualidade no Japão com diferentes métodos estatísticos. O segundo, Joseph Moses Juran, consultor de gestão da qualidade, introduziu um novo conceito na era do controle de qualidade elevando o tema qualidade para uma abordagem mais estratégica (MARSHALL et al., 2012).

Kaoru Ishikawa, um discípulo de Deming, fomentou as ferramentas de controle estatístico da qualidade integrando e expandindo as ideias do próprio Deming e de Juran (LOBO, 2020). A gestão da qualidade pode ser dividida em três pontos fundamentais conhecidos como a trilogia de Juran: planejamento, controle e melhoria, sendo este último com prioridade para o gestor (MARSHALL et al., 2012).

Com o advento da globalização houve necessidade de uniformizar as questões relativas aos sistemas de gestão da qualidade adotados por diferentes países (FERNANDES, 2011). E assim, na década de 1970, foi criada pela *International Organization for Standardization* (ISO) – uma organização internacional de normalização, um comitê técnico 176 (do inglês *Technical Committee - TC 176*) para tratar ações referentes à gestão e garantia da qualidade. Desde então,

diversas edições como revisão de normas e diretrizes foram difundidas no âmbito da gestão da qualidade (FERNANDES, 2011).

No Brasil, somente no final da década de 80, é que a adoção de normas internacionais de sistemas de gestão da qualidade teve maior impacto, onde as organizações passaram a desenvolver novas competências e habilidades (CARPINETTI & GEROLAMO, 2019).

4.1.1 Gestão da qualidade na saúde

A adoção das boas práticas de gestão da qualidade nos diferentes serviços de saúde é uma decisão estratégica das organizações e requer uma abordagem de gestão moderna (BÁO et al., 2018).

A qualidade nos serviços de saúde pode ser entendida, de acordo com Las Casas (1999), em quatro dimensões: i) segurança – propriedade em que clientes esperam dos prestadores de serviços a habilidade de transmitir segurança e confiança; ii) confiabilidade – propriedade importante na prestação de serviços de qualidade, podendo ser gerada pela habilidade de entregar o que foi prometido de forma segura e precisa; iii) empatia – propriedade em cuidar e ser atencioso com os clientes, tendo a capacidade de se colocar no lugar dos outros, além de ser receptível e ajudar os clientes; e iv) aspectos tangíveis – propriedade de dar importância a fatores como influência, instalações, equipamentos, aparência dos funcionários, entre outros, para aspectos físicos que cercam a atividade de prestação de serviço.

A qualidade na saúde teve seu pioneirismo em 1854 com a enfermeira inglesa Florence Nightingale quando implantou, no hospital Scutari da Criméia, rígidos padrões sanitários reduzindo as taxas de mortalidade. Na área da saúde esse feito foi considerado o primeiro modelo de melhoria contínua da qualidade em saúde tendo como base dados estatísticos (WEBER, 2012).

No Brasil, o movimento por qualidade iniciou-se somente em 1930, em São Paulo, através de Odair Pedroso, que criou a Ficha de Inquérito Hospitalar para a Comissão de Assistência Hospitalar do Ministério da Saúde (MS). Na história da área laboratorial, foi fundada em 1944 a Sociedade Brasileira de Patologia Clínica/Medicina Laboratorial (SBPC/ML) com o objetivo de estabelecer padrões para os diferentes exames laboratoriais (WEBER, 2012).

Publicação de portarias e normas na área da qualidade e avaliação hospitalar ocorre desde a década de 70 pelo MS e se faz presente na implantação de um sistema ativo de controle à assistência na área da saúde. O MS lançou, em 1994, o programa de qualidade para promover

a cultura da qualidade na saúde e constituiu a Comissão Nacional de Qualidade e Produtividade em Saúde (CNQPS) que atuou na elaboração de diretrizes do programa (FELDMAN et al. 2004).

4.1.2 Gestão da qualidade em laboratórios de pesquisa em saúde: a importância das boas práticas na pesquisa científica

A pesquisa científica é entendida como toda investigação original que tem por finalidade favorecer a constituição da ciência e que possui, dentro da atividade científica, toda ação que objetiva a concepção e realização de pesquisas científicas, a comunicação dos resultados, o intercâmbio científico entre pesquisadores e a orientação de processos na formação de pesquisadores (LAFER et al. 2014).

A atividade de pesquisa tem intrinsecamente a confiança como pilar e que deve estar relacionada entre pesquisadores e os dados levantados e compartilhados por seus colegas da comunidade científica (ACADEMIA BRASILEIRA DE CIÊNCIAS, 2013).

Já a atividade científica, entende-se como sendo as atividades que vão desde a concepção da ideia e levantamento da hipótese, passando pelo desenvolvimento de pesquisas científicas, pela divulgação de seus resultados e sua interação com a comunidade científica (LAFER et al, 2014).

Profissionais que atuam na função de pesquisador, bem como estudantes, precisam se orientar sobre boas práticas em pesquisa. A Fiocruz, através da portaria 966/2016-PR, orienta os pesquisadores da instituição em relação as melhores práticas da qualidade com objetivo de apoiar o processo investigativo e criativo no campo da pesquisa científica (BARBOSA, 2016).

A adoção de boas práticas na pesquisa científica é indispensável visando o bom andamento da pesquisa, considerando a garantia de produzir dados com confiabilidade e reprodutibilidade (BARBOSA, 2016).

A Fiocruz adota documentos que definem critérios importantes e fundamentais para subsidiar as pesquisas científicas institucionais, tais como:

- Manual: Práticas de Qualidade na Pesquisa Biomédica Básica (CPqRR, 2010), que enfoca nas práticas da qualidade em pesquisa biomédica básica para um sistema de gestão da qualidade não regulatório;
- Código de Boas Práticas Científicas (LAFER et al, 2014)., que constitui diretrizes éticas para as atividades científicas.

Durante a atividade científica, dados científicos e informações coletadas são tratados como evidência potencial e são necessários para validarem os resultados da pesquisa. Estes dados devem ser devidamente atribuíveis, confiáveis e reprodutíveis (LEONELLI, 2015). Além disso, os dados científicos gerados e coletados devem ser registrados de forma legível e permanente, bem como de forma contemporânea, original onde o registro inclua a primeira ou a captura de dados ou informações e todos os dados subsequentes necessários para reconstrução total da conduta da atividade, além de garantir a precisão dos resultados e registros (LEONELLI, 2015).

Estes adjetivos contribuem com as boas práticas na pesquisa científica e consequentemente para o avanço da ciência.

Nos últimos anos, a temática qualidade na pesquisa em saúde tem sido destaque em revistas científicas. Fato esse justificado pela ausência de qualidade no dado adquirido, falta de reprodutibilidade e tratamento inadequado do dado em diversos trabalhos, evidenciando, assim, a necessidade de uma ação imediata em ambientes laboratoriais de pesquisa (RIEDL & DUNN, 2013; BAERLOCHER et al., 2010).

Segundo Riedl & Dunn (2013), existem quatro pilares da qualidade dos dados, a saber:

- (i) Rastreabilidade: busca a descrição completa dos métodos e insumos utilizados na pesquisa, e que os dados brutos estejam íntegros e disponíveis adequadamente;
- (ii) Precisão: baseada na consistência do método experimental escolhido pelo pesquisador a partir de princípios científicos sólidos e na análise do dado com estudo estatístico adequado;
- (iii) Clareza/integridade: compreende documentos, desenho do estudo, métodos e resultados claros e consistentes; e
- (iv) Pontualidade: objetiva criar contemporaneidade do registro no momento da atividade de pesquisa.

Os princípios de integridade científica – honestidade, confiabilidade, objetividade, imparcialidade, cuidado, respeito, veracidade, justiça e responsabilidade – ressaltam que o perfil profissional do pesquisador, desde os primeiros passos rumo à sua jornada de cientista, deve ser construído sob estes fundamentos e, que, estes princípios devem ser intrínsecos ao contorno da instituição que se propõe a realizar pesquisa (ACADEMIA BRASILEIRA DE CIÊNCIAS, 2013).

Em 06 de março de 2020, a Fiocruz, mediante a Portaria nº 5.318, instituiu o Guia de Integridade em Pesquisa da Fiocruz com a finalidade de orientar a atuação de profissionais que atuam na função de pesquisador, dos pesquisadores visitantes e dos estudantes, sobre as boas práticas em pesquisa nos projetos realizados e financiados pela instituição e as complexas questões relacionadas com a pesquisa científica e a divulgação de seus resultados (LIMA, 2020).

Neste contexto, os documentos (procedimentos, projetos e relatórios) precisam ser submetidos à análise em conformidade com essas premissas básicas e um processo de auditoria pode ser um mecanismo de qualidade compactuado para caracterizar este atendimento (VOLSEN & MASSON, 2009).

4.1.3 Aspectos éticos na pesquisa em saúde

Para Elias et al., (2018), o respeito, a honestidade e a beneficência são princípios formadores da ética que permeiam a reflexão sobre a moralidade e o caráter, além de nos cercar a todo momento, em todos os campos do conhecimento.

Características como honestidade intelectual, objetividade e imparcialidade, veracidade, justiça e responsabilidade, devem ser conduzidas por cientistas durante as etapas de concepção, proposição e realização de pesquisas, na comunicação dos resultados e entre cooperações e tutorias com demais pesquisadores (LAFER et al, 2014).

A ciência é um instrumento eficaz para a ampliação do conhecimento humano nas diversas dimensões. Tem nos preceitos éticos, a construção e a apropriação coletivas da ciência e, para os cientistas, em seus princípios fundamentais, o dever de exercer sua profissão da maneira mais correta para que então desta resulte a melhor contribuição para o avanço da ciência (LAFER et al., 2014).

A preocupação com relação à ética e à integridade nas pesquisas científicas vem desde 1980, quando inúmeros casos de fraudes nas instituições de pesquisa foram descobertos, com maior ênfase nos Estados Unidos da América (EUA). Já no Brasil, esta preocupação referente ao tema é fato recente (ELIAS et al., 2018).

Na história das ciências a desonestidade não é um fato recente e sim um fenômeno antigo que apresentou ser um problema com maior evidência com o advento da globalização e o desenvolvimento tecnológico que tanto propiciaram quanto dificultaram a desonestidade na ciência (LINS, 2014).

A preocupação com relação à ética e à integridade nas pesquisas científicas vem desde 1980, quando inúmeros casos de fraudes nas instituições de pesquisa foram descobertos, com maior ênfase nos Estados Unidos da América (EUA). Já no Brasil, esta preocupação referente ao tema é fato recente (ELIAS et al., 2018).

Na história das ciências a desonestidade não é um fato recente e sim um fenômeno antigo que apresentou ser um problema com maior evidência com o advento da globalização e o desenvolvimento tecnológico que tanto propiciaram quanto dificultaram a desonestidade na ciência (LINS, 2014).

A retratação, dentro do campo científico, é vista como um fenômeno reprovável e que vem crescendo ao longo dos últimos anos porque as práticas editoriais estão cada vez melhores e os editores sendo incentivados pelas revistas a levar este fenômeno a sério (BRAINARD & YOU, 2018).

Para Azoulay et al. (2017), quando um cientista tem um dos seus artigos retratados, todo o trabalho anterior dele se modifica, contribuindo para uma queda de 10% em média na taxa de citação de seus artigos anteriores não retratados.

A retratação causa um declínio imediato, grave e duradouro em futuras citações (AZOULAY et al., 2012). Na comunidade científica, onde a reputação funciona como uma moeda, as consequências decorrentes de retratações são sobretudo importantes (PARTHA & DAVID, 1994 apud AZOULAY et al., 2017).

Em 1987, o importante cientista Charles Glueck – conhecido por estudos sobre o papel do colesterol nas doenças cardíacas, teve seu artigo retirado da revista *Pediatrics*. O *National Institutes of Health* (NIH) censurou o cientista por má conduta científica e por adulterar dados. O cientista que era, até o momento, autor de 200 publicações e que havia recebido mais de 10.000 citações, teve que renunciar ao cargo na Faculdade de Medicina da Universidade de Cincinnati e nunca mais recebeu financiamento do NIH (ALTMAN, 1987).

Recentemente, um novo evento envolvendo retratação em artigo científico veio ao conhecimento público. No dia 04 de junho de 2020, a revista científica “*The Lancet*”, comentou em seu site a retratação do artigo *Hydroxychloroquine or chloroquine with or without a macrolide for treatment of COVID-19: a multinational registry analysis*, que, após sua publicação, recebeu diversas preocupações do meio científico com relação à integridade dos dados e análises conduzidas na pesquisa (MEHRA et al., 2020). O artigo, assim que foi publicado, interrompeu os testes globais de hidroxicloroquina para o Covid-19 por causa do medo de aumento de mortes (BOSELEY & DAVEY, 2020).

Segundo MEHRA et al. (2020), a revista solicitou uma revisão independente por pares com objetivo de avaliar a origem dos elementos do banco de dados, confirmar a integridade do banco de dados e replicar as análises apresentadas no artigo. Como a revisão por pares não foi atendida, devido à não disponibilização do banco de dados, a garantia da integridade das fontes de dados primárias não pôde ser confirmada, contribuindo para a retratação do artigo.

4.1.4 Reprodutibilidade da pesquisa em saúde

Para WHO/IRR (2006), reprodutibilidade é o modo de testar a confiabilidade dos dados através do processo de repetição do experimento, sob condições semelhantes em que o próprio investigador ou terceiros geraram os dados originais.

A reprodutibilidade também pode ser entendida quando a medição pode ser obtida com precisão declarada por uma equipe diferente, um sistema de medição diferente, em um local diferente mediante várias tentativas (ASSOCIATION FOR COMPUTING MACHINERY, 2016).

A ciência vem sendo posta em dúvida devido ao crescente número de não reprodutibilidade de resultados de pesquisa e vem merecendo atenção especial da comunidade científica e da sociedade nos últimos anos (NASSI-CALÒ, 2014).

Segundo Nassi-Calò (2016), a confiabilidade e a reprodutibilidade dos resultados são alguns dos pilares da pesquisa científica, pois estudos prévios são a alavanca para o progresso da ciência. Com base no conhecimento adquirido, a ausência de reprodutibilidade é considerada uma falha grave que contribui para pôr em risco a credibilidade da ciência como um todo.

A pesquisa pré-clínica e o desenvolvimento de novos fármacos e tratamentos requerem, como premissa inicial, que os resultados possam ser confirmados através da reprodutibilidade por outros cientistas em diferentes laboratórios (NASSI-CALÒ, 2017).

Neste interim, a reprodutibilidade dos resultados da pesquisa pré-clínica contribui para o desenvolvimento de novos medicamentos e tratamentos médicos, o que torna a reprodutibilidade da pesquisa em saúde o pilar da ciência (eLife, 2017).

Segundo Baker (2016), uma pesquisa realizada *on-line* pela *Nature* sobre reprodutibilidade em pesquisas com 1.576 pesquisadores revelou que mais de 70% deles tentaram reproduzir os experimentos de outros cientistas e falharam, e que mais da metade tentaram reproduzir seus próprios experimentos e não conseguiram.

Já para Nassi-Calò (2014), alguns fatores contribuem para a baixa confiabilidade das pesquisas, entretanto, a má conduta científica parece ser menor em relação a questões que

incluem treinamento insuficiente de pessoal técnico e pesquisadores. A baixa reprodutibilidade em pesquisa é apontada devido a protocolos mal elaborados, testes estatísticos inadequados e baixo número de amostras.

Já na Fiocruz, o tema ética e reprodutibilidade na pesquisa fortalece a relação do estudo com as áreas de pesquisa, ensino e desenvolvimento tecnológico e possui alinhamento com a seguinte diretriz e tese do relatório final do VIII Congresso Interno da Fiocruz:

Diretriz 18 (T3) - Traçar estratégias de enfrentamento da crise de reprodutibilidade na pesquisa, fortalecer as políticas institucional e nacional de uso de biomodelos experimentais e a formação de pessoal qualificado e garantir investimentos para assegurar o bem-estar animal, a preservação da vida, a ética e a aplicação de boas práticas, além do desenvolvimento e emprego de métodos alternativos ao uso de animais, sempre que possível, em alinhamento com o conceito dos 3Rs (LIMA et al., 2018).

Trabalhar a ética e ações que garantam a reprodutibilidade na pesquisa é indispensável para assegurar a confiança e a integridade dos dados científicos gerados.

4.2 GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

A literatura sobre a trajetória da TI, desde seu surgimento, revela a sua influência contemporânea na vida das organizações – públicas ou privadas – e da sociedade, despontando como um dos maiores campos de pesquisas e discussões das últimas décadas (PACHECO & TAIT (2000).

Na década de 60, segundo Reinhard (1996), a TI tem sua introdução nas empresas ainda com poucas opções tecnológicas (*software* e *hardware*), pouco suporte de ferramentas para processos de construção de aplicativos, com necessidade de metodologias para atendimento a demandas com maior celeridade, automação de rotinas manuais, com escassez de mão-de-obra técnica, entre outras características.

A TI, na década de 70, se incorpora ainda mais na rotina das empresas que passam a considerar o desenvolvimento organizacional através do aumento do impacto dos sistemas, do processo decisório, da adoção de inovações, do estímulo à construção de sistemas de apoio à decisão, entre outras (REINHARD, 1996). Para Brito (1996), esta década representa a era do processamento de dados, onde a TI passou a ser adotada nas empresas como recurso organizacional estratégico.

Na década de 80 as mudanças no ambiente externo das empresas apresentam outras características para a TI, como a terceirização, necessidade de sistemas interorganizacionais e

o desenvolvimento de sistemas atendendo aspectos econômicos, políticos, legais e culturais (REINHARD, 1996). Nesta década a TI exerce um papel ainda mais estratégico para a execução dos negócios nas empresas (BRITO, 1996).

O conhecimento, na década de 90, é utilizado na TI como fonte de geração de valor, proporcionando a transformação dos negócios (REINHARD, 1996).

Neste contexto, a disseminação das NTIC na sociedade vem provocando profundas mudanças em organizações no mundo inteiro e contribuindo para um grande volume de informações produzidas e espalhadas livremente, principalmente pela velocidade proporcionada através da rede mundial de computadores (Internet). Tal evolução tecnológica envolve não somente organizações e pessoas, mas praticamente todas as atividades econômicas, políticas, sociais e culturais em todo o mundo (ALVES, c2021).

O conceito de TI pode ser entendido como a associação de tudo que abarca o processamento, armazenamento e disponibilização de informações, além de envolver diversas tecnologias interligadas e integradas de *software* e *hardware* em conjunto com aspectos organizacionais (PORTER & MILLAR, 1985; KEEN, 1993; ALBERTIN, 2004).

Já para Cruz (2008), a TI é entendida como um conjunto de elementos tecnológicos individuais, como *software*, *hardware*, telecomunicações, entre outras tecnologias que geram ou tratam a informação.

A TI, segundo Davenport e Prusak (1997), é essencial na adoção de uma perspectiva gerencial e fundamental para que organizações consigam desenvolver efetivos processos de gerenciamento da informação, além do seu uso efetivo por parte de pessoas, bem como nos fenômenos políticos que interferem no compartilhamento da informação e do conhecimento.

As práticas de TI em ambientes organizacionais, segundo Marchand et al. (2001), podem ser classificadas em quatro categorias:

- i) Práticas de TI para apoio gerencial;
- ii) Práticas de TI para apoio à inovação;
- iii) Práticas de TI para apoio a processos de negócio; e
- iv) Práticas de TI para apoio operacional.

Neste contexto, a informação é fundamental para a tomada de decisões estratégicas, pois além de possuir um papel importante é um elemento redutor de incertezas no desempenho das organizações (LESCA & ALMEIDA, 1994).

Os dados, a informação e o conhecimento têm grande capacidade de agregar valor a processos, produtos e serviços e são cada vez mais classificados como ativos intangíveis para o alcance da missão e dos objetivos organizacionais (CARUSO & STEFFEN, 1999). Tais ativos, críticos para as organizações, precisam ser protegidos contra ameaças que podem levar à sua destruição, adulteração ou divulgação não autorizada e indisponibilidade temporária.

Ainda, a informação, como um dos bens mais valiosos para qualquer organização, sendo a todo instante criada, utilizada, armazenada, divulgada e compartilhada, faz-se necessário garantir sua disponibilidade, integridade, confidencialidade e autenticidade (VIEIRA, 2014).

4.2.1 Segurança da informação

Segurança da informação (SI) é o processo que visa proteger a informação das ameaças contra a integridade, confiabilidade e disponibilidade (BEAL, 2005). Estes princípios fundamentais são conhecidos como o tripé da segurança da informação que tem em suas referências internacionais a denominação “*CIA-triad*” para os termos *Confidentiality*, *Integrity* e *Availability* (LAI et al., 2017).

Segundo Sêmola (2003), a segurança da informação é definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, sua indisponibilidade e alterações indevidas.

Já para Loureano (2005), as informações são o ativo mais importante para o negócio e a sua proteção é o principal foco da segurança da informação, onde deve ser colocado em prática os requisitos responsáveis pela segurança que são, conforme a NBR/ISO/IEC 27002, a confidencialidade, integridade e disponibilidade.

Proteger de maneira acertada os ativos de informação depende de uma visão clara e pontual das informações que precisam ser preservadas de ameaças por parte das organizações e seus gestores e, assim, buscar soluções de segurança eficazes (BEAL, 2005).

Ainda segundo Beal (2005), controles de segurança com medidas de proteção que sejam capazes de proteger adequadamente dados, informações e conhecimentos, levando-se em conta os riscos reais a que estão sujeitos, precisam ser adotados pelas organizações.

O tripé da segurança da informação é definido como (LAI et al., 2017).:

- i) Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
- ii) Integridade – propriedade de proteção da exatidão e completeza de ativos;

- iii) Disponibilidade – propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

A segurança da informação é padronizada por meio da família de normas ISO/IEC (*International Organization for Standardization/ International Electrotechnical Commission*) 27000, que tem por objetivo a proteção das informações organizacionais e ativos de TI, que contribuem para redução de riscos, otimização dos processos e proteção dos dados em organizações de todos os portes (ABNT NBR ISO/IEC 27001:2013). Dentro da família, as duas normas mais conhecidas são:

- ISO/IEC 27001: modelo focado em determinar, implantar, operar, monitorar, rever, manter e melhorar um Sistema de Gestão da Segurança da Informação;
- ISO/IEC 27002: estabelece o código de práticas para Segurança da Informação.

Neste contexto, a segurança da informação preserva a confidencialidade, a integridade e a disponibilidade da informação através da aplicação de um processo de gestão de riscos e fornece confiança entre as partes interessadas de que os riscos são adequadamente gerenciados.

As organizações – públicas ou privadas – precisam considerar a importância de implementar ações de Segurança da Informação e que estas, além de fazerem parte, estejam integradas com os processos organizacionais e com a estrutura de administração global, além de ser considerada no projeto dos processos, sistemas de informação e controles (ABNT NBR ISO/IEC 27001:2013).

Algumas ferramentas da qualidade podem ser utilizadas para assegurar conformidade com as normas ISO 27000. Uma das principais ferramentas de gestão da qualidade, o ciclo PDCA – também chamado de Ciclo de Deming ou Ciclo de Shewhart – permite a identificação, coordenação e execução de melhorias em processos e em serviços de TI (WERKEMA, 2013).

Resguardar as informações da organização e garantir a continuidade do negócio, considerando o grau de qualidade requerido pela organização, pode ser obtido seguindo a ferramenta da qualidade ciclo PDCA (do inglês, *Plan, Do, Check e Act*, do português, Planejar, Fazer, Verificar e Agir) (BASTOS, 2016).

Segundo Bastos (2016), na estrutura do ciclo PDCA, as atividades podem ser descritas como:

- i) Planejar – estabelecimento de política, objetivos, processos e procedimentos relevantes para o gerenciamento de riscos e melhoria da segurança da informação com objetivo de entregar resultados;
- ii) Fazer – implementar e operar a política de segurança da informação, controles, processos e procedimentos;
- iii) Verificar – avaliar e medir, onde aplicável, o desempenho de um processo em relação à política e aos objetivos da segurança da informação relatando os resultados para a revisão dos superiores;
- iv) Agir – tomar as ações corretivas e preventivas de acordo com os resultados de auto auditoria e autoinspeção ou outra informação pertinente, para alcançar a melhoria contínua da segurança da informação.

Um dos elementos importantes no ciclo PDCA é a auditoria onde torna-se base para autoavaliação da capacidade de atendimento a requisitos das partes interessadas, como na qualidade, no meio ambiente, na segurança e na saúde (MORETTO, c2016).

A Norma Brasileira ISO 19011:2002 conceitua auditoria como o processo sistemático, documentado e independente com objetivo de obter evidências através de registros, apresentação de fatos entre outros, e avaliá-las se são atendidos dentro dos critérios da auditoria (MORETTO, c2016).

Portanto, é indispensável o processo de auditoria na gestão da segurança da informação, pois é através deste processo que se consegue manter a conformidade com a política de segurança aprovada pelos gestores responsáveis.

Segundo Loureno (2005), verificar se os requisitos para a segurança da informação estão implementados de maneira satisfatória é um dos objetivos da auditoria, pois contribuirá em manter a segurança nos dados da instituição, além de verificar se os ativos estão sendo protegidos corretamente.

4.3 INTEGRIDADE DE DADOS

Integridade é definida como o exercício de ser honesto, mostrar ser intransigente e ter fortes princípios e valores éticos e morais, sendo uma escolha pessoal defender-se a padrões morais e éticos consistentes (SBCOACHING, 2018).

Na pesquisa, o termo integridade refere-se aos deveres éticos, que os cientistas devem praticar ao realizarem pesquisas científicas (SANTOS, 2011).

Dados, num sentido mais técnico, são um conjunto de valores de variáveis qualitativas ou quantitativas sobre uma ou mais pessoas ou objetos, enquanto dado (no singular) é um valor único de uma única variável (FURNER, 2016).

Nos tratamentos acadêmicos, os dados são simplesmente unidades de informação. Os dados são empregados em pesquisa científica, gerenciamento de negócios, finanças, governança e em praticamente todas as outras formas de atividade organizacional humana (FURNER, 2016).

Dados também são definidos pela MHRA (*Medicines and Healthcare products Regulatory Agency*) como sendo informações derivadas de dados brutos e o termo pode ser explicado pela diferença entre dados brutos e metadados, conforme Tabela 1.

Tabela 1: Dados brutos *versus* metadados

Dados brutos	Metadados
São os registros e a documentação originais, mantidos no formato em que foram originalmente gerados, podendo ser em papel ou eletrônicos e devem ser registrados de maneira contemporânea e precisa por meios permanentes. Em situações de uso de equipamentos eletrônicos básicos, como um medidor de pH ou uma balança, que não armazenam dados eletrônicos ou fornecem apenas uma saída de dados impressos, a impressão constitui os dados brutos.	São os dados que fornecem contexto e significado e descrevem os atributos de outros dados. Normalmente, os metadados descrevem a estrutura, elementos de dados, interrelações e outras características dos dados, permitindo, também, que os dados sejam atribuíveis a um indivíduo. Sem o contexto fornecido pelos metadados os dados não têm significado, como exemplificado abaixo: <i>Dado: 3.5</i> <i>Metadados, fornecendo contexto e significado ao dado acima (texto em itálico):</i> <i>Sujeito do estudo Z123, amostra ref. Y567 tirada em 15/10/17 às 195hrs.</i> <i>3,5 mg. Analista: B Carvalho 16 / Out / 17</i>

Fonte: Adaptado de MHRA, 2018.

Já o tema integridade de dados, segundo Lopez (2014), é a certeza da propriedade em que os dados não foram alterados de maneira não autorizada e que sua abrangência contempla desde o armazenamento, passando o processamento até durante o transporte.

Neste contexto de integralidade e confiabilidade de dados, o tema é um dos problemas de maior relevância da atualidade, pois chega ao fundamento do relacionamento entre a área da saúde e as agências reguladoras (ARAUJO, 2020; COSGROVE, 2014).

Nos últimos anos, houve um crescimento significativo do número de cartas de advertência emitidas pelo FDA USA, como também notificações de preocupação da OMS e de

declarações de não conformidade da Agência Europeia de Medicamentos (da sigla em inglês, EMA – *European Medicines Agency*) aonde informações falsas ou enganosas foram identificadas durante inspeções regulatórias em indústrias farmacêuticas e em fornecedores pertencentes à cadeia de suprimentos (PÉREZ, 2017).

As falhas identificadas nas inspeções regulatórias se aplicam igualmente aos dados em papel e eletrônicos no gerenciamento inadequado da integridade de dados e surgem do controle sistemático ineficaz dos sistemas de gerenciamento de dados devido à falta de conhecimento, de dados intencionalmente falsificados, ocultos ou enganosos, assim como ausência de cuidado no trabalho (WHO, 2016).

Outra razão, segundo MHRA (2018), está relacionada aos sistemas informatizados, que de acordo com o desenvolvimento contínuo de tecnologias de suporte, como o uso crescente de captura eletrônica de dados, introduziram outra modalidade de falha na integridade de dados, a eletrônica que está distribuída por diferentes campos e áreas de um sistema informatizado.

As definições de integridade de dados, segundo várias fontes reguladoras estão descritas na Tabela 2.

Tabela 2: Definição de integridade de dados segundo várias fontes

Fonte	Definição
FDA (USA)	Refere-se à integridade, consistência e precisão dos dados onde dados completos, consistentes e precisos devem ser atribuíveis, legíveis, contemporâneos, original ou cópia verdadeira e acurada (ALCOA) (FDA, 2018).
WHO	Refere-se ao grau em que os dados são completos, consistentes, precisos, autênticos e confiáveis e que essas características dos dados são mantidas durante todo o ciclo de vida dos dados. Os dados devem ser coletados e mantidos de forma segura, de modo que sejam atribuíveis, legíveis, contemporaneamente registrados, originais ou uma cópia verdadeira e acurada (ALCOA) (WHO, 2016).
PIC/S	Refere-se à extensão em que todos os dados estão completos, consistentes e precisos ao longo do ciclo de vida dos dados e que devem satisfazer aos princípios do ALCOA + (PIC/S, 2018).
MHRA	Refere-se ao grau em que os dados são completos, consistentes, precisos e confiáveis e que essas características são mantidas durante todo o ciclo de vida dos dados, devendo ser coletados e mantidos de maneira segura, para que sejam atribuíveis, legíveis, gravados contemporaneamente, originais (ou uma cópia fiel) e acurados (ALCOA) (MHRA, 2018).

Fonte: Elaboração própria a partir de (FDA, 2018; WHO, 2016; PIC/S, 2018; MHRA, 2018)

A primeira diretriz (21 CFR Part 11) abordando indiretamente o tema integridade de dados foi publicada em 1963 pela FDA e, desde então, a União Europeia (UE) e a FDA publicaram inúmeras diretrizes sobre vários tópicos relacionados à integridade de dados com objetivo de garantir que a indústria farmacêutica capturasse dados precisos durante o ciclo de vida de desenvolvimento de medicamentos (RATTAN, 2018).

No Brasil, com a criação da Agência Nacional de Vigilância Sanitária (ANVISA) em 1999, essa autarquia começou a regular e fiscalizar todas as áreas diretamente relacionadas à saúde no país, especialmente as indústrias farmacêuticas e de seus processos.

Com o estabelecimento da ANVISA, o objetivo era induzir as indústrias locais na adoção de práticas regulatórias em harmonia com o ambiente regulatório mundial, conferindo-lhes a responsabilidade de controle de qualidade de seus produtos e cumprimento das Boas Práticas de Fabricação (BPF) através da criação e execução de regulamentações.

Em 2001, a ANVISA publicou para o setor regulado a Resolução da Diretoria Colegiada (RDC) nº 134 contendo o Regulamento Técnico das BPF de Medicamento, que incorporava os princípios contidos no documento da OMS (BRASIL, 2001).

Posteriormente, outras resoluções foram publicadas pela ANVISA, tais como:

- RDC nº 210/2003, que aprovou e atualizou as BPF determinando em seu Guia as exigências mínimas para validação de processos, metodologia analítica, procedimentos de limpeza e qualificação de fornecedores;

- RDC nº 249/2005, que estabelece sobre o Regulamento Técnico das BPF de Produtos Intermediários e Insumos Farmacêuticos Ativos (IFA);
- RDC nº 204/2006, que estabelece sobre o Regulamento Técnico de Boas Práticas de Distribuição (BPD) e Fracionamento de Insumos Farmacêuticos;
- RDC nº 67/2007, que estabelece sobre as Boas Práticas de Manipulação de Preparações Magistrais e Oficiais para Uso Humano em farmácias;
- RDC nº 17/2010, que alterou e agregou outros temas ao texto da primeira RDC (210/2003), além de ter incorporado em sua abrangência os medicamentos destinados a ensaios clínicos. Esta RDC é baseada nos conceitos da OMS, que sofreu três revisões, e a Anvisa não as acompanhou.

Atualmente, a legislação vigente da ANVISA é a RDC nº 301, publicada em 2019, fruto da formalização de se tornar membro do PIC/S (Esquema de Cooperação de Inspeção Farmacêutica, em inglês, *Pharmaceutical Inspection Co-operation Scheme*) (BRASIL, 2019).

Esta resolução, aprovada no dia 21 de agosto de 2019 como revisão da RDC nº 17/2010, aborda um novo marco regulatório de BPF mediante a internalização de um conjunto de guias de Boas Práticas de Fabricação de medicamentos do PIC/S, cuja norma já é adotada por 47 países (DOU, 2019).

A associação da ANVISA ao PIC/S resultou, além da RDC 301, na publicação da Instrução Normativa (IN) nº 43 de 21 de agosto de 2019, que tinha como objetivo adotar as diretrizes de BPF relacionadas aos sistemas computadorizados do PIC/S, como requisitos complementares a serem seguidos na fabricação de medicamentos em adição às Diretrizes Gerais de BPF de Medicamentos (BRASIL, 2019).

Segundo Lopes (2019), a revisão da RDC 17/2010 e associação da ANVISA ao PIC/S aumentarão o nível de exigências em dois sentidos: em toda a cadeia produtiva de medicamentos e no conhecimento técnico dos inspetores de campo para realização de auditorias.

Essa associação permitirá ao Brasil expandir as exportações de medicamentos, pois estará implícito que os produtos fabricados no país estarão de acordo com altos e mais recentes padrões de qualidade disponíveis no mercado internacional, tornando-os mais competitivos dentro e fora do país.

O tema integridade de dados é tratado tanto na RDC 301/2019 quanto na IN nº 43/2019 com regras claras e direcionadas para o setor farmacêutico abordando a gestão da documentação

como parte essencial do sistema de garantia de qualidade, sendo fundamental para operar em conformidade com os requisitos das Boas Práticas de Fabricação (LOPES, 2019).

Desde a publicação pela FDA em 1963, vários regulamentos foram escritos e implementados por outras agências reguladoras ao longo das últimas cinco décadas. Segundo Rattan (2018), a integridade de dados fez parte diretamente desses regulamentos a partir de 2015, compondo as atividades de Boas Práticas – clínicas, de fabricação, de controle de qualidade, de distribuição, de laboratório entre outras (BPx), conforme pode ser observado na Tabela 3.

Tabela 3: Lista cronológica de regulamentos

Ano	Agência	Descrição	
1963	FDA USA	1.	21 CFR Part 133, alterado em 1975 para as atuais Parts 210 e 211
1973	FDA USA	2.	21 CFR Part 610 <i>General Biological Products Standards</i>
1975	FDA USA	3.	21 CFR Part 201 <i>Labeling</i>
		4.	21 CFR Part 202 <i>Prescription Drug Advertising</i>
1978	FDA USA	5.	21 CFR Part 58 <i>Good Laboratory Practice for Nonclinical Laboratories Studies</i>
		6.	21 CFR Part 210 <i>cGMP in Manufacturing, Processing, or Holding of Drugs; General</i>
1993	FDA USA	7.	<i>Inspection of Pharmaceutical Quality Control Laboratories</i>
1996	FDA USA	8.	21 CFR Part 820 <i>Quality System Regulation</i>
1997	FDA USA	9.	21 CFR Part 11
	OECD	10.	<i>OECD Principles of Good Laboratory Practices</i>
1999	FDA USA	11.	21 CFR Part 203 <i>Prescription Drug Marketing</i>
2001	ANVISA	12.	RDC nº 134 – dispõe sobre o Regulamento Técnico das BPF de Medicamento, que incorporava os princípios contidos no documento da OMS
2002	FDA USA	13.	<i>7356.002 Compliance Program Guidance Manual Program</i>
2003	FDA USA	14.	<i>Electronic Records; Electronic Signatures – Scope and Application, 21 CFR Part 11</i>
	FDA USA	15.	<i>Pharmaceutical cGMPs for the 21st Century – A Risk-Based Approach; Second Progress Report and Implementation Plan</i>
	EU	16.	<i>Good Manufacturing Practice in respect of Medicinal Products for Human Use and Investigational Medicinal Products for Human Use, 2003/94/EC</i>
	ANVISA	17.	RDC nº 2010, aprovou e atualizou as Boas Práticas de Fabricação
2004	FDA USA	18.	<i>Pharmaceutical cGMPs for the 21st Century – A Risk-Based Approach</i>
2005	ISPE	19.	<i>GAMP Good Practice Guide, A Risk-Based Approach to Compliant Electronic Records and Signatures</i>
	ANVISA	20.	RDC nº 249 – Dispõe sobre o Regulamento Técnico das BPF de Produtos Intermediários e Insumos Farmacêuticos Ativos (IFA)
2006	ICH	21.	<i>Q10 Pharmaceutical Quality System</i>
	FDA USA	22.	<i>Quality Systems Approaches to Pharmaceutical cGMP Regulations, 21 CFR Parts 210 and 211</i>
	WHO	23.	<i>Validation of Computerized Systems Technical Report Series, No. 937</i>
	ANVISA	24.	RDC nº 204 – Dispõe sobre o Regulamento Técnico de Boas Práticas de Distribuição (BPD) e Fracionamento de Insumos Farmacêuticos
2007	PIC/S	25.	<i>Good Practices for Computerized Systems in Regulated “GxP” Environments PI 011-3</i>
	ANVISA	26.	RDC nº 67 – Dispõe sobre as Boas Práticas de Manipulação de Preparações Magistrais e Oficiais para Uso Humano em farmácias
	FDA USA	27.	<i>Computerized Systems Used in Clinical Investigations</i>

	PIC/S	28.	<i>Inspection of Pharmaceutical Quality Control Laboratories</i>
2008	FDA USA	29.	<i>CGMP for Phase I Investigational Drugs, 501(a)(2)(B)</i>
	ANVISA	30.	RDC nº 69/2008 - Dispõe sobre as Boas Práticas de Fabricação de Gases Medicinais
2009	ANVISA	31.	RDC nº 63/2009 - Dispõe sobre Boas Práticas de Fabricação de Gases Medicinais
2010	FDA USA	32.	<i>Data Integrity Inspection Focus</i>
	FDA USA	33.	<i>Compliance Program Guide. 7346.832 Pre-approval Inspections, Chapter 46, New Drug Evaluation</i>
	ANVISA	34.	RDC nº 9/2010 - Altera dispositivos da RDC nº 69, de 1º de outubro de 2008, que dispõe sobre as Boas Práticas de Fabricação de Gases Medicinais.
		35.	RDC nº 17/2010 - Dispõe sobre as Boas Práticas de Fabricação de Medicamentos
2012	ORA USA	36.	<i>ORA Quality Manual</i>
2013	ANVISA	37.	RDC nº 13/2013 - Dispõe sobre Boas Práticas de Fabricação de Produtos Tradicionais Fitoterápicos
2015	MHRA	38.	<i>MHRA GMP Data Integrity Definitions and Guidance for Industry</i>
	MHRA	39.	<i>MHRA GMP Data Integrity, Part I, 25th June</i>
	MHRA	40.	<i>MHRA GMP Data Integrity, Part II 14th July</i>
	MHRA	41.	<i>MHRA GMP Data Integrity, Part III 27th August</i>
	WHO	42.	<i>WHO Draft Guidance on Good Data and Record Management Practices</i>
	FDA USA	43.	<i>Current Good Manufacturing Practice Requirements for Combination Products, 21 CFR Part 4</i>
	FDA USA	44.	<i>Current Good Manufacturing Practice for Finished Pharmaceuticals, 21 CFR Part 211</i>
	ANVISA	45.	RDC nº 33/2015 - Altera a RDC nº 17/2010
2016	FDA USA	46.	<i>Data integrity and Compliance With cGMP</i>
	WHO	47.	<i>50th Technical Report Expert Committee on Specifications for Pharmaceutical Preparations – Annex 05 Guidance on Good Data and Record Management Practices</i>
2018	MHRA	48.	<i>MHRA GXP Data Integrity Guidance and Definitions; Revision 1</i>
	PIC/S	49.	<i>Good Practices for Data Management and Integrity in Regulated GMP-GDP Environments PI 041-1 (Draft 3)</i>
	FDA USA	50.	<i>Data Integrity and Compliance with Drug CGMP Questions and Answers Guidance for Industry</i>
2019	ANVISA	51.	RDC nº 301 – Dispõe sobre as Diretrizes Gerais de Boas Práticas de Fabricação de Medicamentos
		52.	IN nº 43 – Dispões sobre as Boas Práticas de Fabricação complementares aos sistemas computadorizados utilizados na fabricação de Medicamentos

Fonte: Adaptado de RATTAN, 2018 e Regularização de Empresas – Medicamentos (ANVISA)

É notório que o tema integridade de dados, com base na tabela 3, não se trata de uma nova expectativa regulatória, mas que vem sendo atualizados regularmente e conscientizando, desde o início, os dados, suas modificações e sobre questões importantes que garantam a integridade de dados (RATTAN, 2018).

Agências como FDA, WHO e MHRA usam o acrônimo ALCOA para definir suas expectativas com relação aos dados. Já o PIC/S acrescentou ao acrônimo ALCOA o termo “Plus” ou “+” como referência à extensão em que todos os dados estão completos, consistentes

e precisos ao longo do ciclo de vida dos dados. A tabela 4 mostra as características do acrônimo ALCOA+.

Tabela 4: Acrônimo ALCOA+ (*Plus*)

Termo ALCOA+	Característica em inglês	Característica em português
A	<i>Attributable</i>	Atribuíveis
L	<i>Legible</i>	Legíveis
C	<i>Contemporaneous</i>	Contemporâneos
O	<i>Original</i>	Originais
A	<i>Accurate</i>	Acurados
+	<i>Complete</i>	Completo
	<i>Consistent</i>	Consistente
	<i>Enduring</i>	Duradouro
	<i>Available</i>	Disponível

Fonte: Elaboração própria a partir de PIC/S (2018).

Segundo MHRA (2018), não há diferença nas expectativas, independentemente de qual sigla é utilizada, pois as medidas de governança de dados devem garantir que os dados sejam atribuíveis, legíveis, contemporaneamente registrados, originais ou cópia verdadeira e acurados, além de serem completos, consistentes, duradouros e disponíveis durante todo o ciclo de vida dos dados.

Os princípios básicos de integridade de dados (ALCOA+) segundo as agências PIC/S (2018) e WHO (2016) conforme são apresentados na Tabela 5:

Tabela 5: Princípios básicos de integridade de dados (ALCOA+)

Princípio ALCOA+	PIC/S (2018)	WHO (2016)
Atribuível	Deve ser possível identificar a pessoa ou o sistema computadorizado que executou a tarefa registrada. A necessidade de documentar quem executou a tarefa/função é, em parte, para evidenciar que a função foi realizada por pessoal treinado e qualificado. Isso também se aplica a alterações feitas nos registros como correções, exclusões, alterações etc.	Significa que a informação é capturada no registro para que seja identificada exclusivamente como executada pelo originador dos dados (por exemplo, uma pessoa ou um sistema computadorizado).
Legível	Todos os registros devem ser legíveis para que possam ser úteis, sendo aplicados a todas as informações que seriam consideradas completas, incluindo todos os registros ou entradas originais. A capacidade de interagir com os dados usando um aplicativo adequado é importante para a disponibilidade do registro.	Referem-se aos requisitos que os dados são legíveis, compreensíveis e permitem uma imagem clara do sequenciamento das etapas ou eventos no registro, de modo que todas as atividades de boas práticas conduzidas possam ser totalmente reconstruídas pelas pessoas que revisam esses registros a qualquer ponto durante o período de retenção de registros definido pela boa prática aplicável.

Contemporâneo	A evidência de ações, eventos ou decisões devem ser registrados à medida em que elas ocorrem. Esta documentação deve servir como um atestado preciso do que foi feito ou do que foi decidido e por que, ou seja, o que influenciou a decisão naquele momento.	Dados contemporâneos são dados registrados quando são gerados ou observados.
Original	O registro original pode ser descrito como a primeira captura de informações, seja em papel (estático) ou eletronicamente (geralmente dinâmico, dependendo da complexidade do sistema). As informações capturadas originalmente em um estado dinâmico devem permanecer disponíveis nesse estado.	Os dados originais incluem a primeira captura ou fonte de dados ou informações e todos os dados subsequentes necessários para reconstruir completamente a condução da atividade de boas práticas. Os requisitos de qualquer boa prática (BPx) para dados originais incluem o seguinte: <ul style="list-style-type: none"> ▪ Os dados originais devem ser revisados; ▪ Os dados originais e/ou as cópias verdadeiras e verificadas que preservam o conteúdo e o significado dos dados originais devem ser mantidos; ▪ Como tal, os registros originais devem estar completos, duradouros e facilmente recuperáveis e legíveis durante todo o período de retenção de registros.
Acurado	Garantir a acurácia ou a precisão dos resultados e registros através de elementos de um sistema robusto de qualidade farmacêutica, podendo ser composto por: <ul style="list-style-type: none"> ▪ Fatores relacionados ao equipamento, como: qualificação, calibração, manutenção e validação por computador; ▪ Políticas e procedimentos para controlar ações e comportamentos, incluindo procedimentos de revisão de dados para verificar a aderência aos requisitos processuais; ▪ Gerenciamento de desvios, incluindo análise de causa raiz, avaliações de impacto e Ações Corretivas e Ações Preventivas (CAPA, do inglês, <i>Corrective Action and Preventive Action</i>); ▪ Pessoal treinado e qualificado que entende a importância de seguir procedimentos estabelecidos e documentar suas ações e decisões. 	O termo acurado ou preciso significa que os dados são corretos, verdadeiros, completos, válidos e confiáveis.
Completo	Todas as informações que seriam críticas para recriar um evento são importantes ao tentar entender o evento. O nível de detalhe necessário para que um conjunto de informações seja considerado completo dependeria da criticidade das informações. Um registro completo dos dados gerados eletronicamente inclui metadados.	Está implícito nos requisitos listados acima para a ALCOA que os registros devem estar completos, consistentes, duradouros e disponíveis (ALCOA-plus).
Consistente	Boas práticas de documentação devem ser aplicadas em qualquer processo, sem exceção, incluindo desvios que podem ocorrer durante o processo. Isso inclui capturar todas as alterações feitas nos dados.	
Duradouro	Os registros devem ser mantidos de maneira a existirem durante todo o período em que possam ser necessários. Isso significa que eles precisam permanecer intactos e	

	acessíveis como um registro permanente/durável durante todo o período de retenção de registros.	
Disponível	Os registros devem estar disponíveis para revisão a qualquer momento durante o período de retenção exigido, acessível em um formato legível para todo o pessoal responsável por sua revisão, seja para decisões rotineiras de liberação, investigações, tendências, relatórios anuais, auditorias ou inspeções.	

Fonte: Elaboração própria a partir de WHO (2016) e PIC/S (2018).

4.3.1 Governança de dados

A exatidão e a integridade dos registros de dados são essenciais para o ciclo de vida do produto, desde a área de pesquisa básica, passando por estudos pré-clínicos e clínicos, produção e controle de qualidade até a área de armazenamento e distribuição (VALÉCIO, 2020).

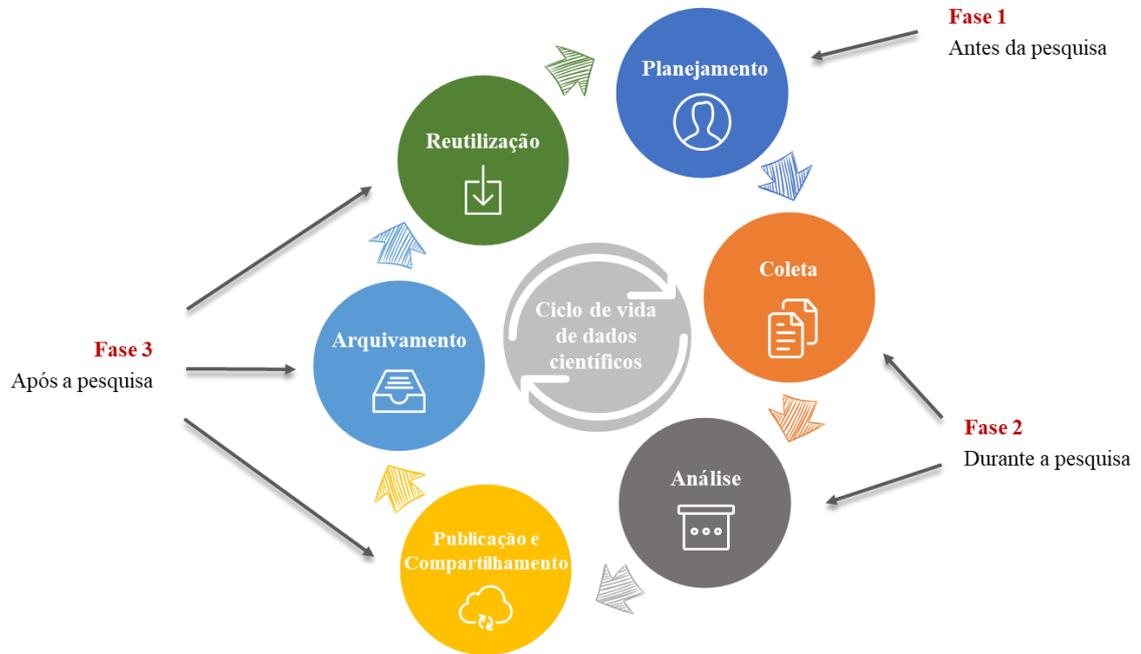
Segundo WHO (2016), em todo o mundo, os sistemas reguladores de produtos médicos dependem do conhecimento das organizações públicas ou privadas que desenvolvem, fabricam e embalam, testam, distribuem e monitoram produtos farmacêuticos, de biotecnologia e equipamentos médicos. No íntimo do processo de avaliação e revisão está implícita a confiança entre regulador e o regulado de que os dados e as informações enviadas em dossiês e utilizadas na tomada de decisões do dia a dia são compreensivas, completas e confiáveis.

Para PIC/S (2018), governança de dados é a soma total de ajustes que garantam a qualidade dos dados, independentemente do processo, formato – se papel e/ou eletrônico – ou tecnologia em que são gerados, gravados, processados, retidos, armazenados, recuperados, utilizados e descartados e que garantam que o registro seja atribuível, legível, contemporâneo, original e acurado (ALCOA) durante todo o ciclo de vida dos dados.

O ciclo de vida dos dados, segundo Goben et al. (2015), é a constituição de todas as fases do dado ao longo de sua vida, desde o momento da sua criação e passando pelos estágios do armazenamento, do seu uso ou reuso, do arquivamento até sua destruição.

Todavia, os dados científicos possuem um ciclo de vida próprio e que pode ser dividido em 3 fases, onde a primeira fase corresponde a etapa de planejamento, iniciado pelos cientistas responsáveis pela pesquisa antes de se começar a coleta de dados; a segunda fase com as etapas de coleta e análise de dados que perduram durante o andamento da pesquisa; e finalmente, a terceira fase com as etapas de publicação e compartilhamento, arquivamento e reutilização que ocorrem após a conclusão da pesquisa, conforme ilustrado na figura 1 (YORK UNIVERSITY, 2004).

Figura 1: Fases e etapas envolvidas no ciclo de vida de dados científicos alcançados em trabalhos de pesquisa



Fonte: Adaptado de York University, c2004.

Uma abordagem das etapas do ciclo de vida de dados, através do modelo da UK *Data Archive* (BALL, 2012), considerando seu relacionamento com o gerenciamento de dados, podem contribuir para um processo de implantação de integridade dados na pesquisa, através de características como demonstrado no quadro 1.

Quadro 1: Relacionamento do gerenciamento de dados com o ciclo de vida de um projeto de pesquisa

Etapas do ciclo de vida de dados	Características do gerenciamento de dados
Criando dados	<i>Research by design</i>
	Plano de gerenciamento de dados (formatos, armazenamento etc.)
	Plano de consentimento para compartilhamento
	Localizar dados existentes
	Coletar dados (experimental, observar, medir, simular)
	Capturar e criar metadados
Processando dados	Inserir dados, digitalizar, transcrever, traduzir
	Verificar, validar, limpar dados
	Anonimizar os dados quando necessário
	Descrever dados
	Gerenciar e armazenar dados
Analisando dados	Interpretar dados
	Dados derivados
	Produzir resultados de pesquisa
	Publicações do autor
	Preparar dados para preservação
Preservando dados	Migrar os dados para o melhor formato
	Migrar dados para um meio adequado
	Fazer backup e armazenar dados
	Criar metadados e documentação
	Dados de arquivo
Dando acesso aos dados	Distribuir dados
	Compartilhar dados
	Controlar o acesso
	Estabelecer direitos autorais
	Promover dados
Reutilizando dados	Pesquisa de acompanhamento
	Nova pesquisa
	Realizar análises de pesquisa
	Examinar as descobertas
	Ensinar e aprender

Fonte: Adaptado de Ball, 2012.

Dados bem documentados contribuem para saber como e onde buscar as informações e os resultados desejados são exatamente o que se espera. No campo da pesquisa científica, dados precisos podem ajudar na redução de litígios e recursos, pois são dados legais e cientificamente defensáveis (ARAGON, 2017).

Os dados relacionados à Pesquisa e Desenvolvimento (P&D) de produtos ou processos podem cruzar várias fronteiras dentro do ciclo de vida, podendo incluir a transferência de dados

entre papel e sistemas computadorizados ou entre diferentes limites organizacionais, sendo estes internos (por exemplo, entre laboratórios de pesquisa científica experimental, garantia da qualidade e controle da qualidade) e externos (por exemplo, entre prestadores de serviços e a instituição) (BRASIL, 2010).

A garantia da integridade de dados se torna cada vez mais preocupante e necessária por ser um componente crítico da responsabilidade do setor de garantir a segurança, eficácia e qualidade de produtos médicos, kits para diagnósticos, dispositivos médicos entre outros e a capacidade dos reguladores de proteger a saúde pública (PÉREZ, 2017).

Na área da saúde regulamentada, a integridade de dados é um requisito global obrigatório além de ser um elemento básico das boas práticas de documentação e um dos pilares mais fundamentais de qualquer sistema de gestão da qualidade (SGQ), incluindo as boas práticas de fabricação (BPF), de laboratório (BPL) entre outras (MCDOWALL et al., 2017).

Segundo Pérez (2017), a robustez e a precisão dos dados enviados pelos fabricantes às autoridades reguladoras são decisivas, pois desenvolver e levar um produto médico ao mercado envolve diferentes atores e atividades. Neste sentido, para garantir a qualidade dos estudos, os dados devem ser abrangentes, completos, precisos e verdadeiros, pois dão suporte aos pedidos de produtos médicos a serem colocados nos sistemas de saúde e no mercado global como um todo.

Para PIC/S (2018), o sistema de gestão da qualidade farmacêutica deve ter como parte integrante os sistemas de governança de dados com objetivo de abordar a propriedade dos dados durante o ciclo de vida, considerando as fases de projeto, operação e monitoramento de processos e sistemas e, assim, cumprir os princípios de integridade de dados, incluindo controle de alterações intencionais, não intencionais e exclusões.

Segundo MHRA (2018), a organização precisa assumir responsabilidades pelos sistemas utilizados e pelos dados gerados com objetivo, através da sua cultura organizacional, de garantir que os dados sejam completos, consistentes e precisos em todas as suas formas, ou seja, em papel e eletrônicos.

Para WHO (2016), a liderança é imprescindível para estabelecer e manter um compromisso de toda a empresa com a confiabilidade dos dados como um elemento essencial do sistema de gestão da qualidade. Sua integralidade começa com o gerenciamento, tendo a responsabilidade geral das operações técnicas e pelo fornecimento de recursos para assegurar a qualidade exigida nas operações em atividades de qualquer boa prática, promover uma cultura de qualidade, implementar medidas organizacionais e técnicas.

Segundo Shafiei et al. (2015), os principais fatores que influenciam a integridade de dados em atividades de boas práticas (BPx), são de natureza organizacional, operacional ou técnica, conforme demonstrado na Figura 2.

Figura 2: Principais fatores que influenciam a integridade de dados.



Fonte: Adaptado de SHAFIEI et al., (2015).

Deve haver, na organização, um programa de governança de dados que inclua políticas e procedimentos de governança que abordem os princípios gerais listados na Tabela 6 (WHO, 2016).

A liderança deve garantir que o risco à integridade de dados seja avaliado, mitigado e comunicado de acordo com os princípios do gerenciamento de risco da qualidade (GRQ) (WHO, 2016).

Segundo Ahmad et al. (2019), o GRQ refere-se a um processo sistemático de avaliação, controle, comunicação e revisão dos riscos para a qualidade do medicamento durante todo o ciclo de vida do produto.

Tabela 6: Princípios de governança de dados

Princípios de governança de dados	Descrição
Para dados eletrônicos e em papel	Devem ser aplicados igualmente os requisitos de boas práticas de gestão de dados e registros que garantam um controle robusto da validade dos dados não removendo das organizações a necessidade dos controles de gerenciamento dos dados quando ocorrer reversão de sistemas computadorizados ou automatizados para manuais ou baseados em papel.
Para as organizações e fornecedores	Devem ser aplicados tanto para organizações contratantes quanto para prestadores de serviços. Os prestadores de serviços devem, portanto, executar a devida diligência com base no risco para garantir às organizações contratantes programas apropriados para garantir a veracidade, integridade e confiabilidade dos dados fornecidos.
Para boas práticas de documentação	Devem ser seguidos para garantir que todos os registros, tanto em papel quanto eletrônicos, permitam a total reconstrução e rastreabilidade das atividades de qualquer boa prática (BPx) na organização.
Gestão da Governança	<p>Devem ser garantidas a implementação de programas adequados de governança de gerenciamento de dados através do estabelecimento de um sistema eficiente e sustentável de gestão de dados. Exemplos de controles com objetivos de garantir boas estratégias de gerenciamento de dados e registros podem incluir:</p> <ul style="list-style-type: none"> ▪ Uma abordagem de Gestão de Riscos da Qualidade (GRQ) que garanta a segurança efetiva do paciente, a qualidade e a validade dos dados; ▪ Monitoramento de processos e alocação dos recursos necessários para garantir e melhorar, conforme necessidades, a infraestrutura. Segundo ANVISA (2018), todos os componentes de um sistema da qualidade farmacêutica (SQF) devem dispor de quadro pessoal competente, instalações, equipamentos e meios apropriados satisfatórios; ▪ Adoção de uma cultura da qualidade na instituição com objetivo de incentivar os funcionários e colaboradores a serem transparentes sobre falhas para que a administração tenha um entendimento preciso dos riscos e possa fornecer os recursos necessários para atingir as expectativas no atendimento aos padrões de qualidade de dados; ▪ Mapeamento de processos de dados e aplicação de GRQ e sólidos princípios científicos ao longo do ciclo de vida dos dados; ▪ Garantir a atualização por meio de treinamentos aos funcionários e colaboradores sobre a aplicação de boas práticas de documentação (BPDoc), garantindo que os princípios ALCOA sejam compreendidos e aplicados a dados eletrônicos da mesma forma que historicamente tem sido aplicado a registros em papel; ▪ Treinamento do quadro de pessoal que utiliza sistemas computadorizados e analisa os dados eletrônicos quanto ao entendimento de como os sistemas computadorizados funcionam e como revisar de forma eficiente os dados eletrônicos, o que inclui metadados e trilhas de auditoria; ▪ Definição e gestão eficiente de funções e responsabilidades adequadas para contratos e acordo de qualidade firmados pela organização e prestadores de serviços, incluindo a necessidade de monitoramento baseado em risco de dados gerados e gerenciados pelo contratado em nome da organização; ▪ Modernização de técnicas de inspeção de garantia da qualidade para identificar com eficiência e eficácia os riscos e oportunidades com objetivo de melhorar os processos de dados.
Cultura da Qualidade	Devem ser estabelecidos e mantidos um ambiente de trabalho que minimize o risco de não conformidades de registros e dados errados, tomando medidas para prevenir e detectar e corrigir deficiências em sistemas e procedimentos que possam levar a erros de dados, de modo a melhorar continuamente a robustez da tomada de decisões científicas dentro da organização.
Gestão de risco da qualidade e princípios científicos sólidos	A tomada de decisão eficiente requer sistemas adequados de gestão de risco da qualidade e adesão a sólidos princípios científicos e estatísticos, sendo objetivo e imparcial em relação, por exemplo, na manutenção de registros que exige que todos os resultados rejeitados sejam registrados, juntamente com uma justificativa documentada para sua rejeição, e que esta documentação esteja sujeita a revisão e retenção.

Gerenciamento do ciclo de vida dos dados	Para garantir que a organização, a assimilação e a análise de dados em informações facilitem a tomada de decisões confiáveis e baseadas em evidências, a governança de dados deve abordar a propriedade dos dados e a responsabilidade pelo(s) processo(s) de dados e o gerenciamento de riscos do ciclo de vida dos dados.
Desenho de metodologias e sistemas de manutenção de registros	Metodologias e sistemas de manutenção de registros eletrônicos devem ser projetados de forma a incentivar a conformidade com os princípios de integridade de dados.
Mídia de registro e dados devem ser duráveis	Para registros em papel, a tinta deve ser indelével e o uso de tintas sensíveis à temperatura ou fotossensíveis e outras tintas apagáveis não devem ser utilizadas assim como o papel também não deve ser sensível à temperatura, fotossensível ou facilmente oxidável. Se não for viável ou limitado (como pode ser o caso em impressões de impressoras antigas de balanceamento e outros instrumentos em laboratórios de controle de qualidade), cópias verdadeiras ou certificadas devem estar disponíveis até que este equipamento seja retirado ou substituído pela organização.
Manutenção de sistemas e registros	Devem levar em conta o progresso científico e técnico, revisando periodicamente os sistemas, procedimentos e metodologias usados para registrar e armazenar dados.

Fonte: Adaptado de WHO (2016).

O sistema de governança de dados deve garantir controles sobre o ciclo de vida dos dados que são proporcionais aos princípios do gerenciamento de riscos da qualidade e tais controles podem ser conforme descrito na Tabela 7.

Tabela 7: Tipos de controles sobre o ciclo de vida dos dados

Tipo de Controle	Exemplo de aplicação de controle
Organizacional	<ul style="list-style-type: none"> ▪ Procedimentos Operacionais Padrão (POP) ou Procedimentos de Uso (PU), por exemplo, com instruções para preenchimento de registros e retenção de registros preenchidos; ▪ Treinamento de pessoal e autorização documentada para geração e aprovação; ▪ Projeto de sistema de governança de dados, considerando como os dados são gerados, registrados, processados, retidos e usados, e como os riscos ou vulnerabilidades são efetivamente controlados; ▪ Verificação de dados de rotina; ▪ Adoção de processos de autoinspeção como ações de vigilância periódica a fim de verificar a eficácia do sistema de governança de dados.
Técnico	<ul style="list-style-type: none"> ▪ Qualificação, controle e validação de sistemas computadorizados; ▪ Automação;

Fonte: Adaptado de PIC/S (2018).

O risco, segundo a ABNT NBR ISO 31000:2018, é entendido como o efeito da incerteza no alcance dos objetivos, sendo o efeito um desvio em relação ao esperado, podendo ser positivo, negativo ou ambos, no qual pode abordar, criar ou resultar em oportunidades e ameaças.

É parte da governança e liderança o gerenciamento de riscos, além de ser fundamental para a maneira como a organização é gerenciada em todos os níveis, contribuindo para a melhoria dos sistemas de gestão (ABNT NBR ISO 31000:2018).

De acordo com a ABNT NBR ISO 31000:2018, organizações de qualquer estrutura enfrentam influências de acordo com mudanças nos contextos externos e internos que conferem determinado grau de insegurança ao alcance de seus objetivos, denominando o efeito desta insegurança nos objetivos de “risco”.

O risco tem origem na incerteza que existe em todos os projetos, sendo os riscos conhecidos os que foram identificados e corretamente analisados e, que possibilitam planejar as respostas no caso de ocorrência reduzindo os possíveis impactos causados (PMBOK, 2010).

Gerenciar riscos contribui na melhoria dos sistemas de gestão e é parte da governança e liderança, sendo fundamental na maneira como a organização é gerenciada em todos os níveis, auxiliando no estabelecimento de estratégias, na tomada de decisões e no alcance de objetivos (ABNT NBR ISO 31000:2018).

Segundo a RDC 301 (2019), o GRQ é um processo sistemático de avaliação, controle, comunicação e revisão de riscos para a qualidade do medicamento.

O gerenciamento de riscos deve ser empregado para determinar a importância de cada etapa dos dados. Segundo PIC/S (2018), um tratamento eficaz de gerenciamento de riscos à governança de dados deve considerar:

- A criticidade dos dados no impacto da tomada de decisão e qualidade do produto;
- O risco de dados como oportunidade de considerar a vulnerabilidade de dados para alterações involuntárias, exclusão, perda ou recriação ou falsificação deliberada e probabilidade de tais ações, além de considerar a possibilidade de garantir a recuperação os dados em casos de desastres.

Segundo Pérez (2017), a ineficiência das organizações em aplicar sistemas robustos com objetivo de mitigar os riscos dos dados são as principais causas que contribuem para a falta de integridade de dados. O autor destaca, ainda, a necessidade das instituições na área da saúde de modernizar estratégias de controle e aplicar o gerenciamento de risco da qualidade e princípios científicos adequados.

Os riscos inerentes à integridade de dados relacionados aos equipamentos analíticos e sistemas computadorizados podem diferir dependendo do grau em que o sistema analítico gera

ou utiliza os dados é configurado e o potencial de manipulação dos dados durante a transferência entre sistemas informatizados durante o ciclo de vida (PÉREZ, 2017).

Ainda, segundo Pérez (2017), o esforço e os recursos atribuídos às medidas de integridade de dados devem ser proporcionais ao risco para a qualidade do produto e a violação da integridade de dados deve ser considerada seriamente, pois apresenta grande risco podendo, inclusive, impactar na qualidade, eficácia e segurança de produtos.

4.3.2 Impactos da não adoção da prática de integridade de dados

No âmbito da pesquisa científica que é uma fase que ocorre antes do processo de fabricação de medicamentos, vacinas e kits de diagnósticos, a preocupação com relação à ética e à integridade vem aumentando consideravelmente devido aos inúmeros casos de fraudes descobertos nas instituições de pesquisa (RUSSO, 2014).

A retratação de artigos científicos é uma causa da não adoção da prática de integridade de dados, além de ser considerado um fenômeno reprovável. Seu impacto causa um declínio imediato, grave e duradouro em futuras citações (AZOULAY et al., 2012).

Os sistemas de regulação de medicamentos em todo o mundo sempre dependeram do conhecimento das organizações de P&D e a descoberta de falhas e ausência de integridade de dados acabam abalando a confiança estabelecida que os reguladores têm sobre as empresas de produtos farmacêuticos, de biotecnologia e equipamentos médicos (WHO, 2016; UNGER, 2016).

Segundo Unger (2016), durante uma inspeção regulatória, os dados gerados pelas organizações durante todas as fases da cadeia produtiva de um medicamento, por exemplo, não são revisados em sua total plenitude pelas autoridades reguladoras, sendo, portanto, revisados apenas uma pequena fração dos dados gerados.

Ainda segundo Unger (2016), na descoberta que dados eletrônicos foram falsificados ou manipulados, as autoridades reguladoras perdem a confiança em todos os dados apresentados pela organização, ocasionando consequências contraproducentes devastadoras às organizações.

Tais ações regulatórias, segundo Singh e Joshi (2015), afetam não só o fluxo de receita das organizações, mas também a capacidade da instituição de obter aprovação para novas aplicações de medicamentos e as violações de ausência e falhas de integridade de dados podem originar possíveis implicações, conforme Tabela 8.

Tabela 8: Possíveis implicações por violações de Boas Práticas (BPx)

Possíveis implicações	Possíveis prejuízos
Perda de negócios	<i>Recall</i> de produtos ou alertas de importação podem ocorrer com a emissão de cartas de advertências, que podem, inclusive, ter impacto nas ações das empresas listadas com a queda no preço das ações
Danos à reputação	Os reguladores divulgam em seus sítios eletrônicos a lista de empresas que violam as diretrizes, tornando pública as informações que podem ser posteriormente obtidas pela mídia, manchando a reputação das empresas
Influência regulatória	Inspeções adicionais podem ser realizadas por outros órgãos reguladores ou clientes que mancham a reputação da empresa
Desvantagem competitiva	Com as implicações e possíveis consequências, os concorrentes podem aproveitar essa oportunidade para aumentar sua participação de mercado
Desvio para remediação de não conformidades	Com a necessidade de ações corretivas e ações preventivas (CAPA) após o recebimento das observações de inspeção, ocorrem desvios da atenção da gerência e dos funcionários de suas atividades diárias, para se concentrar na resolução das não conformidades. O longo processo de remediação tende a custar tempo, dinheiro e muitas vezes perda de talento nas organizações

Fonte: Adaptado de SINGH e JOSHI, 2015.

Em 2018, o FDA emitiu um total de 85 cartas de advertência (*warning letters*) de Boas Práticas de Fabricação de medicamentos em todo o mundo, deste total, 49% incluíam componentes de integridade de dados (UNGER, 2019).

Em 2015, o *Committee for Medicinal Products for Human Use* (CHMP) da *European Medicines Agency* (EMA) suspendeu o uso de aproximadamente 700 medicamentos da empresa *GVK Biosciences*, da Índia, após ter sido citada por problemas relacionados a integridade de dados em alguns ensaios clínicos vinculados às aprovações de medicamentos (EMA, 2015; BRENNAN, 2015).

Segundo Unger (2016), a ausência e falhas de integridade de dados continuam sendo citadas até hoje nas inspeções regulatórias pelo FDA USA em formas de formulários e cartas de advertência e com aumento significativo a cada ano, resultando impactos, por exemplo, em alertas de importação para empresas de países como da Índia e China.

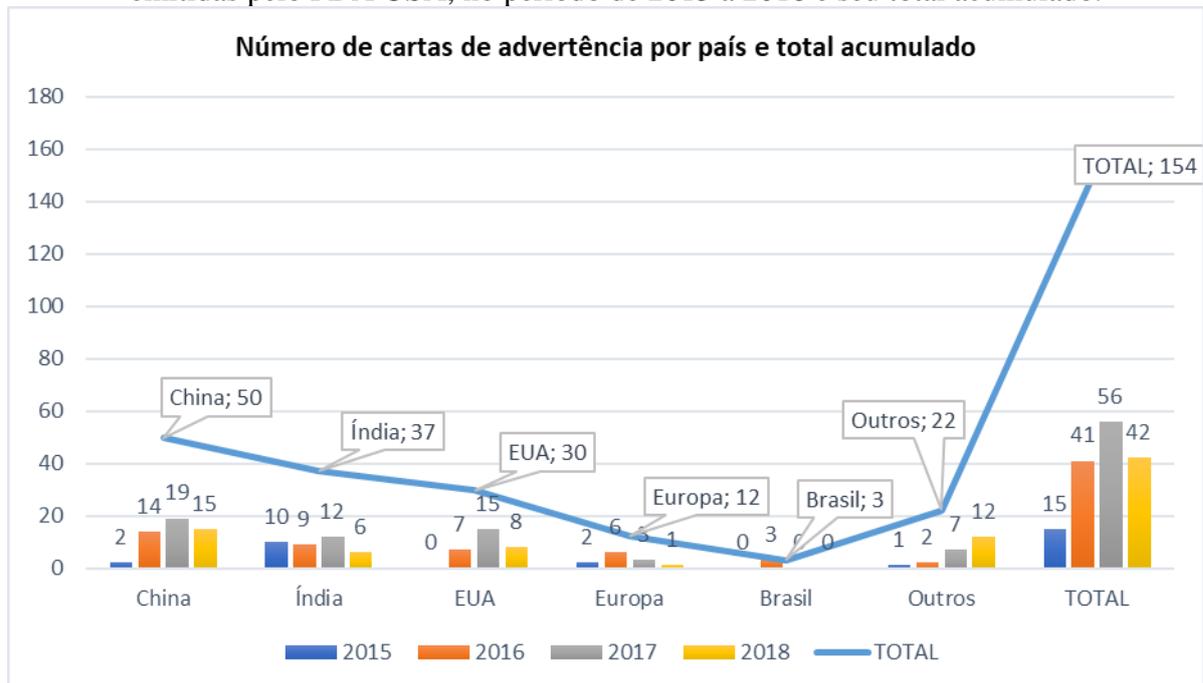
O percentual correspondente aos problemas de integridade de dados nas observações e cartas de advertência tem acompanhado o mesmo ritmo de crescimento, impactando ainda mais na relação de confiança entre regulador e regulado. É exigido, cada vez mais, a gestão e implementação de ações relacionadas à governança dos dados por parte das organizações de saúde, e ainda mais controle nas auditorias por parte dos técnicos de campo das agências reguladoras (UNGER, 2019).

Unger (2019) reitera que o tema integridade de dados faz parte das inspeções realizadas pelo FDA USA há mais de 20 anos e um número crescente de não conformidades neste tema

em auditorias realizadas em organizações de saúde do mundo, que possui qualquer boa prática (BPx), é preocupante.

Entre 2008 e 2014, o FDA USA emitiu 40 cartas de advertência contendo alguma não conformidade com o tema integridade de dados e esse número mais que dobrou de 2015 até 2018, totalizando 154 cartas de advertência e pico no ano de 2017 com 56 cartas de advertências, conforme pode ser observado na Figura 3 (UNGER, 2019).

Figura 3: Número de cartas de advertência associadas à integridade de dados por país, emitidas pelo FDA USA, no período de 2015 a 2018 e seu total acumulado.



Fonte: Elaboração própria a partir de UNGER, 2019.

O Brasil, dentro do período analisado, registrou 3 cartas de advertência contendo falhas de integridade de dados. Outros países que entraram na lista foram: Japão, Coreia do Sul, Canadá, México, Tailândia, Emirados Árabes Unidos, Jamaica, Singapura, Austrália, Taiwan e República Dominicana.

Segundo Lopez (2014), as deficiências encontradas em inspeções regulatórias referentes à ausência ou falhas de integridade de dados, incluem:

- Controles de segurança insuficientes;
- Inconsistências entre registros eletrônicos e registros em papel;
- Usuários de computador no laboratório com permissão de excluir dados das análises;
- Função trilha de auditoria desativada;

- Falta de registros para aquisição ou modificação de dados laboratoriais;
- Usuários que compartilham ID de login para acesso a sistemas de equipamentos laboratoriais;
- Nenhum procedimento para backup e proteção de dados dos equipamentos analíticos;
- Analistas que compartilham o nome de usuário e a senha do sistema operacional Windows;
- Nenhum mecanismo de bloqueio do computador configurado para impedir o acesso não autorizado aos sistemas operacionais e a sistemas de equipamentos analíticos.

Lopez (2014), evidenciou entre os anos de 2013 e 2014 não conformidades aplicadas a diferentes indústrias farmacêuticas referentes à integridade de dados após inspeções realizadas.

5. METODOLOGIA

Neste capítulo são apresentados os procedimentos metodológicos aplicados para a realização da pesquisa. Para isso, são abordados os seguintes tópicos: caracterização da pesquisa, etapas do trabalho, bem como o estudo preliminar, amostra da pesquisa e instrumento de coleta de dados.

A metodologia, na definição de Minayo (2001), pode ser entendida como o caminho do pensamento e a prática exercida na abordagem da realidade, ocupando um lugar central no interior das teorias e está sempre referida a elas. E, segundo Laville (1999), a metodologia representa mais do que um instrumento descritivo dos métodos e técnicas abordados.

5.1 CARACTERIZAÇÃO DA PESQUISA

Esta pesquisa teve por objetivo responder ao seguinte questionamento:

- a) Os dados eletrônicos gerados pelos sistemas computadorizados dos equipamentos analíticos nos laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada da Fiocruz adotam princípios e diretrizes de boas práticas de gerenciamento de dados para garantir sua integridade?

5.2 DESENHO DO ESTUDO

A pesquisa é classificada como exploratória, com o objetivo de proporcionar maior familiaridade com o tema e aprimorar a governança destes dados gerados eletronicamente nos laboratórios.

O estudo exploratório, segundo Gil (1987, p. 41), tem objetivo de proporcionar maior familiaridade com a questão da pesquisa, além de torná-lo mais explícito ou a construir hipóteses. Já para Zikmund (2000), os estudos exploratórios geralmente proporcionam o diagnóstico de situações, exploram alternativas ou descobrem novas ideias, além de ser um estudo em estágio inicial de um processo de pesquisa mais amplo esclarecendo e definindo a natureza da questão ou problema e possibilitando a geração de informações que podem ser adquiridas para realização de futuras pesquisas conclusivas.

Quanto à natureza da pesquisa, o estudo foi quali-quantitativo com aplicação de questionário semiestruturado para avaliar o grau da adoção de princípios e diretrizes de

integridade de dados em registros eletrônicos gerados em sistemas computadorizados de equipamentos analíticos pelos laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada da Fiocruz, com base no guia de boas práticas em gerenciamento de dados presente no anexo 5 do 50º relatório técnico da OMS descrito no capítulo teórico normativo (WHO, 2016).

Todavia, ressalta-se que o guia de boas práticas em gerenciamento de dados em registros eletrônicos da OMS foi desenvolvido com a finalidade de orientar a indústria farmacêutica na efetiva implementação de elementos, como por exemplo medidas de controles, que contribuem na integridade de dados que regem as atividades pré-clínico, clínico, fabricação, testes, armazenamento, distribuição e pós-comercialização para produtos farmacêuticos, biológicos e dispositivos médicos regulamentados, como boas práticas de laboratório, boas práticas clínicas, boas práticas de fabricação, boas práticas de farmacovigilância e boas práticas de distribuição.

A Fiocruz para dar conta da missão de prover soluções em saúde para o SUS, dispõe de diversos recursos tangíveis e intangíveis onde, articulados, permitem gerar soluções necessárias para a segurança em saúde da população brasileira, buscando atuar em toda a cadeia produtiva, desde a pesquisa básica até a fabricação de produtos (LIMA, 2018).

Entretanto, na ausência de um guia ou normatização específica de integridade de dados em registros eletrônicos oriundo de um equipamento analítico aplicado à laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada, foram utilizadas as medidas de controle organizacional, operacional e técnico do referido guia como documento norteador de ações que viabilizaram a análise, a comparação do grau de adoção de práticas de gerenciamento de dados, assim como a proposição de um modelo para garantir os requisitos mínimos de integridade de dados em registros eletrônicos gerados pelos sistemas computadorizados dos equipamentos analíticos para estes laboratórios da Fiocruz.

As medidas de controle descritas no guia da OMS foram organizadas como organizacional, operacional e técnico, e utilizadas para construção dos questionários e mesmo tendo sido desenhadas para a indústria farmacêutica podem ser aplicadas em qualquer segmento de atividade que precise tomar decisões estratégicas com base em dados e/ou informações geradas em suas respectivas instituições.

5.3 POPULAÇÃO E AMOSTRA DA PESQUISA

A Fiocruz possui atualmente, dentro da sua estrutura organizacional, 16 unidades técnico-científicas (órgãos específicos singulares) e 04 escritórios regionais, além de extensões em seu arranjo institucional e da estrutura administrativa (LIMA, 2018).

Para realização da pesquisa, foi delimitado que a população escolhida é composta pelas unidades técnico-científicas e escritórios técnicos da Fiocruz que possuem laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada e onde são gerados dados eletrônicos oriundos de sistemas computadorizados de equipamentos analíticos.

Dentro deste universo delimitado foram selecionados, como participantes da pesquisa, 13 unidades técnico-científicas e 03 escritórios técnicos regionais. Foram convidados, para cada unidade técnico-científica e escritório técnico, 01 gestor da área da Qualidade e 01 gestor da área de Tecnologia da Informação e Comunicação.

5.4 ETAPAS DO TRABALHO

O trabalho foi organizado em três etapas, conforme descrito abaixo:

- a) Construção do referencial teórico;
- b) Estudo exploratório; e,
- c) Estudo com base na população escolhida.

A primeira etapa metodológica versou na pesquisa bibliográfica em livros, periódicos, teses, dissertações, artigos científicos e guias de forma geral para aprofundar o entendimento no tema e para a construção de uma base teórica conceitual na qual este trabalho se baseia.

A segunda etapa metodológica consistiu na realização de um estudo exploratório mediante pesquisa documental, onde buscou-se informações em relatórios dos congressos internos da Fiocruz, plano de desenvolvimento institucional, relatórios de execução, políticas de integridade, riscos e controles internos da gestão, programas e guias envolvendo temas como integridade da Fiocruz e em todo o referencial teórico para a formulação de protocolo de coleta de dados que consistiu na construção de dois questionários na qual este trabalho se apoiou, além da análise preliminar e metodologia de análise.

A terceira etapa abordou um trabalho de campo, aplicado em 13 unidades técnico-científicas e 03 escritórios técnicos regionais, bem como na análise e interpretação dos resultados encontrados durante o estudo.

Com o intuito de facilitar o desenvolvimento da pesquisa, as etapas do trabalho foram subdivididas conforme segue:

- a) Etapa 1 – pesquisa bibliográfica
 - Levantamento bibliográfico;
 - Leitura e sistematização por assunto;
 - Análise e interpretação do referencial.

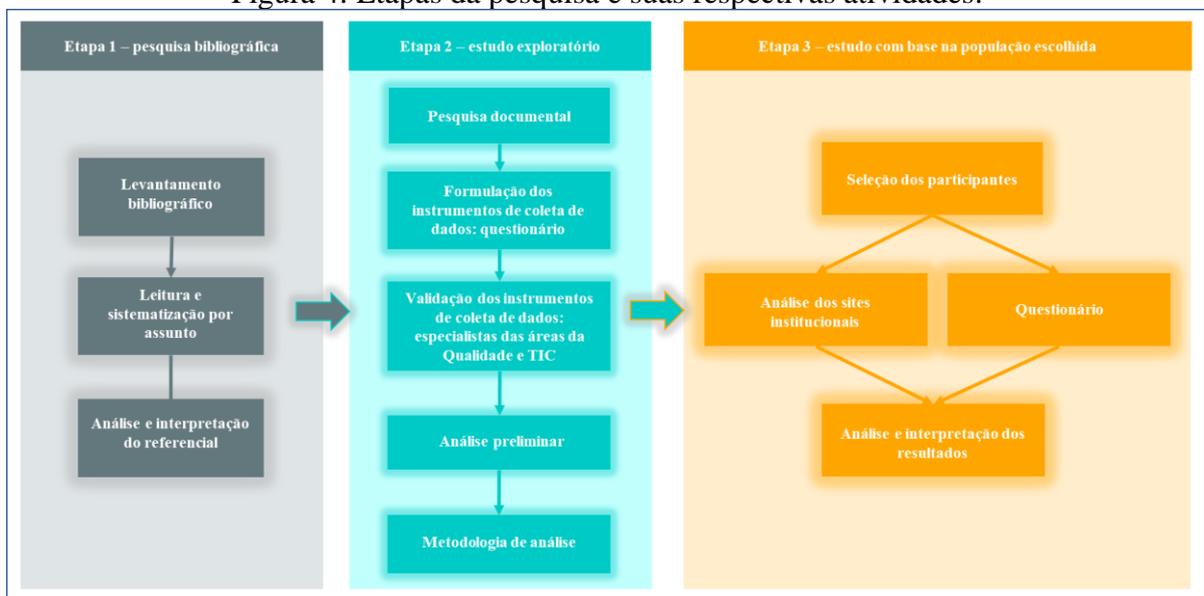
- b) Etapa 2 – estudo exploratório
 - Pesquisa documental;
 - Formulação dos instrumentos de coleta de dados: questionário;
 - Validação dos instrumentos de coleta de dados: especialistas das áreas da Qualidade e TIC;
 - Análise preliminar;
 - Metodologia de análise.

- c) Etapa 3 – estudo com base na população escolhida
 - Seleção dos participantes para estudo;
 - Análise dos sites institucionais;
 - Questionário 1: Questionário de integridade de dados em registros eletrônicos – Qualidade
 - Convite ao gestor da área da Qualidade por unidade técnico-científica e escritório técnico, totalizando 16 gestores da área da Qualidade na Fiocruz;
 - Envio de e-mail com solicitação formal da colaboração das pessoas escolhidas;
 - Envio do questionário *online*;
 - Tabulação das respostas.
 - Questionário 2: Questionário de integridade de dados em registros eletrônicos – TIC

- Convite ao gestor da área de TIC por unidade técnico-científica e escritório técnico, totalizando 16 gestores da área de TIC na Fiocruz;
 - Envio de e-mail com solicitação formal da colaboração das pessoas escolhidas;
 - Envio do questionário *online*;
 - Tabulação das respostas.
- Análise e interpretação dos resultados;

A figura 4 ilustra cada etapa da pesquisa e as atividades que fazem parte dela.

Figura 4: Etapas da pesquisa e suas respectivas atividades.



Fonte: Elaboração própria (2021).

5.5 COLETA DE DADOS

Para o desenvolvimento da pesquisa foram selecionadas as fontes de coleta de dados de acordo com os objetivos específicos do trabalho, assim como de acordo com as metodologias utilizadas para cumprimento desses objetivos, conforme apresentado na tabela 9.

Tabela 9 - Relacionamento entre objetivos específicos, metodologia e fontes de coletas de dados da pesquisa

Item	Objetivos específicos	Metodologia	Fonte de coleta de dados
a	Analisar o grau de adoção de práticas de gerenciamento de dados em registros eletrônicos gerados em laboratórios de pesquisa científica experimental da Fiocruz	▪ Levantamento e construção do referencial teórico	Livros, periódicos nacionais e internacionais, teses, dissertações, artigos científicos, guias de boas práticas de integridade de dados nacionais e internacionais, pesquisa documental
		▪ Análise e interpretação do referencial teórico	
		▪ Aplicação do questionário	Gestores da área da Qualidade e da área de TIC
		▪ Análise das respostas do questionário	Questionário respondido pelos gestores da área da Qualidade e da área de TIC
b	Comparar as práticas de gerenciamento de dados em registros eletrônicos gerados em laboratórios de pesquisa científica experimental da Fiocruz com as normas de integridade de dados eletrônicos estabelecidas pela OMS	▪ Análise e interpretação do referencial teórico	Livros, periódicos nacionais e internacionais, teses, dissertações, artigos científicos, guias de boas práticas de integridade de dados nacionais e internacionais, pesquisa documental
		▪ Aplicação do questionário	Gestores da área da Qualidade e da área de TIC
		▪ Análise das respostas do questionário	Questionário respondido pelos gestores da área da Qualidade e da área de TIC
c	Propor ações que auxiliem a implementação de uma política institucional de Integridade de Dados em Registros eletrônicos em laboratórios de pesquisa científica experimental para a Fiocruz	▪ Análise e interpretação do referencial teórico	Livros, periódicos nacionais e internacionais, teses, dissertações, artigos científicos, guias de boas práticas de integridade de dados nacionais e internacionais, pesquisa documental
		▪ Análise das respostas do questionário	Questionário respondido pelos gestores da área da Qualidade e da área de TIC

Fonte: Elaboração própria (2021)

A pesquisa baseou-se em fontes de conhecimento advindas de dois diferentes perfis de participantes: gestores da área de Gestão da Qualidade e gestores da área de Gestão de TIC, propiciando maior qualidade a pesquisa.

5.6 INSTRUMENTO PARA COLETA DE DADOS DA POPULAÇÃO ESTUDADA

Com base na leitura do material levantado e elaboração do referencial teórico, foi possível desenvolver dois questionários (Apêndices A e B), conforme referido logo abaixo:

Apêndice A: Questionário 1: Questionário de integridade de dados em registros eletrônicos – Qualidade

Apêndice B: Questionário 2: Questionário de integridade de dados em registros eletrônicos – TIC

Os questionários desenvolvidos e aplicados para os gestores das áreas da Qualidade e de TIC consistiram em uma ferramenta de caráter quali-quantitativo com propósito de avaliar o grau de adoção de práticas de gerenciamento de dados em registros eletrônicos gerados em sistemas computadorizados de equipamentos analíticos pelos laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada da Fiocruz.

Para atingir este propósito mencionado acima, foi elaborada uma síntese no final da análise e interpretação dos resultados de ambos os questionários que proporcionou no desenvolvimento de tabelas, quadros e gráficos.

Foram sintetizadas tabelas com os principais elementos e ações encontrados nos dois questionários e associados aos principais princípios identificados não apenas no guia de boas práticas de gerenciamento de dados da OMS, mas também, em todo referencial teórico. Para identificar o grau de adoção utilizou-se a soma da frequência e porcentagem referente às repostas apenas positivas dos elementos e ações. Assim, estabeleceu-se os seguintes níveis de graus de adoção:

- Grau Baixo de adoção: a porcentagem menor ou igual a 40% ($\leq 40\%$);
- Grau Médio de adoção: a porcentagem maior que 40% e menor ou igual a 70% ($> 40\%$ e $\leq 70\%$);
- Grau Alto de adoção: a porcentagem maior que 70% ($> 70\%$);

Procurou-se, também, entender a compreensão dos gestores-respondentes a respeito da relevância do tema integridade de dados gerados eletronicamente pelos laboratórios considerando que muitos dados são estratégicos dentro de um processo de geração de conhecimento científico e inovativo dentro da instituição.

Foi realizado um piloto para validar ambos os questionários. Neste piloto, os questionários foram respondidos por dois profissionais especialistas na área de Gestão da Qualidade e dois profissionais especialistas na área de Gestão de TIC que não faziam parte da amostra selecionada para a realização da pesquisa. A validação de ambos os questionários teve como objetivo obter retorno sobre o entendimento do questionário, se houve dúvidas,

dificuldades ou sugestões, além de verificar a abrangência, aplicabilidade, clareza e objetividade do instrumento para posterior utilização.

O Questionário 1 intitulado como Questionário de integridade de dados em registros eletrônicos – Qualidade, foi construído com 21 questões de múltipla escolha com algumas delas com opção de campo livre para respostas complementares, agrupadas em quatro categorias (partes) principais, referentes ao tema integridade de dados e gestão de dados, conforme segue:

- a) Parte I – Perfil dos entrevistados: 05 questões. Esta parte do questionário teve como objetivo identificar informações importantes sobre o entrevistado da unidade ou escritório técnico analisado;
- b) Parte II – Perfil da unidade/escritório: 06 questões. Esta parte do questionário teve como objetivo identificar informações importantes do perfil de cada unidade ou escritório técnico referente ao Sistema de Gestão da Qualidade, sobre o(s) tipo(s) de laboratório(s) existente(s), sobre o(s) equipamento(s) analítico(s) existente(s), sobre processos de auditoria/verificação/inspeção e sobre possuir ou não um ou mais ensaio(s) e/ou laboratório(s) acreditado(s) e/ou pré-qualificado(s);
- c) Parte III – Medidas de controles organizacionais: 08 questões, elaboradas pelo autor com base no referencial teórico e normativo e nos princípios e diretrizes do guia de boas práticas em gerenciamento de dados em registros eletrônicos da OMS. Teve como objetivo identificar a adoção de práticas e diretrizes organizacionais quanto ao planejamento de compra de equipamentos analíticos, à BPDoc, treinamento, cultura e procedimentos relacionados à garantia de integridade dos dados gerados eletronicamente.
- d) Parte IV – Gestão e compartilhamento de dados: 02 questões, elaboradas pelo autor com base no referencial teórico e normativo. Teve como objetivo identificar informações sobre a relação entre tecnologias emergentes e inovação nos processos organizacionais, além de informações referentes a plano de gestão de dados.

O Questionário 2 intitulado como Questionário de integridade de dados em registros eletrônicos – TIC, foi construído com 24 questões de múltipla escolha com algumas delas com opção de campo livre para respostas complementares, agrupadas em três categorias (partes) principais, referentes ao tema gestão de dados e integridade de dados, conforme segue:

- a) Parte I – Perfil dos entrevistados: 04 questões. Esta parte do questionário teve como objetivo obter informações importantes sobre o entrevistado da unidade ou escritório técnico analisado;
- b) Parte II – Medidas de controles organizacionais: 05 questões, elaboradas pelo autor com base no referencial teórico e normativo e nos princípios e diretrizes do guia de boas práticas em gerenciamento de dados em registros eletrônicos da OMS. Teve como objetivo identificar a adoção de práticas e diretrizes organizacionais quanto ao planejamento de compra de equipamentos analíticos, sobre participação de treinamento(s) nos equipamentos adquiridos, sobre processos de auditoria/verificação/inspeção e sobre processos e fluxos de trabalho entre a Gestão de TIC e Gestão de laboratórios;
- c) Parte III – Medidas de controles operacionais: 15 questões, elaboradas pelo autor com base no referencial teórico e normativo e nos princípios e diretrizes do guia de boas práticas em gerenciamento de dados em registros eletrônicos da OMS. Teve como objetivo identificar a adoção de práticas e diretrizes operacionais quanto a infraestrutura elétrica, controles de acesso, infraestrutura e gestão de dados, procedimentos técnicos operacionais em computadores e equipamentos analíticos, entre outros.

Antes do questionário ser enviado aos participantes, foi submetido ao Comitê de Ética em Pesquisa (CEP) da Escola Nacional de Saúde Pública Sérgio Arouca (ENSP) para aprovação, considerando o respeito pela dignidade humana e pela especial proteção devida aos participantes das pesquisas científicas envolvendo seres humanos. Os dados da pesquisa foram coletados somente após aprovação do projeto de pesquisa pelo CEP supracitado.

Foi elaborado o Termo de Consentimento Livre e Esclarecido (TCLE – Anexo A) e enviado juntamente ao link para acesso ao questionário online, garantindo sigilo, privacidade e acesso aos resultados a todos os participantes e seus respectivos laboratórios, além de não serem armazenados dados que possibilitem a sua identificação.

O arquivo referente ao TCLE e o link para acesso ao questionário online foram enviados a todos os participantes por e-mail institucional, contendo no corpo do e-mail o texto com apresentação do pesquisador, informação sumária do objetivo e da importância da pesquisa, assim como, solicitado a gentileza do participante de responder ao questionário, além de conter, também, o link de acesso ao questionário online.

6. RESULTADOS E DISCUSSÃO

6.1 PERFIL DA AMOSTRA

A amostra da pesquisa consistiu na participação de 12 unidades técnico-científicas de um total de 13 unidades possíveis (92,31%) e na participação de 03 escritórios técnicos de um total de 03 escritórios possíveis (100%).

Cada unidade e escritório do universo pesquisado recebeu dois questionários, sendo um enviado para o Gestor da área da Qualidade (Questionário – Qualidade) e outro enviado para o Gestor da área de TIC (Questionário – TIC).

Considerando que apenas 01 unidade não respondeu nenhum dos dois questionários enviados aos gestores das áreas da Qualidade e TIC, que 03 unidades responderam apenas um dos questionários e que 02 escritórios técnicos responderam apenas um dos questionários, a amostra da pesquisa consistiu na participação total de 25 gestores, o que representou 78,13% de um total de 32 gestores possíveis que foram convidados a participar da pesquisa.

Destes 25 gestores, obteve-se como resultado:

- 12 (48%) foram gestores da área da Qualidade, o que representou:
 - 09 (69,23%) unidades técnico-científicas de um total de 13 (100%) unidades possíveis; e
 - 03 (100%) escritórios técnicos de um total de 03 escritórios possíveis;
- 13 (52%) foram gestores da área de TIC, o que representou:
 - 12 (92,31%) unidades técnico-científicas de um total de 13 (100%) unidades possíveis; e
 - 01 (33,33%) escritório técnico de um total de 03 (100%) escritórios possíveis.

A relação de unidades técnico-científicas e escritórios técnicos do universo pesquisado está representado na tabela 10.

Tabela 10: relação de unidades técnico-científicas e escritórios técnicos do universo pesquisados

Unidades técnico-científicas (UTC) - Código de identificação	Gestores da área da Qualidade que responderam o questionário	Gestores da área de TIC que responderam o questionário	Frequência por Unidade	Percentual por Unidade
UTC-1	✓	✓	2	100%
UTC-2		✓	1	50%
UTC-3	✓	✓	2	100%
UTC-4	✓	✓	2	100%
UTC-5	✓	✓	2	100%
UTC-6			0	0%
UTC-7		✓	1	50%
UTC-8	✓	✓	2	100%
UTC-9	✓	✓	2	100%
UTC-10	✓	✓	2	100%
UTC-11		✓	1	50%
UTC-12	✓	✓	2	100%
UTC-13	✓	✓	2	100%
Escritórios técnicos (ET) - Código de identificação	Gestores da área da Qualidade que responderam o questionário	Gestores da área de TIC que responderam o questionário	Frequência por Escritório	Percentual por Escritório
ET-1	✓	✓	2	100%
ET-2	✓		1	50%
ET-3	✓		1	50%
TOTAL			25	

Fonte: Elaboração própria a partir dos questionários (2021).

A caracterização dos profissionais que responderam os questionários está representada na tabela 11.

Tabela 11: Caracterização dos profissionais que responderam os questionários

Relação de participantes (Unidade + Escritório + Gestores respondentes)				
Cargo	Relação de GESTOR por UNIDADE que respondeu o questionário	Relação de GESTOR por ESCRITÓRIOS que respondeu o questionário	Total de GESTORES da Qualidade que responderam os questionários	Total de GESTORES de TIC que responderam os questionários
Gestor da Qualidade	9 (69,23%) de 13 (100%)	3 (100%) de 3 (100%)	12 (75%) de 16 (100%)	N/A
Gestor de TIC	12 (92,31%) de 13 (100%)	1 (33,3%) de 3 (100%)	N/A	13 (81,25%) de 16 (100%)
Total	21	4	25 (78,13%) de 32 (100%)	

Fonte: Elaboração própria a partir dos questionários (2021).

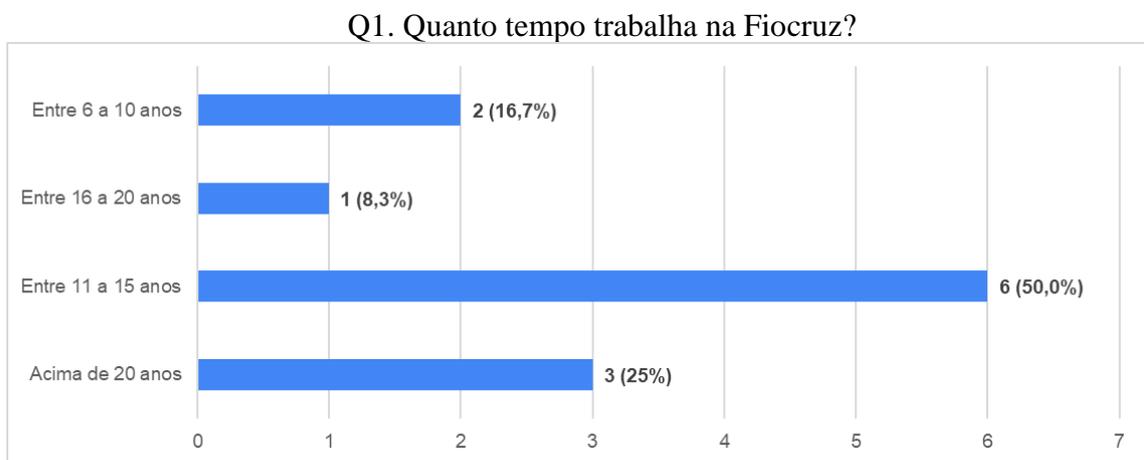
6.2 ANÁLISE DOS RESULTADOS E DISCUSSÃO

A realização e aplicação do questionário nas unidades técnico-científicas e escritórios técnicos da Fiocruz que participaram da pesquisa, teve como objetivo identificar, pela percepção dos respondentes, a situação referente à adoção de princípios e diretrizes de integridade de dados eletrônicos, a comparação de práticas existentes ou a sua parcial ou total ausência, além da identificação de um conjunto de ações que auxiliem a implementação de requisitos mínimos de integridade de dados em registros eletrônicos gerados por sistemas computadorizados de equipamentos analíticos em laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada da Fiocruz.

Questionário 1: Questionário de integridade de dados em registros eletrônicos – Qualidade

Parte I – Perfil dos entrevistados

Quanto ao perfil dos gestores da área da Qualidade pesquisados, foram obtidos os seguintes resultados:



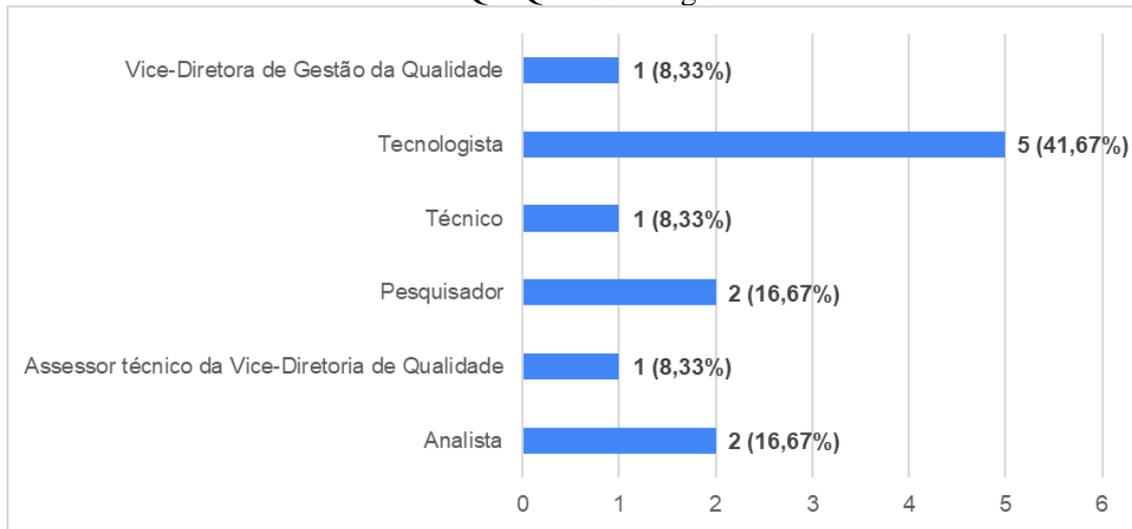
Fonte: Elaboração própria a partir dos questionários (2021).

Nenhum dos 12 gestores trabalha há menos de 05 anos na Fiocruz (0%); 02 gestores trabalham entre 06 e 10 anos (16,7%); 06 gestores trabalham entre 11 e 15 anos (50%); 01 gestor trabalha entre 16 e 20 anos (8,3%) e 03 gestores trabalham na Fiocruz acima de 20 anos (25%). Dos 03 gestores que trabalham acima de 20 anos, um trabalha há 24 anos e outro há 25 anos. O terceiro gestor não especificou o número de anos.

Dentro do universo pesquisado, 83,3% dos atuais gestores da área da Qualidade possuem mais de 10 anos de tempo de trabalho na instituição.

Obtendo das respostas acima o somatório do mínimo possível de cada faixa existente e respondida, pode-se concluir que a média do tempo de trabalho na Fiocruz dos 12 gestores da área da Qualidade é de 12,8 anos. Essa média representa uma expectativa de uma enorme bagagem de conhecimento institucional, profissional e de processos de trabalho que o corpo de gestores da área da Qualidade possui.

Q2. Qual seu cargo?

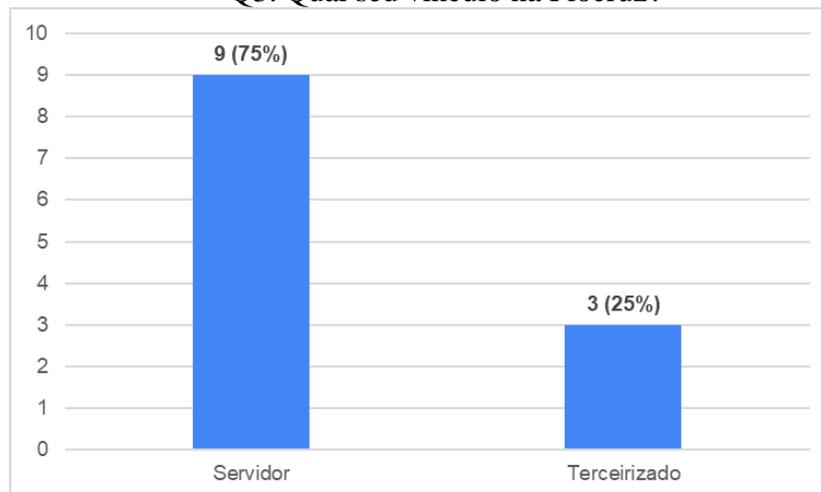


Fonte: Elaboração própria a partir dos questionários (2021).

Nenhum dos 12 gestores respondeu ter cargo de Assistente Técnico e nem de Especialista. 01 gestor possui cargo de Técnico (8,3%); 02 gestores possuem cargo de Analista (16,7%); 05 gestores possuem cargo de Tecnologista (41,7%); 02 gestores possuem cargo de Pesquisador (16,7%); 01 gestor respondeu possuir cargo de Vice-Diretor(a) de Gestão da Qualidade (8,3%) e 01 gestor respondeu possuir cargo de Assessor Técnico da Vice-Diretoria de Qualidade (8,3%).

Dentro do universo pesquisado, a maior representatividade na gestão da área da Qualidade corresponde ao cargo de Tecnologista (41,7%).

Q3. Qual seu vínculo na Fiocruz?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 12 gestores da área da Qualidade, 09 responderam ter o vínculo Servidor (75%) e 03 responderam ter o vínculo Terceirizado (25%).

Dentro do universo pesquisado, a maior representatividade na gestão da área da Qualidade é de servidores públicos (75%), o que pode representar uma maior estabilidade nas ações da qualidade, considerando que há maior atuação de servidores públicos.

Q4. Em qual unidade ou escritório técnico você trabalha?

Os 12 gestores da área da Qualidade que responderam ao questionário marcaram respectivamente sua unidade técnico-científica ou escritório técnico que trabalhavam até o presente momento da pesquisa. Por medida de precaução e proteção do participante, os riscos foram mitigados mediante o total sigilo da identidade e dados pessoais dos participantes e, nesta questão específica, utilizou-se de códigos de identificação para representar cada unidade técnico-científica (UTC-X) e cada escritório técnico (ET-X), conforme tabela 12.

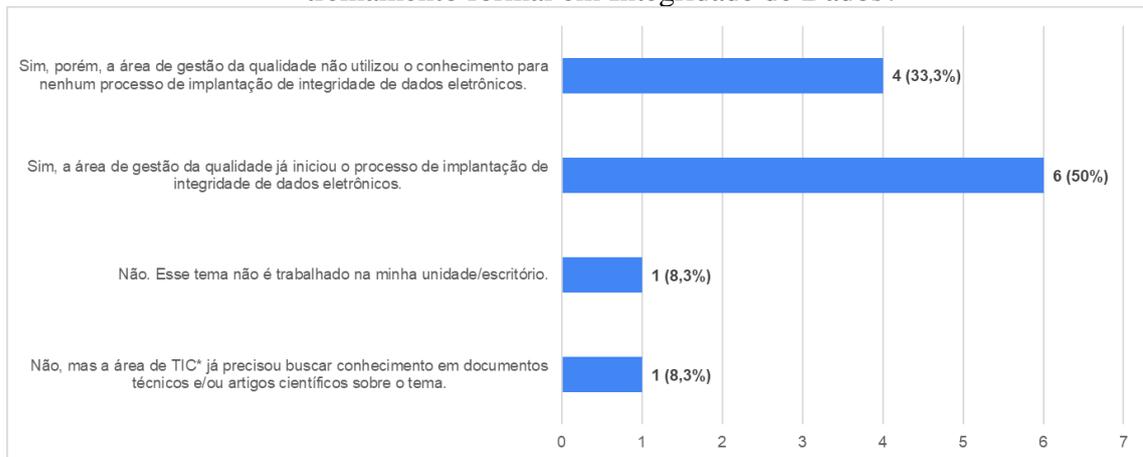
Tabela 12: Relação dos gestores da área da Qualidade por código de identificação que participaram da pesquisa

Unidades técnico-científicas - Código de identificação	Gestores da área da Qualidade que responderam o questionário
UTC-1	✓
UTC-2	
UTC-3	✓
UTC-4	✓
UTC-5	✓
UTC-6	
UTC-7	
UTC-8	✓
UTC-9	✓
UTC-10	✓
UTC-11	
UTC-12	✓
UTC-13	✓
Escritórios técnicos - Código de identificação	Gestores da área da Qualidade que responderam o questionário
ET-1	✓
ET-2	✓
ET-3	✓

Fonte: Elaboração própria a partir dos questionários (2021).

Verifica-se que dos 16 (100%) gestores da área da Qualidade que receberam o questionário, 09 (56,25%) responderam sob a percepção de suas respectivas unidades técnico-científicas e 03 (18,75%) responderam sob a percepção de seus respectivos escritórios técnicos.

Q5. Familiaridade com o termo Integridade de Dados: a) Você já obteve algum tipo de treinamento formal em Integridade de Dados?



Fonte: Elaboração própria a partir dos questionários (2021).

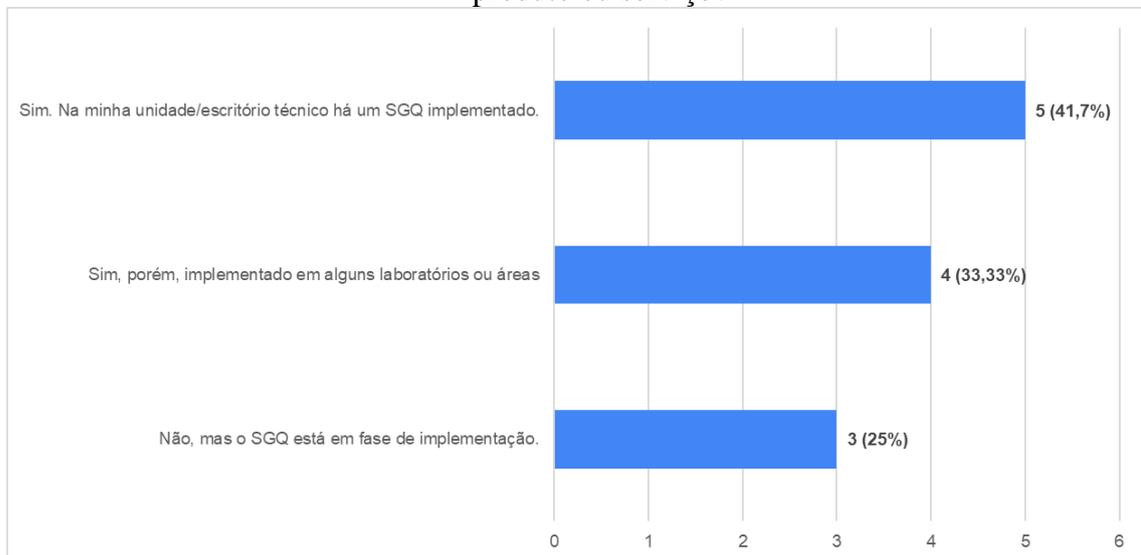
Dos 12 gestores da área da Qualidade, 06 (50%) responderam que já obtiveram treinamento formal no tema integridade de dados e já iniciaram o processo de implantação de integridade de dados eletrônicos; 04 (33,3%) responderam que obtiveram treinamento formal no tema, porém, a área de gestão da Qualidade não utilizou o conhecimento adquirido para nenhum processo de implantação de integridades de dados eletrônico; 01 (8,3%) gestor respondeu que não obteve nenhum treinamento formal no tema em questão, porém, a área de TIC da sua respectiva unidade técnico-científica ou escritório técnico já precisou buscar conhecimento em documentos técnicos e/ou artigos científicos sobre o tema; e 01 (8,3%) gestor respondeu, também, que não obteve nenhum treinamento formal no tema em questão e que sua respectiva unidade ou escritório não trabalha este tema de integridade de dados eletrônico.

Observa-se nestes resultados que 83,3% dos gestores da área da Qualidade que responderam esta questão receberam algum tipo de treinamento acerca do tema, o que representa um ótimo percentual e corrobora com a recomendação citada no guia de boas práticas em gerenciamento de dados (WHO, 2016), onde o pessoal deve ser efetivamente treinado para detectar problemas de integridade de dados e, assim, implementar boas práticas de integridade.

Parte II – Perfil da unidade/escritório

Quanto ao perfil das unidades técnico-científicas ou escritórios técnicos, sob a percepção dos gestores da área da Qualidade pesquisados, foram obtidos os seguintes resultados:

Q6. Na sua unidade/escritório existe um Sistema de Gestão da Qualidade efetivamente implementado que abrange a estrutura organizativa, os procedimentos, processos e recursos, e as ações sistemáticas necessárias para assegurar a confiança adequada de um produto ou serviço?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 12 gestores da área da Qualidade, nenhum respondeu não possuir um SGQ implementado e que não esteja sendo implementado. Apenas 03 (25%) gestores da área da Qualidade responderam que não têm um SGQ implementado, mas que está em fase de implementação; 04 (33,3%) responderam que possuem um SGQ implementado, porém, somente em alguns laboratórios ou áreas; e 05 (41,7%) responderam que possuem um SGQ implementado em suas unidades ou escritórios.

Apenas 04 gestores acrescentaram um comentário pertinente à questão 06. Os gestores consideram que nem todos os recursos (humanos e financeiros) são suficientes para uma adequada implementação do SGQ em sua unidade ou escritório; que a implementação se dá de forma voluntária onde existem desejos de melhorar seus processos de trabalho e em alguns itens da norma; e quando a unidade ou escritório possui laboratório(s) ligado(s) à parte industrial farmacêutica.

Analisando os resultados, observa-se que em 75% das unidades ou escritórios existe um Sistema de Gestão da Qualidade efetivamente implementado para abranger a estrutura organizativa, os procedimentos, processos e recursos, e as ações sistemáticas necessárias para assegurar a confiança adequada de um produto ou serviço, sendo que destes, 33,33% estão implementados apenas em alguns laboratórios ou áreas

Segundo PIC/S (2018), os sistemas de governança de dados devem ser parte integrante do sistema de gestão da qualidade e objetivam abordar ações ou elementos para cumprir os princípios de integridade de dados.

Já para WHO (2016), o sistema de gestão da qualidade tem como um dos seus elementos essenciais a confiabilidade dos dados e que deve ser estabelecido e mantido, através das lideranças, como um compromisso por toda organização.

Q7. Na sua unidade/escritório existem laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica e/ou aplicada?



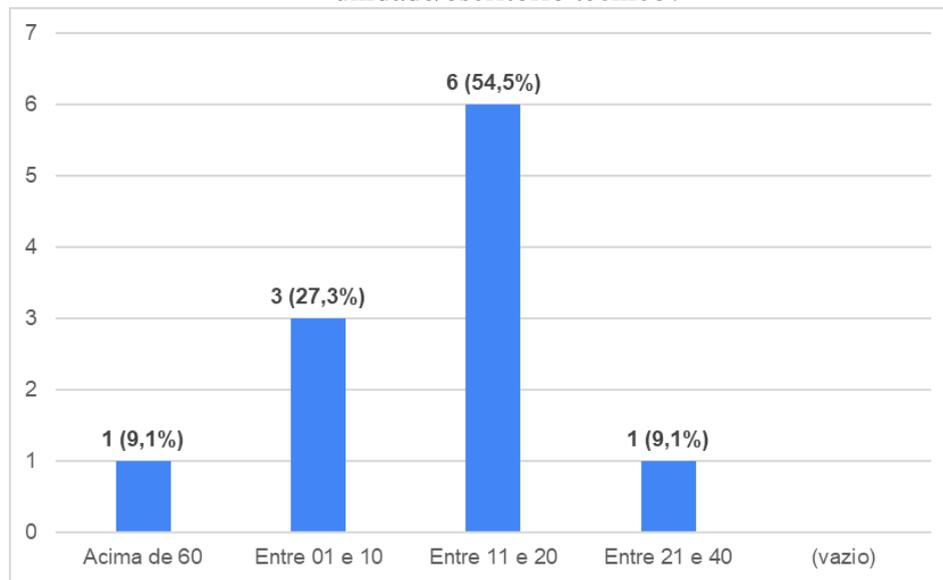
Fonte: Elaboração própria a partir dos questionários (2021).

11 (91,7%) dos 12 gestores da área da Qualidade responderam que possuem em suas respectivas unidades ou escritórios, laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica e/ou aplicada; apenas 01 (8,3%) gestor respondeu não possuir laboratórios com estas atividades em sua respectiva unidade ou escritório.

Q8. Se sua resposta na questão anterior (Q7) foi positiva, responda por favor à questão abaixo:

a) No total, existem quantos laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica e/ou aplicada instalados em sua unidade/escritório técnico?

Q8. No total, existem quantos laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica e/ou aplicada instalados em sua unidade/escritório técnico?



Fonte: Elaboração própria a partir dos questionários (2021).

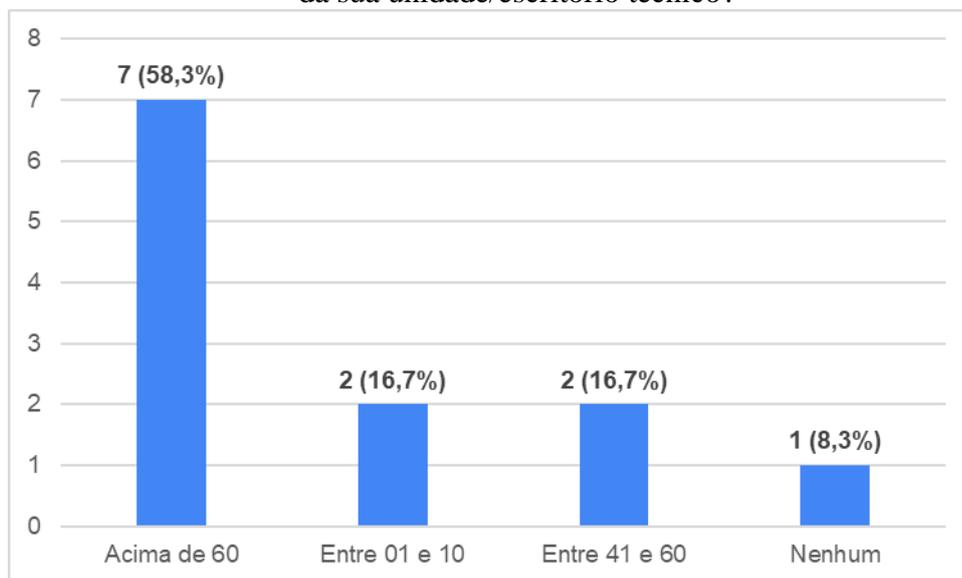
Dos 12 respondentes desta pergunta, nenhum respondeu ter entre 41 e 60 laboratórios em sua unidade ou escritório; 01 (9,1%) respondeu ter acima de 60 laboratórios; 01 (9,1%) respondeu ter entre 21 e 40 laboratórios; 03 (27,3%) responderam ter entre 01 e 10 laboratórios e 06 (54,5%) responderam ter entre 11 e 20 laboratórios com atividades de ensaio, plataforma tecnológica e pesquisas experimentais básica e/ou aplicada.

04 gestores da área da Qualidade acrescentaram alguns comentários que julgaram pertinentes à questão 08, conforme mencionado abaixo:

- Comentário 1: “Todas as estruturas técnicas (laboratórios e seus respectivos setores) se encaixam, em pelo menos uma, das atividades citadas. A contagem, pura e simples, de laboratórios não pode ser considerada como um indicador representativo”;
- Comentário 2: “72 labs de pesquisa, 26 labs referência, 20 coleções e 15 plataformas”;
- Comentário 3: “Considerando a estrutura física, temos apenas um Laboratório com as características de multiusuário, no entanto, existem vários grupos de pesquisa, aqui denominados de "Laboratórios", que atuam, parcial ou totalmente, no mesmo ambiente multiusuário”;
- Comentário 4: “São 10 laboratórios, 4 plataformas tecnológicas implementadas, 2 plataformas a implantar e um ambulatório”.

Obtendo das respostas acima o somatório do mínimo possível de cada faixa existente e respondida, pressupõe-se que das 09 unidades técnico-científica e dos 03 escritórios técnicos participantes desta pesquisa, existem, no mínimo, 151 laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica e/ou aplicada instalados em toda a Fiocruz e possivelmente gerando algum tipo de dado eletrônico crítico ou sensível para a pesquisa científica.

Q9. Quantos equipamentos analíticos existem em funcionamento no parque tecnológico da sua unidade/escritório técnico?

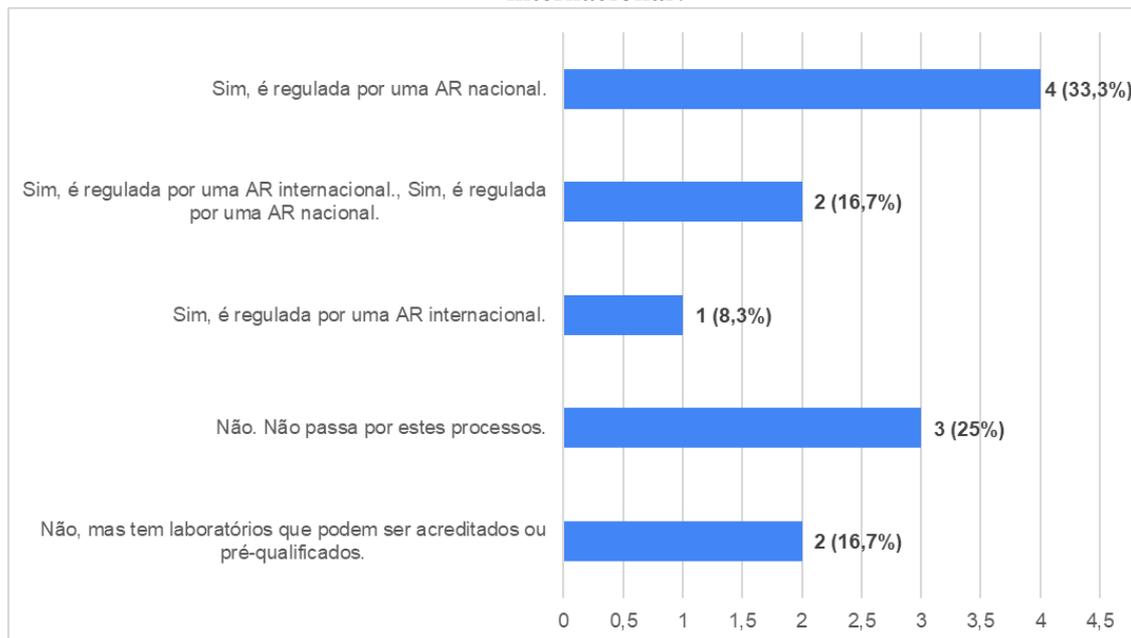


Fonte: Elaboração própria a partir dos questionários (2021).

Dos 12 gestores da área da Qualidade, apenas 01 (8,3%) respondeu não ter nenhum equipamento analítico em funcionamento na sua unidade ou escritório; 02 (16,7%) responderam ter entre 01 e 10 equipamentos analíticos em funcionamento; 02 (16,7%) responderam ter entre 41 e 60 equipamentos analíticos em funcionamento; e 07 (58,3%) gestores responderam ter acima de 60 equipamentos analíticos em funcionamento em sua unidade ou escritório.

Obtendo das respostas acima o somatório do mínimo possível de cada faixa existente e respondida, pressupõe-se que das 12 unidades técnico-científica e dos 03 escritórios técnicos participantes desta pesquisa, existem, no mínimo, 511 equipamentos analíticos em funcionamento em toda a Fiocruz e possivelmente gerando algum tipo de dado eletrônico em laboratórios com atividades de ensaio, plataformas tecnológicas e/ou de pesquisa básica e/ou aplicada nestes equipamentos.

Q10. Sua unidade/escritório técnico passa por processo de auditoria / verificação / inspeção ou regulação por órgãos/agências reguladoras e/ou de fomento nacional e/ou internacional?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 12 gestores da área da Qualidade, 03 (25%) responderam que suas respectivas unidades ou escritórios não passam por processos de auditoria/verificação/inspeção ou regulação; 02 (16,7%) responderam que não passam por estes processos, mas têm laboratórios em suas respectivas unidades ou escritórios que podem ser acreditados ou pré-qualificados; 04 (33,3%) responderam que são regulados por uma Agência Reguladora nacional; 01 (8,3%) respondeu que é regulado por uma Agência Reguladora internacional; e 02 (16,7%) responderam ser regulados por Agência Reguladora nacional e internacional.

Pode-se concluir que no universo pesquisado, 03 (25%) unidades ou escritórios passam por processos de auditoria/verificação/inspeção ou regulação de uma Agência Reguladora internacional e que 06 (50%) passam por processos de auditoria/verificação/inspeção ou regulação de uma Agência Reguladora nacional.

09 (75%) gestores da área da Qualidade comentaram na questão 10 sobre qual(is) agência(s) ou organização(ões) aplica(m) algum processo de auditoria/verificação/inspeção ou regulação por órgãos/agências reguladoras e/ou de fomento nacional e/ou internacional, sendo listadas:

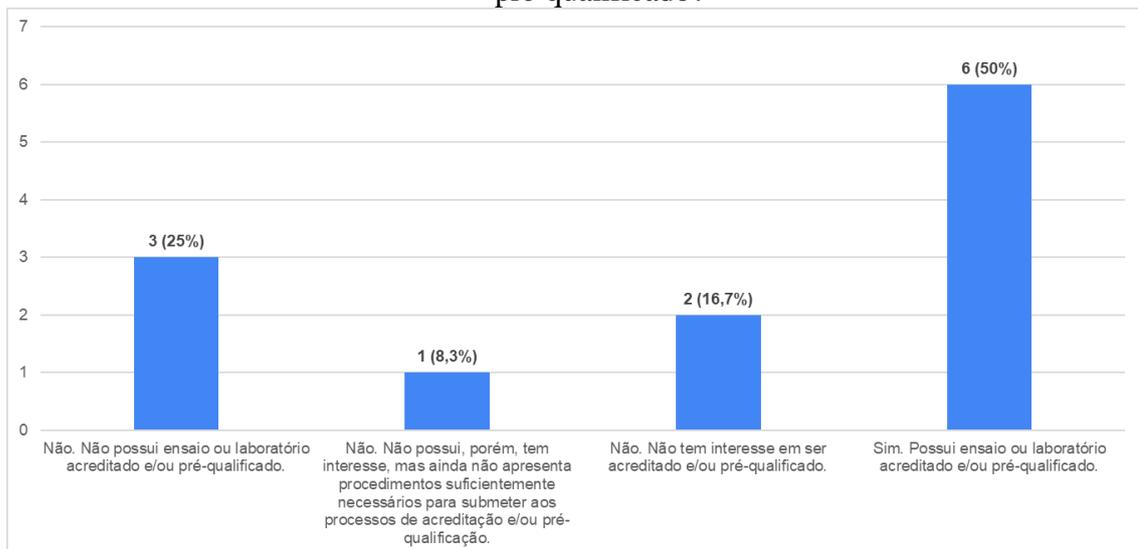
- Órgão de Vigilância Sanitária Estadual;
- Vigilância Sanitária Municipal e alguns laboratórios de ensaios clínicos passam por inspeções externas;

- Anvisa para OGM, Rede Metrológica de Minas Gerais – RMMG;
- Cgcre-Inmetro - Coordenação Geral de Acreditação do Inmetro;
- OMS;
- Anvisa;
- OPAS - Organização Pan-Americana da Saúde;
- NIH;
- SVS/MS - Secretaria de Vigilância em Saúde do Ministério da Saúde; e
- JCI - *Joint Commission International*.

Considera-se que um percentual superior a 50 das unidades e/ou escritórios da Fiocruz, participantes desta pesquisa, passam por algum processo de auditoria / verificação / inspeção ou regulação por órgãos/agências reguladoras e/ou de fomento nacional e/ou internacional. Portanto, podem ser submetidos, em algum momento, à análise de conformidade de documentos, procedimentos, projetos e relatórios.

Segundo Moretto (c2016), o processo de auditoria contribui para obter evidências através de registros, apresentação de fatos, entre outros e avaliá-las se são atendidos dentro dos critérios estabelecidos.

Q11. Sua unidade/escritório técnico possui algum ensaio ou laboratório acreditado e/ou pré-qualificado?



Fonte: Elaboração própria a partir dos questionários (2021).

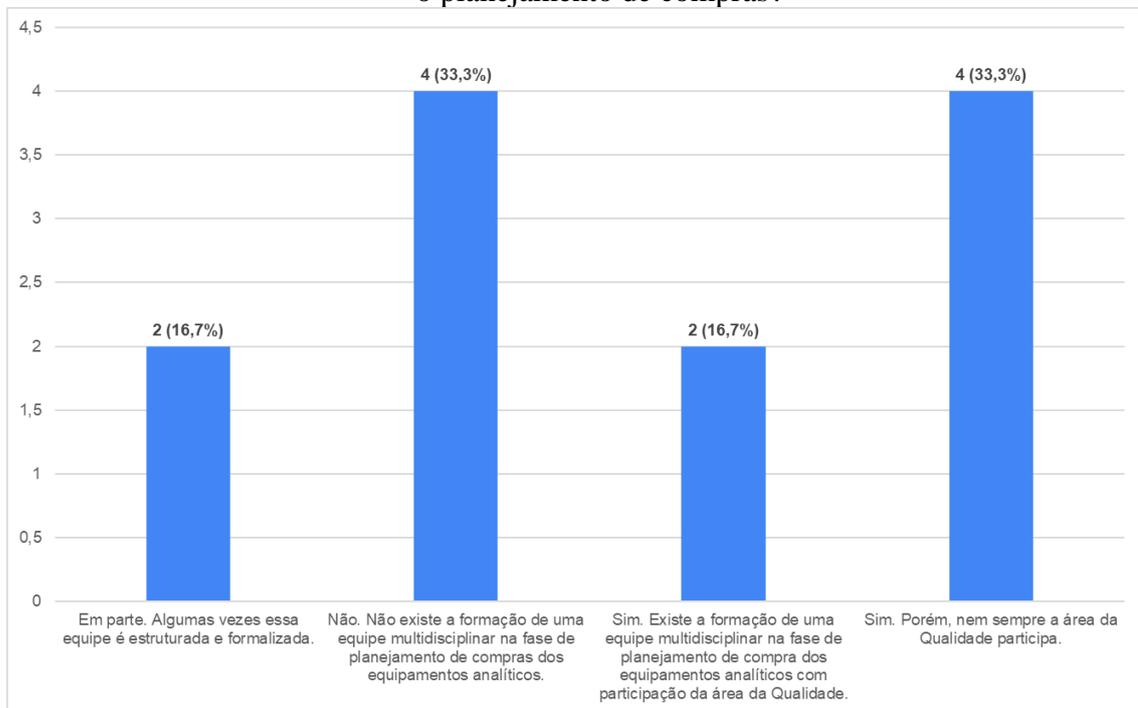
Dos 12 gestores da área da Qualidade, 06 (50%) responderam possuir em suas respectivas unidades ou escritórios técnicos, ensaios ou laboratórios acreditados e/ou pré-qualificados; 03 (25%) responderam não possuir ensaios ou laboratórios acreditados e/ou pré-

qualificados; 02 (16,7%) responderam que suas respectivas unidades ou escritórios técnicos não têm interesse em ter ensaios e/ou laboratórios acreditados e/ou pré-qualificados; e 01 gestor da área da Qualidade respondeu que sua respectiva unidade ou escritório técnico não possui acreditação e/ou pré-qualificação em seus ensaios ou laboratórios, porém, existe o interesse, mas que a unidade ou escritório ainda não apresenta procedimentos suficientemente necessários para submeter aos processos de acreditação e/ou pré-qualificação.

Parte III – Medidas de controles organizacionais

Quanto às medidas de controles organizacionais das unidades técnico-científicas ou escritórios técnicos, sob a percepção dos gestores da área da Qualidade pesquisados, foram obtidos os seguintes resultados:

Q12. Durante o processo de compras de equipamentos analíticos, a área da Qualidade é solicitada para formar uma equipe multidisciplinar (pesquisador/técnico da área específica da pesquisa, profissionais de gestão da qualidade, TI, infraestrutura e equipamentos) para o planejamento de compras?



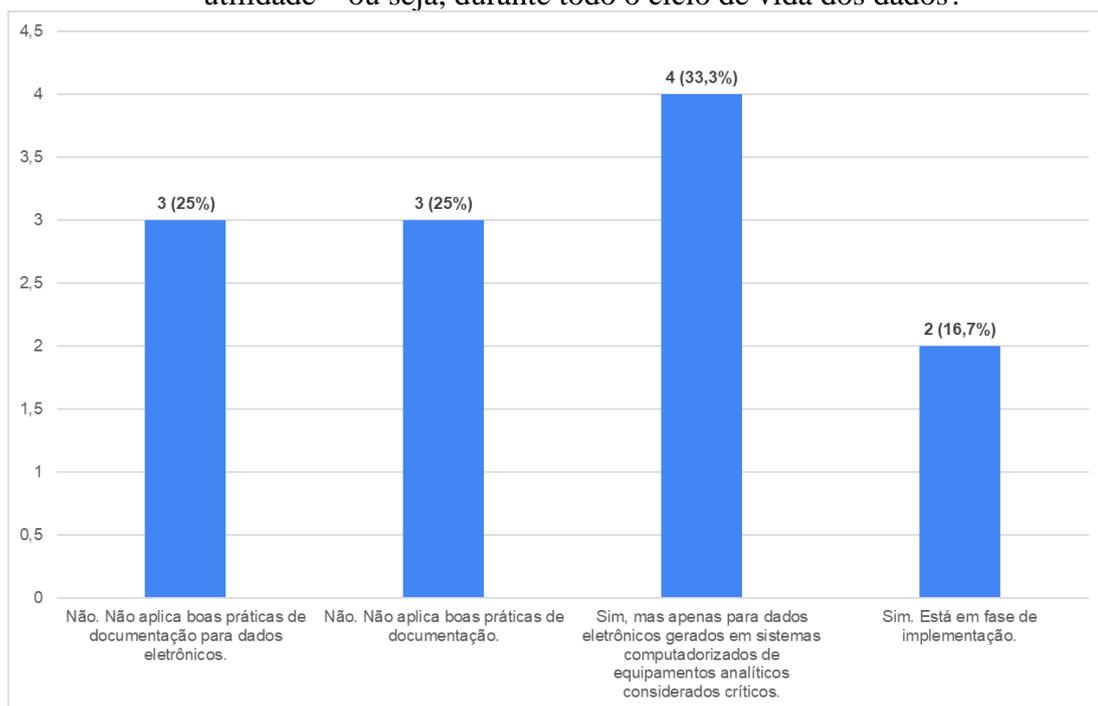
Fonte: Elaboração própria a partir dos questionários (2021).

Dos 12 gestores da área da Qualidade, apenas 02 (16,7%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos existe a formação de uma equipe multidisciplinar na fase de planejamento de compra dos equipamentos analíticos com a participação da área da Qualidade; 02 (16,7%) responderam que algumas vezes essa equipe

multidisciplinar com a participação da área da Qualidade é estruturada e formalizada; 04 (33,3%) responderam que em suas respectivas unidades ou escritórios não existe a formação de uma equipe multidisciplinar para o planejamento de compra; e 04 (33,3%) responderam que em suas unidades ou escritórios existe a formação de uma equipe multidisciplinar para o planejamento de compras de equipamentos analíticos, porém, nem sempre a área da Qualidade participa.

Pode-se concluir que no universo pesquisado, apenas 02 (16,7%) unidades ou escritórios possuem uma equipe multidisciplinar formada e com a participação da área da Qualidade para o planejamento de compra de equipamentos analíticos.

Q13. Sua unidade/escritório segue boas práticas de documentação (BPDoc) para garantir a exatidão, integralidade, consistência e confiabilidade dos dados eletrônicos gerados por sistemas computadorizados de equipamentos analíticos durante todo o seu período de utilidade – ou seja, durante todo o ciclo de vida dos dados?



Fonte: Elaboração própria a partir dos questionários (2021).

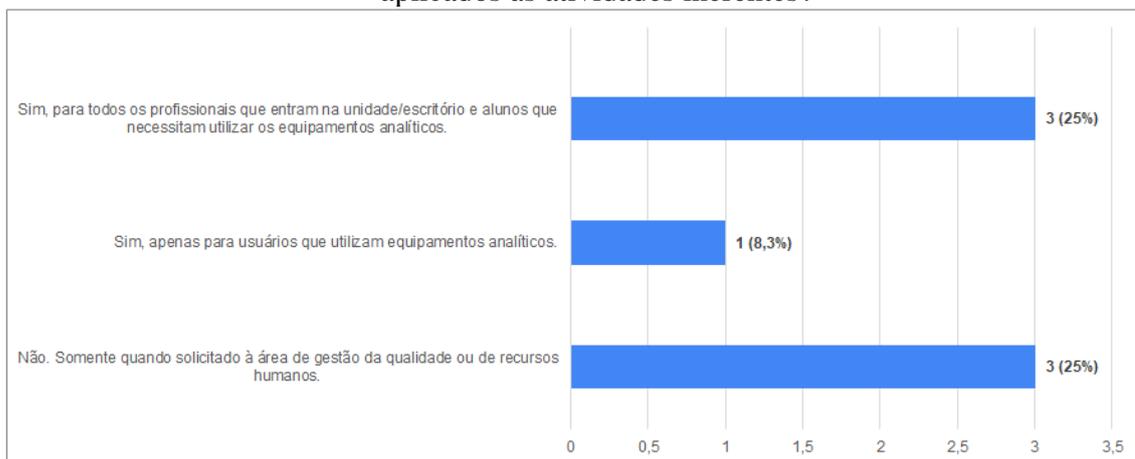
Dos 12 gestores da área da Qualidade, apenas 04 (33,3%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos utilizam boas práticas de documentação (BPDoc) para dados eletrônicos gerados por sistemas computadorizados de equipamentos analíticos durante o ciclo de vida dos dados; 02 (16,7%) responderam que estão em fase de implementação BPDoc; 03 (25%) responderam que não aplicam BPDoc em suas respectivas unidades ou escritórios e outros 03 (25%) responderam que não aplicam BPDoc para dados gerados eletronicamente.

As boas práticas de documentação, segundo WHO (2016), contribuem para o alcance de decisões robustas, pois quando seguidas podem garantir que todos os registros eletrônicos permitam reconstrução e rastreabilidade completas das atividades realizadas.

A documentação, através do registro completo das informações, possibilita ao pesquisador reconstruir o estudo, além de ser imprescindível para interpretação científica verdadeira (CPqRR, 2010).

Q14. Se a resposta da questão anterior (Q13) foi afirmativa, responda por favor esta questão.

Q14. A área de gestão da qualidade ou de recursos humanos provê treinamento aos profissionais, bolsistas e alunos que utilizam os equipamentos analíticos no que se refere às boas práticas de documentação para garantir que os princípios da ALCOA (dados atribuíveis, legíveis, contemporâneos, originais e acurados) sejam compreendidos e aplicados às atividades inerentes?



Fonte: Elaboração própria a partir dos questionários (2021).

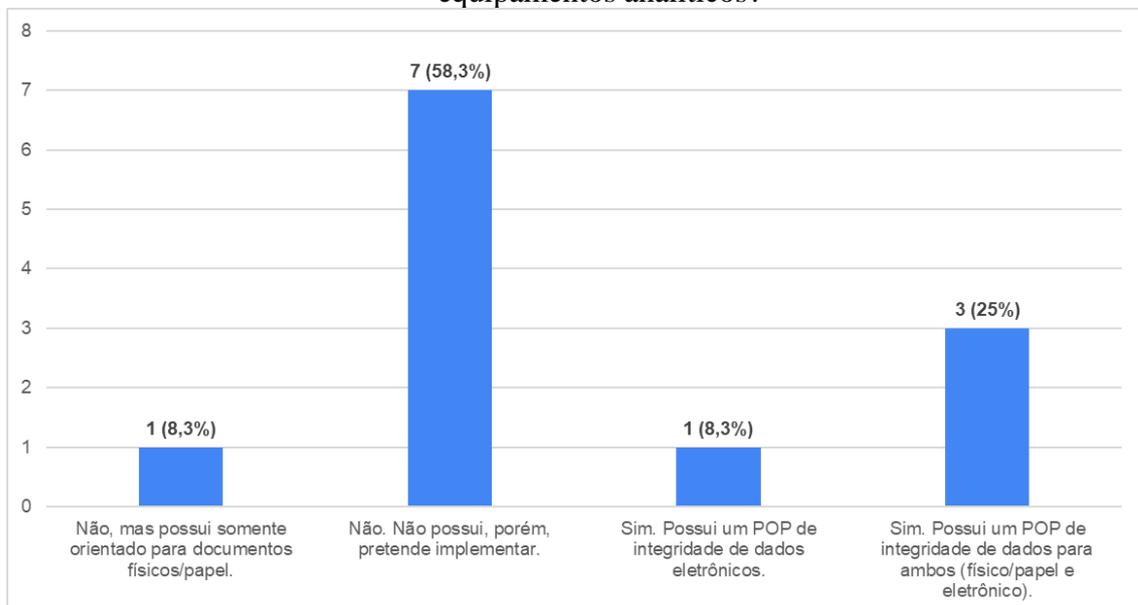
Dos 06 gestores respondentes desta pergunta, 03 (50%) responderam que em suas respectivas unidades ou escritórios, as áreas da Qualidade ou de RH não proveem treinamento para os profissionais, bolsistas e alunos que utilizam os equipamentos analíticos no que se refere às boas práticas de documentação para garantir que os princípios da ALCOA sejam compreendidos, a não ser quando o treinamento é solicitado à área de gestão da Qualidade ou RH; 03 (25%) responderam que o treinamento é dado para todos os profissionais e alunos que entram na unidade ou escritório; e 01 (8,3%) respondeu que o treinamento é dado apenas para usuários que utilizam equipamentos analíticos.

05 gestores da área da Qualidade acrescentaram alguns comentários que acharam pertinentes à questão 14, tais como:

- Comentário 1: A área da qualidade em 2020, organizou a participação de colaboradores nos dois cursos sobre integridade de dados que a CQuali promoveu e a partir de 2021 já tem a previsão da realização de deste curso para toda a unidade;
- Comentário 2: A garantia da competência de quem executa qualquer atividade, incluindo o uso de equipamentos, é requisito de todas as Normas de Gestão da Qualidade;
- Comentário 3: Geralmente os alunos e bolsistas não participam desse tipo de treinamento;
- Comentário 4: Isso depende do segmento ou laboratório. Não há uma regra geral;
- Comentário 5: Somente para os colaboradores da parte industrial farmacêutica.

Segundo WHO (2016), dentro dos princípios de governança de dados, controles com objetivos de garantir boas estratégias de gestão de dados podem incluir a atualização de funcionários e colaboradores através do treinamento sobre boas práticas de documentação, garantindo que os princípios ALCOA sejam compreendidos e aplicados a dados eletrônicos.

Q15. Sua unidade/escritório técnico possui algum procedimento operacional padrão (POP) sobre integridade de dados eletrônicos gerados por sistemas computadorizados de equipamentos analíticos?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 12 (100%) gestores da área da Qualidade, apenas 04 (33,3%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos possuem algum procedimento operacional padrão (POP) sobre integridade de dados eletrônicos gerados por

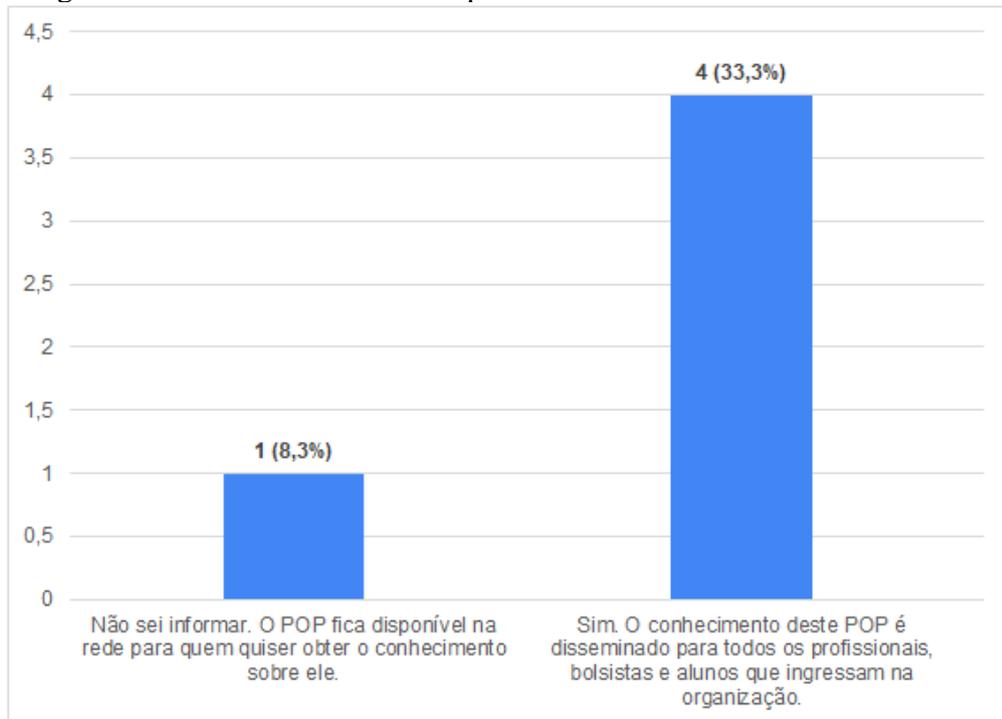
sistemas computadorizados de equipamentos analíticos, sendo que destes, 03 (25%) responderam possuir um POP de integridade de dados tanto para registros físico/papel como eletrônico e 01 (8,3%) gestor respondeu que possui apenas POP de integridade de dados eletrônicos; 07 (58,3%) gestores responderam que em suas respectivas unidades ou escritórios não possuem POP de integridade de dados eletrônicos, porém, pretendem implementar; e 01 (8,3%) gestor respondeu que em sua unidade ou escritório não existe POP de integridade de dados eletrônicos, porém, possui POP de integridade de dados orientado para documentos físicos/papel.

Observou-se que o resultado foi um percentual muito baixo se considerada a importância do tema para a quantidade de unidades ou escritórios que possuem laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica e/ou aplicada na Fiocruz.

O POP, segundo (CPqRR, 2010), refere-se a documento que possui procedimento padrão, escrito e aprovado, além de instruções que detalham sobre atividades que podem ser rotineiras e repetitivas e que são requeridos por técnicas clássicas de garantia da qualidade. Adicionalmente, POP devem ser entendidos como uma 1ª etapa de padronizar e disseminar uma rotina/prática e assim introduzir a mesma nos processos de trabalho.

Q16. Se a resposta da questão anterior (Q15) foi “Sim”, responda à pergunta a seguir:

Q16. Os servidores, colaboradores, bolsistas e alunos possuem conhecimento do POP de integridade de dados eletrônicos implementada na unidade/escritório técnico?



Fonte: Elaboração própria a partir dos questionários (2021).

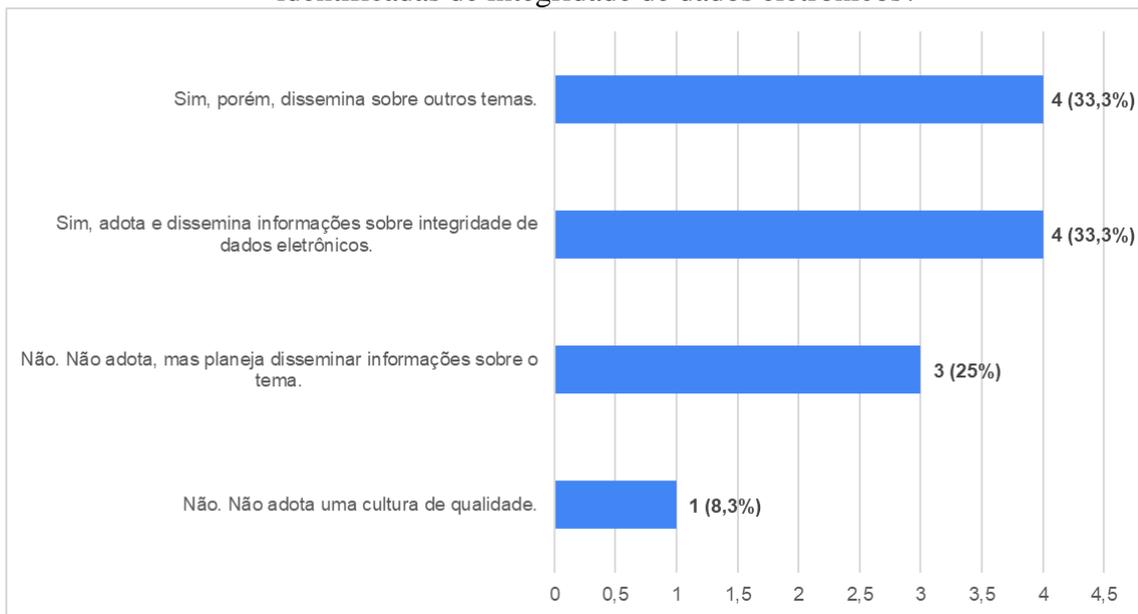
Dos 5 gestores respondentes desta pergunta, 04 (33,3%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos, os servidores, colaboradores, bolsistas e alunos possuem conhecimento do POP de integridade de dados eletrônico e que o conhecimento do POP é disseminado para todos que entram na unidade/escritório; e 01 (8,3%) gestor respondeu não saber informar se na sua respectiva unidade/escritório os servidores, colaboradores, bolsistas e alunos possuem conhecimento do POP e complementou que o POP fica disponível na rede para quem quiser obter o conhecimento sobre ele.

03 gestores da área da Qualidade acrescentaram alguns comentários acerca da questão 16, abordando que em sua respectiva unidade ou escritório este tema não é abordado especificamente em um POP, mas sim em um documento orientativo e que não saberia informar se é disponibilizado com frequência ou sob demanda. Já outro comentário abordou que a garantia da competência de quem executa qualquer atividade, incluindo o uso de equipamentos, é requisito de todas as Normas de Gestão da Qualidade e o último comentário abordou que o conhecimento é disseminado a quem ingressa em um determinado laboratório ou setor e não há procedimento geral para toda unidade.

O guia de boas práticas em gerenciamento de dados da OMS (WHO, 2016), cita que procedimentos adequados sejam desenvolvidos antes da liberação de sistemas para uso em atividades de qualquer boa prática e que treinamento destes procedimentos deve ser

desenvolvido para garantir abordagens como, por exemplo, na administração de sistemas informatizados, no uso de sistemas informatizados, em recursos do sistema que permitem que os usuários processem dados de forma eficientemente e revisem dados e metadados eletrônicos, entre outros.

Q17. Sua unidade/escritório adota uma cultura de qualidade com objetivo, por exemplo, de incentivar os profissionais, alunos e bolsistas a serem transparentes sobre falhas identificadas de integridade de dados eletrônicos?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 12 (100%) gestores da área da Qualidade, apenas 04 (33,3%) responderam que suas respectivas unidades técnico-científicas ou escritórios técnicos adotam uma cultura de qualidade com objetivo, por exemplo, de incentivar os profissionais, alunos e bolsistas a serem transparentes sobre falhas identificadas de integridade de dados eletrônicos; 01 (8,3%) gestor da área da qualidade respondeu que sua unidade ou escritório não adota uma cultura da qualidade; 03 (25%) responderam que não adotam uma cultura da qualidade, porém, planejam disseminar informações sobre o tema integridade de dados eletrônicos em sua cultura da qualidade; e 04 (33,3%) gestores responderam que em suas unidades/escritórios adotam uma cultura da qualidade, porém, disseminam informações acerca de outros temas e não sobre integridade de dados eletrônicos.

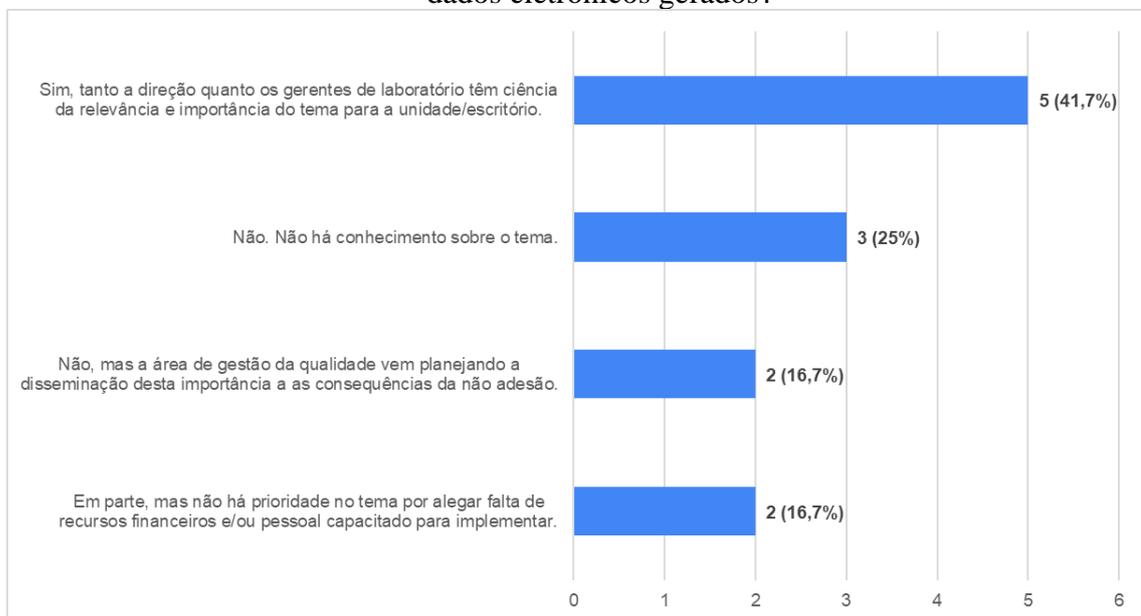
Segundo WHO (2016), uma cultura de qualidade é muito importante e deve estabelecer e manter, através da administração e com o apoio da unidade de qualidade, um ambiente de trabalho que minimize o risco de registros não conformes e registros de dados errados, tornando-se essencial dentro da cultura de qualidade o relato transparente e aberto de desvios,

erros, omissões e resultados irregulares em todos os níveis da organização, independentemente da hierarquia.

Apesar de identificarmos nos resultados que mais de 66% das unidades ou escritórios adotam uma cultura de qualidade, o percentual que desenvolve sobre o tema integridade de dados eletrônicos ainda é baixo (33,3%) na instituição o que impacta negativamente no incentivo aos profissionais, alunos e bolsistas a serem transparentes sobre falhas identificadas de integridade de dados eletrônicos.

Um dos objetivos da adoção de uma cultura de qualidade é de contribuir com o encorajamento e incentivo ao relato transparente e aberto de desvios, erros, omissões e resultados disformes em todos os níveis da organização, independentemente da hierarquia, além de possibilitar que sejam tomadas medidas para prevenir, detectar e corrigir deficiências em sistemas e procedimentos que possam levar a erros de dados, de modo a melhorar continuamente a robustez da tomada de decisão científica dentro da organização (WHO, 2016).

Q18. A direção e as gerências de laboratório com atividades de ensaio, plataformas tecnológicas e/ou de pesquisas experimentais básica e/ou aplicada têm ciência da relevância sobre integridade de dados eletrônicos e da importância de seu papel na proteção da segurança da pesquisa e na reputação de sua organização em relação aos dados eletrônicos gerados?



Fonte: Elaboração própria a partir dos questionários (2021).

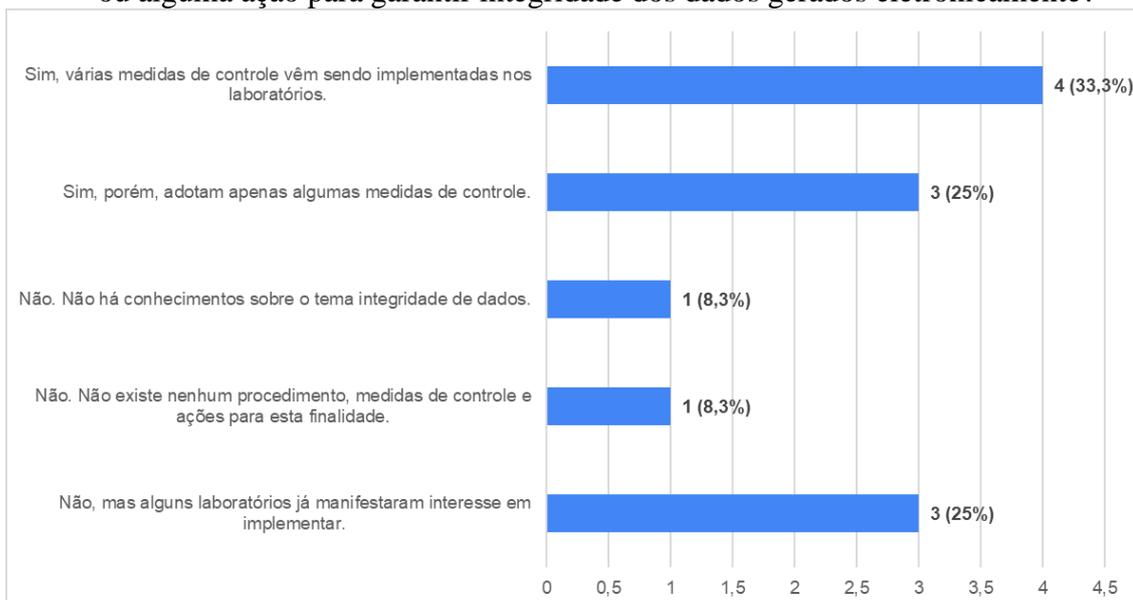
Dos 12 (100%) gestores da área da Qualidade, apenas 05 (41,7%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos tanto a direção quanto os gerentes de laboratórios têm ciência da relevância e importância do tema integridade de dados eletrônico; 03 (25%) responderam que não existe essa ciência e que não há conhecimento sobre

o tema; 02 (16,7%) responderam que não existe essa ciência por parte da direção e/ou das gerências de laboratório, mas que a área de gestão da qualidade planeja disseminar a importância e as consequências da não adesão; e 02 (16,7%) gestores responderam que em parte existe a ciência da relevância e importância sobre o tema, porém, não há prioridade no tema por falta de recursos financeiros e/ou pessoal capacitado para implementar o tema.

Os resultados demonstram que 58,3% das unidades ou escritórios que participaram desta pesquisa não têm ciência da relevância e importância sobre o tema integridade de dados e que sua não implementação seguindo medidas de controles organizacionais, operacionais e técnicos podem contribuir para os riscos de falhas e/ou adulteração de dados, tanto por erros humanos ou por má conduta.

Para WHO (2016), a liderança institucional é essencial para estabelecer e manter um compromisso de toda a instituição com a confiabilidade dos dados como um elemento essencial do sistema de qualidade. Já a gerência sênior tem a responsabilidade final de assegurar que um sistema de qualidade eficaz esteja implementado objetivando alcançar os objetivos de qualidade e que os papéis, responsabilidades e autoridades, incluindo aqueles necessários para os programas de governança de dados eficazes, sejam definidos, comunicados e implementados em toda a organização.

Q19. Os laboratórios com atividades de ensaio, plataformas tecnológicas e/ou de pesquisas experimentais básica e/ou aplicada adotam procedimentos, medidas de controle ou alguma ação para garantir integridade dos dados gerados eletronicamente?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 12 (100%) gestores da área da Qualidade, apenas 04 (33,3%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos existe adoção de procedimentos, medidas de controles ou demais ações com objetivo de garantir a integridade dos dados gerados eletronicamente; 03 (25%) responderam que nas suas respectivas unidades ou escritórios existe a adoção, porém de apenas algumas medidas de controles; 05 (41,7%) responderam que suas respectivas unidades ou escritórios não adotam nenhum procedimento, medidas de controles ou ações para garantir a integridade dos dados eletrônico, porém, destes 05, 03 (25%) responderam que em sua unidade ou escritório alguns laboratórios já manifestaram interesse em implementar, e 01 (8,3%) respondeu que em sua unidade ou escritório não existe nenhum procedimento, medidas de controles ou ações para esta finalidade e o último gestor respondeu que em sua unidade ou escritório não existe conhecimento sobre o tema integridade de dados.

Os 04 gestores que responderam de forma positiva a esta pergunta, 02 especificaram as respectivas áreas de atuações destes laboratórios, tais como:

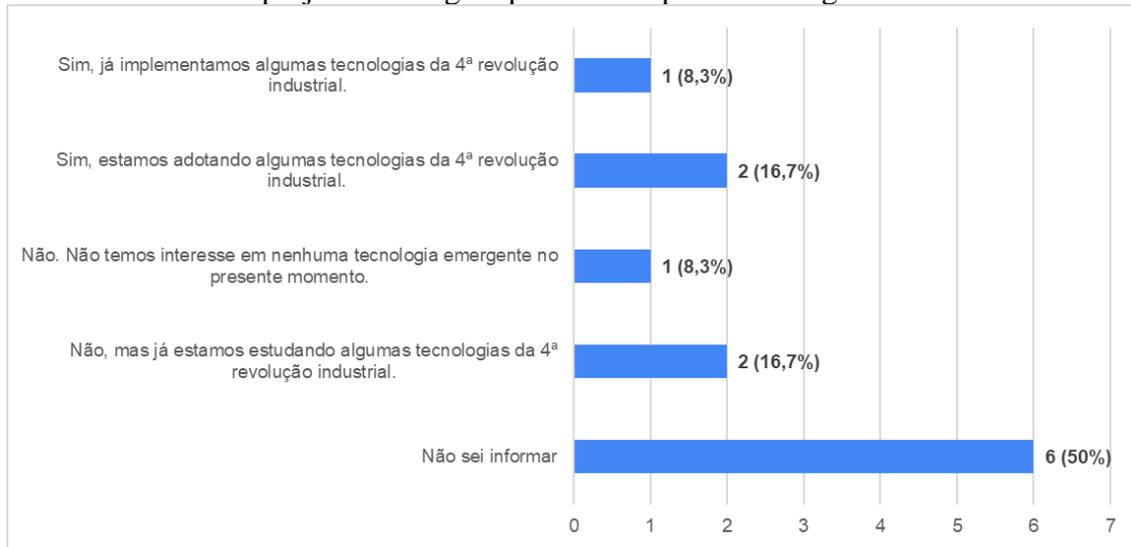
- Laboratório de Controle de Qualidade e Desenvolvimento e Validação analítica;
- O foco principal da atuação dos laboratórios é o controle de qualidade de produtos da área de saúde

WHO (2016), menciona em seu guia de boas práticas em gerenciamento de dados que a ausência de medidas organizadas, se não forem robustamente implementadas podem impactar na confiabilidade e integridade dos dados eletrônicos e prejudicar a robustez da tomada de decisões com base nesses registros de dados gerados, pois impedem diretamente que dados eletrônicos sejam seguros, atribuíveis, legíveis, rastreáveis, permanentes, gravados contemporaneamente, originais e precisos.

Perfil IV – Gestão e compartilhamento de dados

Quanto à gestão e compartilhamento de dados das unidades técnico-científicas ou escritórios técnicos, sob a percepção dos gestores da área da Qualidade pesquisados, foram obtidos os seguintes resultados:

Q20. Existe(m) na unidade/escritório técnico a adoção de tecnologia(s) emergente(s) como projeto estratégico para inovar processos organizacionais?

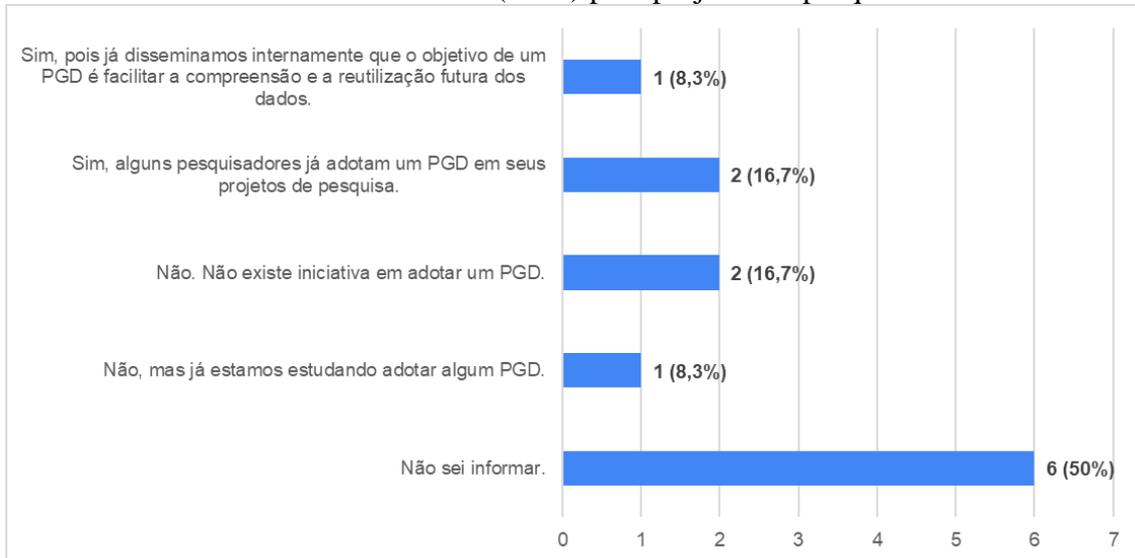


Fonte: Elaboração própria a partir dos questionários (2021).

Dos 12 (100%) gestores da área da Qualidade, apenas 01 (8,3%) respondeu que em sua respectiva unidade técnico-científica ou escritório técnico existe a adoção de tecnologia(s) emergente(s) como projeto estratégico para inovar processos organizacionais e que já implementaram algumas das tecnologias da 4ª revolução industrial. 02 (16,7%) gestores responderam que em suas respectivas unidades ou escritórios estão adotando algumas tecnologias da 4ª revolução industrial; 06 (50%) responderam não saber informar da adoção de alguma tecnologia emergente em suas respectivas unidades ou escritórios; 02 (16,7%) responderam que não adotam nenhuma tecnologia emergente, mas que estão estudando algumas das tecnologias da 4ª revolução industrial; e 01 (8,3%) gestor respondeu que em sua unidade ou escritório não há adoção de nenhuma tecnologia emergente e que não há o interesse em nenhuma tecnologia emergente no presente momento.

Dos 12 gestores da área da Qualidade que participaram da pesquisa, 04 (33,3%) comentaram na resposta da questão 20 quais são as tecnologias emergentes que estão sendo implementadas ou já se encontram implementadas em suas respectivas unidades ou escritórios, abordando ser um projeto com Internet das Coisas (IoT) para monitoramento de temperatura e umidade; que possuem projeto estratégico em andamento para implementação do livro de registros eletrônico; outro gestor comentou que na verdade não há uma opção que atenda. A aplicação de tecnologias emergentes é de interesse, mas ainda não está formalizada como projeto estratégico institucional. Com recursos escassos (financeiros e humanos) a absorção de novas tecnologias, como automação e inteligência artificial, perde lugar para a "sobrevivência" dos processos e recursos em uso.

Q21. Sendo a Fiocruz uma instituição de CT&I em saúde, onde tem nas suas atividades a geração de conhecimento nesta área, sua unidade/escritório técnico adota algum Plano de Gestão de Dados (PGD) para projetos de pesquisa?



Fonte: Elaboração própria a partir dos questionários (2021).

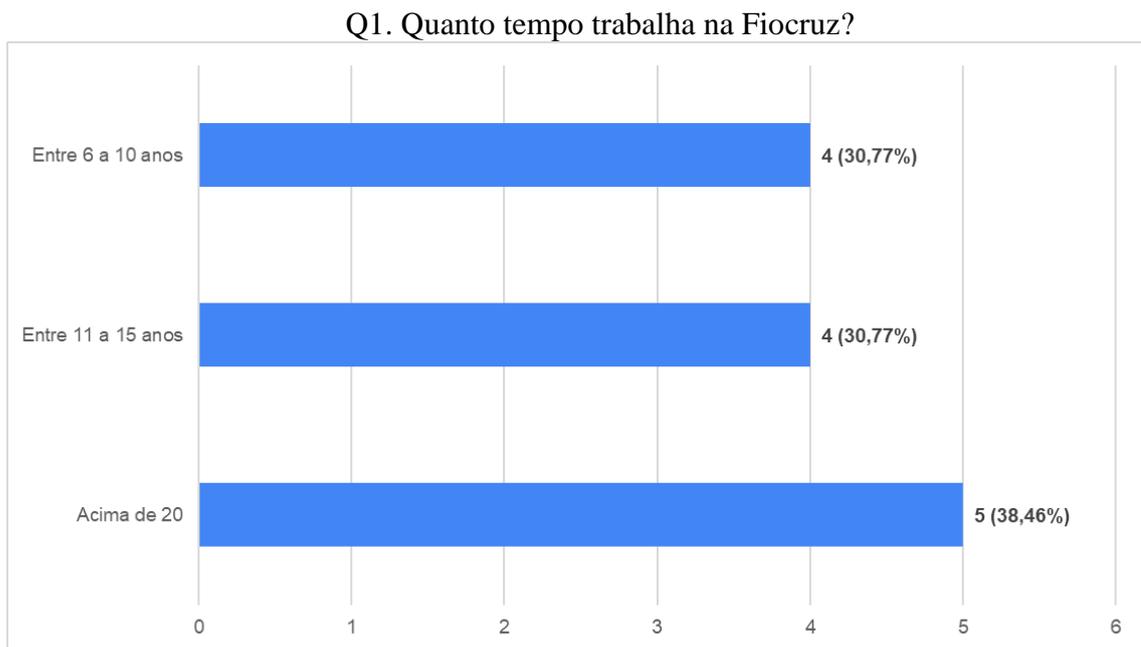
Dos 12 (100%) gestores da área da Qualidade, apenas 03 (25%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos a adoção de um Plano de Gestão de Dados (PGD) é uma realidade, sendo que 01 (8,3%) gestor respondeu que já disseminaram internamente em sua respectiva unidade ou escritório e que o objetivo de um PGD é facilitar a compreensão e a reutilização futura dos dados; 02 (16,7%) responderam que alguns pesquisadores em suas respectivas unidades ou escritórios já adotam um PGD em seus projetos de pesquisa; 06 (50%) responderam não saber informar se em suas respectivas unidades ou escritórios existe a adoção de algum PGD para projetos de pesquisa; 01 (8,3%) gestor respondeu que não adotam em sua unidade ou escritório, mas que já estão estudando adotar algum PGD; e 02 (16,7%) responderam que não adotam um PGD em suas respectivas unidades ou escritórios e que não existe iniciativa em adoção do PGD.

Uma das diretrizes para a pesquisa, descrita no guia de integridade em pesquisa da Fiocruz, menciona que o pesquisador ao elaborar um projeto de pesquisa ou participar efetivamente de um, independentemente da área de conhecimento, deverá organizar sempre um PGD para os dados produzidos e disponibilizados para acesso público uma vez que estejam em consonância com a Política de Gestão, Compartilhamento e Abertura de Dados para Pesquisa (FIOCRUZ, 2020).

Questionário 2: Questionário de integridade de dados em registros eletrônicos – TIC

Parte I – Perfil dos entrevistados

Quanto ao perfil dos gestores da área de TIC pesquisados, foram obtidos os seguintes resultados:



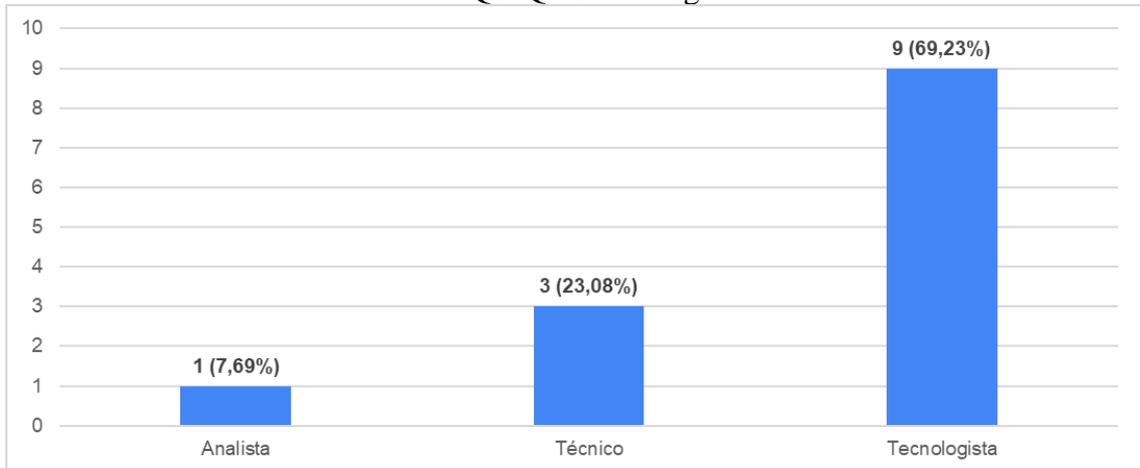
Fonte: Elaboração própria a partir dos questionários (2021).

Nenhum dos 13 gestores da área de TIC trabalha há menos de 05 anos na Fiocruz (0%); 04 trabalham entre 06 a 10 anos (30,8%); 04 trabalham entre 11 a 15 anos (30,8%) e 05 acima de 20 anos (38,5%). Destes, apenas 03 responderam, sendo um há 22 anos; outro há 33 anos e o terceiro há 35 anos e meio.

Dentro do universo pesquisado na Fiocruz, 09 (69,23%) gestores da área de TIC possuem mais de 10 anos de tempo de trabalho na instituição.

Portanto, o perfil dos respondentes da área de TIC das unidades técnico-científicas ou escritórios técnicos é caracterizado pelo predomínio de profissionais com mais de 10 anos na instituição e que na sua totalidade são servidores públicos, demonstrando alto conhecimento na área de gestão e processos de TIC.

Q2. Qual seu cargo?

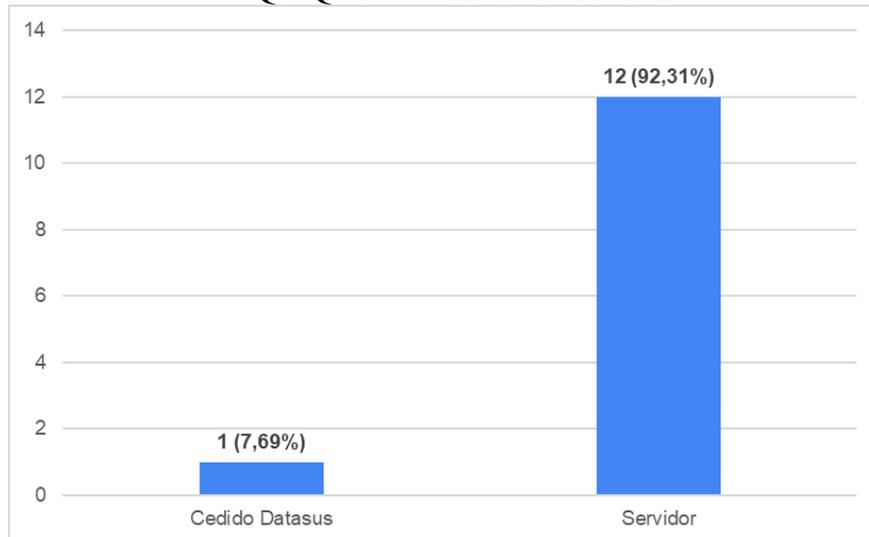


Fonte: Elaboração própria a partir dos questionários (2021).

Nenhum dos 13 gestores da área de TIC respondeu ter cargo de Assistente Técnico, de Pesquisador e nem de Especialista; 03 possuem cargo de Técnico (23,1%); 01 possui cargo de Analista (7,7%) e 09 possuem cargo de Tecnologista (69,2%).

Dentro do universo pesquisado, a maior representatividade na gestão da área de TIC corresponde ao cargo de Tecnologista (69,2%).

Q3. Qual seu vínculo na Fiocruz?



Fonte: Elaboração própria a partir dos questionários (2021).

Nenhum dos 13 gestores da área de TIC respondeu possuir vínculo Terceirizado. 12 (92,3%) responderam ter vínculo Servidor e 01 (7,69%) gestor respondeu ter o vínculo Servidor, mas especificando estar cedido pelo Datasus.

Dentro do universo pesquisado, a total representatividade na gestão da área de TIC é de servidores públicos (100%).

Q4. Em qual unidade ou escritório técnico você trabalha?

Os 13 gestores da área de TIC que responderam ao questionário marcaram respectivamente sua unidade técnico-científica ou escritório técnico que trabalhavam até o presente momento da pesquisa, porém, por medida de precaução e proteção do participante, os riscos foram mitigados mediante o total sigilo da identidade e dados pessoais dos participantes e, nesta questão específica, utilizaram-se códigos de identificação para representar cada unidade técnico-científica (UTC-X) e cada escritório técnico (ET-X), conforme tabela 13.

Tabela 13: Relação dos gestores da área de TIC por código de identificação que participaram da pesquisa

Unidades técnico-científicas - Código de identificação	Gestores da área de TIC que responderam o questionário
UTC-1	✓
UTC-2	✓
UTC-3	✓
UTC-4	✓
UTC-5	✓
UTC-6	
UTC-7	✓
UTC-8	✓
UTC-9	✓
UTC-10	✓
UTC-11	✓
UTC-12	✓
UTC-13	✓
Escritórios técnicos - Código de identificação	Gestores da área de TIC que responderam o questionário
ET-1	✓
ET-2	
ET-3	

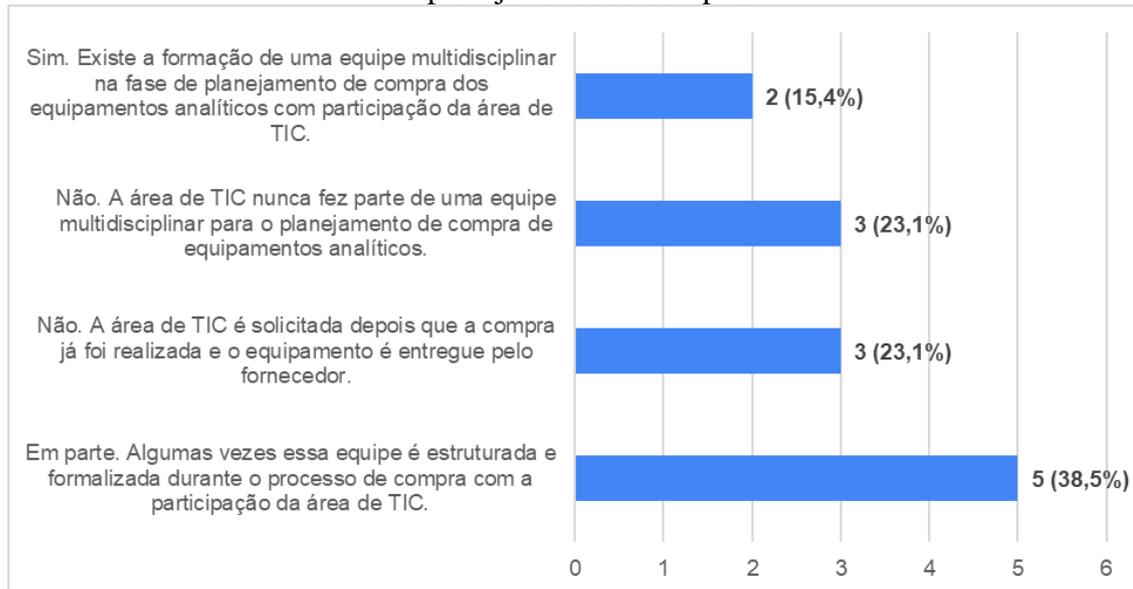
Fonte: Elaboração própria a partir dos questionários (2021).

Pode-se analisar que dos 16 (100%) gestores da área de TIC que receberam o convite para participar da pesquisa respondendo ao questionário, 12 (75%) responderam sob a percepção de suas respectivas unidades técnico-científicas e apenas 01 (6,25%) gestor respondeu sob a percepção de seu respectivo escritório técnico.

Parte II – Medidas de controles organizacionais

Quanto às medidas de controles organizacionais das unidades técnico-científicas ou escritórios técnicos, sob a percepção dos gestores da área de TIC pesquisados, foram obtidos os seguintes resultados:

Q5. Durante o processo de compra de equipamentos analíticos a área de TIC é solicitada para formar uma equipe multidisciplinar (pesquisador/técnico da área específica da pesquisa, profissionais de gestão da qualidade, TI, infraestrutura e equipamentos) para o planejamento de compras?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 02 (15,4%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos existe a formação de uma equipe multidisciplinar na fase de planejamento de compra dos equipamentos analíticos com a participação da área de TIC; 05 (38,5%) responderam que algumas vezes essa equipe multidisciplinar com a participação da área de TIC é estruturada e formalizada; 03 (23,1%) responderam que em suas respectivas unidades ou escritórios a área de TIC nunca fez parte de uma equipe multidisciplinar para o planejamento de compra de equipamentos analíticos; e 03 (23,1%) responderam que nas suas respectivas unidades ou escritórios a área de TIC é solicitada depois que a compra já foi realizada e o equipamento é entregue pelo fornecedor.

Nesta questão, 05 gestores acrescentaram comentários pertinentes que ajudam a aprofundar a percepção dos gestores de TIC quanto ao questionamento, tais como:

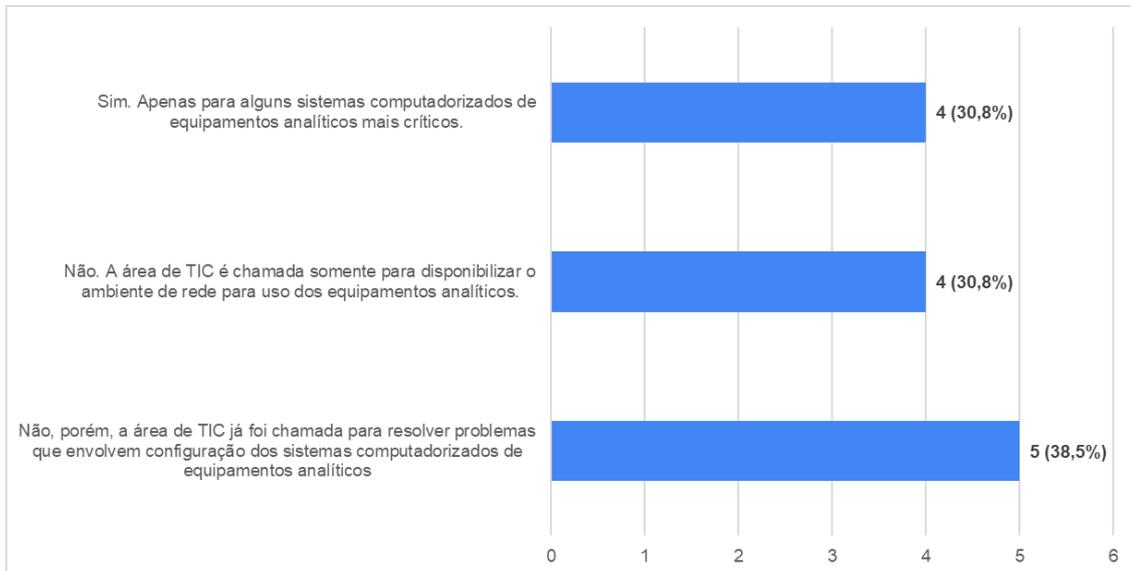
- Comentário 1: “A formação da equipe de planejamento de aquisição de TIC só iniciou em 2020 por exigência do governo. Antes a TIC não participava. Também se apenas o equipamento possuir um item que se enquadre como TIC”;

- Comentário 2: “Como proposta para solucionar esse problema seria interessante um questionário básico para evitar que a TIC não seja informada das compras. Perguntas como: Equipamento possui algum software/hardware que necessite de apoio de TIC?”;
- Comentário 3: “Há necessidade de ampliar o escopo de aquisição de materiais de TIC para os projetos de pesquisas que fogem desta obrigatoriedade”;
- Comentário 4: “Os usuários encaminhas suas demandas para a área de TIC e ela dispara o processo de aquisição”;
- Comentário 5: “Somente acionam a rede TIC quando necessitam de uma solução específica.”

Vale ressaltar que uma equipe multidisciplinar é importante dentro de um processo organizacional para discussão de assuntos relevantes e pertinentes a cada área envolvida, tanto diretamente quanto indiretamente ao uso do equipamento, pois especialmente na área de TIC, tratando-se de um equipamento analítico com uso de recursos de tecnologia da informação, assuntos que podem envolver a relevância e criticidade dos dados eletrônicos a serem gerados no equipamento a ser comprado podem ser abordados, tais como:

- Se a localização física do equipamento analítico possui rede elétrica estabilizada;
- Se o equipamento será acompanhado de um nobreak com potência adequada para a carga elétrica a ser gerada pelo equipamento analítico;
- Se o sistema computadorizado possui funcionalidades de *Audit Trail* (trilha de auditoria), *compliance*, configuração de perfis de usuário e/ou grupos;
- Se o volume de dados a ser gerado com objetivo de avaliar se na infraestrutura atual de TIC da unidade ou escritório possui um dispositivo de armazenamento com capacidade de crescimento para atender o armazenamento dos dados eletrônicos, entre outros.

Q6. A área de TIC participa de alguma fase de treinamento que é dado pelo fabricante do equipamento analítico quando da instalação e configuração dentro dos laboratórios da sua unidade/escritório?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, nenhum respondeu que a área de TIC da sua respectiva unidade técnico-científica ou escritório técnico sempre é uma área participante de treinamentos que envolvem a instalação e configuração dos sistemas computadorizados de equipamentos analíticos; 04 (30,8%) responderam que em suas respectivas unidades ou escritórios a área de TIC participa de treinamentos apenas para alguns sistemas computadorizados de equipamentos analíticos mais críticos; 04 (30,8%) responderam que a área de TIC é chamada somente para disponibilizar o ambiente de rede para uso dos equipamentos analíticos; e 05 (38,5%) responderam que em suas respectivas unidades ou escritórios a área de TIC não participa da fase de treinamentos, porém, já foi chamada para resolver problemas que envolvem configuração dos sistemas computadorizados de equipamentos analíticos.

Observa-se que 69,2% das áreas de TIC não participam da fase de treinamentos que o fornecedor e/ou distribuidor dos equipamentos analíticos oferece aos técnicos, analistas e demais operadores quando o equipamento é instalado fisicamente nos laboratórios.

Um dos gestores que respondeu à questão Q6 fez um comentário abordando que equipamentos específicos de laboratório ficam fora do escopo de transferência de conhecimento devido à limitação da TIC no campo de atuação do laboratório.

Os resultados evidenciam que a área de TIC não é uma disciplina participante do processo de aquisição dos equipamentos analíticos e que não participa efetivamente dos treinamentos dados por fabricantes na fase de instalação e configuração dos equipamentos e seus respectivos sistemas computadorizados.

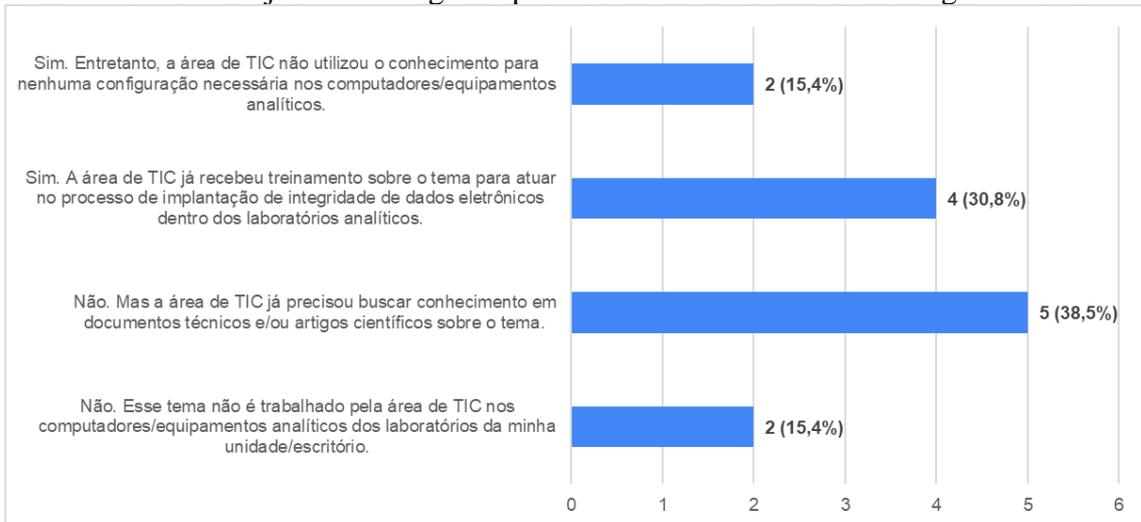
Pode ser considerada uma falha no processo de aquisição quando a área de TIC não é integrada durante a fase de instalação e configuração de um equipamento, pois a área específica de TIC da unidade ou escritório passa a desconhecer tecnicamente procedimentos, configurações importantes, além de deixar de criar documentações como procedimentos operacionais padrão (POP) e/ou instruções de trabalho (IT) que contribuam para a gestão de documentos e conhecimento da própria unidade ou escritório.

Muitas áreas de TIC são convidadas apenas para disponibilizar infraestrutura de rede para uso dos equipamentos analíticos ou para resolver dificuldades de configuração dos sistemas computadorizados. Portanto, perde-se aí uma grande oportunidade de integrar a área de TIC aos processos de gestão de equipamentos e sistemas computadorizados nos laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica e/ou aplicada na Fiocruz.

Segundo WHO (2016), fatores como estes acima podem-se configurar como falhas das organizações em aplicar sistemas robustos que inibem riscos de dados, pois dificultam na melhoria da detecção de situações em que a confiabilidade dos dados pode ser comprometida e/ou investigar e solucionar as causas raiz quando surgem falhas.

Ainda segundo WHO (2016), aplicar controles contribuem para o desenvolvimento e fortalecimento que podem garantir boas estratégias de gerenciamento de dados, como: treinamento das pessoas que utilizam sistemas computadorizados e analisam os dados eletrônicos no entendimento básico de como os sistemas computadorizados funcionam e na implementação e confirmação durante a validação de sistemas informatizados e subsequente controle de mudanças, que todos os controles necessários para as boas práticas de documentação de dados eletrônicos estão em vigor e que a probabilidade da ocorrência de erros nos dados é minimizada.

Q7. Familiaridade com o tema integridade de dados: a) A área de TIC da sua unidade/escritório já recebeu algum tipo de treinamento formal em integridade de dados?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 04 (30,8%) responderam que possuem familiaridade com o termo integridade de dados através da obtenção de algum tipo de treinamento formal e que suas respectivas unidades ou escritórios técnicos já iniciaram o processo de implantação de integridade de dados eletrônicos; 02 (15,4%) responderam que possuem familiaridade com o termo integridade de dados através da obtenção de algum tipo de treinamento formal, porém, não utilizaram até o momento da participação da pesquisa o conhecimento em nenhuma configuração necessária para implantação de integridade de dados em computadores/equipamentos analíticos; 07 (53,8%) responderam que não possuem familiaridade com o termo integridade de dados através de algum tipo de treinamento formal, porém, destes, 05 (38,5%) responderam que a área de TIC das suas respectivas unidade ou escritórios precisaram buscar conhecimento sobre o termo através de documentos técnicos e/ou artigos científicos sobre o tema e, 02 (15,4%) destes gestores, responderam que não possuem familiaridade com o termo integridade de dados através de algum tipo de treinamento formal e que o tema não é trabalhado pelas suas respectivas áreas de TIC nos computadores/equipamentos analíticos dos laboratórios da unidade ou escritório técnico.

Um dado muito interessante acerca da importância do tema integridade de dados eletrônicos, é que 38,5% das áreas de TIC precisaram buscar conhecimento sobre integridade de dados em documentos técnicos e/ou artigos, o que mostra que a aplicação de medidas de controles operacionais e técnicos são cada mais vez mais necessárias para mitigar os riscos iminentes de segurança dos dados eletrônicos gerados por equipamentos analíticos nos laboratórios da Fiocruz objeto desta pesquisa.

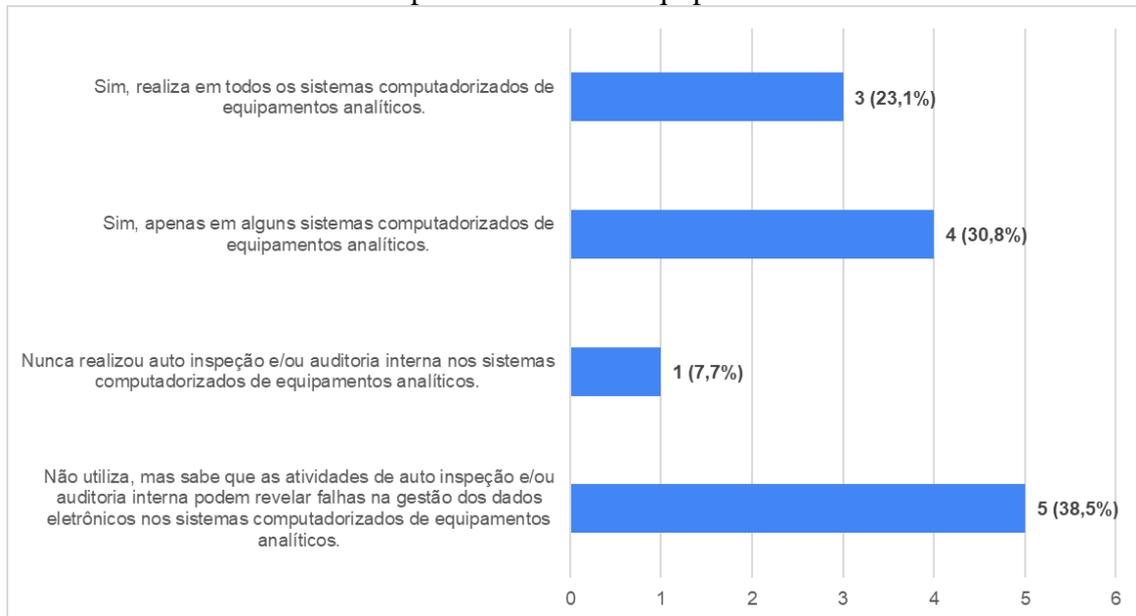
A área de TIC, bem como todos os colaboradores da unidade ou escritório devem ser treinados em políticas de integridade de dados – sejam estas para dados físicos e/ou eletrônicos – e concordar em obedecê-las, cabendo as áreas da Qualidade e Recursos Humanos assegurar que as pessoas sejam treinadas para entender e distinguir entre a conduta apropriada e imprópria, incluindo a falsificação deliberada, e deve estar ciente das possíveis consequências (WHO, 2016).

WHO (2016) recomenda, ainda, a importância do treinamento em medidas para prevenir e detectar problemas nos dados para pessoas chave como gerentes de laboratórios, supervisores, área da qualidade dentre outros. São treinamentos específicos que abordam a validação das configurações de parâmetros e, como trilhas de auditoria, para sistemas informatizados individuais usados na geração, processamento e geração de relatórios de dados eletrônicos.

Somente com pessoas treinadas e seguindo as boas práticas de documentação para dados físicos e eletrônicos será possível garantir integridade dados e que esses princípios contribuam para que os dados tenham as características de ser atribuível, legível, contemporâneo, original e acurado (ALCOA) (WHO, 2016).

A ausência de treinamento e obtenção de conhecimento pela área de TIC junto aos sistemas computadorizados dos equipamentos analíticos é um problema crítico para a implementação e garantia da integridade dos dados eletrônicos gerados em laboratórios, pois as medidas de controles operacionais e técnicos necessárias para que o princípio da ALCOA (dados atribuíveis, legíveis, contemporâneos, originais e acurados) sejam compreendidos e aplicados às atividades inerentes, dificilmente serão implementados nestes equipamentos no momento em que um técnico do fornecedor/distribuidor instalar e configurar os equipamentos, além de treinar os usuários.

Q8. A unidade/escritório possui alguma rotina de autoinspeção e/ou auditoria interna que avalie periodicamente a efetividade e aplicabilidade de segurança da informação dos sistemas computadorizados de equipamentos analíticos?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 03 (23,1%) responderam que em suas respectivas unidades técnico-científica ou escritórios técnicos possui alguma rotina de autoinspeção e/ou auditoria interna para avaliar periodicamente a efetividade e aplicabilidade de segurança da informação em todos os sistemas computadorizados de equipamentos analíticos; 04 (30,8%) responderam que existe uma rotina periódica de auditoria ou autoinspeção, porém, apenas em alguns sistemas computadorizados de equipamentos analíticos; 05 (38,5%) responderam que em suas respectivas unidades ou escritórios não utilizam a atividade de auditoria e/ou autoinspeção para avaliar a efetividade e aplicabilidade de segurança da informação dos sistemas computadorizados de equipamentos analíticos, porém, reconhecem que a atividade pode revelar falhas na gestão dos dados eletrônicos nos sistemas. 01 (7,7%) respondeu que em sua unidade ou escritório nunca foi realizada uma atividade de auditoria interna e/ou autoinspeção nos sistemas computadorizados de equipamentos analíticos.

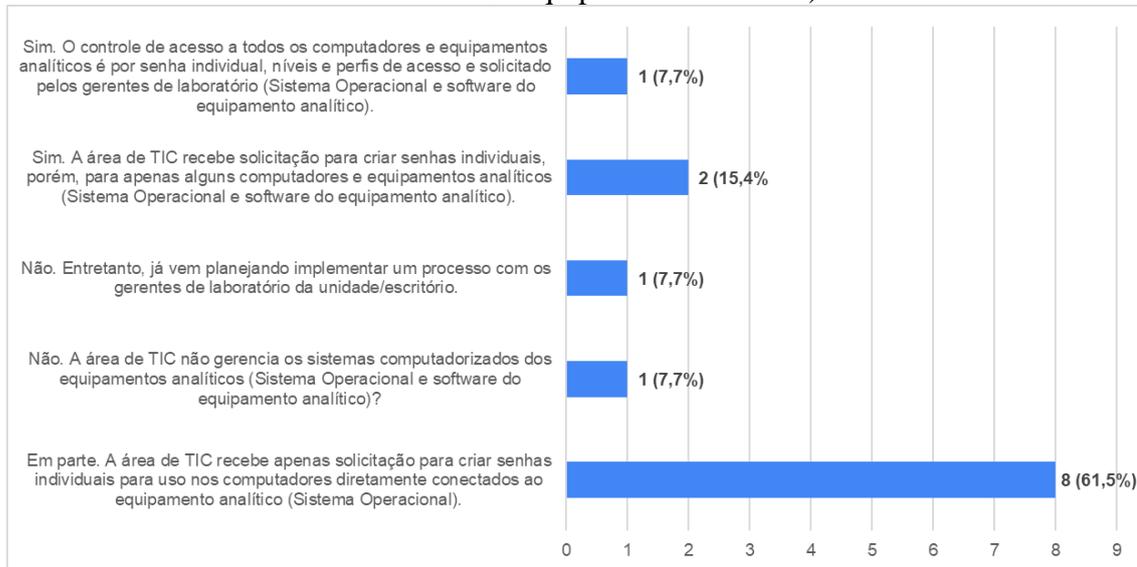
Seis gestores da área de TIC representando 46,2% das unidades ou escritórios não possuem alguma rotina de autoinspeção e/ou auditoria interna para avaliar periodicamente a efetividade e aplicabilidade de segurança da informação dos sistemas computadorizados de equipamentos analíticos.

Portanto, uma rotina de auditoria interna e/ou autoinspeção de sistemas computadorizados, seguindo determinados procedimentos e pontos chave de atenção, devem ser estabelecidos dentro das unidades ou escritórios que não realizam, pois segundo WHO

(2016), estas ações podem revelar falhas nos controles de segurança que inadvertidamente permitem que o pessoal do laboratório acesse e altere potencialmente os registros de data/hora, além de contribuir na conscientização da administração sobre a necessidade de alocar recursos para melhorar os controles de validação de sistemas computadorizados.

Adotar um processo de auditoria não é apenas uma atividade de identificar e registrar os defeitos e problemas em uma organização, mas sim uma ação importante que deve ser considerada como uma forma de contribuir positivamente às estratégias organizacionais da organização (LAUREANO, 2005).

Q9. A área de TIC da sua unidade/escritório possui algum processo estabelecido (POP, política interna etc.) para receber dos gerentes de laboratório a solicitação formalizando a criação de senha individual para uso nos equipamentos analíticos (Sistema Operacional e software do equipamento analítico)?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 01 (7,7%) respondeu que em sua respectiva unidade técnico-científica ou escritório técnico existe um procedimento estabelecido e formalizado para solicitação de criação de usuários e senhas individuais para acesso aos equipamentos analíticos (sistema operacional e software do equipamento analítico) e que este controle é realizado para todos os computadores e equipamentos analíticos em laboratório. 02 (15,4%) responderam que em suas unidades ou escritórios existe um procedimento estabelecido e formalizado, porém, a área de TIC recebe a solicitação para apenas alguns computadores e equipamentos analíticos de laboratórios; 08 (61,5%) responderam que em suas unidades ou escritórios o procedimento funciona em parte, pois a área de TIC recebe apenas solicitação para criar senhas individuais para uso nos computadores diretamente conectados ao equipamento

analítico (Sistema Operacional), ou seja, o controle de acesso aos softwares que gerenciam os equipamentos analíticos não é feito ou realizado pela área de TIC; 01 (7,7%) respondeu que em sua unidade ou escritório não existe o procedimento formalizado e estabelecido, mas que a área de TIC já vem planejando implementar um processo com os gerentes de laboratório da unidade/escritório; 01 (7,7%) respondeu que em sua unidade ou escritório não existe procedimento formalizado e estabelecido e que sua área de TIC não gerencia os sistemas computadorizados dos equipamentos analíticos (Sistema Operacional e software do equipamento analítico) existentes nos laboratórios.

Das 13 unidades técnico-científicas ou escritórios técnicos participantes da pesquisa, podemos analisar com os dados acima que apenas 03 unidades ou escritórios (23,1%) possuem processo formalizado e estabelecido para criação de usuários e senhas de acesso aos equipamentos analíticos através da solicitação feita por gerentes de laboratórios.

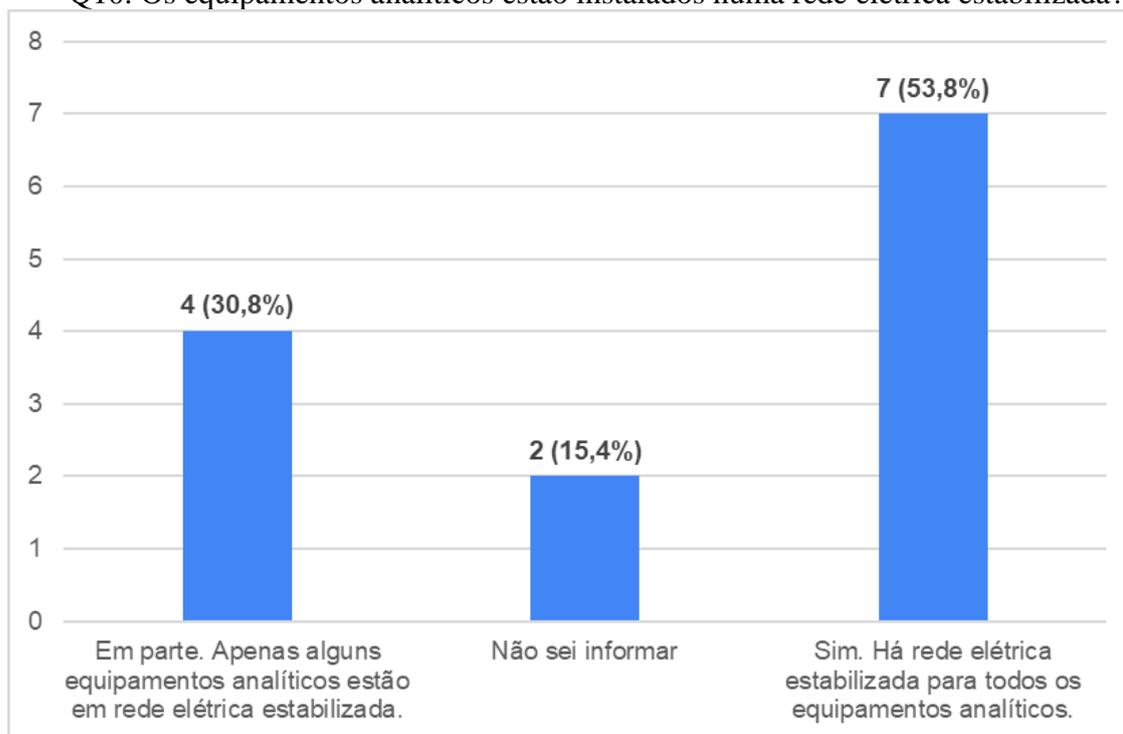
Estabelecer essa medida de controle apenas para o sistema operacional dos computadores diretamente conectados aos equipamentos analíticos permitirá que um determinado dado somente poderá ser atribuível dentro dos princípios ALCOA quando gerado pelo sistema operacional, porém, não aplicando esta mesma medida nos sistemas computadorizados dos equipamentos analíticos não será possível vincular os usuários às ações que criam, modificam ou excluem dados a partir dos sistemas dos equipamentos e, portanto, não atendendo às diretrizes e princípios de gerenciamento de dados, o que possibilita configurações inapropriadas, além de alterações de dados ou metadados sem autorização.

Para WHO (2016), quando os sistemas computadorizados são usados para gerar dados eletrônicos, deve ser possível associar todas as alterações aos dados com as pessoas que fazem essas alterações, e essas alterações devem ter registro de data e hora e a razão para a alteração registrada, quando aplicável.

Parte III – Medidas de controles operacionais

Quanto às medidas de controles operacionais das unidades técnico-científicas ou escritórios técnicos, sob a percepção dos gestores da área da TIC pesquisados, foram obtidos os seguintes resultados:

Q10. Os equipamentos analíticos estão instalados numa rede elétrica estabilizada?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 02 (15,4%) responderam não saber informar se em suas respectivas unidades técnico-científicas ou escritórios técnicos os equipamentos analíticos estão ligados em rede elétrica estabilizada; 04 (30,8%) responderam que em suas respectivas unidades ou escritórios apenas alguns equipamentos analíticos estão em rede elétrica estabilizada e 07 (53,8%) responderam que todos os equipamentos analíticos em suas respectivas unidades ou escritórios estão ligados em rede elétrica estabilizada.

Das unidades técnico-científicas ou escritórios técnicos participantes desta pesquisa, mais de 50% possuem e disponibilizam rede elétrica estabilizada para uso dos equipamentos analíticos em suas instalações.

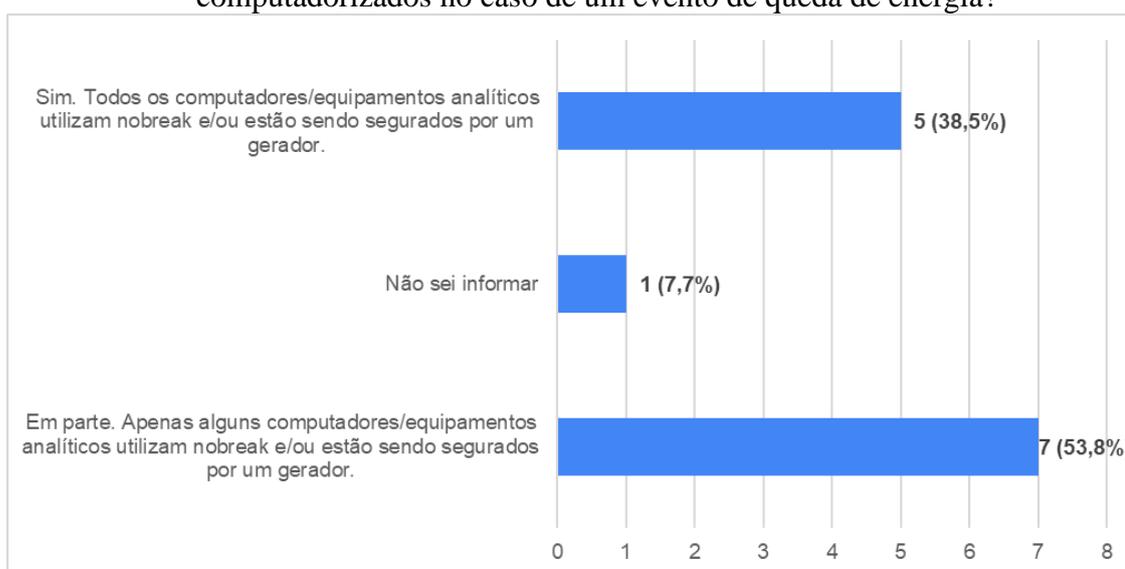
Considerando que a Fiocruz é uma instituição centenária e possui muitas edificações antigas e que ao longo das décadas já passou por mudanças estruturais justamente para atender ao crescimento das unidades e escritórios, o percentual de unidades ou escritórios que disponibilizam rede elétrica estabilizada para uso dos equipamentos analíticos nos laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica e/ou aplicada é bom, pois está acima de 50% quando consideramos que em 07 unidades ou escritórios são todos os equipamentos analíticos usados em rede elétrica estabilizada e mais de 80% se considerarmos as outras 04 unidades ou escritórios que parte dos equipamentos existentes nas unidades ou escritórios estão instalados em uma rede elétrica estabilizada.

O uso de rede elétrica estabilizada contribui para a redução de riscos de perda de dados eletrônicos, pois as instalações elétricas estabilizadas são recomendadas para ambientes computacionais que tenham equipamentos funcionando constantemente e que não podem ser desligados inesperadamente, pois a queda e o retorno repentinos de eletricidade podem comprometer a operação de alguns equipamentos e até mesmo danificá-los, além de contribuir para o risco de corromper dados eletrônicos.

WHO (2016) em seu guia menciona que um dos exemplos de controles que podem exigir desenvolvimento e fortalecimento para garantir boas estratégias de gerenciamento de dados podem incluir:

- Monitoramento de processos e alocação dos recursos necessários pela administração com objetivo de garantir e melhorar a infraestrutura, o que envolve:
 - Garantir projeto e manutenção adequados de edifícios, instalações, equipamentos e sistemas;
 - Garantir energia confiável adequada e abastecimento de água;
 - Garantir o fornecimento de treinamento necessário para os funcionários;
 - Entre outros.

Q11. Os equipamentos analíticos estão protegidos com uso de nobreak e/ou gerador com objetivo de minimizar o risco da perda de dados eletrônicos gerados pelos sistemas computadorizados no caso de um evento de queda de energia?



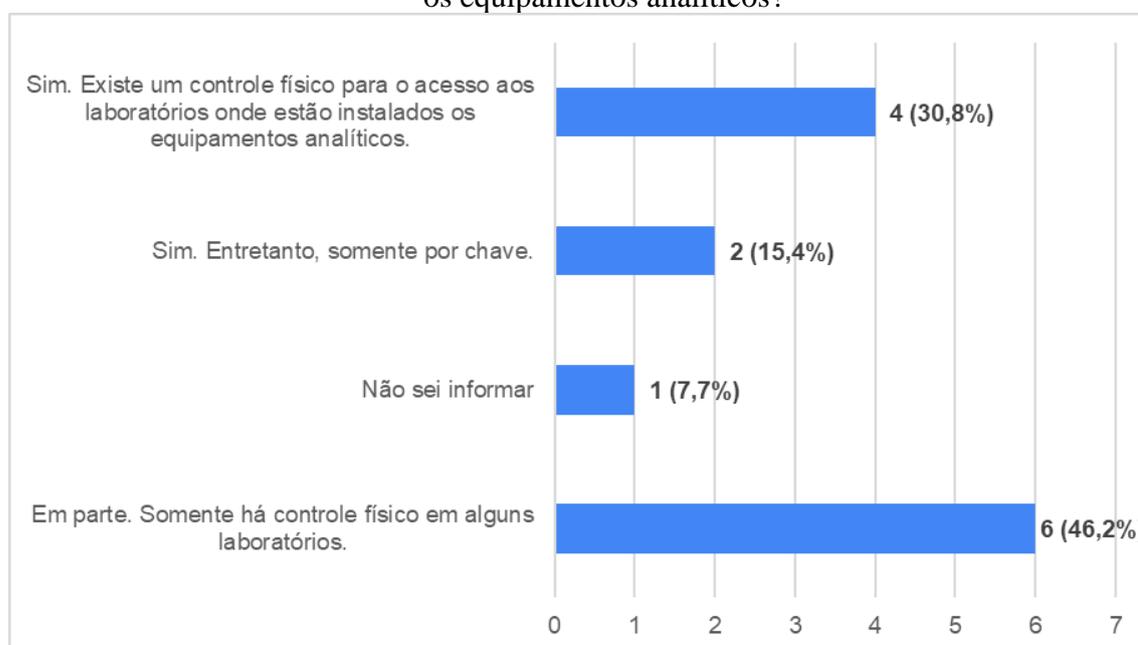
Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 01 (7,7%) respondeu não saber informar se em sua respectiva unidade técnico-científica ou escritório técnico os equipamentos analíticos estão

protegidos pelo uso de nobreak e/ou gerador; 05 (38,5%) responderam que em suas respectivas unidades ou escritórios todos os equipamentos analíticos estão usando nobreak e/ou gerador e 07 (53,8%) responderam que nas suas unidades ou escritórios apenas alguns computadores/equipamentos analíticos utilizam nobreak e/ou gerador com objetivo de mitigar os riscos de perda de dados eletrônicos gerados pelos sistemas computadorizados de equipamentos analíticos no caso de um incidente de queda de energia.

Das unidades técnico-científicas ou escritórios técnicos participantes desta pesquisa, apenas 38,5% possuem todos os seus sistemas computadorizados de equipamentos analíticos protegidos contra o risco de perda de dados através do uso de nobreak e/ou gerador.

Q12. Existe algum controle de acesso físico no laboratório onde se encontram instalados os equipamentos analíticos?



Fonte: Elaboração própria a partir dos questionários (2021).

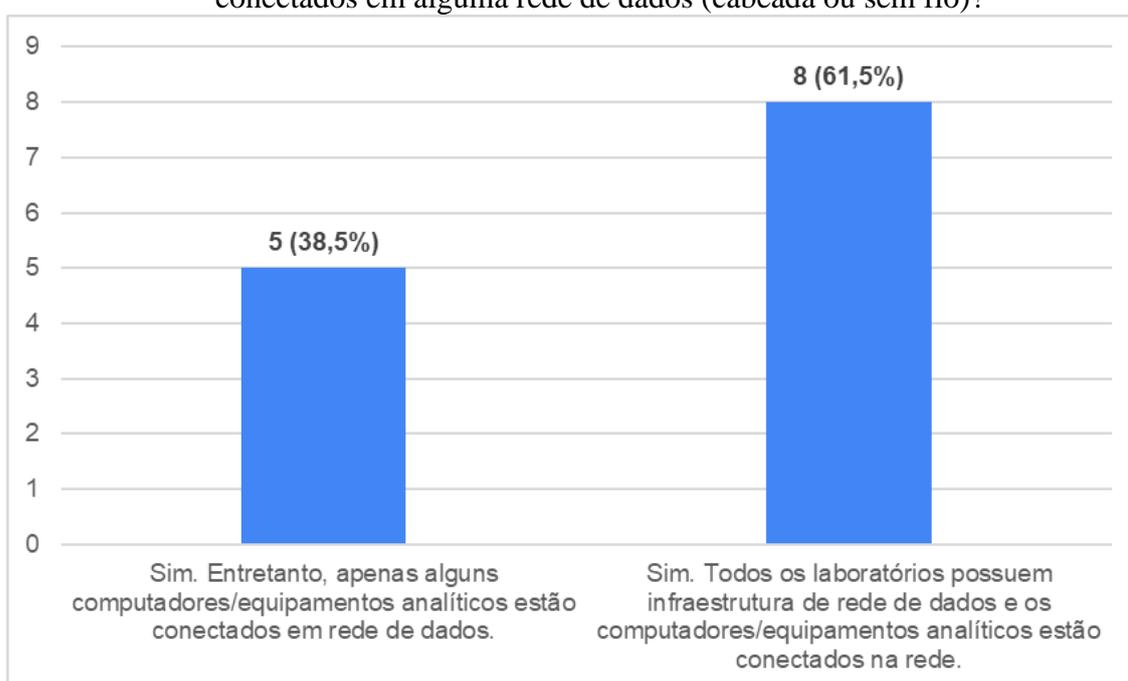
Dos 13 gestores da área de TIC, apenas 01 (7,7%) respondeu não saber informar se existe em sua respectiva unidade técnico-científica ou escritório técnico um controle físico no laboratório onde se encontram instalados os equipamentos analíticos; 02 (15,4%) responderam que em suas unidades ou escritórios existe controle físico, porém, somente por chave; 04 (30,8%) responderam que em suas unidades ou escritórios existe controle de acesso físico nos laboratórios onde estão instalados os equipamentos analíticos; e 06 (46,2%) responderam que em suas respectivas unidades ou escritórios o controle de acesso físico existe somente em alguns laboratórios.

De acordo com os resultados obtidos em relação ao controle físico existente para acesso aos laboratórios onde se encontram instalados os equipamentos analíticos, foi possível observar que mais de 80% das unidades ou escritórios da Fiocruz possuem implementado algum tipo de controle de acesso físico aos laboratórios. Com esses dados é possível concluir que já existe ao menos um nível de proteção no acesso aos laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica e/ou aplicada da Fiocruz, possibilitando um controle no acesso de pessoas não autorizadas.

Segundo Sêmola (2003), existem três aspectos que podem ser classificados dentro da gestão da segurança da informação: o tecnológico, o físico e o humano e que as investidas de ameaças a todo instante são riscos iminentes não somente para os negócios como, também, para seus processos e ativos físicos e que estas ameaças buscam encontrar algum ponto fraco compatível, uma vulnerabilidade que seja capaz de potencializar sua ação.

É importante que as unidades e escritórios da Fiocruz considerem as vulnerabilidades físicas existentes em seus ambientes, levantando os riscos e buscando soluções para correção ou mitigação destes riscos. Segundo Sêmola (2014), o acesso facilitado a ambientes de processamento de dados, a sua deficiência de controles de acesso em locais de armazenamento de informações confidenciais ou sensíveis etc. são exemplos de vulnerabilidades físicas.

Q13. Os equipamentos analíticos e/ou os computadores diretamente conectados estão conectados em alguma rede de dados (cabada ou sem fio)?



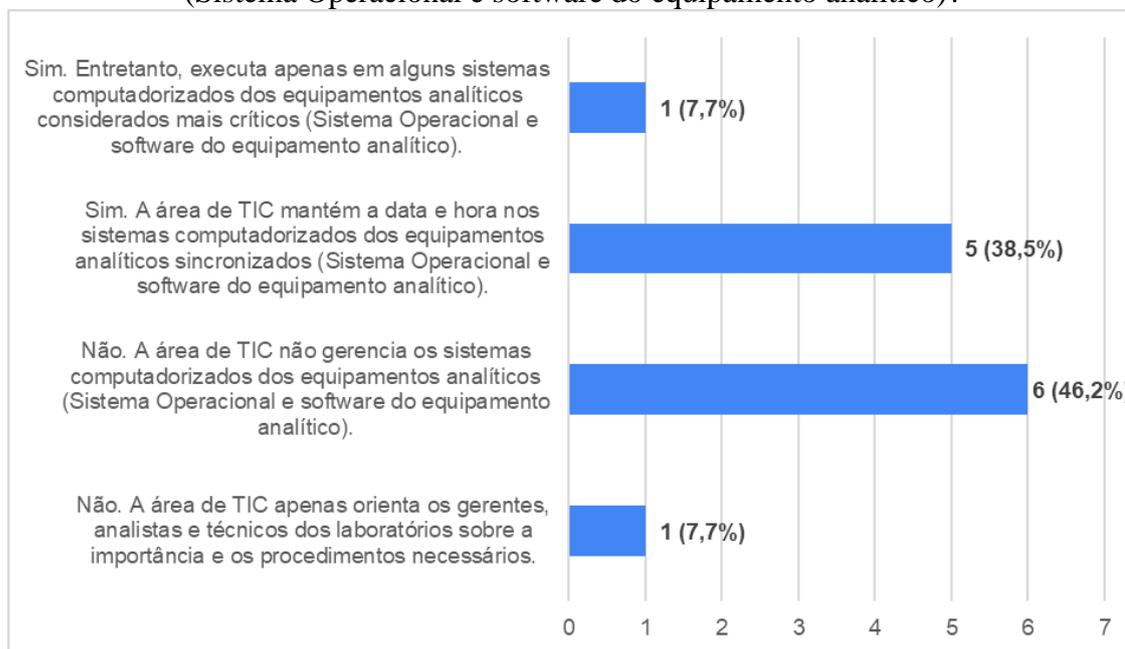
Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, 08 (61,5%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos todos os laboratórios possuem infraestrutura de rede de dados e que equipamentos analíticos e/ou computadores diretamente conectados a eles estão conectados na rede dados; e 05 (38,5%) responderam que em suas unidades ou escritórios apenas alguns equipamentos analíticos e/ou computadores diretamente conectados a eles estão conectados em rede de dados.

Esse percentual de disponibilidade de rede dados e de equipamentos conectados na rede de dados das unidades ou escritórios possibilita uma observação importante relacionada à segurança da informação quando analisados os dados da questão Q15 (Questionário – TIC), pois foi possível identificar que apenas 23,1% das áreas de TIC das unidades ou escritórios atualizam as versões dos sistemas operacionais de todos os computadores localizados nos laboratórios analíticos sempre que há novas atualizações disponíveis. Outras 53,8% áreas de TIC atualizam a versão do SO de apenas alguns computadores e outras 23,1% áreas de TIC não atualizam a versão do SO dos computadores por se tratar de computadores antigos e com versão de SO fora de suporte do fabricante.

Portanto, manter computadores antigos e com SO desatualizados e fora de qualquer suporte por parte dos fabricantes, conectados na rede dados da unidade ou escritório é um alto risco à segurança e integridade dos dados eletrônicos de pesquisa gerados pelos equipamentos analíticos conectados nestes computadores.

Q14. A área de TIC executa algum procedimento técnico para configurar e manter a sincronização de data e hora dos sistemas computadorizados dos equipamentos analíticos (Sistema Operacional e software do equipamento analítico)?



Fonte: Elaboração própria a partir dos questionários (2021).

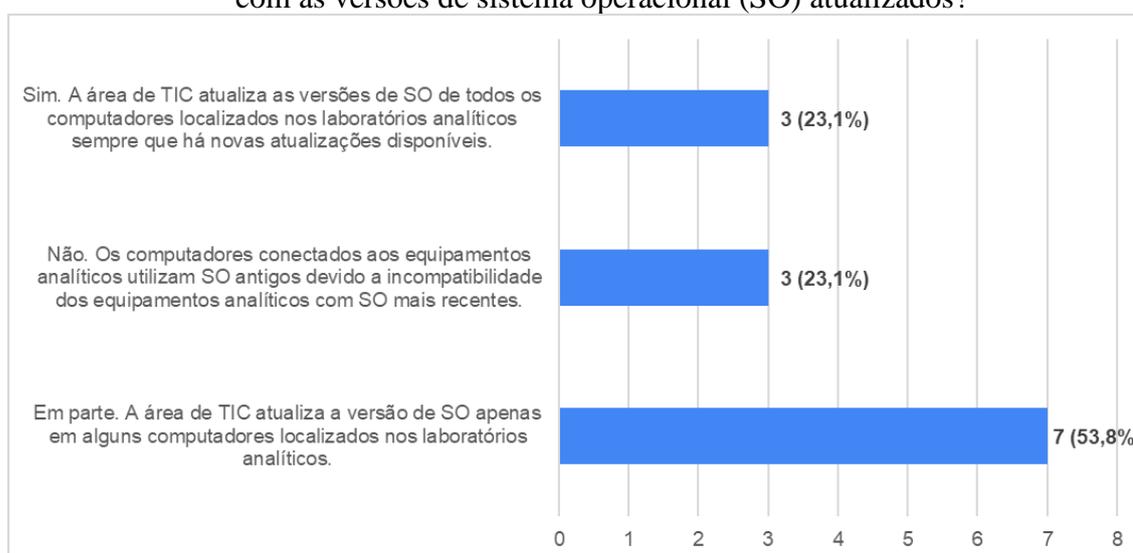
Dos 13 gestores da área de TIC, 05 (38,5%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos a área de TIC mantém a data e hora dos sistemas computadorizados dos equipamentos analíticos sincronizados; 01 (7,7%) respondeu que em sua unidade ou escritório a área de TIC apenas orienta os gerentes, analistas e técnicos dos laboratórios sobre a importância e os procedimentos necessários de manter a data e hora dos sistemas computadorizados sincronizados; 01 respondeu que em sua unidade ou escritório a área de TIC executa procedimento técnico para configurar e manter a sincronização de data e hora apenas dos sistemas computadorizados dos equipamentos analíticos considerados mais críticos; e 06 (46,2%) responderam que em suas respectivas unidades ou escritórios a área de TIC não gerencia os sistemas computadorizados dos equipamentos analíticos.

Outro risco iminente que pode comprometer a integridade dos dados eletrônicos gerados nos laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica e/ou aplicada da Fiocruz é observado em 53,8% das unidades ou escritórios quanto à ausência de procedimento técnico para configurar e manter a sincronização de data e hora dos sistemas computadorizados dos equipamentos analíticos, considerando tanto no SO como também no software do equipamento analítico, sendo que 46,2% deste percentual a área de TIC não gerencia os sistemas computadorizados dos equipamentos analíticos.

Para WHO (2016), dados contemporâneos são os dados registrados quando são gerados ou observados. Todavia, medidas de controles técnicos precisam ser estabelecidos e implementados para garantir que registros contemporâneos de ações ocorram apropriadamente, através de configurações que assegurem que registros de data e hora do sistema não possam ser alterados pelo usuário do computador/equipamento analítico, sendo possível por meio de:

- Procedimentos e programas de manutenção que garantem que os registros de data e hora sejam sincronizados entre as atividades nos equipamentos analíticos;
- e
- Controles que permitam a determinação do tempo de uma atividade em relação a outra, por exemplo, controles de fuso horário, entre outras configurações.

Q15. Todos os computadores diretamente conectados aos equipamentos analíticos estão com as versões de sistema operacional (SO) atualizados?



Fonte: Elaboração própria a partir dos questionários (2021).

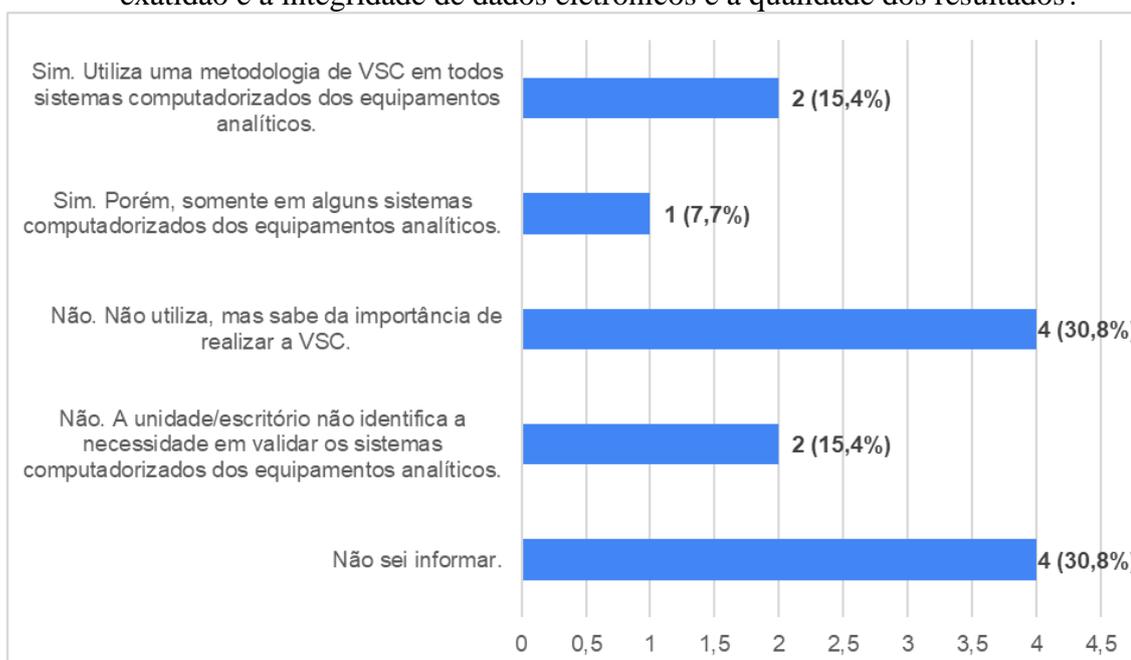
Dos 13 gestores da área de TIC, apenas 03 (23,1%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos os computadores conectados aos equipamentos analíticos utilizam sistemas operacionais antigos (desatualizados) devido à incompatibilidade dos equipamentos analíticos com sistemas operacionais mais recentes; 03 (23,1%) responderam que as suas unidades ou escritórios a área de TIC atualiza as versões de sistema operacional de todos os computadores localizados nos laboratórios analíticos sempre que há novas atualizações disponíveis; e 07 (53,8%) responderam que em suas respectivas unidades ou escritórios a área de TIC atualiza a versão do sistema operacional apenas em alguns computadores localizados nos laboratórios analíticos.

Atualizar os sistemas operacionais e os softwares que gerenciam os equipamentos analíticos é uma das principais medidas de controle técnico adotadas como práticas de manutenção para garantir a estabilidade, desempenho e a segurança dos computadores, pois diariamente novas ameaças são criadas com o objetivo de explorar falhas e vulnerabilidades dos sistemas desatualizados.

Considerando que apenas 23,1% das unidades ou escritórios participantes desta pesquisa mantêm o sistema operacional de todos os computadores diretamente conectados em equipamentos analíticos atualizados e que 53,8% das unidades ou escritórios mantêm apenas alguns computadores com o sistema operacional atualizados em seus laboratórios, é possível analisar o risco eminente da possibilidade de perda de dados por questões de segurança devido à ausência – parcial ou total – de atualização dos sistemas operacionais dos computadores diretamente conectados ao equipamentos analíticos. Este risco é ainda maior se estes mesmos computadores estão conectados na rede de dados da unidade ou escritório.

Portanto, conforme citado na literatura, a ausência de sistemas operacionais e softwares sem atualização, assim como outros componentes importantes, podem favorecer a ações não intencionais e trazer riscos à integridade dos dados eletrônicos de uma organização.

Q16. É utilizada alguma metodologia de Validação dos Sistemas Computadorizados (VSC) dos equipamentos analíticos com o objetivo de minimizar os riscos para garantir a exatidão e a integridade de dados eletrônicos e a qualidade dos resultados?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 02 (15,4%) responderam que suas respectivas unidades técnico-científicas ou escritórios técnicos utilizam uma metodologia de VSC em todos os sistemas computadorizados dos equipamentos analíticos; 01 (7,7%) gestor respondeu que sua unidade ou escritório usa uma metodologia de VSC somente em alguns sistemas computadorizados dos equipamentos analíticos; 04 (30,8%) responderam que em suas unidades ou escritórios não utilizam uma metodologia de VSC, porém, sabem da importância de se utilizar a mesma; 02 (15,4%) responderam que suas unidades não utilizam VSC e que não identificam necessidade em realizar a validação de sistemas computadorizados; e 04 (30,8%) responderam não saber informar se suas respectivas unidades ou escritórios utilizam alguma metodologia de VSC dos equipamentos analíticos.

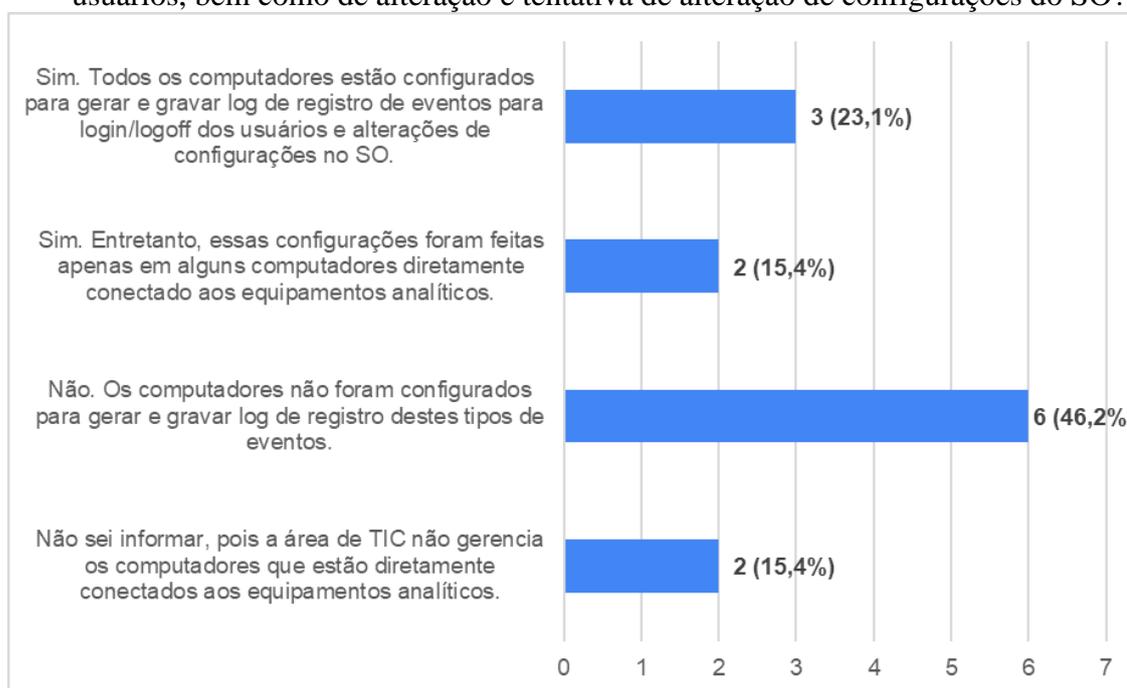
Mais de 76% das unidades ou escritórios participantes desta pesquisa não utilizam uma metodologia de validação de sistemas computadorizados nos equipamentos analíticos, pois observa-se que apenas 23,1% das unidades ou escritórios utilizam alguma metodologia de VSC nos equipamentos analíticos com o objetivo de minimizar os riscos para garantir a exatidão e a integridade de dados eletrônicos e a qualidade dos resultados gerados por sistemas computadorizados.

Segundo a ANVISA (2010), o gerenciamento e a validação de sistemas computadorizados auxiliam na exatidão e na integridade dos registros de dados e são essenciais para o ciclo de vida, por exemplo, de um produto ou serviço, desde a área de pesquisa, passando por estudos pré-clínicos e clínicos, produção e controle de qualidade até a área de armazenamento e distribuição.

Os sistemas devem ser validados para garantir sua integridade durante a transmissão entre os sistemas informatizados e para assegurar a integridade dos dados eletrônicos. A validação deve abordar os controles necessários para garantir a integridade dos dados do sistema (WHO, 2016).

Portanto, submeter os sistemas computadorizados que estão localizados nos laboratórios a processos de validação, incluindo funcionalidades de segurança da informação, controle de acesso e integridade de dados é importante, pois descreve atividades e responsabilidades que proporcionam a mitigação de riscos envolvendo a qualidade e a confiabilidade dos dados eletrônicos.

Q17. O SO dos computadores diretamente conectado aos equipamentos analíticos está configurado para gerar log de registro dos eventos relacionados à login/logoff dos usuários, bem como de alteração e tentativa de alteração de configurações do SO?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 03 (23,1%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos o SO de todos os computadores diretamente conectados nos equipamentos analíticos gera log de registro dos eventos relacionados à login/logoff dos usuários, bem como de alteração e tentativa de alteração de configurações do SO; 02 (15,4%) responderam que em suas unidades ou escritórios a configuração para gerar logs de registro de eventos para ações de login/logoff e tentativas de configurações no SO foram feitas apenas em alguns computadores diretamente conectados em equipamentos analíticos; 02 (15,4%) responderam não saber informar se estas configurações no SO para gerar logs de registro destes eventos foram efetuadas nos computadores diretamente conectados nos equipamentos analíticos em suas unidades ou escritórios; e 06 (46,2%) responderam que em suas unidades ou escritórios não foram configurados no SO dos computadores diretamente conectados aos equipamentos analíticos a geração dos logs de eventos das ações de login/logoff e das alteração e tentativa de alteração de configurações do SO.

Analisando os dados acima, pode-se identificar que das 13 unidades ou escritórios que participaram desta pesquisa, apenas 03 (23,1%) aplicaram esta medida de controle técnico no SO de todos os computadores diretamente conectados aos equipamentos analíticos e apenas 02 (15,4%) aplicam parcialmente em seu parque de computadores conectados aos equipamentos

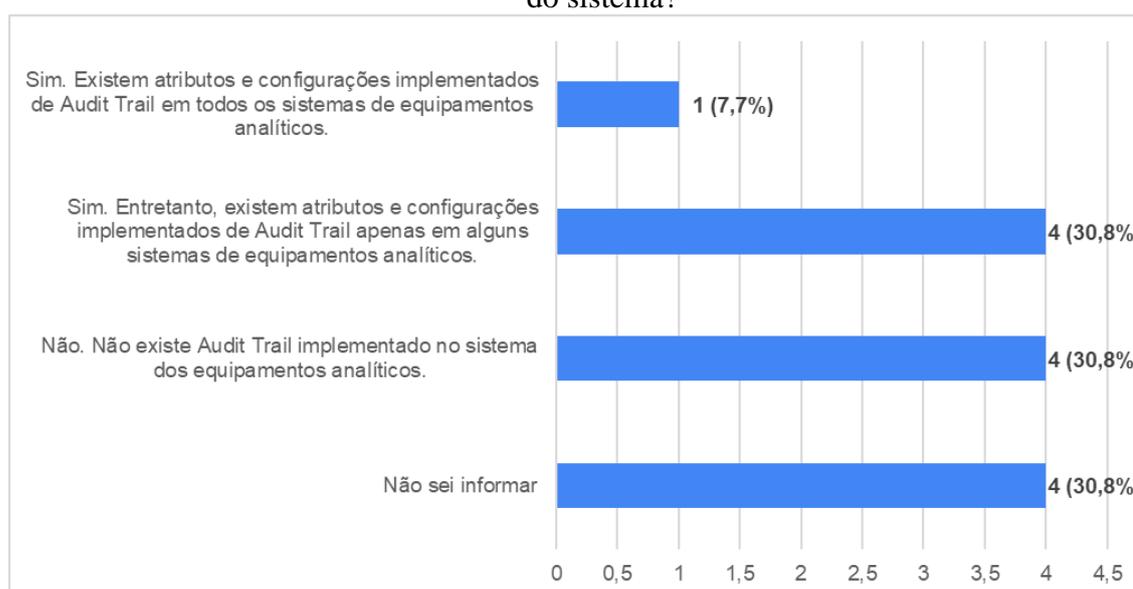
analíticos, enquanto que mais de 61% das unidades ou escritórios responderam não aplicar configuração para gerar logs de registros de eventos para ações de login/logoff de usuários no sistema operacional e nas tentativas de alteração de configuração do SO.

Um comentário feito por um gestor de TIC na questão Q17 citou que em sua respectiva unidade ou escritório geralmente há um número muito restrito de pessoas (2 a 3) que podem operar os equipamentos analíticos e que esta operação se dá em forma de plataforma, onde o usuário cliente requisita o serviço e fornece o material a ser analisado e o técnico da plataforma é quem opera a solução e devolve os resultados ao cliente. O gestor de TIC complementa em seu comentário que as credenciais de acesso ao computador são compartilhadas entre os técnicos das plataformas.

A ausência desta medida de controle técnico compromete atividades de rastreabilidade de ações realizadas pelos usuários no computador como processos de login/logoff no sistema operacional, processos de mudança em configurações de data e hora ou fuso horário ou demais configurações no sistema operacional.

Portanto, a configuração do recurso de gerar logs de registros de eventos do SO atende ao requisito técnico para a rastreabilidade das ações dos usuários nos computadores diretamente conectados aos equipamentos analíticos.

Q18. O sistema executado nos equipamentos analíticos possui configurações de trilha de auditoria (Audit Trail) implementados para capturar a identificação dos usuários (IDs) e os registros de data e hora das ações que criam, modificam ou excluem dados eletrônicos do sistema?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 01 (7,7%) respondeu que em sua respectiva unidade técnico-científica ou escritório técnico existem atributos e configurações implementadas de trilha de auditoria em todos os sistemas de equipamentos analíticos; 04 (30,8%) responderam que em suas unidades ou escritórios apenas alguns sistemas de equipamentos analíticos foram implementados atributos e configurações de trilha de auditoria; 04 (30,8%) responderam não saber informar se nas suas respectivas unidades ou escritórios existe a implementação de trilha de auditoria nos sistemas de equipamentos analíticos; e outros 04 (30,8%) responderam que nas suas unidades ou escritórios não existe trilha de auditoria implementada no sistema dos equipamentos analíticos.

Estes resultados evidenciam o distanciamento existente das áreas de TIC não apenas com as áreas de gestão da qualidade que conduzem as auditorias como, também, com os laboratórios das unidades ou escritórios que têm atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica e/ou aplicada gerando dados de pesquisa importantes e sensíveis

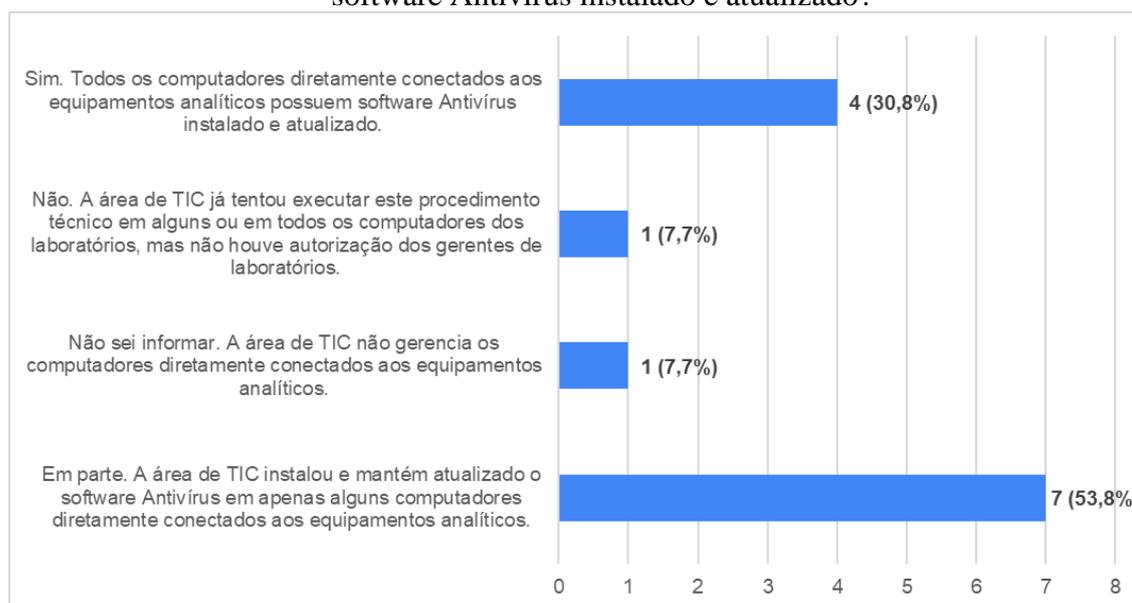
O *Audit Trail* ou trilha de auditoria é uma funcionalidade que quando disponível por um sistema ou software que gerencia o equipamento analítico, deve ser habilitada e configurada corretamente, pois é um recurso em forma de metadados que contém informações associadas às ações relacionadas à criação, modificação ou exclusão de registros (WHO, 2016).

Uma trilha de auditoria fornece a gravação segura de detalhes do ciclo de vida dos dados, como criação, acréscimos, exclusões ou alterações de informações em um registro eletrônico, sem obscurecer ou sobrescrever o registro original. Portanto, é um recurso de auditoria que contribui na reconstrução do histórico de tais eventos relacionados ao registro, independentemente de seu meio, incluindo quem realizou a ação, o que foi efetuado, quando ocorreu tal ação e por que foi executada a ação.

Segundo WHO (2016), para softwares que gerenciam equipamentos analíticos mais novos e possuem a função de trilha de auditoria (*Audit Trail*) configurada, somente através da existência de login único é que será possível capturar a identificação do usuário (ID) e os registros de data e hora de cada ação executada pelo usuário dentro do software.

Portanto, as trilhas de auditoria contribuem para documentar os registros de rastreabilidade das ações do usuário geradas por computador (WHO, 2016).

Q19. Os computadores diretamente conectados aos equipamentos analíticos possuem software Antivírus instalado e atualizado?

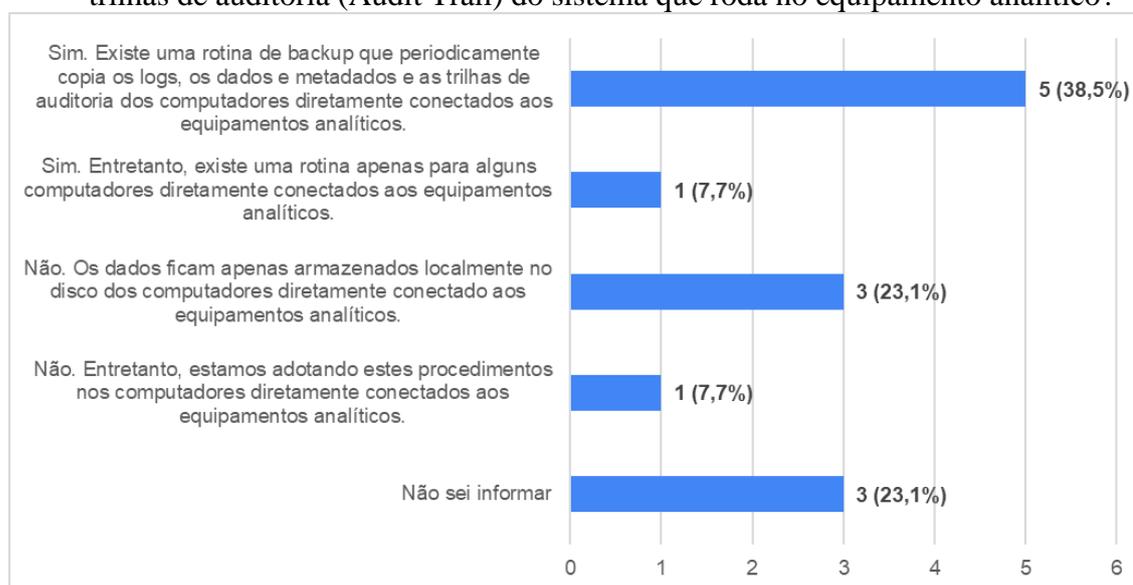


Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 04 (30,8%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos todos os computadores diretamente conectados nos equipamentos analíticos possuem software antivírus instalado e atualizado; 07 (53,8%) responderam que em suas unidades ou escritórios a área de TIC instalou e mantém atualizado o software antivírus em apenas alguns computadores diretamente conectados nos equipamentos analíticos; 01 (7,7%) gestor respondeu que na sua unidade ou escritório a área de TIC já tentou instalar em alguns ou em todos os computadores dos laboratórios, mas não foi autorizado pelos gerentes dos laboratórios; e 01 (7,7%) respondeu não saber informar se na sua unidade ou escritório existem softwares antivírus instalado e atualizado nos computadores diretamente conectados nos equipamentos analíticos, pois a área de TIC não gerencia os computadores instalados dentro dos laboratórios.

Analisando os dados coletados da questão Q19, pode-se afirmar que das 13 unidades ou escritórios participantes desta pesquisa, 84,6% possuem uma política interna ou procedimento operacional padrão de instalação de software antivírus nos computadores diretamente conectados aos equipamentos analíticos e os mantém atualizados, representando um alto percentual quando considerado que um software antivírus é um dos principais mecanismos utilizados na defesa contra código malicioso e/ou *software* mal-intencionado.

Q20. É realizada alguma rotina de backup dos logs que registram os eventos do SO, dos dados e metadados gravados pelos usuários do sistema computadorizado, bem como das trilhas de auditoria (Audit Trail) do sistema que roda no equipamento analítico?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 05 (38,5%) responderam que em suas respectivas unidades técnicas-científicas ou escritórios técnicos existe uma rotina de backup dos logs de registros e eventos do SO, dos dados e metadados gravados pelos usuários do SO, bem como das trilhas de auditoria do sistema que gerencia o equipamento analítico; 01 (7,7%) respondeu que na sua unidade ou escritório a rotina de backup existe, porém, para alguns computadores diretamente conectados aos equipamentos analíticos; 03 (23,1%) responderam não saber informar se em suas unidades ou escritórios existe alguma rotina de backup para os dados eletrônicos gerados pelos computadores diretamente conectados aos equipamentos analíticos; outros 03 (23,1%) responderam que em suas unidades ou escritórios não existe uma rotina de backup sendo realizado pela área de TIC e que os dados eletrônicos gerados nos equipamentos analíticos e computadores diretamente conectados a eles ficam armazenados localmente; e apenas 01 (7,7%) respondeu que em sua unidade ou escritório a rotina de backup não é realizada, mas estão adotando os procedimentos nos computadores diretamente conectados aos equipamentos analíticos.

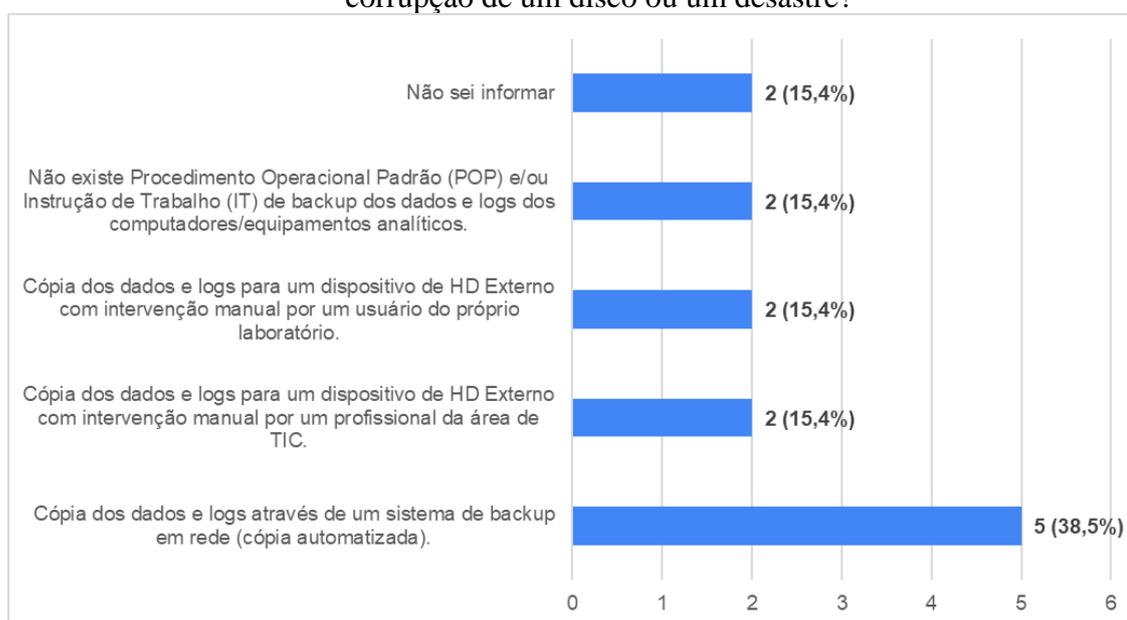
Analisando os dados da questão 20, pode-se concluir que apenas 46,2% das unidades ou escritórios participantes da pesquisa possuem alguma rotina de backup para os dados gerados eletronicamente pelos equipamentos analíticos e computadores diretamente conectados a eles. Mais de 53% das unidades ou escritórios não realizam qualquer procedimento para cópia e backup dos dados eletrônicos gerados pelos equipamentos analíticos.

Segundo WHO (2016), um *backup* significa uma cópia de um ou mais arquivos eletrônicos criados como alternativa, caso os dados ou sistemas originais sejam perdidos ou se tornem inutilizáveis devido a casos de uma falha do sistema ou corrupção de um disco, por exemplo.

Todavia, é muito importante e imprescindível que as unidades ou escritórios adotem em seus processos organizacionais de segurança da informação, procedimentos operacionais padrão para cópias de rotina de *backup* de registros eletrônicos originais armazenados em outro local como uma garantia em caso de desastre que provoque a perda dos registros eletrônicos originais.

Lopez (2014) cita na literatura que a ausência de procedimento referente a backup e proteção de dados é uma das deficiências encontradas para a ausência ou falhas relacionadas à integridade de dados eletrônicos.

Q21. Qual é a metodologia de backup dos dados eletrônicos (dados, metadados, trilhas de auditoria etc.) utilizada nos sistemas computadorizados de equipamentos analíticos para mitigar o risco de perda dos dados eletrônicos em casos de uma falha no sistema, corrupção de um disco ou um desastre?



Fonte: Elaboração própria a partir dos questionários (2021).

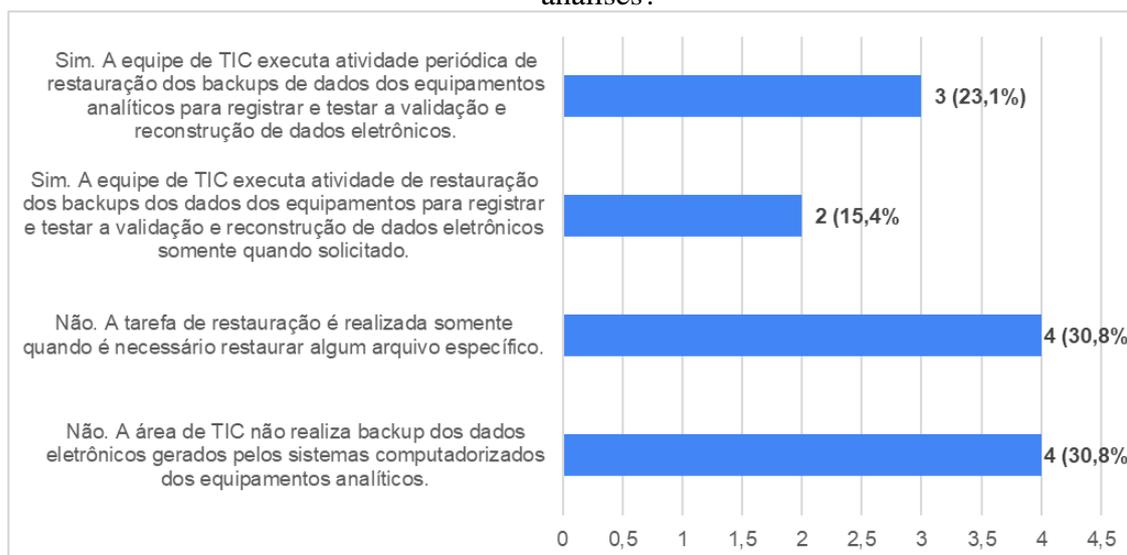
Dos 13 gestores da área de TIC, apenas 05 (38,5%) responderam que em suas respectivas unidades ou escritórios a cópia dos dados é realizada através de um sistema de backup em rede, de forma mais automatizada; 02 (15,4%) responderam que nas suas unidades ou escritórios a cópia dos dados é realizada de forma manual para um HD externo e com intervenção de um profissional da área de TIC; 02 (15,4%) outros responderam que em suas

unidades ou escritórios, a cópia dos dados é feita para um HD externo e com intervenção manual por um usuário do laboratório; 02 (15,4%) responderam que em suas unidades ou escritórios não existe POP e/ou IT para backup dos dados gerados eletronicamente pelos computadores diretamente conectados aos equipamentos analíticos; os 02 (15,4%) últimos responderam não saber informar qual é a metodologia de backup dos dados utilizada em suas respectivas unidades ou escritórios.

A garantia de ter um dado eletrônico disponível para utilização a qualquer momento ou necessidade após um evento de perda passa por um processo de *backup* realizado através de uma metodologia. Os sistemas de *backup* em rede com procedimentos mais automatizados são essenciais para uma gestão mais eficiente e organizada, pois podem ser adotados procedimentos operacionais e técnicos para garantir com maior velocidade a recuperação dos dados.

A ausência de uma metodologia para um sistema de *backup*, bem como de uma padronização para realização das tarefas de *backup* podem comprometer a segurança das informações geradas nos equipamentos analíticos tornando um ou mais dados indisponíveis em casos de perda, o que pode comprometer todo um processo de pesquisa científica, bem como sua necessidade de reconstrução.

Q22. A área de TIC possui algum Procedimento Operacional Padrão (POP) e/ou Instrução de Trabalho (IT) para processo de validação dos backups que foram realizados dos logs, dados, metadados e trilhas de auditoria com objetivo de garantir a recuperação de dados eletrônicos em caso de perda dos dados ou para evidências de reprodutibilidade das análises?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 03 (23,1%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos a área de TIC possui algum POP

ou IT para processo de validação dos backups realizados de logs, dados, metadados e trilhas de auditoria dos sistemas computadorizados nos equipamentos analíticos e que executam essa atividade periodicamente; 03 (23,1%) responderam que em suas unidades ou escritórios a área de TIC possui algum POP ou IT para processo de validação de backups dos dados gerados pelos sistemas computadorizados dos equipamentos analíticos, porém, essa atividade é realizada apenas quando a área de TIC é solicitada e não como uma atividade periódica ou programada; 08 (61,5%) responderam que nas suas respectivas unidades ou escritórios não existe um POP ou IT para processo de validação de backups de dados eletrônicos gerados pelos equipamentos analíticos, sendo que 04 (30,8%) responderam que a tarefa de restauração é realizada somente quando é necessário restaurar algum arquivo específico e outros 04 (30,8%) responderam que a área de TIC não realiza backup dos dados eletrônicos gerados pelos sistemas computadorizados dos equipamentos analíticos.

Analisando os dados coletados na questão 22, pode-se concluir que mais de 60% das unidades ou escritórios que participaram desta pesquisa não adotam um procedimento planejado e periódico de validação dos backups que foram realizados dos logs, dados, metadados e trilhas de auditoria com objetivo de garantir a recuperação de dados eletrônicos em caso de perda dos dados ou para evidências de reprodutibilidade das análises.

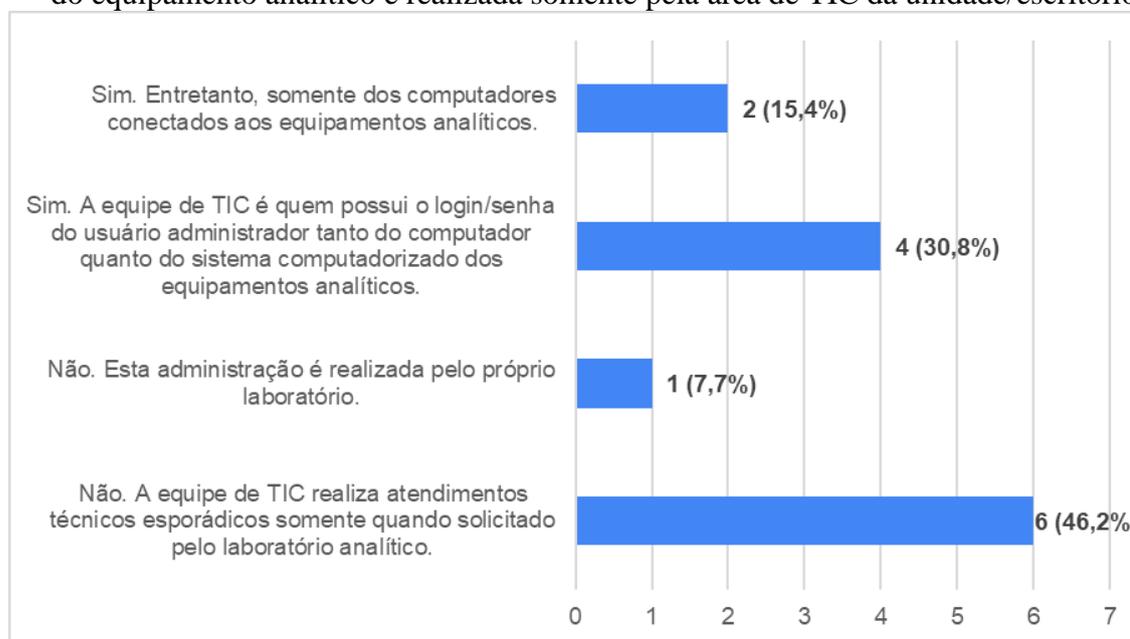
Segundo WHO (2016), os dados originais incluem a primeira ou a origem da captura de dados ou informações e todos os dados subsequentes necessários para reconstruir totalmente a conduta da atividade de qualquer boa prática dentro dos laboratórios analíticos. Os dados eletrônicos originais gerados por sistemas computadorizados em equipamentos analíticos devem ser revisados e mantidos para que as cópias verdadeiras e verificadas preservem o conteúdo e o significado dos dados originais.

Portanto, o processo de validação de *backup* é importante, pois quando o sistema original é retirado ou desativado, a migração dos dados para outros sistemas ou outros meios de preservação dos dados deve ser usada de forma a preservar o contexto e o significado dos dados, permitindo que as etapas relevantes sejam reconstruídas.

Tarefas de validação de *backup* contribuem para verificações de acessibilidade aos dados arquivados, independentemente do formato e incluindo metadados relevantes e para confirmar que os dados são duradouros e continuam disponíveis, legíveis e compreensíveis por outras pessoas e sistemas, quando necessários. Num processo de validação os erros identificados podem ser corrigidos através de ações técnicas e contribuir, assim, para permitir disponibilidade dos dados eletrônicos a qualquer momento.

Para PIC/S (2018), considerar a possibilidade de garantir a recuperação dos dados é uma das etapas do gerenciamento de riscos que deve ser implementado.

Q23. A administração do sistema operacional como também do sistema computadorizado do equipamento analítico é realizada somente pela área de TIC da unidade/escritório?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, apenas 04 (30,8%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos a área de TIC é quem possui o login/senha do usuário administrador tanto do computador quanto do sistema computadorizado dos equipamentos analíticos; 02 (15,4%) responderam que nas suas unidades ou escritórios a área de TIC possui apenas a administração dos computadores diretamente conectados aos equipamentos analíticos; 01 (7,7%) respondeu que na sua unidade ou escritório a área de TIC não administra ou não possui o perfil de administrador dos computadores diretamente conectados aos equipamentos analíticos, bem como do sistema computadorizado dos equipamentos analíticos e que essa função de administração é realizada pelo próprio laboratório; e 06 (46,2%) responderam que em suas unidades ou escritórios a área de TIC não tem o perfil de administrador dos computadores e equipamentos analíticos localizados nos laboratórios e que a equipe de TIC realiza atendimentos técnicos esporádicos somente quando solicitado pelo laboratório analítico.

Com esses dados coletados pode-se destacar que a administração completa da área de TIC sobre o sistema operacional dos computadores diretamente conectados nos equipamentos analíticos, bem como dos sistemas computadorizados dos equipamentos é realizada apenas por

04 (30,8%) unidades ou escritórios e que uma administração parcial é feita apenas por 02 (15,4%) unidades ou escritórios, sendo realizada somente do SO dos computadores diretamente conectados aos equipamentos analíticos.

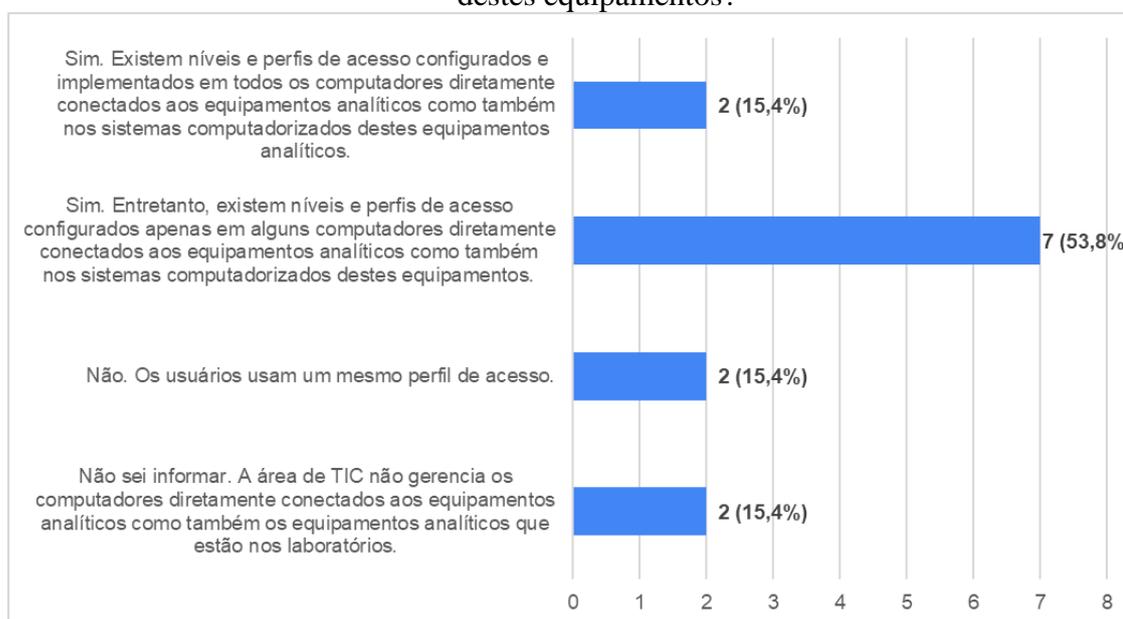
Mais de 53% das unidades ou escritórios participantes desta pesquisa não tem na sua respectiva área de TIC a responsabilidade e tarefa de administração do sistema operacional dos computadores e dos sistemas computadorizados dos equipamentos analíticos instalados em seus respectivos laboratórios.

De acordo com WHO (2016), a alocação de pessoal de suporte técnico independente para executar a administração do sistema para sistemas computadorizados, incluindo gerenciamento de segurança, *backup* e arquivamento, reduz possíveis conflitos de interesse e pode otimizar muito e melhorar a eficiência do gerenciamento de dados eletrônicos.

Todavia, as tarefas e responsabilidades de configurações de parâmetros que restringem o acesso a permissões de segurança aprimoradas (como a função de administrador do sistema que pode ser usada para potencialmente desviar de trilhas de auditoria ou permitir sobrescrever e excluir dados), somente para pessoas independentes dos responsáveis pelo conteúdo do registros, como a área de TIC por exemplo, contribuem para atingir que os dados gerados eletronicamente nos equipamentos analíticos sejam legíveis, rastreáveis e permanentes.

Este ponto citado acima quanto à responsabilização sobre funções correspondentes às configurações de parâmetros em sistemas operacionais e sistemas computadorizados de equipamentos analíticos evidenciam a importância da participação efetiva, bem como treinamentos, das áreas de TIC para atuação nas rotinas do dia a dia quanto à administração destes equipamentos nos laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica e/ou aplicada.

Q24. Existem níveis e perfis de acesso configurados nos computadores diretamente conectados aos equipamentos analíticos como também nos sistemas computadorizados destes equipamentos?



Fonte: Elaboração própria a partir dos questionários (2021).

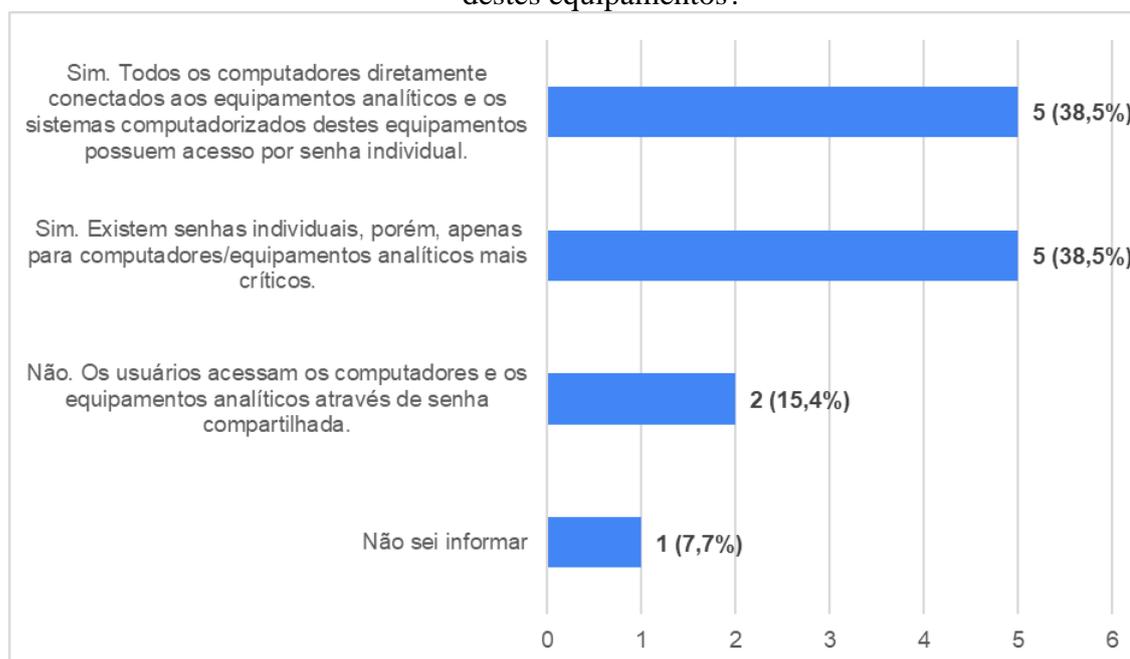
Dos 13 gestores da área de TIC, apenas 02 (15,4%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos existem níveis e perfis de acesso configurados e implementados em todos os computadores diretamente conectados aos equipamentos analíticos como, também, nos sistemas computadorizados destes equipamentos analíticos; 07 (53,8%) responderam que em suas unidades ou escritórios existem níveis e perfis de acesso configurados apenas em alguns computadores diretamente conectados aos equipamentos analíticos como também nos sistemas computadorizados destes equipamentos; 02 (15,4%) responderam não saber informar se nas suas respectivas unidades ou escritórios existem níveis e perfis de acesso configurados, pois a área de TIC não gerencia os computadores diretamente conectados aos equipamentos analíticos como também os equipamentos analíticos que estão nos laboratórios; e 02 (15,4%) gestores responderam que em suas unidades ou escritórios não existem níveis e perfis de acesso configurados nos computadores diretamente conectados aos equipamentos analíticos como, também, nos sistemas computadorizados destes equipamentos, pois os usuários usam o mesmo perfil de acesso.

Esses percentuais mostram que mais da metade das unidades ou escritórios adotam essa prática de implementar níveis e perfis de acesso aos computadores e equipamentos analíticos para separar de forma correta as tarefas a serem executadas pelos usuários do computador/equipamento.

Segundo WHO (2016), a implementação de níveis e perfis de acesso que contribuem para uma separação adequada de tarefas deve ser estabelecida para que os proprietários dos processos de negócio ou outros usuários que possam ter um conflito de interesses não recebam permissões de acesso de segurança aprimoradas em nenhum nível do sistema (por exemplo, sistema operacional, aplicativo e banco de dados).

Todavia, as contas de administrador do sistema altamente privilegiadas devem ser reservadas para o pessoal técnico designado, por exemplo o pessoal da área de TIC, que é totalmente independente do pessoal responsável pelo conteúdo dos registros, pois esses tipos de contas podem incluir a capacidade de alterar configurações para substituir, renomear, excluir, mover dados, alterar configurações de data e hora, desabilitar trilhas de auditoria e executar outras funções de manutenção do sistema que desativam os controles de boas práticas de gerenciamento de dados eletrônicos legíveis e rastreáveis.

Q25. Existem senhas individuais criadas e configuradas para uso nos computadores diretamente conectados aos equipamentos analíticos e nos sistemas computadorizados destes equipamentos?



Fonte: Elaboração própria a partir dos questionários (2021).

Dos 13 gestores da área de TIC, 05 (38,5%) responderam que em suas respectivas unidades técnico-científicas ou escritórios técnicos existem senhas individuais criadas e configuradas para todos os computadores diretamente conectados aos equipamentos analíticos e aos sistemas computadorizados destes equipamentos; 05 (38,5%) outros gestores de TIC responderam que em suas unidades ou escritórios existem senhas individuais criadas e

configuradas apenas para computadores/equipamentos analíticos mais críticos; 02 (15,4%) responderam que em suas unidades ou escritórios não existem senhas individuais criadas e configuradas e que os usuários acessam os computadores e os equipamentos analíticos através de senha compartilhada; e 01 (7,7%) respondeu não saber informar se na sua unidade ou escritório existem senhas individuais criadas e configuradas para uso nos computadores diretamente conectados aos equipamentos analíticos e nos sistemas computadorizados destes equipamentos.

Analisando os dados coletados da questão Q25, pode-se concluir que apenas 38,5% das unidades ou escritórios responderam que são criadas senhas individuais para uso tanto nos computadores diretamente conectados aos equipamentos analíticos como, também, nos sistemas computadorizados dos equipamentos analíticos. Outras 05 (38,5%) unidades ou escritórios responderam que criam senhas individuais apenas para uso nos computadores diretamente conectados aos equipamentos analíticos.

Segundo WHO (2016), o uso de senhas individuais e não compartilhadas contribui para um dado ser atribuível, pois possibilita que a informação capturada no registro do dado seja identificada exclusivamente como tendo sido executada pelo originador dos dados, sendo uma pessoa ou sistema de computador.

As unidades ou escritórios que ainda utilizam conta de usuário compartilhada ou permitem acesso a computadores e demais sistemas computadorizados nos laboratórios analíticos sem qualquer tipo de autenticação, devem adotar medidas de controle técnico para evitar estes procedimentos, pois não garantem que as ações documentadas em registros eletrônicos possam ser atribuídas a um indivíduo exclusivo, se aplicado ao nível de aplicativo de software e a todos os ambientes de rede aplicáveis, nos quais a equipe pode executar ações, por exemplo, em sistemas operacionais de estação de trabalho e servidor.

O uso de senhas individuais é importante para assegurar a integridade de dados, pois associa todas as alterações aos dados com as pessoas que fazem essas alterações, e essas alterações devem ter registro de data e hora, além da razão para a alteração registrada, quando aplicável. Essa rastreabilidade das ações do usuário deve ser documentada por meio de trilhas de auditoria, geradas por computador ou em outros campos de metadados ou recursos do sistema que atendam a esses requisitos.

Assim, com base nos resultados e nas análises obtidas, foi possível sintetizar os principais elementos e ações relacionadas à integridade de dados eletrônicos, bem como avaliar o grau de adoção de práticas de gerenciamento de dados em registros eletrônicos.

Estes elementos e ações contribuem minimamente para um processo de implantação de integridade de dados eletrônicos e estão associados aos princípios implícitos nas diretrizes do guia de boas práticas de gerenciamento de dados da OMS.

O grau de adoção de práticas de gerenciamento de dados eletrônicos, sob a percepção dos gestores das áreas da Qualidade e de TIC podem ser observadas nas tabelas 14 e 15, respectivamente.

Conforme mencionado na metodologia, o grau de adoção foi calculado utilizando-se a soma da frequência e porcentagem referente às repostas apenas positivas dos elementos e ações. Assim, estabeleceu-se os seguintes níveis de graus de adoção:

- Grau Baixo de adoção: a porcentagem menor ou igual a 40% ($\leq 40\%$);
- Grau Médio de adoção: a porcentagem maior que 40% e menor ou igual a 70% ($> 40\%$ e $\leq 70\%$);
- Grau Alto de adoção: a porcentagem maior que 70% ($> 70\%$);

Tabela 14: Grau de adoção de práticas de gerenciamento de dados eletrônicos, obtidos sob a percepção dos gestores da área da Qualidade.

Princípios	Principais elementos e ações	Frequência	Porcentagem	Grau Baixo de Adoção (até ≤ 40%)	Grau Médio de Adoção (> 40% e ≤ 70%)	Grau Alto de Adoção (> 70%)
Gestão de Governança e auditorias de Qualidade:	Existe ciência e importância da relevância sobre integridade de dados eletrônicos?	5	41,7%			
	Adota algum Plano de Gestão de Dados (PGD) para projetos de pesquisa?	3	25,0%			
	Possui formação de equipe multidisciplinar para processo de compras de equipamentos analíticos?	6	50,0%			
Sistemas de Gestão da Qualidade:	Possui sistema de Gestão da Qualidade efetivamente implementado?	9	75,0%			
	Adota uma cultura de qualidade e dissemina informações sobre o tema integridade de dados?	4	33,3%			
Boas práticas de documentação:	Segue boas práticas de documentação (BPDoc)?	6	50,0%			
	Fornece treinamento sobre boas práticas de documentação?	4	33,3%			
	Possui algum procedimento operacional padrão (POP) sobre integridade de dados eletrônicos?	4	33,3%			
	Adotam procedimentos, medidas de controle ou alguma ação para garantir integridade dos dados gerados eletronicamente?	7	58,3%			
Treinamento/Conhecimento sobre integridade de dados:	Possui familiaridade com o termo Integridade de Dados?	10	83,3%			
	Dissemina conhecimento do POP de integridade de dados eletrônicos implementada na unidade/escritório técnico?	4	33,3%			

Fonte: Elaboração própria (2021).

Observando a tabela 14, referente à síntese realizada a partir dos resultados obtidos do Questionário – Qualidade, foi possível inferir que apenas dois elementos e ações possuem grau alto de adoção de práticas de gerenciamento de dados eletrônicos e estão relacionados aos princípios de “Sistema de Gestão da Qualidade” e “Treinamento/Conhecimento sobre integridade de dados”, com porcentagem acima de 70% que correspondeu às respostas positivas. Quatro elementos e ações tiveram uma porcentagem acima de 40% e menor ou igual a 70% e foram classificados com grau médio de adoção, estando relacionados aos princípios de “Gestão da Governança e Auditorias de Qualidade” e “Boas Práticas de Documentação”. Já com grau baixo de adoção, foram identificados 5 elementos e ações que tiveram a porcentagem menor ou igual a 40% e relacionados com todos os 4 princípios.

Tabela 15: Grau de adoção de práticas de gerenciamento de dados eletrônicos, obtidos sob a percepção dos gestores da área de TIC.

Princípios	Principais elementos e ações	Frequência	Porcentagem	Grau Baixo de Adoção (até ≤ 40%)	Grau Médio de Adoção (> 40% e ≤ 70%)	Grau Alto de Adoção (> 70%)
Gestão de Governança e auditorias de TIC:	Possui alguma rotina periódica de auto inspeção e/ou auditoria interna nos sistemas computadorizados de equipamentos analíticos com vies em segurança da informação?	7	53,8%			
	Possui formação de equipe multidisciplinar para processo de compras de equipamentos analíticos?	2	15,4%			
Boas práticas de documentação:	Possui algum processo estabelecido para receber solicitação formalizando a criação de senha individual para uso nos equipamentos analíticos?	3	23,1%			
	Possui algum POP e/ou IT para processo de validação dos backups que foram realizados dos logs, dados, metadados e trilhas de auditoria?	5	38,5%			
Validação de sistemas para garantir a qualidade e confiabilidade dos dados:	Possui algum procedimento técnico para configurar e manter a sincronização de data e hora dos sistemas computadorizados?	6	46,2%			
	Os computadores diretamente conectados aos equipamentos analíticos estão com as versões de sistema operacional (SO) atualizados?	10	76,9%			
	É utilizada alguma metodologia de Validação dos Sistemas Computadorizados (VSC) dos equipamentos analíticos?	3	23,1%			
	Possui configuração para gerar log dos eventos relacionados à login/logoff dos usuários, bem como de alteração e tentativa de alteração de configurações do SO?	5	38,5%			
	Possui configurações de trilha de auditoria (Audit Trail) implementados nos sistemas computadorizados?	5	38,5%			
	Possui software antivírus instalado e atualizado nos computadores diretamente conectados aos equipamentos analíticos?	11	84,6%			
	Possui alguma rotina de backup dos logs de eventos do SO, dados e metadados, bem como das trilhas de auditoria do sistema que roda no equipamento analítico?	6	46,2%			
	Possui POP e/ou IT para para processo de validação dos backups que foram realizados dos logs, dados, metadados e trilhas de auditoria?	5	38,5%			
	A área de TIC administra o SO como também do sistema computadorizado do equipamento analítico?	4	30,8%			
	Possui níveis e perfis de acesso configurados nos computadores e nos sistemas computadorizados dos equipamentos analíticos?	9	69,2%			
	Possui senhas individuais criadas e configuradas para uso nos computadores e nos sistemas computadorizados dos equipamentos analíticos?	10	76,9%			
Treinamento/Conhecimento:	Participa de alguma fase de treinamento com o fabricante do equipamento analítico quando da instalação e configuração dentro dos laboratórios?	4	30,8%			
	Possui familiaridade com o termo Integridade de Dados?	6	46,2%			

Fonte: Elaboração própria (2021).

Observando a tabela 15, referente à síntese realizada a partir dos resultados obtidos do Questionário – TIC, foi possível inferir que apenas três elementos e ações possuem grau alto de adoção de práticas de gerenciamento de dados eletrônicos e estão relacionados somente ao princípio de “Validação de sistemas para garantir a qualidade e confiabilidade dos dados”, com porcentagem acima de 70% que correspondeu às respostas positivas.

Cinco elementos e ações tiveram uma porcentagem acima de 40% e menor ou igual a 70% e foram classificados com grau médio de adoção, estando relacionados aos princípios de “Gestão da Governança e Auditorias de TIC”, “Validação de sistemas para garantir a qualidade e confiabilidade dos dados” e “Treinamento/Conhecimento”.

Já com grau baixo de adoção, foram identificados nove elementos e ações que tiveram a porcentagem menor ou igual a 40% e relacionados com todos os 4 princípios.

7. CONSIDERAÇÕES FINAIS

A importância sobre a integridade de dados eletrônicos no campo da saúde consiste na confiabilidade e precisão dos dados e devem ser atribuíveis, legíveis, contemporâneos, originais e acurados, além de indispensáveis para as tomadas de decisões e para as atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica ou aplicada da Fiocruz.

Considerando os resultados analisados, foi possível identificar indícios de práticas que já apoiam e contribuem para o desenvolvimento e implantação de integridade de dados eletrônicos gerados por sistemas computadorizados de equipamentos analíticos nos laboratórios, tanto pelos elementos e ações identificados pela percepção dos gestores da área da Qualidade, quanto pela percepção dos gestores da área de TIC.

As principais práticas de gerenciamento de dados eletrônicos identificadas nos resultados, considerando os graus “Médio” e “Alto” de adoção, foram:

- Gestão da Qualidade:
 - ✓ Possuir ciência e importância da relevância sobre integridade de dados eletrônicos (Grau Médio de adoção);
 - ✓ Possuir sistema de Gestão da Qualidade efetivamente implementado (Grau Alto de adoção);
 - ✓ Seguir boas práticas de documentação (BPDoc) (Grau Médio de adoção);
 - ✓ Possuir procedimentos, medidas de controle ou alguma ação para garantir integridade dos dados gerados eletronicamente (Grau Médio de adoção);
 - ✓ Possuir familiaridade com o termo Integridade de Dados (Grau Alto de adoção);
 - ✓ Possuir formação de equipe multidisciplinar para processos de compras de equipamentos analíticos (Grau Médio de adoção).

- Gestão de TIC:
 - ✓ Possuir rotina de autoinspeção e/ou auditoria interna nos sistemas computadorizados de equipamentos analíticos (Grau Médio de adoção);
 - ✓ Possuir procedimento técnico para configurar e manter a sincronização de data e hora dos sistemas computadorizados (Grau Médio de adoção);

- ✓ Manter o SO dos computadores diretamente conectados aos equipamentos analíticos atualizados (Grau Alto de adoção);
- ✓ Possuir software antivírus instalado e atualizado nos computadores diretamente conectados aos equipamentos analíticos (Grau Alto);
- ✓ Possuir alguma rotina de backup dos logs de eventos do SO, dados e metadados, bem como das trilhas de auditoria do sistema que roda no equipamento analítico (Grau Médio de adoção);
- ✓ Possui níveis e perfis de acesso configurados nos computadores e nos sistemas computadorizados dos equipamentos analíticos (Grau Médio);
- ✓ Possuir senhas individuais criadas e configuradas para uso nos computadores e nos equipamentos analíticos (Grau Alto de adoção);
- ✓ Possuir familiaridade com o termo integridade de dados (Grau Médio de adoção).

Entretanto, diante dos resultados obtidos neste trabalho, é importante destacar alguns aspectos:

- ✓ Necessidade de disseminar e desenvolver, de forma mais eficaz, o tema integridade de dados por meio dos sistemas de gestão da qualidade das unidades e escritórios com objetivo de mitigar não conformidades em registros de dados eletrônicos, assim como tornar transparente qualquer desvio, erro, deleções e resultados aberrantes em todas as esferas da instituição;
- ✓ Notória deficiência de participação e integração das áreas de TIC junto às áreas de Gestão da Qualidade e aos laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica e/ou aplicada da Fiocruz, o que impacta negativamente na entrega de soluções e procedimentos operacionais e/ou técnicos que contribuam para a adoção de princípios e diretrizes de integridade de dados eletrônicos nestes ambientes de trabalho finalístico;
- ✓ Inequívoca que a capacitação direcionada em princípios e diretrizes de gerenciamento de dados eletrônicos aos profissionais das áreas de Qualidade e TIC é necessária para a adoção de práticas que contribuam para implementação de integridade de dados eletrônicos, objetivando evidenciar quais medidas de controles organizacional, operacional e/ou técnico apoiarão em ações que contribuam para

garantir que os dados gerados eletronicamente sejam atribuídos, legíveis, contemporâneos, originais e acurados durante todo o ciclo de vida dos dados (ALCOA), além de serem completos, consistentes, duradouros e disponíveis (ALCOA+).

Assim, dentre as ações que podem auxiliar uma proposta de implementação de requisitos mínimos de integridade de dados em registros eletrônicos, tendo como base os resultados encontrados neste trabalho a luz do guia de boas práticas de gerenciamento de dados da OMS e das demais referências bibliográficas utilizadas neste trabalho, destacam-se:

- Em medidas de controles organizacionais:
 - ✓ Adotar uma cultura de qualidade com abordagens sobre integridade de dados eletrônicos e que incentive funcionários a serem transparentes sobre falhas para que a administração tenha um entendimento preciso dos riscos e possa fornecer os recursos necessários para atingir as expectativas e atender aos padrões de qualidade e confiabilidade de dados;
 - ✓ Fornecer treinamentos sobre:
 - Boas práticas de documentação e garantir que todo o pessoal seja mantido atualizado sobre as aplicações de boas práticas de documentação com objetivo de desenvolver conhecimento para que os princípios da ALCOA sejam compreendidos e aplicados a dados eletrônicos;
 - Utilização dos sistemas computadorizados e respectivas opções de configuração de como os sistemas computadorizados funcionam e como parametrizar de forma eficiente os ajustes necessários, o que inclui metadados e trilhas de auditoria para as equipes de TIC da unidade ou escritório;
 - Integridade de dados e seus principais princípios e diretrizes;
 - Aquisição de equipamentos que gerem ou possam gerar registros eletrônicos;
 - Entre outros.

- ✓ Formar equipe multidisciplinar para processos de compras de equipamentos analíticos com a participação, principalmente, das áreas de gestão da Qualidade e de TIC;
 - ✓ Monitorar processos e alocação de recursos necessários para garantir e melhorar a infraestrutura, como por exemplo:
 - Projeto e manutenção adequados de edifícios, instalações, equipamentos e sistemas;
 - Garantir energia confiável adequada para fornecer aos equipamentos analíticos;
 - Entre outros;
 - ✓ Criar POP e/ou IT para os equipamentos analíticos e atividades que necessitam de implantação de integridade de dados;
 - ✓ Implantar gestão de riscos de gerenciamento de dados eletrônicos com objetivo de assegurar a validade, integridade e confiabilidade dos dados, sempre alinhada com a gestão de riscos da unidade ou escritório;
 - ✓ Estabelecer processo de trabalho para solicitação de criação de contas de usuário e perfis de acesso nos computadores e equipamentos analíticos nos laboratórios;
- Em medidas de controles operacionais:
- ✓ Disponibilizar os computadores e/ou equipamentos analíticos em uma rede elétrica estabilizada, quando possível;
 - ✓ Proteger os equipamentos analíticos com através do uso de nobreaks, quando possível;
 - ✓ Disponibilizar controle de acesso físico nos laboratórios e salas onde estão localizados os computadores e/ou equipamentos analíticos;
 - ✓ Não manter os computadores e os equipamentos analíticos em rede de dados (cabada ou sem fio) se estiverem com sistema operacional e versão de softwares desatualizados e/ou fora da cobertura de suporte do(s) fabricante(s);
 - ✓ Manter sincronização de data e hora dos sistemas computadorizados dos equipamentos analíticos;
 - ✓ Criar documentos de gerenciamento de riscos, segurança da informação e sobre desvios.

- Em medidas de controles técnicos:
 - ✓ Manter atualizado, quando possível, os sistemas operacionais dos computadores diretamente conectados aos equipamentos analíticos e, na impossibilidade técnica, criar documentos sobre os riscos à integridade de dados eletrônicos que envolvem a impossibilidade;
 - ✓ Configurar o sistema operacional dos computadores para gerar logs de registros de evento de *login/logoff* dos usuários;
 - ✓ Configurar, quando disponível, trilhas de auditoria (*Audit Trail*) nos sistemas computadorizados dos equipamentos analíticos;
 - ✓ Criar rotina de backup dos logs de registros de eventos do SO, dados e metadados, bem como das trilhas de auditoria do sistema que roda nos equipamentos analíticos;
 - ✓ Criar rotina de validação dos backups realizados com objetivo de verificar a confiabilidade e disponibilidade dos dados copiados para uso futuro;
 - ✓ Reservar o uso da conta de administrador do sistema altamente privilegiada para o pessoal técnico designado, por exemplo, o pessoal da gestão de TIC, que é totalmente independente do pessoal responsável pelo conteúdo dos registros, e com isso mitigar os riscos quanto à capacidade de alterar configurações para substituir, renomear, excluir, mover dados, alterar configurações de hora/data, desabilitar trilhas de auditoria e executar outras funções de manutenção do sistema que desativam os controles de boas práticas de gerenciamento de dados eletrônicos legíveis e rastreáveis;
 - ✓ Criar senhas individuais tanto para uso dos computadores diretamente conectados aos equipamentos analíticos quanto para os sistemas computadorizados destes equipamentos analíticos;
 - ✓ Realizar validação de sistemas computadorizados;
 - ✓ Configurar níveis e perfis de acesso tanto nos computadores diretamente conectados aos equipamentos analíticos quanto nos sistemas computadorizados destes equipamentos analíticos.

O conjunto destas ações propostas podem apoiar as unidades ou escritórios no sentido de sistematizar e organizar o processo de gestão dos dados eletrônicos gerados por equipamentos analíticos em laboratórios com atividades de ensaio, plataformas

tecnológicas e pesquisas experimentais básica e/ou aplicadas da Fiocruz, porém, existem desafios importantes a serem alcançados e vencidos, além de benefícios que podem fortalecer a gestão do conhecimento e o engajamento das pessoas no processo e contribuir para implantar soluções inovadoras para a Instituição.

Os elementos e ações deste estudo contribuem para um debate acerca da confiabilidade, integridade e rastreabilidade de dados eletrônicos gerados por equipamentos analíticos dentro dos processos de pesquisa científica nos laboratórios e podem subsidiar a implementação de um modelo de gestão de dados eletrônicos gerados em laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica e/ou aplicadas da Instituição.

REFERÊNCIAS

ALISSON, E. Má conduta científica é um problema global. 2014. Disponível em: <<https://www.ufrgs.br/blogdabc/ma-conduta-cientifica-e-um-problema/>> Acesso em: 08 de dezembro de 2019.

ALTMAN, L. K. Cholesterol Researcher Is Censured For Misrepresenting Data in Article. **Nytimes**, 1987. Disponível em: <https://www.nytimes.com/1987/07/18/us/cholesterol-researcher-is-censured-for-misrepresenting-data-in-article.html> . Acesso em: 27 de ago. de 2020.

ALVES, D. C. Estado e Sociedade na era da informação: A Relação entre as transformações sociais e as novas tecnologias da informação na contemporaneidade. **Brasilecola**, 2021. Disponível em: <https://monografias.brasilecola.uol.com.br/historia/estado-sociedade-na-era-informacao-relacao-entre-as-transformacoes-sociais-novas-tecnologias.htm> . Acesso em: 09 de ago. de 2020.

ARAGON, J. R. 502.6 - Fundamental Science Practices: Scientific Data Management. Usgs, 2017. Disponível em: <https://www.usgs.gov/about/organization/science-support/survey-manual/5026-fundamental-science-practices-scientific-data>. Acesso em: 19 de out. de 2020.

ARAÚJO, L. C. C. Como a Tecnologia Da Informação pode ser uma aliada estratégica do negócio. **Revista Científica Multidisciplinar Núcleo do Conhecimento**. Ano 05, Ed. 05, v. 04, p. 37-51, 2020.

ASSOCIAÇÃO BRASILEIRA DE AUTOMAÇÃO (2017). Qualidade de dados: o que é e qual a importância para negócios? Disponível em: <<https://blog.gs1br.org/qualidade-de-dados-o-que-e-e-qual-a-importancia-para-negocios/>> Acesso em: 08 de junho de 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2018). NBR ISO 31000:2018: Gestão de riscos - Diretrizes. Rio de Janeiro: ABNT

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2006). NBR ISO/IEC 27001:2013 Sistemas de Gestão de Segurança da Informação - Requisitos. Rio de Janeiro: ABNT

ACADEMIA BRASILEIRA DE CIÊNCIAS – Rigor e integridade na condução da pesquisa científica – Guia de recomendações de práticas responsáveis. Rio de Janeiro: ABC, 2013. Disponível em: <<http://www.abc.org.br/IMG/pdf/doc-4311.pdf>> Acesso em: 08 de fevereiro de 2020.

AHMAD, S., KUMAR, A., HAFEEZ, A. Importance of data integrity & its regulation in pharmaceutical industry. **The Pharma Innovation Journal**: v.8, n.1, p. 306-31, 2019. Disponível em: <https://www.researchgate.net/publication/334131228_Importance_of_data_integrity_its_regulation_in_pharmaceutical_industry> Acesso em: 24 de março de 2020.

ALBERTIN, A. L. Administração de informática: funções e fatores críticos do sucesso. São Paulo: Ed. Atlas, 2004.

ASSOCIATION FOR COMPUTING MACHINERY. Artifact Review and Badging. [online], 2016. Disponível em: <<https://www.acm.org/publications/policies/artifact-review-badging>> Acesso em 25 de março de 2020.

AZOULAY, P.; BONATTI, S.; KRIEGER, J. L. The career effects of scandal: evidence from scientific retractions. NBER Working Paper: n. 21146, Jul., 2017. Disponível em: <<https://www.nber.org/papers/w21146.pdf>> Acesso em 09 de junho de 2020.

AZOULAY, P., FURMAN, J. L., KRIEGER, J. L., & MURRAY, F. E. Retractions. NBER Working Paper: n. 18499, Cambridge, MA: National Bureau of Economic Research, 2012. Disponível em: <<https://www.nber.org/papers/w18499.pdf>> Acesso em 09 de junho de 2020.

BAERLOCHER et al. Data integrity, reliability and fraud in medical research. **European Journal of Internal Medicine**: v.21, p. 40-45, 2010.

BALL, A. Review of Data Management Lifecycle Models. Bath, UK: University of Bath, 2012. Disponível em: <https://purehost.bath.ac.uk/ws/portalfiles/portal/206543/redm1rep120110ab10.pdf> . Acesso em: 17 de dez. 2020.

BÁO, A. P. et al., Indicadores de qualidade: ferramentas para o gerenciamento de boas práticas em saúde. Rev Bras Enferm. 2019;72(2):360-6. Disponível em: <https://www.scielo.br/j/reben/a/T89wNCjgBwCKCYS9whxjSsm/?format=pdf&lang=pt> . Acesso em: 07 de set. de 2020.

BARBOSA, P. R. Adotar o documento editado pela WHO/IRR e intitulado como Práticas de qualidade na pesquisa biomédica básica e o documento editado pela FAPESP intitulado como Código de Boas Práticas Científicas para subsidiar as pesquisas científicas institucionais. PORTARIA N° 966, de 26 de setembro de 2016. Disponível em: <https://portal.fiocruz.br/sites/portal.fiocruz.br/files/documentos/p966_2016.pdf> Acesso em: 04 de fevereiro de 2021.

BASTOS, L. C. S. Método de Análise e Solução de Problemas (MASP) apoiado no ciclo PDCA: um estudo bibliográfico. **Revista Brasileira de Administração Científica**: v.7, n. 1, Mar., 2016.

BAKER, M., PENNT, D. Is there a reproducibility crisis? **Nature**: v. 533, p. 452-54, 2016.

BEAL, A. Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações - São Paulo: Ed. Atlas, 2005.

BRAINARD, J; YOU, J. What a massive database of retracted papers reveals about science publishing's 'death penalty'. Science: 2018. Disponível em:

<<https://www.sciencemag.org/news/2018/10/what-massive-database-retracted-papers-reveals-about-science-publishing-s-death-penalty>> Acesso em: 09 de junho de 2020.

BRASIL. Ministério da Saúde. Agência Nacional da Vigilância Sanitária. **Guia de Validação de Sistemas Computadorizados**. Brasília, Abr. 2010. Disponível em: <<http://portal.anvisa.gov.br/documents/33836/2501339/Guia+de+valida%C3%A7%C3%A3o+de+sistemas+computadorizados/034889a7-6b3f-439d-b8e5-32a0061ab395>> Acesso em: 07 de novembro de 2019.

BRASIL. Ministério da Saúde. Agência Nacional da Vigilância Sanitária. **Guia para boas práticas de fabricação de medicamentos. Parte I**. Jul. 2018. Disponível em: <<http://portal.anvisa.gov.br/documents/33880/5373593/Guia+para+boas+pr%C3%A1ticas+de+medicamentos.pdf/620bcd0d-54a4-40b4-9694-71df4a36056c>> Acesso em: 21 de janeiro de 2020.

BRASIL. Ministério da Saúde. Agência Nacional da Vigilância Sanitária. **Instrução Normativa – IN Nº 43**, de 21 de agosto de 2019. Diário Oficial da União, Poder Executivo, 22 de agosto de 2019. Disponível em: <http://portal.anvisa.gov.br/documents/10181/5389382/IN_43_2019_.pdf/a3785371-2556-4f11-9cb2-ded8a005e681> Acesso em: 09 de fevereiro de 2020.

BRASIL. Ministério da Saúde. Agência Nacional da Vigilância Sanitária. Resolução RDC 301, de 21 DE AGOSTO de 2019. Dispõe sobre Boas Práticas de Fabricação de Medicamentos. Diário Oficial da União, Poder Executivo, 22 de agosto de 2019. Disponível em: <<http://www.in.gov.br/web/dou/-/resolucao-rdc-n-301-de-21-de-agosto-de-2019-211914064>> Acesso em: 05 de março de 2020.

BRASIL. Ministério da Saúde. Agência Nacional da Vigilância Sanitária. Resolução RDC 134, de 13 DE JULHO de 2001. Dispõe sobre Boas Práticas de Fabricação de Medicamentos. Diário Oficial da União, Poder Executivo, 16 de JULHO de 2001. Disponível em: <<https://www.diariodasleis.com.br/busca/exibelink.php?numlink=1-9-34-2001-07-13-134>> Acesso em: 05 de junho de 2020.

BRASIL. Ministério da Saúde. Fundação Oswaldo Cruz (Fiocruz). Unidades e escritório. 2020. Disponível em: <<https://portal.fiocruz.br/unidades-e-escritorios>> Acesso em: 11 de junho de 2020.

BRASIL. Lei Nº 13.709, DE 14 DE AGOSTO DE 2018. Diário Oficial da União, Poder Executivo, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 10 de maio de 2020.

BRENNAN, Z. EMA re-confirms drug suspensions due to faulty trial data from GVK Biosciences. **Outsourcing-pharma**, 2015. Disponível em: https://www.outsourcing-pharma.com/Article/2015/05/25/EMA-re-confirms-drug-suspensions-due-to-faulty-trial-data-from-GVK-Biosciences?utm_source=copyright&utm_medium=OnSite&utm_campaign=copyright. Acesso em: 23 de mar. de 2020.

BRITO, M. J. Tecnologia da informação e mercado futuro - O caso da BM&F.
In: MARCOVITCH, J. (Org.) **Tecnologia da informação e estratégia empresarial**.
São Paulo: FEA/USP, 1996

BOSELEY S., DAVEY, M. Covid-19: Lancet retracts paper that halted hydroxychloroquine trials. **Support The Guardian**: Jun. 2020. Disponível em: <
<<https://www.theguardian.com/world/2020/jun/04/covid-19-lancet-retracts-paper-that-halted-hydroxychloroquine-trials>> Acesso em: 09 de junho 2020.

BURKE, J; ORNSTEN, R. O Presente do Fazedor de Machados. 1ª edição, Rio de Janeiro: Bertrand Brasil, 1998

CALIXTO, J. Integridade de dados [livro eletrônico]: Guia Sindusfarma para Indústria Farmacêutica. 1. ed; São Paulo: SINDUSFARMA, 2017. Disponível em:
https://www.farmaceuticas.com.br/wp-content/uploads/2017/10/SINDUSFARMA_Manual_Integridade_de_Dados-1.pdf

CARPINETTI, L. C. R., GEROLAMO, M. C. *Gestão da Qualidade ISO 9001: 2015*: requisitos e integração com a ISO 14001:2015, 1. ed. - [3. Reimpr.] - São Paulo: Ed. Atlas, 2019.

CARUSO, C. A. A.; STEFFEN, F. D. Segurança em Informática e de Informações - São Paulo: Editora SENAC, São Paulo, 1999.

CARVALHO, J. P. P. Os laboratórios de saúde pública nos programas de saúde. **Rev. Saúde Pública**: v.10, n.2, Jun, 1976. Disponível em:
<https://www.scielo.br/j/rsp/a/59qjKZTpFLn4CvRXYD3ybBn/?lang=pt>.

CIANCONI, R. B.; CORDEIRO, R. I. N.; ALMEIDA, C. H. M. Gestão do conhecimento, da informação e de documentos em contextos informacionais: estudos da Informação: Vol. 3, 298 p., Ed. Eduff, Rio de Janeiro, 2013.

CINTRA, L. P. et al., Indústria 4.0 e transformação digital: uma discussão conceitual, sob perspectiva neoschumpeteriana, que inclui políticas de CT&I e *catch up*. E&G Economia e Gestão, Belo Horizonte, v. 19, n. 54, p. 114-32, Set./Dez. 2019. Disponível em: <http://periodicos.pucminas.br/index.php/economiaegestao/article/view/19244/>. Acesso em: 10 de junho de 2020.

COSGROVE, T. Data Integrity. Pharmaceutical Engineering The official technical Magazine of ISPE: Opening Remarks. Presented at the ISPE-FDA CGMP Conference, v. 34, n. 4, p. 1-6, 2014. Disponível em:
<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKewjSv8a8t5vpAhUjxKYKHQitAjqQFjABegQIAxAB&url=http%3A%2F%2Fwww.gmp1st.com%2Fpharmaceutical_engineering%2F14ja-ispe_update_cgmpconf.pdf&usq=AOvVaw0U3x8U7LILzy_V94jal670> Acesso em: 16 de novembro de 2019.

CENTRO DE PESQUISAS RENÉ RACHOU CPqRR – FIOCRUZ (2010). Manual: práticas de qualidade na pesquisa biomédica básica / World Health Organization. Disponível em:

http://www.cpqrr.fiocruz.br/temporario/qualidade/95700_Manual.WHO.pdf Acesso em: 14 de janeiro de 2021.

CRUZ, T. Sistemas, organizações e métodos: estudo integrado das novas tecnologias de informação. 3ª edição São Paulo: Atlas, 2008.

CUOGO, F. C. O reflexo da terceira revolução industrial no Desenvolvimento tecnológico e sua relação com a Educação a distância. 2012. 70 f. [Monografia] (Licenciatura em História) Universidade Regional do Noroeste do Estado do Rio Grande do Sul. 2012. Disponível em:

<https://bibliodigital.unijui.edu.br:8443/xmlui/handle/123456789/2832> Acesso em: 13 de junho 2020.

DAVENPORT T. H.; PRUSAK L. Information ecology: mastering the information and knowledge environment. New York: Oxford University Press, 1997.

ELIAS, R. A. et al., Ética e integridade: condutas para produções científicas no Brasil. **Cogitare Enferm**: v. 23, n. 3, p. 543-67, 2018.

EMA – European Medicines Agency. GVK Biosciences: **European Medicines Agency confirms recommendation to suspend medicines over flawed studies**. Julho, 2015.

Disponível em: <https://www.ema.europa.eu/en/documents/referral/gvk-biosciences-article-31-referral-gvk-biosciences-european-medicines-agency-confirms_en-0.pdf> Acesso em: 16 de fevereiro de 2020.

FDA – Food and Drug Administration. **What does FDA regulate?** 2018. Disponível em: <<https://www.fda.gov/about-fda/fda-basics/what-does-fda-regulate>> Acesso em: 18 de fevereiro de 2020.

FDA – Food and Drug Administration. **Data Integrity and Compliance With CGMP. Guidance for Industry**. April, 2016. Disponível em:

<<https://www.fda.gov/files/drugs/published/Data-Integrity-and-Compliance-With-Current-Good-Manufacturing-Practice-Guidance-for-Industry.pdf>> Acesso em: 06 de agosto de 2019.

FDA – Food and Drug Administration. **Data Integrity and Compliance With Drug CGMP. Questions and Answers. Guidance for Industry**. December, 2018.

Disponível em: <<https://www.fda.gov/media/119267/download>> Acesso em: 07 de outubro de 2019.

FELDMAN, L. B. et al. **História da evolução da qualidade hospitalar: dos padrões a acreditação**. Artigos de Revisão. Acta paul. enferm. 18 (2). 2004. Disponível em:

<<https://www.scielo.br/j/ape/a/MbZtTx43DzGsMFyjz4RyMGC/?lang=pt>> Acesso em: 13 de setembro de 2020.

FERNANDES, W. A. **O movimento da qualidade no Brasil**. Ministério do Desenvolvimento, Indústria e Comércio Exterior, Instituto Nacional de Metrologia, Qualidade e Tecnologia – Inmetro, 2011.

FURNER J. “Dados”: os dados. In: Kelly M., Bielby J. (eds) Culturas da Informação na Era Digital. Springer VS, Wiesbaden, 2016. Disponível em: <https://link.springer.com/chapter/10.1007%2F978-3-658-14681-8_17> Acesso em: 17 de janeiro de 2019.

GADELHA, C.A.G., MALDONADO, J.M.S.V., VARGAS, M.; BARBOSA, P.R., COSTA, L.S. **A Dinâmica do Sistema Produtivo da Saúde: inovação e complexo econômico-industrial**. Rio de Janeiro: Ed. Fiocruz, 2012.

GIL, A. C. Como Elaborar Projetos de Pesquisa. 1. ed. São Paulo: Atlas, 1987.

GOBEN, A. RASZEWSKI, R. The data life cycle applied to our own data. **Journal of the Medical Library Association**, v. 103, n. 1, p. 40–44, 2015. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4279933/> . Acesso em: 25 de jan. de 2021.

GUERRA, B. O que é integridade de dados e por que ela é importante? Inteligência de Negócios, 2020. Disponível em: ><https://blog.in1.com.br/o-que-%C3%A9-integridade-de-dados-e-por-que-ela-%C3%A9-importante>> Acesso em: 14 de fevereiro de 2021.

IVAMA, A. M. Prevenção e combate à falsificação e fraude de medicamentos: uma responsabilidade compartilhada. Organização Pan-Americana da Saúde/Organização Mundial da Saúde. Brasília, 2005.

KEEN, P.G.W. "Information Technology And The Management Theory: The Fusion Map". IBM Systems Journal, v.32, n.1, p.17-38, 1993

LAFER, C. et al. **Código de Boas Práticas Científicas**. Fundação de Amparo à Pesquisa do Estado de São Paulo, 2014. Disponível: <http://www.fapesp.br/boaspraticas/FAPESP-Codigo_de_Boas_Praticas_Cientificas_2014.pdf> Acesso em: 01 de março de 2020.

LAI, C., et al. Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators. SANDIA REPORT, 2017. Disponível em: < <http://sunspec.org/wp-content/uploads/2017/08/DERCyberPrimer-DraftforReview.pdf>> Acesso em: 02 de fevereiro de 2020.

LAS CASAS, A. L. Qualidade total em serviços: conceitos, exercícios e casos práticos. 3. ed. São Paulo: Atlas, 1999. 206 p.

LAUREANO, M. A. P. Gestão de Segurança da Informação. **Mlaureano**, 2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf . Acesso em: 29 de set. de 2020.

LAVILLE, C.; DIONNE, J. **A construção do saber: manual de metodologia da pesquisa em Ciências humanas**. Trad. Heloísa Monteiro e Francisco Settineri. Porto Alegre: Artmed; Belo Horizonte: Editora UFMG, 1999.

LOBO, R. N. Gestão da Qualidade. 2 ed., Ed. Erika, São Paulo, 2020.

LEONARDI, E. Falhas em integridade de dados derrubam a reputação da empresa. **ICTQ**, 2018. Disponível em: <https://cdpipharma.com.br/falhas-em-integridade-de-dados-derrubam-a-reputacao-da-empresa/>. Acesso em: 20 de mar. de 2020.

LEONARDI, E.; MATOS, J. Por que a qualidade dos medicamentos depende da integridade de dados. **ICTQ**, 2020. Disponível em: < <https://www.ictq.com.br/industria-farmaceutica/1022-por-que-a-qualidade-dos-medicamentos-depender-da-integridade-de-dados>> Acesso em: 20 de mar. de 2020.

LEONELLI, S. What Counts as Scientific Data? A Relational Framework. **Philos Sci.**: v.82, n. 5, p 810-821, 2015.

LESCA, H.; ALMEIDA, F. C. Administração estratégica da informação. Revista de Administração – RAUSP: v.29, n.03, p.66-75, São Paulo, jul./set., 1994.

LIMA, N. V. T. et al. **Relatório de Gestão do exercício de 2018**. Fundação Oswaldo Cruz. 2018. Disponível em: <https://portal.fiocruz.br/sites/portal.fiocruz.br/files/documentos/fiocruz_relaorio_anual_2018.pdf> Acesso em: 20 de Março de 2020.

LIMA, N. V. T. Instituir o Guia de Integridade em Pesquisa da Fiocruz, aprovado pelo Conselho Deliberativo da Instituição em novembro de 2019, que orienta a atuação de profissionais de pesquisa sobre as boas práticas em pesquisa. PORTARIA Nº 5318, de 06 de março de 2020. Disponível em: <https://portal.fiocruz.br/sites/portal.fiocruz.br/files/documentos/final_-_portaria_5318_-_presidencia_fiocruz.pdf> Acesso em: 09 de junho de 2020.

LINS, L. Retratação científica e pseudociência [online]. SciELO em Perspectiva, 2014. Disponível em: <<https://blog.scielo.org/blog/2014/09/30/retratacao-cientifica-e-pseudociencia/>> Acesso em : 08 de junho de 2020.

LOPES, A. Integridade de dados em evidência na indústria farmacêutica. **Revista SBCC**, 2019. Disponível em: <<http://revistasbcc.com.br/sem-categoria/integridade-de-dados-em-evidencia-na-industria-farmaceutica/>> Acesso em: 05 de fevereiro de 2020.

LOPEZ, O. Revisão por pares: validação por computador. **IVT Network**, 2014. Disponível em: <<https://www.ivtnetwork.com/article/eu-annex-11-and-integrity-erecs>> Acesso em: 05 de fevereiro de 2020.

MARCHAND, D.A., KETTINGER, W.J. e ROLLINS, J.D. Information orientation: the link to business performance. New York: Oxford University Press, 2001.

MARSHALL, I. J. et al. Gestão da qualidade e processos. Rio de Janeiro: Ed. FGV, 2012

MESQUITA, C. T. **Integridade na Pesquisa Científica**. International Journal of Cardiovascular Sciences: v. 30, n.2, p. 1-3, 2017.

MEHRA, M. R., RUSCHITZKA, F., PATEL, A. M. Retraction—Hydroxychloroquine or chloroquine with or without a macrolide for treatment of COVID-19: a multinational

registry analysis. *The Lancet*: v. 395, Jun. 2020. Disponível em: <<https://www.thelancet.com/action/showPdf?pii=S0140-6736%2820%2931324-6>>
Acesso em: 10 de junho de 2020.

MCDOWALL, B., MENGES, K., SAMSON, Y. **Data Integrity. Requirements for a GMP-compliant Data Life Cycle**. Fevereiro, 2017. Disponível em: <<https://www.gmp-navigator.com/files/eca/userFiles/seminarpdf/ECA-Data-Integrity-2017.pdf>> Acesso em: 10 de março de 2020.

MHRA – Medicines & Healthcare products Regulatory Agency. **About us**. Disponível em: <<https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency/about>> Acesso em: 18 de fevereiro de 2020.

MHRA – Medicines & Healthcare products Regulatory Agency. **‘GXP’ Data Integrity Guidance and Definitions**. Rev. 1, março 2018. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf>
Acesso em: 17 de janeiro de 2020.

MINAYO, M. C. de S. (org.). *Pesquisa Social. Teoria, método e criatividade*. 18 ed. Ed. Vozes, Petrópolis, 2001.

MORETTO, S. Auditoria Farmacêutica. **ICTQ**, 2016. Disponível em: <https://ictq.com.br/industria-farmacautica/348-auditoria-farmacautica> . Acesso em: 17 de novembro de 2020.

MOSCHETTA, L. C. Integridade de dados: um desafio antigo cada vez mais atual na indústria farmacêutica. Junho, 2017. Disponível em: <https://pt.linkedin.com/pulse/integridade-de-dados-um-desafio-antigo-cada-vez-mais-atual-moschetta> Acesso em: 12 de janeiro de 2021.

MUELLER, S. P. M. O impacto das tecnologias de informação na geração do artigo científico: tópicos para estudo. **Ci. Inf.**, Brasília, v. 23, n. 3, p. 309-317, set./dez. 1994 Disponível em: <http://revista.ibict.br/ciinf/article/view/528>. Acesso em: 14 de junho de 2020.

NASSI-CALÒ, L. Reprodutibilidade em resultados de pesquisa: iniciativas em curso [online]. *SciELO em Perspectiva*, 2014. Disponível em: <<https://blog.scielo.org/blog/2014/03/07/reprodutibilidade-em-resultados-de-pesquisa-iniciativas-em-curso/#.Xr3-SGhKg2x>> Acesso em: 24 de março de 2020.

NASSI-CALÒ, L. Reprodutibilidade em resultados de pesquisa: os desafios da atribuição de confiabilidade [online]. *SciELO em Perspectiva*, 2016. Disponível em: <<https://blog.scielo.org/blog/2016/03/31/reprodutibilidade-em-resultados-de-pesquisa-os-desafios-da-atribuicao-de-confiabilidade/>> Acesso em: 24 de março de 2020.

NASSI-CALÒ, L. Avaliação sobre a reprodutibilidade de resultados de pesquisa traz mais perguntas que respostas [online]. *SciELO em Perspectiva*, 2017. Disponível em: <<https://blog.scielo.org/blog/2017/02/08/avaliacao-sobre-a-reprodutibilidade-de>>

[resultados-de-pesquisa-traz-mais-perguntas-que-respostas/](#)> Acesso em: 24 de março de 2020.

NELSON, R. Foreword. In: Freeman, C; LOUÇÃ; F. As time goes by: from the Industrial Revolution to the Information Revolution. Oxford: Oxford University Press, 2001.

PACHECO, R. C. S.; TAIT, T. F.C. Tecnologia de informação: evolução e Aplicações. Teor. Evid. Econ.: Passo Fundo, v. 8, n. 14, p. 97-113, maio 2000
Disponível em: <http://seer.upf.br/index.php/rtee/article/view/4816>. Acesso em: 11 de março de 2020.

PALADINI, E. P. Gestão da Qualidade - Teoria e Prática. Ed. Atlas Ltda, São Paulo 2019.

PÉREZ, J. R. **Maintaining Data Integrity. Avoiding regulator scrutiny in the medical products industry.** Março, 2017. Disponível em: <<http://asq.org/quality-progress/2017/03/data-quality/field-notes-maintaining-data-integrity.html>> Acesso em: 04 de fevereiro de 2020.

PIC/S – Pharmaceutical Inspection Convention Pharmaceutical Inspection Co-Operation Scheme. **Good Practices for Data Management and Integrity In Regulated GMP/GDP Environments.** Novembro, 2018. Disponível em: <<https://picscheme.org/layout/document.php?id=1566>> Acesso em: 15 de janeiro de 2020.

PMBOK. **Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK).** Quarta Edição. 2010.

PINOCHET, L. H.C., LOPES, A. S., SILVA, J. S. Inovações e tendências aplicadas nas tecnologias de informação e comunicação na gestão da saúde. **Revista de Gestão em Sistemas de Saúde:** v. 3, n. 2. Julho/Dezembro. 2014

PORTER, M. E.; MILLAR, V. E. How information gives you competitive advantage. **Harvard Business Review**, v.63, n.4, p. 149-60, Jul./Aug. 1985.

RATTAN, A. K. Data Integrity: History, Issues, and Remediation of Issues. **PDA Journal of Pharmaceutical Science and Technology:** v. 72, n. 2, p. 105-116, Mar. 2018.

REINHARD, N. Evolução das Ênfases gerenciais e de pesquisa na Área de tecnologia de informática e de telecomunicações aplicada nas empresas. **RAUSP- Revista de Administração**, São Paulo, v.31, n.4, 1996, pp 5-6.

Reproducibility in Cancer Biology: The challenges of replication. **eLife**, 2017.
Disponível em: <https://elifesciences.org/articles/23693> . Acesso em: 28 de mai. de 2020.

Research data management overview. **Yorku**, 2004. Disponível em: <https://www.library.yorku.ca/web/open/overview/>. Acesso em: 02 de fev. 2021.

- RIEDL, D. H.; DUNN, M. K. Quality assurance mechanisms for the unregulated research environment. **Trends in Biotechnology**: v. 31, n. 10, p. 552-54, 2013.
- RUSSO, M. Ética e integridade na ciência: da responsabilidade do cientista à responsabilidade coletiva. **Estudos Avançados**, v.28, n.80, São Paulo: Jan./Apr. 2014
- SANTOS, I. M. F. **Uma proposta de governança de dados baseada em um método de desenvolvimento de arquitetura empresarial**. 2010. 140 p. [Dissertação] (Mestrado em Informática) – Centro de Ciências Exatas e Tecnologia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2010. Disponível em: <<http://www2.uniriotec.br/ppgi/banco-de-dissertacoes-ppgi-unirio/ano-2010/uma-propostade-governanca-de-dados-baseada-em-um-metodo-de-desenvolvimento-de-arquiteturaempresarial/view>> Acesso em: 11 de dezembro de 2019.
- SANTOS, L. H. L. **Sobre a integridade ética da pesquisa**. Fundação de Amparo à Pesquisa do Estado de São Paulo, 2011. Disponível: <<http://www.fapesp.br/6566>> Acesso em: 01 de março de 2020.
- SÊMOLA, M. **Gestão da Segurança da Informação: uma visão executiva** - Rio de Janeiro: Ed. Campus, 2003.
- SÊMOLA, M. **Gestão da segurança da informação: uma visão executiva**. 2. ed. - Rio de Janeiro : Elsevier, 2014.
- SBCOACHING. **Integridade: O que é, Importância e Diferente Tipos**. 2018 Disponível em: <<https://www.sbcoaching.com.br/blog/integridade/>> Acesso em: 07 janeiro de 2020.
- SHAFIEI, N.; MONTARDY, R; RIVERA-MARTINEZ, E. Data Integrity – A Study of Current Regulatory Thinking and Action. **PDA Journal of Pharmaceutical Science and Technology**: v. 69, n. 6, p. 762-70, 2015.
- SHEWHART, W. A. **Economic control of quality of manufactured product**. Nova York: D. Van Nostrand Company, 1931.
- SINGH, A.; JOSHI, R. Analyzing the State of Data Integrity Compliance in the Indian Pharmaceutical Industry. **A survey by Fraud Investigation & Dispute Services**: p.1-20, 2015. Disponível em: <<https://rx-360.org/wp-content/uploads/2018/08/ey-data-integrity-compliance-in-the-pharma-industry.pdf>> Acesso em: 10 de agosto de 2019.
- SILVA, F. D. et al. Ética e integridade: condutas para produções científicas no Brasil. **Cogitare Enferm.** (23)3: e54367, 2018.
- SOARES NETO, R. N. A. Revolução informacional, novas tecnologias e consumo imediatista. **Cadernos de Campo: Revista de Ciências Sociais**: n. 16, p. 111-24, 2012. Disponível em: < <https://periodicos.fclar.unesp.br/cadernos/article/view/7319/5181>> Acesso em: 14 de junho de 2020.

SPINATO, P. A importância do fluxo de informações organizacional. Maio, 2010. Disponível em: <<https://administradores.com.br/artigos/a-importancia-do-fluxo-de-informacoes-organizacional>> Acesso em: 09 de abril de 2021.

TENÓRIO, M; MELLO, G.A.; VIANA, A. L. D. Políticas de fomento à ciência, tecnologia e inovação em saúde no Brasil e o lugar da pesquisa clínica. *Ciência & Saúde Coletiva*, 22(5):1441-1454. 2017. Disponível em: <<https://www.scielo.br/pdf/csc/v22n5/1413-8123-csc-22-05-1441.pdf>> Acesso em: 07 de outubro de 2019.

UNGER, B. **Data Integrity: Surveying The Current Regulatory Landscape**. Agosto, 2016. Disponível em: <<https://www.pharmaceuticalonline.com/doc/data-integrity-surveying-the-current-regulatory-landscape-0001>> Acesso em: 06 de janeiro de 2020.

UNGER, B. **An Analysis Of 2018 FDA Warning Letters Citing Data Integrity Failures**. Junho, 2019. Disponível em: <<https://www.pharmaceuticalonline.com/doc/an-analysis-of-fda-warning-letters-citing-data-integrity-failures-0001>> Acesso em: 08 de janeiro de 2020.

VALECIO, M. Importância da integridade de dados para a qualidade dos medicamentos. *ICTQ*, 2020. Disponível em: <<https://www.ictq.com.br/industria-farmaceutica/778-importancia-da-integridade-de-dados-para-a-qualidade-dos-medicamentos>> Acesso em: 08 de janeiro de 2020.

VIEIRA, E. A percepção da informação e da sua relevância no cenário institucional: sob a perspectiva de gestores e líderes. **Cad. EBAP.EBR**, v. 12, Edição Especial, artigo 8, Rio de Janeiro, Ago. 2014.

VOLSEN, S. G.; MASSON, M. M. A Novel Audit Model for Assessing Quality in Non-Regulated Research. **The Quality Assurance Journal**: v. 12, n. 2, p. 57-63, 2009.

WEBER C. **Garantia da qualidade no setor de bioquímica do Laboratório de análises clínicas de um hospital Público de Porto Alegre**. 2012. 35 p. Trabalho de Conclusão de Curso (Especialização) - Instituto de Comunicação e Informação Científica e Tecnológica em Saúde – ICICT, Fiocruz, Rio de Janeiro, 2012. Disponível em: <<https://www.arca.fiocruz.br/bitstream/icict/6721/1/Carolina%20Weber%5B1%5D.pdf>> Acesso em: 24 de abril de 2020.

WERKEMA, C. Métodos PDCA e DMAIC e suas ferramentas analíticas. Rio de Janeiro: Elsevier, 2013.

WHO – World Health Organization. Expert Committee on Specifications for Pharmaceutical Preparations. Annex 5 **Guidance on good data and record management practices**. Genebra, 2016. Disponível em: <<http://apps.who.int/medicinedocs/documents/s22397en/s22397en.pdf>> Acesso em: 12 de dezembro de 2019.

WHO – World Health Organization. Guideline on Data Integrity. Draft for comments. Out., 2019. Disponível em:

<https://www.who.int/medicines/areas/quality_safety/quality_assurance/QAS19_819_data_integrity.pdf?ua=1> Acesso em: 12 de março de 2020.

ZIKMUND, W. G. Business research methods. 5.ed. Fort Worth, TX: Dryden, 2000.

APÊNDICE A - QUESTIONÁRIO 1: QUESTIONÁRIO DE INTEGRIDADE DE DADOS EM REGISTROS ELETRÔNICOS – QUALIDADE

Prezado(a) participante,

Você está sendo convidado(a) a participar da pesquisa **“BOAS PRÁTICAS DE INTEGRIDADE DE DADOS EM REGISTROS ELETRÔNICOS GERADOS EM SISTEMAS COMPUTADORIZADOS DE EQUIPAMENTOS ANALÍTICOS: UMA PROPOSTA PARA OS LABORATÓRIOS DE PESQUISA CIENTÍFICA EXPERIMENTAL DA FIOCRUZ”**, desenvolvida por **Bruno Bezerra Carvalho**, discente do Mestrado Profissional em Saúde Pública da Escola Nacional de Saúde Pública Sergio Arouca da Fundação Oswaldo Cruz (ENSP/FIOCRUZ), sob orientação do Professor Dr. José Manuel Santos de Varge Maldonado e pela Profa. Dra. Renata Almeida de Souza.

O objetivo central do estudo é avaliar a adoção de princípios e diretrizes de integridade de dados gerados eletronicamente por sistemas computadorizados de equipamentos analíticos em laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada da Fiocruz segundo o guia de boas práticas em gerenciamento de dados da Organização Mundial da Saúde (OMS).

O convite a sua participação se deve à sua atuação dentro do fluxo de processos de trabalho existente nos laboratórios com atividades de ensaio, plataforma tecnológica e/ou de pesquisa experimental básica e/ou aplicada na sua unidade ou escritório técnico da Fiocruz, seja por ser um profissional da área de Gestão da Qualidade (GQ) ou da área de Gestão de Tecnologia da Informação e Comunicação (TIC).

Os riscos serão mitigados mediante o total sigilo da identidade e dados pessoais dos participantes e, na redação final do estudo, quando necessário, utilizar-se-á de nomes fictícios. Para assegurar a confidencialidade e a privacidade das informações prestadas, apenas o pesquisador responsável pela pesquisa e seus orientadores, que se comprometem com o dever de sigilo e confidencialidade, terão acesso a seus dados e a todos os demais dados decorrentes dessa pesquisa, e não farão uso destas informações para outras finalidades.

Ao responder o questionário *online* os participantes não terão nenhum benefício direto ou imediato. No entanto, os resultados desta pesquisa poderão propor uma solução

para ausência de integridade de dados eletrônicos em laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica ou aplicada da Fiocruz mediante ações e diretrizes que auxiliem a implementação de um modelo para garantia de requisitos mínimos de integridade de dados em registros eletrônicos.

As perguntas a seguir devem ser respondidas pela área da **GESTÃO DA QUALIDADE** e estão relacionadas às estratégias da sua unidade/escritório técnico relacionadas ao gerenciamento de dados em registros eletrônicos (Integridade de Dados) oriundos de sistemas computadorizados de equipamentos analíticos pelos laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada desenvolvida internamente.

PARTE I – PERFIL DOS ENTREVISTADOS

Q1. Quanto tempo trabalha na Fiocruz?

- entre 1 a 5 anos
- entre 6 a 10 anos
- entre 11 a 15 anos
- entre 16 a 20 anos
- acima de 20. Especifique: _____ .

Q2. Qual seu cargo?

- Assistente técnico
- Técnico
- Analista
- Tecnologista
- Pesquisador
- Especialista
- Outro. Especifique: _____ .

Q3. Qual seu vínculo na Fiocruz?

- Servidor

- Terceirizado
- Outro. Especifique: _____ .

Q4. Em qual unidade ou escritório técnico você trabalha?

- IOC – Instituto Oswaldo Cruz
- INI – Instituto Nacional de Infectologia Evandro Chagas
- IFF – Instituto Nacional de Saúde da Mulher, da Criança e do Adolescente Fernandes Figueira
- IAM – Instituto Aggeu Magalhães
- IGM – Instituto Gonçalo Moniz
- IRR – Instituto Renne Rachou
- ILMD – Instituto Leonidas e Maria Deanne
- ICC – Instituto Carlos Chagas
- ENSP – Escola Nacional de Saúde Pública Sergio Arouca
- ICICT – Instituto de Comunicação e Informação Científica e Tecnológica
- Bio-Manguinhos – Instituto de Tecnologia em Imunobiológicos
- Farmanguinhos – Instituto de Tecnologia em Fármacos
- INCQS – Instituto Nacional de Controle de Qualidade em Saúde
- ICTB – Instituto de Ciência e Tecnologia em Biomodelos
- Escritório técnico Fiocruz Ceará
- Escritório técnico Fiocruz Mato Grosso do Sul
- Escritório técnico Fiocruz Rondônia

Q5. Familiaridade com o termo Integridade de Dados:

a) Você já obteve algum tipo de treinamento formal em Integridade de Dados?

- Não. Esse tema não é trabalhado na minha unidade/escritório
- Não. Mas a área de TIC já precisou buscar conhecimento em documentos técnicos e/ou artigos científicos sobre o tema
- Sim, porém, a área de TIC não utilizou o conhecimento para nenhuma configuração necessária nos equipamentos analíticos

() Sim, a área de TIC já recebeu treinamento sobre o tema para atuar no processo de implantação de integridade de dados eletrônicos

Acrescente algum comentário que julgar pertinente: _____

_____ .

PARTE II – PERFIL DA UNIDADE/ESCRITÓRIO

Q6. Na sua unidade/escritório existe um Sistema de Gestão da Qualidade efetivamente implementado que abrange a estrutura organizativa, os procedimentos, processos e recursos, e as ações sistemáticas necessárias para assegurar a confiança adequada de um produto ou serviço?

() Sim, na minha unidade/escritório técnico há um SGQ implementado

() Sim, mas o SGQ está em fase de implementação

() Não, não há interesse em implementar um SGQ na minha unidade/escritório técnico

() Não, não há um SGQ implementado na minha unidade/escritório técnico

() Não, mas esse tema já vem sendo discutido internamente na intenção de se implementar um SGQ

Acrescente algum comentário que julgar pertinente: _____

_____ .

Q7. Na sua unidade/escritório existem laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada?

() Possui somente laboratórios com atividades de ensaio

() Possui somente laboratórios com plataformas tecnológicas

() Não possui laboratórios com estas atividades

() Possui somente laboratórios com atividades de pesquisas experimentais básicas e/ou aplicadas

() Possui laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica ou aplicada

Acrescente algum comentário que julgar pertinente: _____

_____ .

Q8. Se sua resposta na questão anterior (Q8) foi positiva, responda por favor a questão abaixo:

a) Existem quantos laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica ou aplicada instalados em sua unidade/escritório técnico?

Entre 01 e 10

Entre 11 e 20

Entre 21 e 40

Entre 41 e 60

Acima de 60

Acrescente algum comentário que julgar pertinente: _____
_____ .

Q9. Quantos equipamentos analíticos existem em funcionamento no parque tecnológico da sua unidade/escritório técnico?

Entre 01 e 10

Entre 11 e 20

Entre 21 e 40

Entre 41 e 60

Acima de 60

Nenhum

Q10. Sua unidade/escritório técnico passa por processo de auditoria/verificação/inspeção ou regulação por órgãos/agências reguladoras e/ou de fomento nacional e/ou internacional?

Não passa por estes processos

Não, mas já foi regulada

Não, mas tem laboratórios que podem ser acreditados ou pré-qualificados

Sim, é regulada por uma AR internacional

Sim, é regulada por uma AR nacional

Se afirmativo, qual(is): _____ .

Q11. Sua unidade/escritório técnico possui algum ensaio ou laboratório acreditado e/ou pré-qualificado?

- Não possui
- Não possui, porém, tem interesse mas ainda não apresenta procedimentos suficientemente necessários para submeter aos processos de acreditação e/ou pré-qualificação
- Não tem interesse em ser acreditado e/ou pré-qualificado
- Não possui, mas já submeteu aos processos de acreditação e/ou pré-qualificação
- Sim, possui ensaio ou laboratório acreditado e/ou pré-qualificado
- Se afirmativo, qual(is): _____ .

PARTE III – MEDIDAS DE CONTROLES ORGANIZACIONAIS

Q12. Durante o processo de compras de equipamentos analíticos, a área da Qualidade é solicitada para formar uma equipe multidisciplinar (pesquisador/técnico da área específica da pesquisa, profissionais de gestão da qualidade, TI, infraestrutura e equipamentos) para o planejamento de compras?

- Sim. Existe a formação de uma equipe multidisciplinar na fase de planejamento de compra dos equipamentos analíticos com participação da área da Qualidade
- Sim. Porém nem sempre a área da Qualidade participa
- Não sei informar
- Em parte. Algumas vezes essa equipe é estruturada e formalizada
- Não. Não existe a formação de uma equipe multidisciplinar na fase de planejamento de compras dos equipamentos analíticos

Acrescente algum comentário que julgar pertinente: _____
_____ .

Q13. Sua unidade/escritório segue boas práticas de documentação (BPDoc) para garantir a exatidão, integralidade, consistência e confiabilidade dos dados eletrônicos gerados por sistemas computadorizados de equipamentos analíticos durante todo o seu período de utilidade – ou seja, durante todo o ciclo de vida dos dados?

- Não aplica boas práticas de documentação
- Não aplica boas práticas de documentação para dados eletrônicos

- Está em fase de implementação
- Sim, mas apenas para dados eletrônicos gerados em sistemas computadorizados de equipamentos analíticos considerados críticos
- Sim, para todos os dados eletrônicos gerados em sistemas computadorizados de equipamentos analíticos

Acrescente algum comentário que julgar pertinente: _____
_____ .

Q14. Se a resposta da questão anterior (Q14) foi afirmativa, responda por favor esta questão.

A área de gestão da qualidade ou de recursos humanos provê treinamento aos profissionais, bolsistas e alunos que utilizam os equipamentos analíticos no que se refere às boas práticas de documentação para garantir que os princípios da ALCOA (dados atribuíveis, legíveis, contemporâneos, originais e acurados) sejam compreendidos e aplicados às atividades inerentes?

- Não fornecem treinamento sobre BPDoc
- Não, somente quando solicitado à área de gestão da qualidade ou de recursos humanos
- A unidade/escritório não identifica esta necessidade de treinamento sobre BPdoc
- Sim, apenas para usuários que utilizam equipamentos analíticos
- Sim, para todos os profissionais que entram na unidade/escritório e alunos que necessitam utilizar os equipamentos analíticos

Acrescente algum comentário que julgar pertinente: _____
_____ .

Q15. Sua unidade/escritório técnico possui algum procedimento operacional padrão (POP) sobre integridade de dados eletrônicos gerados por sistemas computadorizados de equipamentos analíticos?

- Não possui e não tem interesse em implementar
- Não possui, porém, pretende implementar
- Sim, possui somente orientado para documentos físicos/papel
- Sim, possui um POP de integridade de dados eletrônicos
- Sim, possui um POP de integridade de dados para ambos (físico/papel e eletrônico)

Acrescente algum comentário que julgar pertinente: _____
_____ .

Q16. Se a resposta da questão anterior (Q16) foi “Sim”, responda à pergunta a seguir:

Os servidores, colaboradores, bolsistas e alunos possuem conhecimento do POP de integridade de dados eletrônicos implementada na unidade/escritório técnico?

Sim. O conhecimento deste POP é disseminado para todos os profissionais, bolsistas e alunos que ingressam na organização

Em parte. O conhecimento deste POP é disseminado somente para quem é usuário dos sistemas computadorizados de equipamentos analíticos

Não sei informar. O POP fica disponível na rede para quem quiser obter o conhecimento sobre ela

Acrescente algum comentário que julgar pertinente:

_____ .

Q17. Sua unidade/escritório adota uma cultura de qualidade com objetivo, por exemplo, de incentivar os profissionais, alunos e bolsistas a serem transparentes sobre falhas identificadas de integridade de dados eletrônicos?

Não adota uma cultura de qualidade

Não adota, mas planeja disseminar informações sobre o tema

Não identifica necessidade de adotar uma cultura de qualidade

Sim, porém, dissemina sobre outros temas

Sim, adota e dissemina informações sobre integridade de dados eletrônicos

Acrescente algum comentário que julgar pertinente: _____

_____ .

Q18. A direção e as gerências de laboratório com atividades de ensaio, plataformas tecnológicas e/ou de pesquisa experimental básica ou aplicada têm ciência da relevância sobre integridade de dados eletrônicos e da importância de seu papel na proteção da segurança da pesquisa experimental e na reputação de sua organização em relação aos dados eletrônicos gerados?

Não há conhecimento sobre o tema

Não, mas a área de gestão da qualidade vem planejando a disseminação desta importância a as consequências da não adesão

Em parte, mas não há prioridade no tema por alegar falta de recursos financeiros e/ou pessoal capacitado para implementar

Sim, tanto a direção quanto os gerentes de laboratório têm ciência da relevância e importância do tema para a unidade/escritório

Acrescente algum comentário que julgar pertinente: _____

_____ .

Q19. Os laboratórios com atividades de ensaio, plataformas tecnológicas e de pesquisa experimental básica ou aplicada adotam procedimentos, medidas de controle ou alguma ação para garantir integridade dos dados gerados eletronicamente?

Não existe nenhum procedimento, medidas de controle e ações para esta finalidade

Não, mas alguns laboratórios já manifestaram interesse em implementar

Não há conhecimentos sobre o tema integridade de dados

Sim, porém, adotam apenas algumas medidas de controle

Sim, várias medidas de controle vêm sendo implementadas nos laboratórios

Se afirmativo, especifique quais são as áreas de atuação destes laboratórios: _____

_____ .

PARTE VI – GESTÃO E COMPARTILHAMENTO DE DADOS

Q20. Existe(m) na unidade/escritório técnico a adoção de tecnologia(s) emergente(s) como projeto estratégico para inovar processos organizacionais?

Não temos interesse em nenhuma tecnologia emergente no presente momento

Não, mas já estamos estudando algumas tecnologias da 4ª revolução industrial

Sim, estamos adotando

Sim, já implementamos

Se afirmativo, qual(is): _____ .

Q21. Sendo a Fiocruz uma instituição de CT&I em saúde, onde tem nas suas atividades a geração de conhecimento nesta área, sua unidade/escritório técnico adota algum Plano de Gestão de Dados (PGD) para projetos de pesquisa?

- Não tem iniciativa em adotar um PGD
- Não, mas já estamos estudando adotar algum PGD
- Sim, alguns pesquisadores já adotam um PGD em seus projetos de pesquisa
- Sim, pois já disseminamos internamente que o objetivo de um PGD é facilitar a compreensão e a reutilização futura dos dados

Se afirmativo, qual(is) ferramenta(s): _____

Muito obrigado por dispor do seu tempo para responder este questionário. Suas respostas serão de extrema importância para análise dos resultados e contribuirão com este projeto de pesquisa que objetiva identificar o nível de maturidade do gerenciamento de dados eletrônicos gerados por sistemas computadorizados de equipamentos analíticos nos laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisa experimental básica ou aplicada na Fiocruz.

APÊNDICE B - QUESTIONÁRIO 2: QUESTIONÁRIO DE INTEGRIDADE DE DADOS EM REGISTROS ELETRÔNICOS - TIC

Prezado(a) participante,

Você está sendo convidado(a) a participar da pesquisa “**BOAS PRÁTICAS DE INTEGRIDADE DE DADOS EM REGISTROS ELETRÔNICOS GERADOS EM SISTEMAS COMPUTADORIZADOS DE EQUIPAMENTOS ANALÍTICOS: UMA PROPOSTA PARA OS LABORATÓRIOS DE PESQUISA CIENTÍFICA EXPERIMENTAL DA FIOCRUZ**”, desenvolvida por **Bruno Bezerra Carvalho**, discente do Mestrado Profissional em Saúde Pública da Escola Nacional de Saúde Pública Sergio Arouca da Fundação Oswaldo Cruz (ENSP/FIOCRUZ), sob orientação do Professor Dr. José Manuel Santos de Varge Maldonado e pela Profa. Dra. Renata Almeida de Souza.

O objetivo central do estudo é avaliar a adoção de princípios e diretrizes de integridade de dados gerados eletronicamente por sistemas computadorizados de equipamentos analíticos em laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada da Fiocruz segundo o guia de boas práticas em gerenciamento de dados da Organização Mundial da Saúde (OMS).

O convite a sua participação se deve à sua atuação dentro do fluxo de processos de trabalho existente nos laboratórios com atividades de ensaio, plataforma tecnológica e/ou de pesquisa experimental básica e/ou aplicada na sua unidade ou escritório técnico da Fiocruz, seja por ser um profissional da área de Gestão da Qualidade (GQ) ou da área de Gestão de Tecnologia da Informação e Comunicação (TIC).

Os riscos serão mitigados mediante o total sigilo da identidade e dados pessoais dos participantes e, na redação final do estudo, quando necessário, utilizar-se-á de nomes fictícios. Para assegurar a confidencialidade e a privacidade das informações prestadas, apenas o pesquisador responsável pela pesquisa e seus orientadores, que se comprometem com o dever de sigilo e confidencialidade, terão acesso a seus dados e a todos os demais dados decorrentes dessa pesquisa, e não farão uso destas informações para outras finalidades.

Ao responder o questionário *online* os participantes não terão nenhum benefício direto ou imediato. No entanto, os resultados desta pesquisa poderão propor uma solução

para ausência de integridade de dados eletrônicos em laboratórios com atividades de ensaio, plataformas tecnológicas e pesquisas experimentais básica ou aplicada da Fiocruz mediante ações e diretrizes que auxiliem a implementação de um modelo para garantia de requisitos mínimos de integridade de dados em registros eletrônicos.

As perguntas a seguir devem ser respondidas pela área da **GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO** e estão relacionadas às estratégias da sua unidade/escritório técnico relacionadas ao gerenciamento de dados em registros eletrônicos (Integridade de Dados) oriundos de sistemas computadorizados de equipamentos analíticos pelos laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisas experimentais básica ou aplicada desenvolvida internamente.

PARTE I – PERFIL DOS ENTREVISTADOS

Q1. Quanto tempo trabalha na Fiocruz?

- entre 1 a 5 anos
- entre 6 a 10 anos
- entre 11 a 15 anos
- entre 16 a 20 anos
- acima de 21. Especifique: _____ .

Q2. Qual seu cargo?

- Assistente técnico
- Técnico
- Analista
- Tecnologista
- Pesquisador
- Especialista
- Outro. Especifique: _____ .

Q3. Qual seu vínculo na Fiocruz?

- Servidor
- Terceirizado
- Outro. Especifique: _____ .

Q4. Em qual Unidade ou Escritório Técnico você trabalha?

- IOC – Instituto Oswaldo Cruz
- INI – Instituto Nacional de Infectologia Evandro Chagas
- IFF – Instituto Nacional de Saúde da Mulher, da Criança e do Adolescente Fernandes Figueira
- IAM – Instituto Aggeu Magalhães
- IGM – Instituto Gonçalo Moniz
- IRR – Instituto Renne Rachou
- ILMD – Instituto Leonidas e Maria Deanne
- ICC – Instituto Carlos Chagas
- ENSP – Escola Nacional de Saúde Pública Sergio Arouca
- ICICT – Instituto de Comunicação e Informação Científica e Tecnológica
- Bio-Manguinhos – Instituto de Tecnologia em Imunobiológicos
- Farmanguinhos – Instituto de Tecnologia em Fármacos
- INCQS – Instituto Nacional de Controle de Qualidade em Saúde
- ICTB – Instituto de Ciência e Tecnologia em Biomodelos
- Escritório técnico Fiocruz Ceará
- Escritório técnico Fiocruz Mato Grosso do Sul
- Escritório técnico Fiocruz Rondônia

PARTE II – MEDIDAS DE CONTROLES ORGANIZACIONAIS

Q5. Durante o processo de compra de equipamentos analíticos a área de TIC é solicitada para formar uma equipe multidisciplinar (pesquisador/técnico da área específica da pesquisa, profissionais de gestão da qualidade, TI, infraestrutura e equipamentos) para o planejamento de compras?

- Sim, existe a formação de uma equipe multidisciplinar na fase de planejamento de compra dos equipamentos analíticos com participação da área de TIC
- Sim, porém, nem sempre a área de TIC participa
- Não sei informar
- Em parte. Algumas vezes essa equipe é estruturada e formalizada
- Não, a área de TIC é solicitada somente quando o equipamento é entregue pelo fornecedor

Acrescente algum comentário que julgar pertinente: _____
_____ .

Q6. A área de TIC participa de alguma fase de treinamento que é dado pelo fabricante do equipamento analítico quando da instalação e configuração dentro dos laboratórios da sua unidade/escritório?

- Não. A área de TIC é chamada somente para disponibilizar o ambiente de rede para uso dos equipamentos analíticos
- Não, porém, a área de TIC já foi chamada para resolver problemas que envolvem configuração dos sistemas computadorizados de equipamentos analíticos
- Nunca foi chamado e também nunca precisou atender chamados que envolvem os sistemas computadorizados de equipamentos analíticos
- Sim, apenas para alguns sistemas computadorizados de equipamentos analíticos mais críticos
- Sim. A área de TIC sempre é uma área participante de treinamentos que envolvem a instalação e configuração dos sistemas computadorizados de equipamentos analíticos

Acrescente algum comentário que julgar pertinente: _____
_____ .

Q7. Familiaridade com o termo integridade de dados:

a) Você já obteve algum tipo de treinamento formal em integridade de dados?

Não. Esse tema não é trabalhado na minha unidade/escritório

Não. Mas a área de TIC já precisou buscar conhecimento em documentos técnicos e/ou artigos científicos sobre o tema

Sim, porém, a área de TIC não utilizou o conhecimento para nenhuma configuração necessária nos equipamentos analíticos

Sim, a área de TIC já recebeu treinamento sobre o tema para atuar no processo de implantação de integridade de dados eletrônicos

Acrescente algum comentário que julgar pertinente: _____

_____ .

Q8. A unidade/escritório possui alguma rotina de auto inspeção e/ou auditoria interna que avalie periodicamente a efetividade e aplicabilidade de segurança da informação dos sistemas computadorizados de equipamentos analíticos?

Nunca realizou auto inspeção e/ou auditoria interna nos sistemas computadorizados

Não utiliza, mas sabe que as atividades de auto inspeção e/ou auditoria interna podem revelar falhas na gestão dos dados eletrônicos nos sistemas computadorizados

Não identifica necessidade em realizar auto inspeção e/ou auditorias internas

Sim, apenas em alguns equipamentos analíticos

Sim, realiza em todos os equipamentos analíticos

Acrescente algum comentário que julgar pertinente: _____

_____ .

Q9. A área de TIC da sua unidade/escritório recebe dos gerentes de laboratório e-mail de solicitação formalizando a criação de senha individual, bem como dos níveis e perfis de acesso para utilização dos sistemas computadorizados dos equipamentos analíticos?

- Não, a área de TIC apenas recebe solicitação para criar senhas individuais para uso dos sistemas computadorizados dos equipamentos analíticos
- A área de TIC não gerencia os sistemas computadorizados dos equipamentos analíticos
- Não, mas já vem planejando implementar esse processo com os gerentes de laboratório da unidade/escritório
- Sim, recebe e-mail solicitando senha individual, porém, para apenas alguns equipamentos analíticos
- Sim, o acesso a todos os equipamentos analíticos é por senha individual e solicitado por e-mail pelos gerentes de laboratório

Acrescente algum comentário que julgar pertinente: _____

_____ .

PARTE III – MEDIDAS DE CONTROLES OPERACIONAIS

Q10. Os equipamentos analíticos estão instalados numa rede elétrica estabilizada?

- Sim. Todos os equipamentos
- Alguns equipamentos somente
- Não sei informar
- Não há rede elétrica estabilizada nos laboratórios analíticos

Acrescente algum comentário que julgar pertinente: _____

_____ .

Q11. Os equipamentos analíticos estão protegidos com uso de nobreak e/ou gerador com objetivo de minimizar o risco da perda de dados eletrônicos gerados pelos sistemas computadorizados no caso de um evento de queda de energia?

- Sim. Todos os equipamentos
- Alguns equipamentos somente
- Não sei informar
- Não há nobreak sendo utilizado nos equipamentos
- Não há Gerador instalado na unidade/escritório

Acrescente algum comentário que julgar pertinente: _____

Q12. Existe algum controle de acesso físico no laboratório onde se encontram instalados os equipamentos analíticos?

- Sim, existe em todos os laboratórios
- Sim, somente em alguns laboratórios
- Sim, porém, somente por chave
- Não sei informar
- Não há controle físico

Acrescente algum comentário que julgar pertinente: _____

Q13. Os equipamentos analíticos ou os computadores diretamente conectados estão conectados em alguma rede de dados (cabada ou sem fio)?

- Não, pois são equipamentos antigos que não possuem funcionalidade para rede de dados
- Não, pois não há infraestrutura de rede de dados disponível nos laboratórios
- Não sei informar
- Sim, porém alguns equipamentos apenas estão conectados em rede de dados
- Sim, todos os laboratórios possuem infraestrutura de rede de dados e os equipamentos analíticos estão conectados na rede

Acrescente algum comentário que julgar pertinente: _____

Q14. A área de TIC executa algum procedimento técnico para configurar e manter a sincronização de data e hora dos sistemas computadorizados dos equipamentos analíticos?

Não, estas configurações não são feitas pela área de TIC nos sistemas computadorizados dos equipamentos analíticos. Somente em computadores fora dos laboratórios

Não, apenas orientamos aos gerentes, analistas e técnicos dos laboratórios sobre a importância e os procedimentos necessários

A área de TIC não é responsável pelas configurações nos sistemas computadorizados dos equipamentos analíticos

Sim, a área de TIC mantém a data e hora nos sistemas computadorizados dos equipamentos analíticos sincronizados

Sim, porém em alguns sistemas computadorizados dos equipamentos analíticos
Acrescente algum comentário que julgar pertinente: _____

Q15. Todos os computadores diretamente conectados aos equipamentos analíticos estão com as versões de sistema operacional (SO) atualizados?

Não, os computadores ainda são antigos e precisam usar um SO antigo devido à incompatibilidade dos equipamentos analíticos

A área de TIC não gerencia os computadores diretamente conectados aos equipamentos analíticos, somente os que estão fora dos laboratórios

Sim, a área de TIC atualiza as versões de SO sempre que há novas atualizações disponíveis

Acrescente algum comentário que julgar pertinente: _____

Q16. É utilizada alguma metodologia de Validação dos Sistemas Computadorizados (VSC) dos equipamentos analíticos com o objetivo de minimizar os riscos para garantir a exatidão e a integridade de dados eletrônicos e a qualidade dos resultados?

- Nunca validou os sistemas computadorizados dos equipamentos analíticos
- Não utiliza, mas sabe da importância de realizar a VSC
- Não identifica a necessidade em validar os sistemas computadorizados
- Sim, mas somente em alguns equipamentos
- Sim, utiliza em todos os equipamentos analíticos

Acrescente algum comentário que julgar pertinente: _____

_____ .

Q17. O SO dos computadores diretamente conectado aos equipamentos analíticos está configurado para gerar log de registro dos eventos relacionados à *login/logoff* dos usuários, bem como de alteração e tentativa de alteração de configurações do SO?

- Não, os computadores não foram configurados para gravar log de registro destes tipos de evento
- Não sei informar, pois a área de TIC não gerencia os computadores que estão diretamente conectados aos equipamentos analíticos
- Sim, porém, essas configurações foram feitas apenas em alguns computadores conectados aos equipamentos analíticos
- Sim, todos os computadores estão configurados para gerar log de registro de eventos para *login/logoff* dos usuários e alterações de configurações no SO

Acrescente algum comentário que julgar pertinente: _____

_____ .

Q18. O sistema executado nos equipamentos analíticos possui configurações de trilha de auditoria (*Audit Trail*) implementados para capturar a identificação dos usuários (IDs) e os registros de data e hora das ações que criam, modificam ou excluem dados eletrônicos do sistema?

- Sim, existem atributos e configurações implementados de *Audit Trail* em todos os equipamentos analíticos
- Sim, existem atributos e configurações implementados de *Audit Trail*, porém, somente em alguns equipamentos analíticos
- Não sei informar
- Não, não existe *Audit Trail* implementado nos equipamentos
- Não, mas estamos adotando este procedimento de configuração nos equipamentos analíticos

Acrescente algum comentário que julgar pertinente: _____
_____ .

Q19. É realizada alguma rotina de *backup* dos *logs* que registram os eventos do SO, dos dados e metadados gravados pelos usuários do sistema computadorizado, bem como das trilhas de auditoria (*Audit Trail*) do sistema que roda no equipamento analítico?

- Sim, existe uma rotina de backup que periodicamente copia os logs, os dados e metadados e as trilhas de auditoria dos computadores diretamente conectado aos equipamentos analíticos
- Sim, porém, somente de alguns computadores diretamente conectados aos equipamentos analíticos
- Não sei informar
- Não, mas estamos adotando estes procedimentos nos computadores dos laboratórios e nos sistemas computadorizados
- Não, os dados ficam apenas armazenados localmente no disco dos computadores diretamente conectado aos equipamentos analíticos

Acrescente algum comentário que julgar pertinente: _____
_____ .

Q20. Qual é a metodologia de backup dos dados eletrônicos (dados, metadados, trilhas de auditoria etc.) utilizada nos sistemas computadorizados de equipamentos analíticos para mitigar o risco de perda dos dados eletrônicos em casos de uma falha no sistema, corrupção de um disco ou um desastre?

- Cópia dos dados e logs para um dispositivo de HD Externo com intervenção manual por um usuário do próprio laboratório
- Cópia dos dados e logs para um dispositivo de HD Externo com intervenção manual por um profissional da área de TIC
- Não sei informar
- Cópia dos dados e logs através de um sistema de backup em rede (cópia automatizada)
- Não existe Procedimento Operacional Padrão (POP) e/ou Procedimento de Uso (PU) de backup dos dados e logs dos computadores/equipamentos analíticos

Acrescente algum comentário que julgar pertinente: _____

_____ .

Q21. A área de TIC possui algum Procedimento Operacional Padrão (POP) e/ou Procedimento de Uso (PU) para processo de validação dos backups que foram realizados dos logs, dados, metadados e trilhas de auditoria com objetivo de garantir a recuperação de dados eletrônicos em caso de perda dos dados ou para evidências de reprodutibilidade das análises?

- Sim, a equipe de TIC executa atividade periódica de restauração dos backups de dados dos equipamentos analíticos para registrar e testar a validação e reconstrução de dados eletrônicos
- Sim, a equipe de TIC executa atividade de restauração dos backups dos dados dos equipamentos para registrar e testar a validação e reconstrução de dados eletrônicos somente quando solicitado

- Não sei informar
- Não, a tarefa de restauração é realizada somente quando é necessário restaurar algum arquivo específico
- Não, a área de TIC não realiza backup dos dados eletrônicos gerados pelos sistemas computadorizados dos equipamentos analíticos

Acrescente algum comentário que julgar pertinente: _____

_____ .

Q22. A administração do sistema operacional como também do sistema computadorizado do equipamento analítico é realizada somente pela área de TIC da unidade/escritório?

- Sim, a equipe de TIC é quem possui o login/senha do usuário administrador tanto do computador quanto do sistema computadorizado dos equipamentos analíticos
- Sim, porém, somente dos computadores conectados aos equipamentos analíticos
- Não sei informar
- Não, esta administração é realizada pelo próprio laboratório
- Não, a equipe de TIC realiza atendimentos técnicos esporádicos somente quando solicitado pelo laboratório analítico

Acrescente algum comentário que julgar pertinente: _____

_____ .

Q23. Existem níveis e perfis de acesso configurados nos computadores diretamente conectados aos equipamentos analíticos como também nos sistemas computadorizados destes equipamentos?

- Não, os usuários usam o computador e o sistema computadorizado dos equipamentos analíticos com o mesmo perfil de acesso

A área de TIC não gerencia os computadores e os equipamentos analíticos que estão nos laboratórios

Não sei informar

Sim, porém, apenas em alguns computadores e equipamentos com níveis e perfis de acesso configurados

Sim, existem níveis e perfis de acesso configurados e implementados nos equipamentos analíticos dos laboratórios

Acrescente algum comentário que julgar pertinente: _____
_____ .

Q24. Existem senhas individuais criadas e configuradas para uso nos computadores diretamente conectados aos equipamentos analíticos e nos sistemas computadorizados destes equipamentos?

Não, o acesso aos computadores e aos equipamentos analíticos é sem senha, ou seja, acesso aberto e irrestrito

Não, os usuários acessam os computadores e os equipamentos analíticos através de senha compartilhada

Não sei informar

Sim, existem senhas individuais, porém, para os sistemas computadorizados de equipamentos analíticos mais críticos

Sim, todos os computadores diretamente conectados aos equipamentos analíticos e os sistemas computadorizados destes equipamentos possuem acesso por senha individual

Acrescente algum comentário que julgar pertinente: _____
_____ .

Muito obrigado por dispor do seu tempo para responder este questionário. Suas respostas serão de extrema importância para análise dos resultados e contribuirão com este projeto de pesquisa que objetiva identificar o nível de maturidade do gerenciamento de dados eletrônicos gerados por sistemas computadorizados de equipamentos analíticos nos

laboratórios com atividades de ensaio, plataformas tecnológicas e/ou pesquisa experimental básica ou aplicada na Fiocruz.