UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE PRODUÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

RAFAEL CAMARGO CONEGLIAN

MFV-SI – Mapa de Fluxo de Valor da Segurança da Informação: uma ferramenta de apoio para a segurança de dados pessoais à luz dos conceitos *Lean* e LGPD

Maringá
2021

RAFAEL CAMARGO CONEGLIAN

MFV-SI – Mapa de Fluxo de Valor da Segurança da Informação: uma ferramenta de apoio para a segurança de dados pessoais à luz dos conceitos *Lean* e LGPD

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção do Departamento de Engenharia de Produção, Centro de Tecnologia da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Engenharia de Produção.
Área de concentração: Engenharia de Produção

Orientador: Prof. Dr. Marco Antonio Ferreira

Maringá
2021

Dados Internacionais de Catalogação-na-Publicação (CIP)
(Biblioteca Central - UEM, Maringá - PR, Brasil)

Coneglian, Rafael Camargo

C747m MFV-SI – Mapa de fluxo de valor da segurança da informação: uma ferramenta de apoio para a segurança de dados pessoais à luz dos conceitos Lean e LGPD / Rafael Camargo Coneglian. -- Maringá, PR, 2021.

101 f.: il. color., figs., tabs.

Orientador: Prof. Dr. Marco Antonio Ferreira.

Dissertação (Mestrado) - Universidade Estadual de Maringá, Centro de Tecnologia, Departamento de Engenharia de Produção, Programa de Pós-Graduação em Engenharia de Produção, 2021.

1. Mapa de fluxo de valor da segurança da informação (MFV-SI). 2. Lei geral de proteção de dados (LGPD). 3. Mapa de fluxo de valor (MFV). 4. Segurança da Informação. 5. Segurança de dados. I. Ferreira, Marco Antonio, orient. II. Universidade Estadual de Maringá. Centro de Tecnologia. Departamento de Engenharia de Produção. Programa de Pós-Graduação em Engenharia de Produção. III. Título.

CDD 23.ed. 658.472

Rosana de Souza Costa de Oliveira - 9/1366

FOLHA DE APROVAÇÃO

RAFAEL CAMARGO CONEGLIAN

MFV-SI – Mapa de Fluxo de Valor da Segurança da Informação: uma ferramenta de apoio para a segurança de dados pessoais à luz dos conceitos *Lean* e LGPD

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção do Departamento de Engenharia de Produção, Centro de Tecnologia da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Engenharia de Produção pela Banca Examinadora composta pelos membros:

BANCA EXAMINADORA

Prof. Dr. Marco Antonio Ferreira
Universidade Federal Tecnológica do Paraná – DEP/UTFPR

Profa. Dra. Francielle Cristina Fenerich
Universidade Estadual de Maringá – DEP/UEM

Prof. Dr. Renato Balancieri
Universidade Estadual do Paraná – UNESPAR/Apucarana

Aprovada em: 28 de fevereiro de 2021.
Local da defesa: Sala de Projeção, Bloco 19, *campus* da Universidade Estadual de Maringá.

AGRADECIMENTOS

Agradeço primeiramente a Deus, que me guiou e deu forças durante essa brilhante jornada.

À minha esposa Tamara, pelo amor e parceria incondicional, que contribuiu com seus conhecimentos técnicos e sabedoria emocional.

Aos meus pais, Angelo Coneglian e Maria Dalva Coneglian, e minha irmã Daniela Coneglian, que me proporcionaram, entre outras coisas, a possibilidade de estudar em uma grande instituição, como a Universidade Estadual de Maringá.

Por fim, agradeço ao meu orientador, Prof. Dr. Marco Antonio Ferreira, pelos seus ensinamentos e assertividade na condução do desenvolvimento deste trabalho.

MFV-SI – mapa de fluxo de valor da segurança da informação: uma ferramenta de apoio para a segurança de dados pessoais à luz dos conceitos *Lean* e LGPD

RESUMO

A gestão empresarial moderna passa pela abordagem da gestão e proteção dos dados pessoais. Para tanto, este trabalho executa uma releitura da ferramenta MFV (Mapa de Fluxo de Valor), criando MFV-SI (Mapa de Fluxo de Valor – Segurança da Informação) de forma a contribuir com a privacidade do indivíduo e para com o processo de adequação aos requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD). A LGPD do Brasil, sancionada em agosto de 2018, surge em uma conjuntura onde as relações comerciais globais, cada vez mais integradas pela evolução tecnológica, buscam respostas para a proteção de dados. Já o MFV, amplamente estudado, tem por definição ser uma representação gráfica dos fluxos de materiais e de informações, mapeando atividades de agregação e não agregação de valor, de acordo com o propósito de valor do cliente. Dessa forma, este trabalho classifica uma nova classe de desperdício: a vulnerabilidade dos dados pessoais. O estudo está dividido em quatro fases. A primeira apresentará uma revisão da literatura, trazendo a contextualização da transformação digital nos processos de negócios contemporâneos, o cenário da segurança de informação no Brasil, e os conceitos e aplicações da gestão da informação e gestão enxuta nas organizações. A segunda fase é dedicada à concepção do modelo MFV-SI, seguido pela terceira etapa de testagem do instrumento, por meio de sua aplicação em três estudos de casos. Por fim, a quarta etapa apresenta os resultados obtidos e uma discussão acerca dos benefícios alcançados e oportunidades de estudos futuros. O trabalho conclui que, diante das evoluções tecnológicas e normativas, é possível classificar de uma nova ordem de desperdício, o desperdício da vulnerabilidade dos dados pessoais e que, diante disso, a criação do índice de vulnerabilidade, a avaliação do propósito de valor e a avaliação do legítimo interesse na proposição de valor, por meio do MFV-SI, contribuem para uma gestão empresarial moderna focada na segurança dos dados pessoais.

Palavras-chave: Mapa de Fluxo de Valor. MFV. MFV-SI. LGPD. Segurança da Informação.

VSM-IS - value stream map- information security: a support tool for personal data security under de Lean and LGPD concepts

ABSTRACT

Modern business management takes the approach of managing and protecting personal data. To this end, this work performs a re-reading of the tool VSM (Value Stream Map) creating VSM-IS (Value Stream Map - Information Security) in order to contribute to the individual's privacy and to the process of adaptation to the requirements of the General Personal Data Protection Act (LGPD). The LGPD do Brasil, sanctioned in August 2018, appears in a context where global commercial relations increasingly integrated by technological evolution, seek answers for data protection. The VSM, which has been extensively studied, has the definition of being a graphical representation of material and information flows, mapping activities of aggregation and non-aggregation of value, according to the purpose of the customer's value. Thus, this work classifies a new class of waste: the vulnerability of personal data. The study is divided into four phases. The first will present a literature review bringing the context of digital transformation in contemporary business processes, the scenario of information security in Brazil, and the concepts and applications of information management and lean management in organizations. The second phase is dedicated to the design of the VSM-IS model followed by the third stage of testing the proposed instrument through its application in 3 case studies. Finally, the fourth step, presents the results obtained and a discussion about the benefits achieved and opportunities for future studies. The work concludes that in view of technological and regulatory developments, it is possible to classify a new waste order, the waste of the vulnerability of personal data, and that, in view of this, the creation of the vulnerability index, the evaluation of the value purpose and the evaluation the legitimate interest in the value proposition, through the VSM-IS, contribute to a modern business management focused on the security of personal data.

***Keywords*:** Value Stream Map. VSM. VSM-IS. LGPD. GDPR. Information Security.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

BPMN	*Businnes Process Model and Notation*
BPR	*Businnes Process Redesign*
CF	*Constituição Federal*
CRS	*Corporate Responsabilidade Social*
DEP	*Dados Extra Propósito*
DICQ	*Sistema Nacional de Acreditação de Laboratórios*
ERP	*Enterprise Resourse Planning*
EU	*União Europeia*
GDPR	*General Data Protection Regulation*
GI	*Gestão da Informação*
IA	*Inteligência Artificial*
INSS	*Instituto Nacional do Seguro Social*
IoT	*Internet das Coisas*
JIT	*Just-in-Time*
LGPD	*Lei Geral de Proteção de Dados*
LIM	*Lean Information Management*
LM	*Lean Manufacturing*
LO	*Lean Office*
MFV	*Mapa de Fluxo de Valor*
MFV-SI	*Mapa de Fluxo de Valor – Segurança da Informação*
OEE	*Overall Equipment Effectiveness*
OMS	*Organização Mundial da Saúde*
ONU	*Organização das Nações Unidas*
PCP	*Planejamento e Controle da Produção*
PIB	*Produto Interno Bruto*
PMEs	*Pequenas e Médias Empresas*
SGSI	*Sistema de Gestão da Segurança da Informação*
SI	*Segurança da Informação*
TBL	*Triplle Botton Line*

SUMÁRIO

1 INTRODUÇÃO

Nessa seção, serão apresentados os fatores relacionados ao contexto de pesquisa e seus elementos motivadores. Serão expostos também a questão e os objetivos de pesquisa, uma visão geral a respeito dos temas envolvidos, suas respectivas relevâncias e, por fim, a justificativa para a realização deste trabalho.

1.1 Contexto da pesquisa

Essa pesquisa foi concebida diante do atual cenário de atualizações legislativas, evoluções tecnológicas e de técnicas gerenciais alinhadas à proteção dos dados pessoais.

O advento da informática e consequentemente suas respectivas mudanças políticas e sociais têm mudado a forma de tratamento de dados pessoais, não somente em termos de aumento da quantidade de informação processada, mas também nos aspectos qualitativos atribuídos a sofisticadas técnicas de programação (DONEDA, 2011).

Pardolesi (2003), desde então, alertava que o custo de manutenção do sigilo de informações pessoais, cresceria exponencialmente devido à evolução dos sistemas de armazenamento e capacidade de processamento de dados, à medida que se economizaria com a eficiência operacional na manipulação de dados.

Ao olhar sobre o aspecto social, mais especificamente sobre o aspecto da garantia aos direitos de privacidade do ser humano, a primeira forma de lei redigida foi a Declaração Americana dos Direitos e Deveres do Homem, de 1948, que determinou, em seu artigo V, o seguinte: “Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar”. No mesmo ano, a Organização das Nações Unidas (ONU) reforçou a garantia desses direitos por meio do lançamento da Declaração Universal dos Direitos Humanos:

> Artigo 12. Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. (DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948).

No Brasil, a primeira manifestação sobre privacidade e intimidade no âmbito legal foi a Constituição de 1988, em que o inciso X diz: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

No entanto, tais legislações se mostraram insuficientes ao longo do tempo, principalmente após o advento da internet e a evolução tecnológica. No Brasil, mesmo com a Lei nº12.965, de 2014, conhecida como Marco Civil da Internet, bem como das previsões genéricas do Código Civil e do Código de Defesa do Consumidor, que previam diretrizes de proteção à privacidade na internet, ainda se fazia necessário uma lei específica que tratasse da proteção de dados pessoais (BRASIL, 2014). Em 2016, o Ministério Público Federal do Espírito Santo iniciou a investigação do vazamento de dados sensíveis de trabalhadores que deram entrada no pedido de aposentadoria no Instituto Nacional do Seguro Social (INSS). Eles tiveram seus dados disponibilizados às instituições financeiras, que por sua vez ligavam oferecendo crédito consignado, antes mesmo da aposentadoria ser concedida. A empresa Uber, em 2018, informou que os dados de 156 mil brasileiros foram vazados devido a um ataque externo. Já o caso conhecido como Cambridge Analytica, que influenciou o debate político e fomentou a propagação de *fake news* no mundo todo, afetou um pouco mais de 443 mil brasileiros, que tiveram seus dados vazados via Facebook (LOTT, 2019).

O objetivo da Lei nº 13.709/2018, popularmente conhecida como Lei Geral de Proteção de Dados (LGPD), é assegurar a proteção de dados pessoais dos brasileiros, de modo a garantir seu direito à privacidade. Direito esse, citado por Elkington (1997), que explica que o desenvolvimento dos aspectos sociais de uma organização pode ser entendido como um conjunto de práticas empresariais benéficas e justas ao trabalho, trabalhador e comunidade, contribuindo com valores morais e de justiça.

Dentre as práticas gerenciais utilizadas ao redor do mundo, destacam-se aquelas ligadas ao conceito de manufatura enxuta, conhecida como *Lean Manufacturing* (LM) ou simplesmente *Lean*. O modelo de gestão *Lean* é baseado na redução ou eliminação de atividades que não agregam valor ao negócio, apoiado por diversas ferramentas que auxiliam no processo de diagnóstico e tratamento destes desperdícios (LIKER, 2004; MOSTAFA & DUMRAK, 2015; WOMACK, JONES, & DANIEL, 1996).

Faulkner e Badurdeen (2014) mostram que uma das ferramentas que mais tem recebido atenção é o Mapa de Fluxo de Valor (MFV), por se tratar de uma ferramenta de identificação de desperdícios, podendo ser adaptada a diversos processos administrativos e operacionais. Rotter et al. (2019) corroboram a relevância e atualidade do MFV em uma revisão sistemática sobre gestão enxuta na área da saúde, que entre 33 estudos analisados 26 descreveram o uso da ferramenta.

Ao estudar o processo de pronto atendimento de um hospital, Worth et al. (2013) utilizaram a ferramenta para analisar a cadeia de valor percorrida pelo paciente, identificando

os processos de tratamento de dados do indivíduo e avaliando os desperdícios inerentes à sua manipulação, como, dados incompletos, dados incorretos ou dados duplicados por exemplo.

Para Mitnick e Simon (2009), o ativo mais impactante para uma organização é o dado ou a informação. Eles explicam que a depreciação de *hardwares* ou grandes parques industriais são menos impactantes do que a perda de dados informacionais relacionados ao desenvolvimento de produto, lista de clientes e planos de negócios, por exemplo.

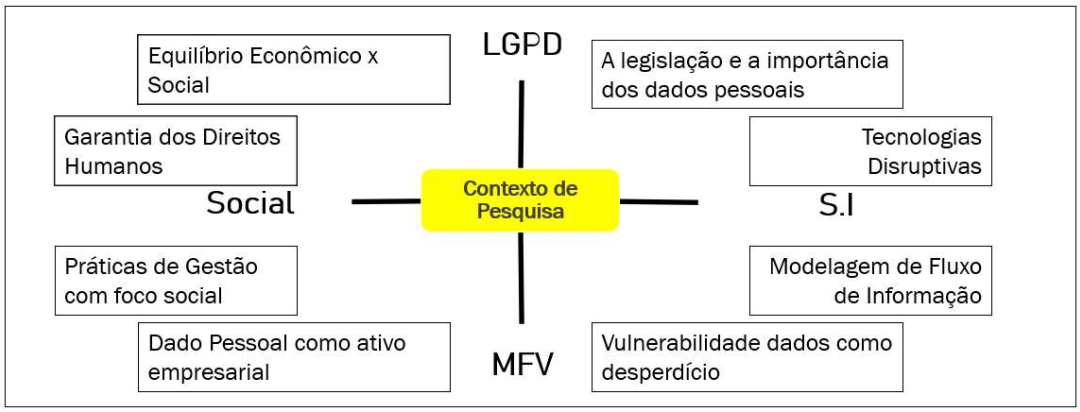
A revista eletrônica *The Economist* (2017) listou as cinco empresas mais valiosas do mundo, em que na centralidade do seu modelo de negócio está a coleta e o tratamento de dados de pessoas. Somados seus lucros, a *Google, Amazon, Apple, Facebook* e *Microsoft* ultrapassaram o valor de US $ 25 bilhões no primeiro trimestre de 2017. É inegável que as soluções trazidas por esses gigantes beneficiaram os consumidores e que poucas pessoas abririam mão das facilidades encontradas no mecanismo de busca do Google ou das notícias do *Facebook.* No entanto, a pelo menos 15 anos, Mitnick e Simon (2005) alertam que a "gratuidade" de seus serviços é, na verdade, financiada pela obtenção dos dados dos usuários, que fomentam um grande aparato publicitário. Morozov (2019) aponta que as grandes firmas de tecnologia adotam estrategicamente o processo de coleta de dados guiadas pela necessidade de superar os concorrentes e obter apoio político, onde a disputa não seria necessariamente por dados, mas por expansão de mercado através dos dados.

Pensar no dado pessoal como um ativo empresarial nos remete à importância de uma boa gestão desse valor. A modelagem do fluxo de informações mostra, mais uma vez, sua importância para organizações, uma vez que sua utilização é motivada pela necessidade de entender melhor como organizar e coordenar processos, eliminar processos redundantes, minimizar a duplicação de informações e gerenciar o compartilhamento de informações entre organizações (SZCZERBICKI, 1991; HOWELLS, 1995).

Neste contexto de pesquisa, este trabalho propõe questionamentos acerca dos atributos da ferramenta MFV no mapeamento dos desperdícios envolvidos na cadeia de valor, relacionados ao sigilo e proteção de dados pessoais.

A Figura 1 traz uma representação gráfica do contexto de pesquisa deste trabalho.

Figura 1 - Contexto de Pesquisa



Fonte: elaborado pelo autor.

1.2 Indagação e objetivos da pesquisa

Por meio deste *background* exposto e ao entender que as ferramentas de gestão *Lean* exercem um papel fundamental e atual como modelo de gestão, considerando a evolução tecnológica, bem como os aspectos legais e regulares da LGPD, a vulnerabilidade social promovida pela inserção das novas tecnologias da informação e modelos de relacionamento entre, empresas, processos e pessoas, surge a pergunta de pesquisa: é possível utilizar os conceitos do MFV para análise da segurança da informação à luz dos requisitos da LGPD? Desta forma, o objetivo geral da pesquisa é elaborar o Mapa de Fluxo de Valor – Segurança da Informação (MFV-SI) à luz dos requisitos da LGPD, por meio da releitura das funcionalidades do MFV convencional, contribuindo para a evolução de aspectos sociais relacionados à privacidade de dados e consequentemente para adequação à lei em questão.

Tendo em vista o objetivo geral e a questão de pesquisa anteriormente declarados, são listados os objetivos específicos deste trabalho. São eles:

- Analisar o impacto do tratamento de dados pessoais na criação de valor;
- Analisar os requisitos da LGPD, visando fundamentar elementos para possível adaptação do MFV à Segurança da Informação;
- Identificar critérios e métricas de vulnerabilidade para análise da cadeia de valor;
- Propor novas representações gráficas para MFV-SI, que traduzam o fluxo informacional e o tratamento dos dados pessoais.

1.3 Relevância e justificativa para a realização da pesquisa

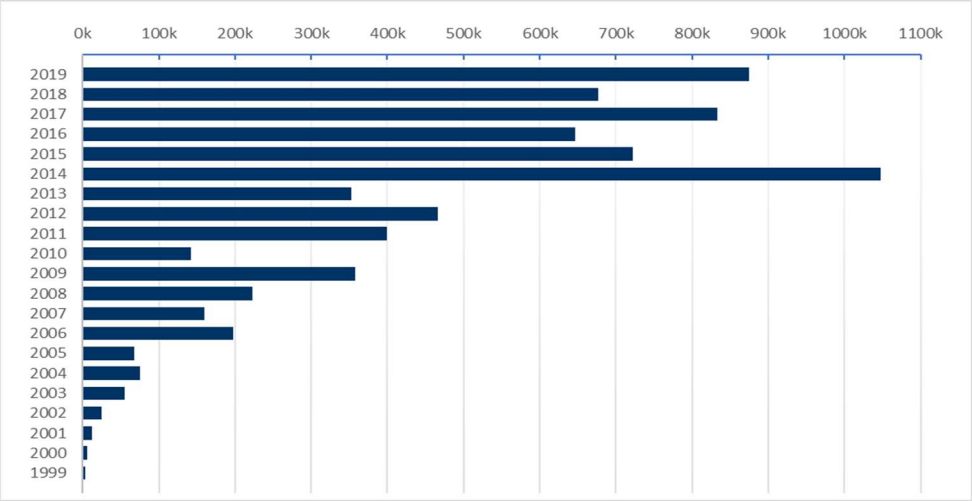
CEA (2018) analisa a dificuldade de obtenção e análise de dados de ataque cibernético devido, principalmente, ao fato das empresas temerem uma avaliação pejorativa ao relatar tais

informações. No entanto, a *Microsoft* avalia um aumento de US$ 325 milhões de 2015 para 2016 em ataques de *ransomware*.

Já a *Word Economic Forum* (2020), através do Relatório Global de Riscos, do Fórum Econômico Mundial de 2020, avalia que os ataques cibernéticos são um dos dez maiores riscos levantados para a próxima década, com impacto profundo em diversas esferas, como a econômica e a social.

No Brasil, não é diferente. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (2019), o CERT.br, aponta que quase 900 mil incidentes com segurança da informação foram reportados de forma voluntária por usuários da rede em 2019, conforme mostra a Figura 2:

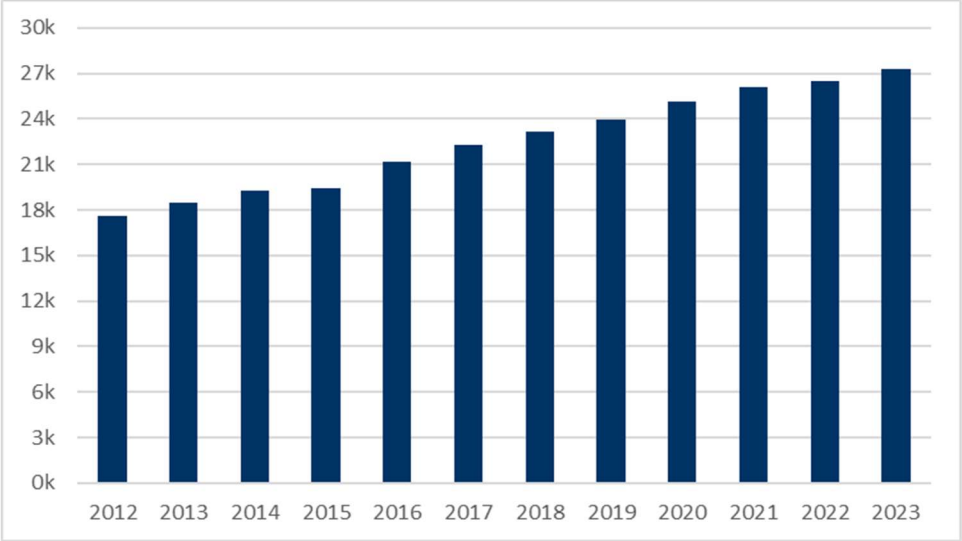
Figura 2 – Total de Incidentes de Segurança no Brasil por ano



Fonte: Adaptado de CERT.br (2019).

A Figura 3 mostra que, de acordo com PreciseSecurity.com (ILIC, 2020), a receita geral de software de segurança cibernética deverá atingir US $ 25,1 bilhões em 2020, crescendo 4,8% ano a ano. A tendência ascendente deve continuar nos anos seguintes, com todo o mercado atingindo US $ 27 bilhões em 2023 (ILIC, 2020).

Figura 3 – Receita global do mercado de software de segurança



Fonte: Adaptado de ILIC (2020).

A relevância desta pesquisa aumenta ainda mais quando identificamos as chamadas especiais em jornais, como *Journal of Information Security and Applications*. Os pedidos por estudos apresentam tópicos de interesse, como análise inteligente de dados para segurança, análise inteligente de dados para privacidade, aprendizado estatístico para segurança e privacidade, publicação de dados que preserva a privacidade entre outros.

Diante de todos esses impactos relacionados à economia, sigilo de dados, bem como às chamadas especiais apresentadas por importantes bases de dados acadêmicas, o tema em questão torna-se relevante no estudo associado a um modelo de gestão de processos e informações, como o caso do MFV-SI.

Tão importante quanto o tema, o uso especifico da ferramenta MFV-SI contribuirá para o entendimento e resolução das vulnerabilidades relacionadas aos dados de clientes e colaboradores, através do mapeamento dos processos de manipulação de dados, a projeção de um processo futuro ajustado e uma estruturação de um plano de ação para a implementação do modelo.

Com o objetivo de fundamentar a proposta deste trabalho, o próximo capítulo apresentará uma revisão conceitual dos quatro contextos trabalhados, sendo: a segurança da informação e as tecnologias disruptivas, a segurança da informação no Brasil, a gestão da cadeia de valor e seus aspectos sociais e, por fim, um panorama dos estudos relacionados ao mapa de fluxo de valor.

2 REFERENCIAL TEÓRICO

Este capítulo abordará os assuntos da contextualização deste trabalho, tendo em vista os trabalhos acadêmicos publicados.

2.1 A segurança da informação e as tecnologias disruptivas

Tratando de Segurança da Informação (SI), um conceito básico e amplamente utilizado para sua definição é o voltado aos riscos envolvidos quanto a sua integridade, disponibilidade e confiabilidade (BEAL, 2005).

Fontes (2006) avalia que a garantia da confidencialidade está relacionada a autorização de pessoas dentro da organização, para que tenham acesso à informação. Já a integridade visa garantir que a informação não tenha sido alterada em nenhum estágio do processo, seja de forma proposital ou não. Por fim, o viés da disponibilidade está relacionado com a garantia de que a informação estará acessível e íntegra no momento necessário para as pessoas corretas.

Para Rhodes e Ousley (2013), a segurança da informação tem como objetivo a proteção da informação em todas as suas formas, seja ela escrita, falada, eletrônica, gráfica ou usando outras formas de comunicação.

Para Moura (2007), o Sistema de Gestão da Segurança da Informação (SGSI) também contribui para a seleção de controles adequados. O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionais, a fim de proteger os ativos de informação e proporcionar confiança das partes interessadas.

O processo de seleção dos controles envolvidos na SI passa pela literatura da gestão de riscos. A norma ABNT NBR ISO/IEC 27001 (2013) determina que a organização deve estabelecer e aplicar um procedimento de gestão de risco de segurança da informação e que é necessário estabelecer critérios para tanto. De acordo com a ABNT NBR ISO/IEC 27005 (2013), risco de segurança da informação é uma métrica calculada em função da probabilidade de ocorrência de um incidente da severidade ou gravidade de suas consequências e do nível de detecção implementado.

Tais medidas de SI vêm tomando destaque no contexto dos atuais modelos de negócio, em que a utilização da informação tem sido influenciada pelas evoluções das práticas produtivas, novos modelos de comercialização e consumo de bens, cooperação e competição, fomentando cada vez mais novas competências e novas tecnologias (LASTRI; ALBAGLI, 1999). Nesse sentido, cada vez mais a transformação digital vem influenciando profundamente pessoas, negócios e sistemas (HUARNG et al., 2015).

Essa revolução está mudando a maneira como as empresas administram negócios, desenvolvem relacionamentos, dentro e entre ecossistemas (por exemplo, com consumidores, fornecedores), apresentando novas oportunidades e desafios gerenciais (VERMA et al., 2012; BRESCIANI et al., 2018; SCUOTTO et al., 2017). É evidente como empresas inovadoras, como *Uber, Airbnb e Spotify*, revolucionaram indústrias, como a de transportes, acomodações e músicas, por meio de modelos de negócios inovadores, através da transformação digital.

A literatura atual enfatiza diversas ferramentas tecnológicas que estão revolucionando a maneira de se fazer negócios, como *Big Data*, Inteligência Artificial, integração homem-máquina, máquina-máquina, impressoras 3D, *Internet of Things (IoT)*, drones, robótica avançada, entre outras.

Em 2014, a *Amazon* registrou uma patente chamada "envio antecipado", cuja ideia principal é usar ferramentas analíticas preditivas para analisar o histórico de compras de um cliente, juntamente com o histórico de compras de outros clientes. Seu objetivo principal é prever a necessidade de compra de seus clientes. Em teoria, um transporte antecipado (possivelmente por drones), permitiria à *Amazon* enviar produtos para seus consumidores até mesmo "antes" que eles façam o pedido (KOPALLE, 2014).

Por outro lado, algoritmos, ao tentar automatizar e facilitar o comércio de dados pessoais com termos de uso ou termos de privacidade propositalmente complexos e extensos, conduzem o usuário à desinformação, tendenciando o aceite dos termos sem a devida avaliação dos seus impactos. Não obstante, extensas e obscuras cláusulas de uso irrestrito dos dados pessoais, que intencionalmente manipulados por algoritmos captam e armazenam aceites do usuário, justificando "livre e espontânea vontade" do mesmo (TANNER, 2013).

Neste caminho, ao passo em que a transformação digital contribui para a melhoria de processos, pessoas e produtos, também corrobora com novos cenários ainda sem respostas. Dasgupta et al. (2020) afirmam que à medida que as organizações evoluem para um modelo de negócio orientado para integração de dados, geram-se novos desafios na complexidade da coleta, no armazenamento e processamento de dados e em particular na segurança e privacidade dos dados. Ele continua deixando evidente a importância de uma análise preditiva aos negócios e explica que, em contraste com os inúmeros trabalhos que apontam os benefícios do uso de *IoT* e da Inteligência Artificial (IA) nas cadeias de suprimentos, existem poucas pesquisas notáveis relacionadas à cadeia de suprimentos, compatíveis aos requisitos legais vigentes.

Uma das últimas novidades relacionadas às regulamentações foi o advento da Lei Geral de Proteção de Dados Pessoais do Brasil (LGPD) em 2018. Com sua aplicação, novos parâmetros de gerenciamento da informação deverão estar presentes na cadeia de valor, como,

por exemplo, a disponibilidade, integridade e confidencialidade dos dados, o propósito da utilização do(s) dado(s) coletado(s) do(s) cliente(s), além do conhecimento e consentimento para o uso dos dados pessoais.

2.2 A segurança da informação no brasil

O surgimento da pandemia, provocada pelo vírus COVID-19, foi um exemplo de relação entre a tecnologia, os processos de negócios e as relações sociais. Entre outras medidas de mitigação da pandemia, a Organização Mundial da Saúde (OMS) recomendou o distanciamento social, desencadeando uma cadeia de mudanças econômicas e sociocomportamentais. Moor (2005) destaca que o surgimento de novos modelos de relacionamentos sociais, que por sua vez levam em conta a utilização maciça de dados pessoais, culmina em inéditas questões éticas legais.

Ao tratar de proteção de dados pessoais, sigilo e transparência no Brasil, a Constituição Federal (CF), de 1988, estabelece em seu Art. 5º os direitos fundamentais sobre privacidade e sobre proteção de dados. No entanto, as diretrizes da CF, no âmbito da privacidade dos dados pessoais, têm tido diversas interpretações por não ser especificamente provida para este fim (BRASIL, 1988). Em 2014, foi lançada a Lei nº 12.965, Marco Civil da Internet (BRASIL, 2014), que estabelece princípios, garantias, direitos e deveres para uso da Internet no Brasil. Apesar do Art. 3º, II e III, prever a proteção à privacidade e aos dados pessoais, tais elementos não contemplam questionamentos específicos.

A Lei 13.709, sancionada em 2018, também conhecida como LGPD, envolve-se com questões contemporâneas dos problemas associados às questões digitais e não digitais, que remetem aos impactos sociais, como o direito à explicação, o direito à autodeterminação informativa, o direito ao esquecimento, o direito à fiscalização e o direito à intimidade (MONTEIRO, 2018; NETO et al., 2017; RAMINELLI & RODEGHERI, 2016).

Além das questões sociais exigidas, a pressão internacional foi mais uma motivação para a adoção da LGPD no Brasil. A *General Data Protection Regulation* (GDPR), da União Europeia (UE), restringe o armazenamento de dados pessoais dos cidadãos da UE apenas às organizações de países com um nível maior ou de igual rigor para proteção de dados em sua legislação. Ainda que, de forma indireta, a lei também propicia o desenvolvimento econômico (DASGUPTA; GILL; HUSSAIN, 2020).

Com a vigência da LGPD europeia em maio de 2018, a GDPR, todos os países que quiserem manter ou iniciar transações comerciais com a Europa serão obrigados a seguirem

procedimentos de segurança da informação equivalentes aos exigidos pela lei europeia. De acordo com o *Official Journal of the European Union* (UNIÃO EUROPEIA, 2016), a Comissão Europeia tem o poder de determinar, com base no artigo 45.º do regulamento 2016/679, se um país fora da UE oferece um nível adequado de proteção. Em 2020, a Comissão Europeia reconheceu Andorra, Argentina, Canadá, Ilhas Faroe, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, Suíça, Uruguai e Estados Unidos como adequados ao fornecimento de proteção de dados.

Para Monteiro (2018), a LGPD propõe colocar as empresas brasileiras em patamar similar ao das empresas adequadas à GDPR, dando-lhes a oportunidade de competição internacional, pois expande seu escopo da proteção de dados quando comparada à norma europeia.

2.3 A gestão da cadeia de valor e seus aspectos sociais

As organizações preocupadas em prosperar no contexto contemporâneo devem estar estrategicamente gerenciadas não somente com foco no sucesso econômico, mas também na sua contribuição para com a longevidade do planeta e das pessoas (BARBOSA-PÓVOA et al., 2018).

A expressão *Triple Botton Line* (TBL) fornece uma estrutura para medir o desempenho do negócio, usando os aspectos econômicos, sociais e ambientais (OZGUR, 2017). Rogers e Hudson (2011) avaliam que este termo, TBL, tem sido cunhado pelas corporações como uma estrutura prática da sustentabilidade. Ao definir uma estratégia sustentável para sua cadeia de valor, as organizações precisam considerar as três dimensões da sustentabilidade em seus objetivos, sendo eles: A) maximizar o lucro ao longo da cadeia de suprimentos; B) reduzir ou eliminar impactos ambientais provenientes de sua operação; e C) melhorar as condições de relacionamento, saúde e segurança das partes interessadas e da sociedade (HEDIGER, 2010; CHAABANE et al., 2012).

Tratando de TBL, é possível afirmar que há uma predominância de estudos com foco no desempenho econômico (49%), seguido pelo desempenho ambiental (35%) e poucos estudos com ênfase em resultados sociais (14%), evidenciando uma lacuna para estudos que analisem especificamente o último viés (FERREIRA, 2014; FERREIRA, JABBOUR, JABBOUR, 2015; FERREIRA, JABBOUR, 2019).

Para fomentar essa questão importante e pouco estudada da área do TBL, a Comissão Europeia promove a *Corporate Responsabilidade Social (CRS)*, que visa criar condições

favoráveis ao crescimento empresarial de forma responsável e sustentável, promovendo uma sinergia de conscientização e esclarecimento sobre os impactos sociais (COMISSÃO EUROPEIA, 2011).

Bubicz et al. (2019) sintetizam diversas dimensões sociais incorporadas no gerenciamento da cadeia de suprimentos. Seu trabalho aponta um crescente interesse acadêmico e da comunidade industrial sobre o tema, reconhecendo a necessidade de uma visão holística da cadeia de valor também para a sustentabilidade do aspecto social. Dentre as dimensões sociais apresentadas, a condição de trabalho está como um dos principais parâmetros medidos. Outra dimensão social apresentada é a de avaliação dos riscos, que, diferentemente das avaliações de riscos tradicionais, deve incluir sob sua análise a capacidade de gerenciar riscos ambientais e sociais, além dos riscos econômicos.

Outro aspecto importante enfrentado pelas empresas são os problemas relacionados à imagem pública, devido a impactos negativos sobre exploração de comunidades e os direitos humanos. Lee (2010) analisou a forma com que empresas, como *Nike, Hewlett & Packard, Starbucks, Toyota, Walmart*, avaliam aspectos sociais, concluindo que as medidas de impacto social negligenciam as considerações da sociedade e dos direitos humanos.

Nesse novo contexto, que abrange comportamentos disruptivos e demandas por produtos e serviços sustentáveis, que cumpram normas e regulamentos governamentais, as organizações estão sendo forçadas a repensar suas estratégias, objetivos e metodologias de gerenciamento de operações e processos (MILLER; PAWLOSKI; STANDRIDGE, 2010; PIERCY; RICH, 2015).

É cada vez mais claro que os modelos de gestão, somados à emergência tecnológica, desafiam as organizações a desenvolverem novas habilidades para lidar com o crescimento do fluxo de informações (BHARADWAJ, EL SAWY, PAVLOU, VENKATRAMAN, 2013).

Hicks (2007) definiu gerenciamento da informação (GI) como sendo a organização, representação e comunicação das informações, agregando valor a elas a medida que flui até o usuário final. Para aumentar a eficiência do GI, o desperdício (ações que não agregam valor) deve ser minimizado. Dessa forma, o gerenciamento enxuto de informações, deve reunir e processar apenas informações agregadoras, garantindo que os usuários possam entender e acessar o valor fornecido pelas informações. Por fim, o processo deve ser orientado pela demanda o mais simples e rápido possível, minimizando tarefas desnecessárias (HICKS, 2007).

Dessa forma, propor um modelo de mapeamento do fluxo de informação, focado na segurança da informação, utilizando uma já experimentada ferramenta de gestão *Lean*, pode contribuir com a evolução das métricas de avaliação do pilar social da sustentabilidade, indo

além dos parâmetros físico e psíquico, incorporando índices de avaliação da intimidade, honra e reputação por meio da segurança de seus dados pessoais.

Esse contexto potencializa o surgimento de um novo tipo de desperdício em processos de gerenciamento de informação: o desperdício da vulnerabilidade dos dados. No capítulo quatro deste trabalho, será apresentado uma análise sobre a questão, trazendo uma avaliação entre os aspectos sociais e as exigências legais envolvidas no tratamento de dados pessoais e a relação de agregação de valor para as organizações e seus desperdícios consequentes.

O objetivo da próxima seção é rever os estudos existentes sobre ferramentas de modelagem de fluxo de informações orientada por função, para posterior análise comparativa com suas respectivas potencialidades e fraquezas. Por fim, será apresentada uma avaliação dessas ferramentas, comparando-as com as exigências da LGPD e as funcionalidades do MFV.

2.4 A gestão da informação

A literatura sobre gestão da informação (GI), em linhas gerais, converge entre seus elementos e modelos. Modelos podem ser considerados representações simplificadas da realidade. Martins e Theóphilo (2009) classificam modelos como elementos que representam fenômenos e interações complexas de forma visual e de fácil entendimento, especificando e explicando de forma lógica suas propriedades e características.

Os modelos de GI, em resumo, são definidos sob a abordagem de processo, abordagem essa que pode ser definida como qualquer atividade que recebe um *input* e, ao adicionar valor, transforma-o em um *output* específico a um cliente (HARRINGTON, 1993).

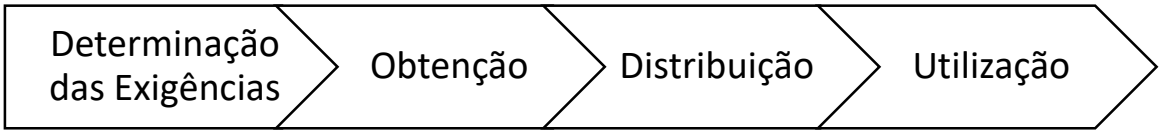
Starck (2011) compara e sintetiza três modelos de GI amplamente estudados e propõe um modelo genérico, simplificado e convergente. O primeiro modelo utilizado em seu estudo é o de McGee e Prusak, descrito, em 1994, no livro Gestão Estratégica da Informação, o segundo, em 1998, escrito por Davenport e Prusak no livro Ecologia da Informação e o terceiro modelo, o de Choo, descrito no livro Gestão da Informação para a Organização Inteligente no ano de 2003. Sua proposta classifica três macroprocessos: aquisição da informação, o tratamento informacional e uso e distribuição das informações. A autora ainda confirma as visões de Choo (2003) e Davenport (1998), de que há uma tendência de transformação de dados em produtos informacionais e que esse direcionamento deve ser associado a uma visão sistêmica e holística de gerenciamento do processo informacional.

> A gestão da informação deve ser vista como uma rede de elementos fortemente inter-relacionados que constituem um todo complexo, onde a saída de um subsistema é a entrada de outro, e, portanto, qualquer modificação no processamento de um

> subsistema afetará os outros imediatamente. É também fortemente influenciado pelo seu ambiente, formado por outros sistemas que se organizam em sistemas cada vez maiores (STARCK, 2011, p. 83).

Davenport e Prusak (1998) entendem que existem diversos elementos envolvidos no processo de gestão da informação e a cooperação entre eles é um elemento fundamental para que a utilização da informação gere resultados positivos, mesmo que, por vezes, essa cooperação aconteça. Os autores classificam o processo de gerenciamento da informação em quatro etapas e o chama de processo genérico de gerenciamento da informação como apresentado na Figura 4.

Figura 4 - Modelo Davenport para fluxo de informação



Fonte: Davenport e Prusak (1998).

Na primeira etapa, ocorre a determinação das exigências, em que os envolvidos definem o porquê e o para que as informações precisam ser coletadas. Essa etapa está diretamente relacionada ao problema que se quer resolver, pois, para que um modelo de processo de gerenciamento informacional venha a ter algum valor real, é necessário refletir a turbulência, a volatilidade e a complexidade dos mercados, dos locais de trabalho e da mente humana (DAVENPORT; PRUSAK, 1998).

A etapa de obtenção de informações, depende da estruturação da etapa anterior e de um processo contínuo de levantamento de dados. Davenport e Prusak (1998) classificam três subetapas do processo de obtenção de informação: exploração do ambiente informacional; classificação da informação em uma estrutura pertinente; formatação e estruturação das informações (DAVENPORT; PRUSAK, 1998).

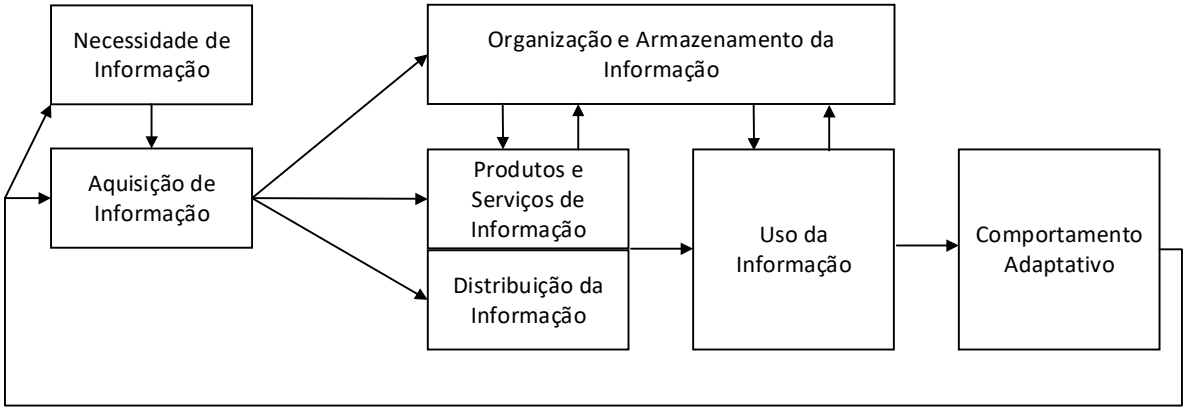
Seguindo, a etapa da distribuição está diretamente relacionada com a forma de formatação proveniente das etapas anteriores e a forma como ela será disponibilizada. Segundo o autor, a distribuição da informação deve ser abrangente o suficiente para que todas as pessoas que dela precisem, tomando cuidado com o processo de reciprocidade, uma vez que, nessa etapa, pode acontecer de que quem forneça a informação acabe recebendo informações.

Por fim, a última etapa desse modelo é o uso. Essa etapa refere-se à obtenção e utilização da informação pelo usuário. Como o indivíduo irá absorver essa informação e como ela será utilizada está atrelado a um conjunto de variáveis. O uso pode ser classificado como um

processo cognitivo e que depende da forma com que o indivíduo irá absorver tal informação, pois a informação disponibilizada irá ser processada junto à base de conhecimento do indivíduo e utilizada conforme suas necessidades pessoais (DAVENPORT; PRUSAK, 1998).

Por sua vez, Choo (2003) propõe um modelo baseado em seis processos, conforme representado na Figura 5. Todos os processos estão vinculados à necessidade, à busca e ao uso da informação organizacional. Para o autor, esse conjunto de processos devem ser correlatos e funcionar como um ciclo contínuo.

Figura 5 - Modelo Choo para fluxo de informação



Fonte: Choo (2003).

Segundo Choo (2003), o primeiro processo desse modelo é a identificação das necessidades de informação. A necessidade de informação emerge de problemas ou dúvidas. Nesse sentido, o autor sugere algumas perguntas de forma que a busca pela informação contribua para elaborar um significado, construir conhecimento e contribuir com a tomada de decisão.

No segundo processo, o de aquisição da informação, o autor avalia a necessidade de equilíbrio entre duas vertentes opostas, a necessidade de informação e a capacidade cognitiva do ser humano, considerado um processo crítico, pois todo o fluxo é percorrido por ela (CHOO, 2003).

Seu terceiro processo é responsável pela organização e armazenamento das informações adquiridas pelo processo anterior. O processo de organização e armazenamento da informação pode ser realizado de diferentes formas, como bancos de dados computacionais e arquivos físicos, por exemplo. Esta etapa tem como simples objetivo o compartilhamento e a posterior recuperação das informações, no entanto, a forma como as informações são armazenadas reflete diretamente como a organização atribui issolor a essa informação. As informações armazenadas geram uma espécie de conhecimento organizacional, ao passo que a falta de administração

adequada desse conhecimento organizacional pode resultar na perda de conhecimentos antes adquiridos (CHOO, 2003).

Vale ressaltar, como antes mencionado, que, para Pardolesi (2003), à medida que os sistemas de armazenamento e a capacidade de processamento de dados aumentam, o custo de manutenção do sigilo de informações pessoais também cresce.

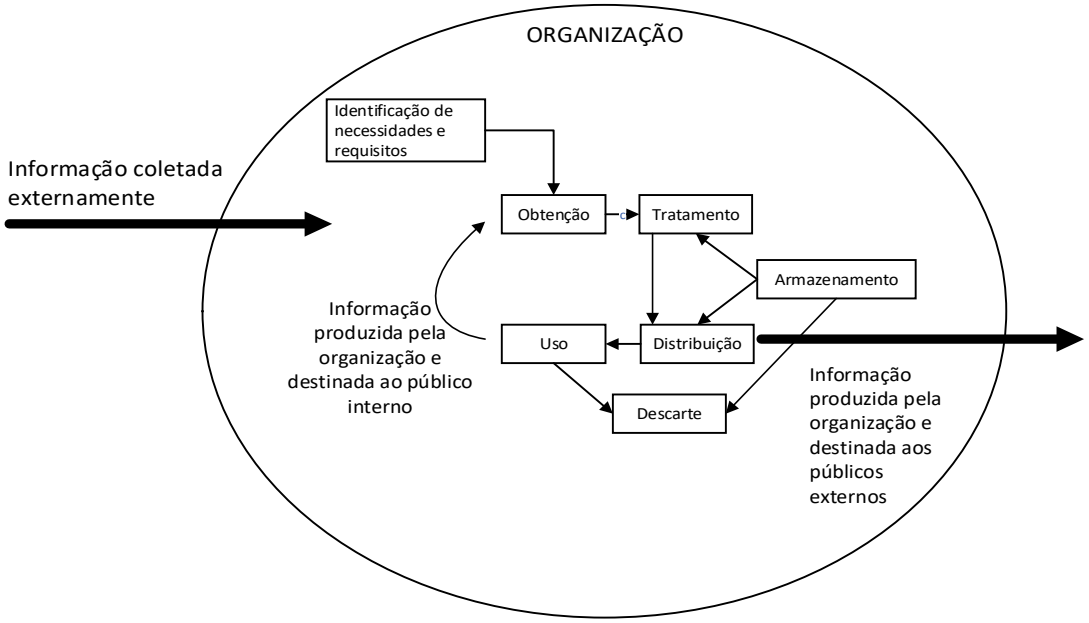
A etapa subsequente, a quarta etapa, a de definição dos produtos e serviços de informação, traduz o processo responsável por garantir que as necessidades informacionais dos usuários sejam atendidas. A agregação de valor aos produtos e serviços de informação objetiva aproximar a informação das necessidades dos usuários. Seis qualidades são atribuídas como importantes para a melhoria dos produtos e serviços de informação: a redução dos problemas, a usabilidade, qualidade, adaptabilidade, redução tempo e economia de custo (CHOO, 2003).

Seguindo, o quinto processo é o de distribuição da informação. Seu objetivo é fluir as informações presentes no fluxo. Essa distribuição deve englobar todos os que precisam de informação e gerar novas informações. Segundo Choo (2003), esse processo promove e é responsável pela criação de significado e construção de conhecimento para a tomada de decisões.

O último processo é o de uso da informação. Esse processo é definido pelo autor como um processo dinâmico de pesquisa e construção, que resulta na criação de conhecimento. Durante a construção do conhecimento, acontece o processo de transformação da informação organizacional em conhecimento tácito, explícito e cultural (CHOO, 2003).

O modelo proposto por Beal (2009) destaca-se por apresentar um elemento não citado pelos modelos anteriores: o processo de descarte da informação. Dentre os modelos apresentados, esse é o que possui mais etapas, sendo um total de sete: a identificação de necessidades e requisitos; obtenção; tratamento; armazenamento; distribuição; uso; e o descarte, como representado na Figura 6.

Figura 6 - Modelo Beal para fluxo de informação



Fonte: Beal (2009).

A primeira etapa do modelo proposto por Beal é a identificação de necessidades e requisitos, etapa esta responsável por definir quais os requisitos informacionais devem ser atendidos. O autor entende que a partir do conhecimento da finalidade da informação adquirida, torna-se mais fácil o atendimento às necessidades do solicitante. Na etapa dois, "[...] são desenvolvidas as atividades de criação, recepção ou captura da informação, provenientes de fonte externa ou interna, em qualquer mídia ou formato" (BEAL, 2009, p. 30).

Segundo Beal (2009), a chamada de etapa de obtenção tem como objetivo atender as demandas identificadas na primeira. A etapa seguinte do modelo é a de tratamento das informações coletadas. O valor do dado coletado só será percebido pelo usuário uma vez que esse dado passe pelos processos "[...] de organização, formatação, estruturação, classificação, análise, síntese e apresentação, com o propósito de torná-la mais acessível e fácil de localizar pelos usuários" (p. 30).

Beal (2009), diz que a quarta etapa, a distribuição da informação, agora tratada, depende da infraestrutura adotada para a fluxo de escoamento da informação. Apenas a disponibilização de informações não é suficiente para que as necessidades de comunicação sejam atendidas.

A quinta etapa, a de uso da informação, é considerada a mais importante do fluxo de informação, "[...] o uso da informação possibilita a combinação de informações e o surgimento de novos conhecimentos, que podem voltar a alimentar o ciclo da informação corporativo, num processo contínuo de aprendizado e crescimento" (BEAL, 2009, p. 31).

Na etapa de armazenamento, o autor explica que essa etapa é a responsável por manter as informações íntegras, além de disponibilizá-las para que se execute a fase de distribuição. Levando-se em consideração que o avanço tecnológico em armazenamento das informações é reconhecido por praticamente não ter limites de espaço e tempo de uso das informações (BEAL, 2009).

Por fim, a autora define o descarte. Essa etapa, tem como característica a exclusão de informações inúteis para as pessoas envolvidas. A decisão de descarte ou não vai depender da política adotada para gestão do fluxo de informação. A autora ainda destaca que o descarte otimiza a gestão da informação, "[...] economizando recursos de armazenamento, aumentando a rapidez e eficiência na localização da informação necessária, melhorando a visibilidade dos recursos informacionais importantes etc." (BEAL, 2009, p. 32).

2.5 A informação como ativo empresarial

As definições adotadas pelos autores na seção anterior convergem para uma espécie de norte consensual na definição do conceito de gestão da informação, podendo ser explicada como um conjunto de atividades interligadas, que relatam o modo de obtenção de dados, bem como os mecanismos de utilização, armazenamento e distribuição da informação, interna ou externamente, com o objetivo principal de apoiar a tomada de decisões estratégicas e obtenção de vantagem competitiva. Sendo assim, mapear o fluxo da informação pode e deve ser considerado como uma estratégia competitiva.

Nos modelos de negócios, em que a informação tem papel principal, o fluxo de valor consiste no próprio fluxo de informações. Portanto, ao focar em melhorias isoladas, o gestor dos processos informacionais pode não alcançar uma transformação estrutural sistêmica, tão pouco estratégica. Ficar restrito a uma parte do todo pode ser também uma fonte de desperdício, uma vez que as grandes oportunidades de ganho estão nas interfaces dos processos, ou seja, nos *inputs* e *outputs* ao longo da cadeia de valor (AHLSTROM, 2004).

A ABNT NBR ISO/IEC 27002 (2013) também considera dados e informações como ativos empresarial, que devem ser gerenciados de forma segura e eficiente. Segundo a norma:

> "Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requer proteção contra vários riscos". (ABNT NBR ISO/IEC 27002, 2013).

Nessa vertente, surge um novo termo, cunhado de *Lean Information Management*

(LIM). Esse termo, oriundo dos conceitos fundamentais do *Lean Thinking,* resume uma abordagem de melhoria de sistemas organizacionais, focado na redução do desperdício e elevação do valor em processos de negócios informacionais, por meio da adoção de práticas de gerenciamento do valor da informação (SOARES; TEIXEIRA, 2014).

Hölttä et al. (2010) se apoiam nos conceitos do *Lean* e classifica os desperdícios relacionados à gestão da informação, associando os sete tradicionais desperdícios do pensamento *Lean* a exemplos de desperdícios na gestão da informação, como mostrado no Quadro 1.

Quadro 1 – Categorização dos Desperdícios em LIM

CATEGORIA DE DESPERDÍCIO	EXEMPLO
Transporte	Informação não disponível no local em que é utilizada. Distância entre o local que a informação é processada do local que é gerada. Distribuição excessiva de informação.
Estoque	Excesso de informações. Informação perdida em fila. Documentação excessiva, detalhamento desnecessário.
Movimento	Intervenção manual devido à falta de integração entre sistemas. Informações transferidas para o destino incorreto.
Espera	Aguardar por informações. Informações paradas (aguardando intervenção).
Processos	Atraso em alterações de informações. Informação imprecisa, ações corretivas necessárias. Aumento de recursos para processar ações corretivas.
Defeito	Informações com erros. Formatos de informação (falta de normas comuns / compatíveis). Sistemas de informação (problemas na conversão de informações).
Superprodução	Número excessivo de sistemas. Múltiplas fontes de dados (vários sistemas com a mesma informação).

Fonte: Hölttä et al. (2010); Iuga, Kifor e Rosca (2014). Adaptado pelo autor.

Dessa forma, é possível encontrar elementos convergentes entre as etapas dos modelos de gestão da informação, os novos requisitos da LGPD diretamente relacionados às novas configurações socioeconômicas, fomentada pela evolução tecnológica, com os tradicionais desperdícios do pensamento *Lean*, como mostra o Quadro 2 abaixo.

Quadro 2 – Relações entre GI, requisitos da LGPD e desperdícios no LIM

ETAPAS DA GI	MODELOS DE GESTÃO DA INFORMAÇÃO	REQUISITOS DA LGPD	DESPERDÍCIOS NO LIM Hölttä et al. (2010)
AQUISIÇÃO	**Devenport e Prusak (1998):** Determinação das exigências da informação. **Choo (2003):** Necessidade de informação e aquisição de informação. **Beal (2009):**	A- Exigência de consentimento do titular. B- Por obrigações legais/administração pública/Exercício regular do Direito.	A- Aguardar por informações. B- Aquisição de dados além do propósito do fluxo de valor para o cliente. C- Informações paradas.

	Identificação de necessidades e requisitos.	C- Proteção da vida/tutela da saúde/proteção ao crédito.	
TRATAMENTO	**NcGee e Prusak (1994):** Coleta, classificação e armazenamento / desenvolvimento de produtos e serviços informacionais / tratamento e apresentação. **Devenport (1998)** Obtenção de Informações. **Choo (2003)** Organização e Armazenamento da informação / Produtos e serviços da informação.	A- Direito ao acesso pelo titular. B- Finalidades específicas para uso do dado de acordo com o consentimento. C- Elaboração de relatório para autoridade nacional. D- Dados com disponibilidade, integridade e confidencialidade.	A- Informação não disponível no local aonde é utilizada. B- Distância entre o local que a informação é processada do local que é gerada. C- Informação perdida em fila D- Documentação excessiva, detalhamento desnecessário. Informações transferidas para o destino incorreto. Atraso em alterações de informações. Informação imprecisa, ações corretivas necessárias. Aumento de recursos para processar ações corretivas. Informações incompletas/incorretas.
DISTRIBUIÇÃO	**NcGee e Prusak (1994):** Distribuição e disseminação de informação / Análise e uso da informação. **Devenport (1998)** Distribuição e utilização da informação. **Choo (2003)** Distribuição e utilização da informação/comportamento adaptativo.	A- Consentimento do titular. B- Acesso aos dados e seus tratamentos pelo titular. C- Proteção e eliminação dos dados pessoais quando solicitado.	A- Distribuição excessiva de informação. B- Espera Formatos de informação (falta de normas comuns/compatíveis) Sistemas de informação (problemas na conversão de informações) C- Número excessivo de sistemas Múltiplas fontes de dados (vários sistemas com a mesma informação)

Fonte: Elaborado pelo autor.

Ao associar as etapas elementares dos três modelos de gestão da informação com as classificações dos desperdícios do LIM e os requisitos da LGPD, é possível avaliar a convergência entre a nova regulamentação e o trato do dado pessoal como um ativo empresarial. No processo de aquisição da informação, por exemplo, a lei destaca a necessidade do consentimento do titular dos dados para um fim específico e, claro, do seu uso. Caso contrário, com a vigência da lei, as empresas que adquirirem dados além do propósito do seu negócio estarão gerando um novo desperdício.

O conceito de desperdício, na abordagem LIM, pode ser entendido como toda atividades de não agregação de valor, ou atividades essas que os clientes não teriam a intenção de pagar por elas (DUMRAK, 2015; LIKER, 2004; MOSTAFA; WOMACK; JONES; DANIEL, 1996).

Seguindo as etapas da GI, é possível associar algumas ações que poderão proporcionar algum tipo de vulnerabilidade. No processo de aquisição de dados, captar dados, além do propósito estabelecido para a atividade fim do fluxo de valor, gerará maiores volumes de tratamento, movimentações, aumentará o nível de risco de exposição social do indivíduo, além de colocar a empresa em situação de não conformidade com a lei.

No processo de tratamento e distribuição de dados, por exemplo, quanto maiores são as cadeias de valor e maior é o trafego percorrido pelos dados, maiores são as exposições a ataques e a situações negligenciais, ou não intencionais a que o dado estará sujeito. Dessa forma, pode ser estabelecido que processos de tratamento de informação, operantes sob tutela da LGPD ou de leis mundialmente similares, passam a estar vinculados a um novo tipo de desperdício: a vulnerabilidade dos dados pessoais.

2.6 Ferramentas para mapeamento de processos

Ernest e Young (1997) definem o mapeamento de processos como um mecanismo de documentação da situação real de um conjunto de atividades, que permite descrever uma visão futura dos mesmos, possibilitando o desenvolvimento de melhoria para as atividades mapeadas.

Leal (2003) avalia que, diante de vasta possibilidade de escolha de ferramentas, em que cada uma apresenta diferentes enfoques e utilidades e variadas técnicas de mapeamento, a correta interpretação dessas técnicas fundamenta o processo de mapeamento, a análise dos resultados e a implementação das melhorias.

Durugbo (2013) analisa as principais abordagens de modelagem de fluxo organizacional, separando-as entre modelagem matemática e modelagem diagramática. Em suma, a modelagem matemática é aplicada nas análises de atributos de fluxo de informações, como ambiguidade, redundância, equívoco e incertezas. Já a modelagem diagramática produz modelos conceituais construídos de forma a representar visualmente procedimentos e transações, a fim de analisar os problemas de informação em uma organização e auxiliar na tomada de decisão.

Do ponto de vista das técnicas disponíveis para o mapeamento das informações, Kettinger (1997) revisou e apontou pelo menos 72 técnicas de mapeamento de processos de gestão, o que ele chama de *Business Process Redesign* (BPR). O autor divide as 72 ferramentas em 11 categorias: 1*) Businnes Planning; 2) Process Capture & Modeling; 3) Change Management; 4) Creative Thinking; 5) Customer Requirements Analysis; 6) IS Systems Analysis and Design; 7) Process Measurement; 8) Organizational Analysis; 9) Problem Solving & Diagnosis; 10) Project Management; 11) Process Prototyping & Simulation.*

Para fins de estudo, neste trabalho, foram selecionadas 11 ferramentas aplicadas na categoria *2) Process Capture & Modeling,* de Kettinger (1997). A escolha de tal categoria se justifica pelo fato de o presente estudo propor uma ferramenta de diagnóstico de processos de gestão da informação aderente aos requisitos da LGPD. Outras duas ferramentas foram

escolhidas para compor este estudo comparativo: o BPMN e o MFV. O elevado número de estudos de casos sobre mapeamento de processos encontrados em bases científicas nos últimos 10 anos, utilizando essas duas ferramentas, corrobora a inserção de ambas no estudo comparativo.

O Quadro 3 apresenta um resumo das características elementares das 13 ferramentas de mapeamento de processos escolhidas, como suas respectivas relações positivas e negativas, quando relacionadas a sete importantes necessidades impostas pela LGPD.

Quadro 3 – Ferramentas de modelagem de processos x requisitos da LGPD

FERRAMENTAS DO BPR (KETTINGER, 1997)	**DEFINIÇÃO (KETTINGER, 1997)**	**RELAÇÃO COM A LGPD**
Data Flow Diagramming	Graficamente retrata o fluxo de dados entre entidades externas, etapas de processamento interno e elementos de armazenamento de dados.	1- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas. 2- Contribui para manutenção de registro das operações de tratamento de dados pessoais. ~~3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos.~~ ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ 5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto. ~~6- Contribui para demonstração dos processos e sua evolução (antes x depois).~~ ~~7- Análise quantitativa de riscos.~~
IDEF 0, 3, 6	Uma metodologia de análise e design de sistemas estabelecida pela Força Aérea dos EUA como resultado de seu Computador Integrado e Fabricação (ICAM) programa IDEF0 é um módulo de modelagem de atividades para captura de requisitos funcionais (“identifique o que preciso fazer”). O IDEF3 incorpora a dimensão do tempo para capturar o comportamento dos objetos na empresa através de diagramas de transição estatal. O IDEF6 captura projetos "meta", ou seja, o conhecimento e o pensamento que foram para enquadrar os outros módulos DEF.	1- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas. 2- Contribui para manutenção de registro das operações de tratamento de dados pessoais. ~~3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos.~~ ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ ~~5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto.~~ 6- Contribui para demonstração dos processos e sua evolução (antes x depois). 7- Análise quantitativa de riscos.
Activity-Based Costing	Esta técnica determina como um processo e seus subprocessos consomem recursos identificando custo baseado em atividades.	~~1- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas.~~ ~~2- Contribui para manutenção de registro das operações de tratamento de dados pessoais.~~ ~~3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos.~~ ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ ~~5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto.~~ ~~6- Contribui para demonstração dos processos e sua evolução (antes x depois).~~

		~~7- Análise quantitativa de riscos.~~
Socio-Tech System Design	Enfatizando os princípios humanísticos de participação, aprendizagem e empoderamento, essa técnica vê uma organização composta por pessoas (o sistema social) utilizando ferramentas, técnicas e conhecimentos (o sistema técnico) para produzir bens ou serviços. Os dois sistemas devem ser efetivamente adequados um ao outro para alcançar o funcionamento ideal (PAVA, 1983). Uma técnica típica de design usando essa abordagem é o método DE ÉTICA de 9 passos desenvolvido por Mumford (1994).	1~~- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas.~~ ~~2- Contribui para manutenção de registro das operações de tratamento de dados pessoais.~~ ~~3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos.~~ ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ ~~5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto.~~ ~~6- Contribui para demonstração dos processos e sua evolução (antes x depois).~~ ~~7- Análise quantitativa de riscos~~.
Role Activity Diagramming	A técnica representa os conceitos de papel, ação, interação, evento, estado, caso, decisão e paralelismo em notações diagramáticas fáceis de entender.	1- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas. 2- Contribui para manutenção de registro das operações de tratamento de dados pessoais. ~~3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos.~~ ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ 5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto. 6- Contribui para demonstração dos processos e sua evolução (antes x depois). ~~7- Análise quantitativa de riscos.~~
Process Flowcharting	Símbolos e métodos típicos de mapeamento de fluxo são aplicados para retratar a lógica e o fluxo de atividades em um processo de negócios.	~~1- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas.~~ 2- Contribui para manutenção de registro das operações de tratamento de dados pessoais. ~~3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos.~~ ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ ~~5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto.~~ ~~6- Contribui para demonstração dos processos e sua evolução (antes x depois).~~ ~~7- Análise quantitativa de riscos.~~
Hierarchical Colored Petri Nets	Uma versão colorida dos modelos tradicionais de sistemas Petri-Net, bem adequado para retratar, simular e analisar grandes sistemas e processos.	1- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas. ~~2- Contribui para manutenção de registro das operações de tratamento de dados pessoais.~~ ~~3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos.~~ ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ ~~5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto.~~ ~~6- Contribui para demonstração dos processos e sua evolução (antes x depois).~~ ~~7- Análise quantitativa de riscos.~~
Soft Systems Method	Originalmente desenvolvida por Peter Checkland (1981) para estruturar problemas não estruturados e definir os requisitos	~~1- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas.~~ ~~2- Contribui para manutenção de registro das~~

	do usuário, a técnica requer um alto grau de participação na primeira pintura de um quadro detalhado ou "rico" de um problema do mundo real. Em seguida, utilizando o pensamento do sistema, a análise desengajada requer o desenvolvimento de modelos conceituais alternativos de processos "deveriam ser". Finalmente, a comparação e integração desses processos reais e imaginários são discutidos para descobrir um novo curso de ação.	~~operações de tratamento de dados pessoais.~~ ~~3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos.~~ ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ ~~5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto.~~ ~~6- Contribui para demonstração dos processos e sua evolução (antes x depois).~~ ~~7- Análise quantitativa de riscos.~~
Information Control Net	Uma ferramenta gráfica para analisar padrões de comunicação e estruturas de controle associadas aos procedimentos de escritório (COOK, 1981).	~~1- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas.~~ ~~2- Contribui para manutenção de registro das operações de tratamento de dados pessoais.~~ ~~3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos.~~ ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ ~~5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto.~~ ~~6- Contribui para demonstração dos processos e sua evolução (antes x depois).~~ ~~7- Análise quantitativa de riscos.~~
Speech Interaction Modeling	Técnica desenvolvida por T. Winograd e F. Flores (1986) para modelar o fluxo de trabalho organizacional utilizando a metáfora da fala-ação. Em vez de ver a coordenação como tarefas ou fluxos de informação entre tarefas, a coordenação é definida pela linguagem que age através da qual as pessoas coordenam. Para os processos de negócios, os compromissos de implementação são a base para a comunicação nas relações cliente-fornecedor. Exemplos de atos de fala incluem solicitação, oferta, acordo, retirada, contraoferta, conclusão do relatório, etc.	~~1- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas.~~ ~~2- Contribui para manutenção de registro das operações de tratamento de dados pessoais.~~ ~~3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos.~~ ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ ~~5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto.~~ ~~6- Contribui para demonstração dos processos e sua evolução (antes x depois).~~ ~~7- Análise quantitativa de riscos.~~
Workflow Design	A noção de fluxo de trabalho está enraizada na ideia de que os processos de negócios são conjuntos de tarefas feitas em ordem prescrita que incorporam informações de várias fontes. Existem três tipos de fluxos de trabalho: baseado em casos, gerais e ad hoc. O objetivo do projeto do fluxo de trabalho é explicitar as relações entre pessoas, procedimentos, informações, tarefas e gerenciamento.	~~1- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas.~~ 2- Contribui para manutenção de registro das operações de tratamento de dados pessoais. ~~3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos.~~ ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ ~~5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto.~~ ~~6- Contribui para demonstração dos processos e sua evolução (antes x depois).~~ ~~7- Análise quantitativa de riscos.~~
MFV	Uma ferramenta de mapeamento de processos utilizada para mostrar os desperdícios presentes no processo através de métricas (ROTHER; SHOOK, 2003).	1- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas. 2- Contribui para manutenção de registro das operações de tratamento de dados pessoais.

		3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos. ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ 5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto. 6- Contribui para demonstração dos processos e sua evolução (antes x depois). ~~7- Análise quantitativa de riscos.~~
BPMN	Segundo Arevalo et al. (2016) BPMN é uma linguagem, que descreve como o processo tem de ser executado exatamente, sendo um conjunto padrão de notações gráficas e fornece, essencialmente, notações para a modelagem de processos de negócios com ênfase no fluxo de controle.	1- Possibilita visão sistêmica do processo, fluxo de entrada e saída de informações e relação com as pessoas envolvidas. 2- Contribui para manutenção de registro das operações de tratamento de dados pessoais. ~~3- Caracteriza a finalidade da obtenção e tratamento dos dados para propósitos legítimos.~~ ~~4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades.~~ ~~5- Contribui para a descrição dos processos de tratamento de dados pessoais, exigido no relatório anual de impacto.~~ ~~6- Contribui para demonstração dos processos e sua evolução (antes x depois).~~ ~~7- Análise quantitativa de riscos.~~

Fonte: Elaborado pelo autor[1].

A análise comparativa do Quadro 3 evidencia que a ferramenta de mapeamento de processos de maior potencial de aderência aos princípios da LGPD, com a menor quantidade de adaptações necessárias a se desenvolver, é o MFV. Entre os sete elementos da LGPD analisados, apenas dois não são atendidos pelo MFV a princípio, são eles: 4- Garante limitação do tratamento ao mínimo necessário para a realização de suas finalidades, e 7- Análise quantitativa de riscos.

Dessa forma, o próximo capítulo será dedicado a uma análise mais detalhada das potencialidades da ferramenta MFV e sua versatilidade para adequação e aderência aos requisitos da LGPD.

2.7 Análise de aderência das ferramentas de mapeamento de processo aos requisitos da LGPD

Como resposta a um dos objetivos de pesquisa, esta subseção apresenta uma análise e justificativa para a escolha do MFV no emprego do mapeamento do fluxo de informação e análise da segurança da informação, baseado nos requisitos da LGPD.

Apoiado pelo entendimento de que os benefícios da filosofia *Lean* são amplamente difundidos na literatura e adaptados a diversos setores de mercado e propósitos de negócio,

[1] Os requisitos considerados como "não atende", foram destacados como "~~texto~~".

Soares e Teixeira (2014) explicam que o *Lean* pode beneficiar qualquer área em que os processos possam ser mapeados. Rother e Shook (2003) afirmam que, além de servir como base de um plano de implementação de melhoria e auxiliar na identificação dos desperdícios, o MFV é a única ferramenta que mostra a relação entre fluxo de informações e fluxo de materiais de forma integrada.

O modelo de gestão *Lean* é baseado na manutenção de atividades de agregação de valor, essas também classificadas como aquelas que os clientes estão dispostos a pagar, ao passo da redução ou eliminação das demais atividades, que seriam, então, as que os clientes não teriam a intenção de pagar por elas, classificadas como atividades de não agregação de valor ou desperdícios (DUMRAK, 2015; LIKER, 2004; MOSTAFA; WOMACK; JONES; DANIEL, 1996).

Nesse sentido, o uso do Mapa de Fluxo de Valor tem recebido atenção, pois trata-se de uma importante ferramenta na LM para identificar desperdício, podendo ser adaptada a manufatura verde ou sustentável, quando necessário (FAULKNER; BADURDEEN, 2014).

Rother e Shook (2003) publicam o livro *Aprendendo a Enxergar*, em que eles ensinam o funcionamento e a aplicação do MFV. Segundo os autores, essa ferramenta facilita a visualização dos fluxos de materiais e informações ao longo da cadeia de valor, abordando todas as ações necessárias para a transformação do produto, chamadas de ações que agregam e que não agregam valor.

> Considerar a perspectiva do fluxo de valor significa levar em conta o quadro mais amplo, não só os processos individuais; melhorar todo o caminho, desde as moléculas até o os braços do consumidor, você precisará seguir o fluxo de valor de um produto por várias empresas e até outras unidades produtivas. (ROTHER; SHOOK, 2003).

Apesar de sua facilidade de uso, o MFV é limitado à representação de um produto ou um fluxo de uma família de produtos, fornecendo uma imagem instantânea estática da cadeia de processo (ALVANDI et al., 2016). Tradicionalmente, a construção do MFV leva em consideração o desempenho dos aspectos econômicos de uma cadeia de valor, muitos dos quais traduzidos em tempo (tempo de ciclo, tempo de entrega, tempo de *setup* etc.) (FAULKNER; BADURDEEN, 2014; HELLENO; MORAES; SIMON, 2016). Faulkner e Badurdeen (2014) afirmam que a capacidade de capturar o desempenho ambiental e social visualmente através do MFV irá aumentar sua utilização como uma ferramenta utilizada para avaliação de processos sob a perspectiva da sustentabilidade.

Helleno, Moraes e Simon (2016) utilizaram o MFV na aplicação do viés social, considerando parâmetros do processo de produção diretamente relacionados com os

empregados e a comunidade onde a empresa está inserida. Absenteísmo, *turnover*, taxa de acidentes e nível de ruído são indicadores relacionados ao nível de satisfação dos empregados e às condições de trabalho. Os autores ainda agregaram aos indicadores de custos operacionais, valores salariais e benefícios financeiros concedidos. Já Faulkner e Badurdeen (2014) propõe um método de Mapeamento de Fluxo de Valor Sustentável, o Sus-VSM, com dois indicadores para o pilar social, sendo o primeiro índice de carga física e o segundo, riscos do ambiente de trabalho.

Jarebrant et al. (2016) propuseram o modelo ErgoVSM, que considerou a exposição física do trabalhador onde há um risco aumentado de desenvolvimento de doenças músculo-esqueléticas. As avaliações de ergonomia classificaram os fatores de risco para esse tipo de doença em quatro categorias principais: posturas, forças, variação física e trabalho intenso.

Analogamente, ao analisar a cadeia de valor do fluxo de um paciente em um pronto atendimento, Worth et al. (2013) identificaram as atividades do tratamento do paciente, avaliando os desperdícios inerentes à manipulação e utilização de dados do prontuário médico ao longo do processo mapeado, como dados incompletos, dados incorretos ou dados duplicados, por exemplo.

Como citado anteriormente, a metodologia *Lean* tem sido aplicada em diversos segmentos e tem mostrado resultados bastante expressivos. Rother e Shook (2003) afirmam que o MFV é a única ferramenta que mostra a relação entre fluxo de informação e fluxo de materiais de forma integrada. Quando empregada de maneira correta, ela tem auxiliado em diversos processos de mapeamento e melhorias operacionais. Em resumo, o Quadro 4 apresenta uma concatenação das interações positivas entre os princípios fundamentais do MFV e as exigências legais relacionadas pela LGPD.

Quadro 4 – Fundamentos do MFV e os requisitos da LGPD

FUNDAMENTOS DO MFV	**REQUISITOS DA LGPD**
Mapa de representação gráfica de fluxos de materiais e informações do recebimento do pedido até a entrega do produto, envolvendo atividades de agregação e não agregação de valor de acordo com o propósito de valor do cliente (ROTHER & SHOOK, 2003). "Olhar muito de longe significa não ser capaz de enxergar precisamente o estado atual e não ter visão de futuro. Olhar muito de perto implica enxergar apenas melhorias pontuais e não sistêmicas". (FERRO, 2005).	Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

A produção de um fluxo de valor deve ser feia a parir da seleção de famílias de produtos, que por sua vez estão associadas às similaridades operacionais e de entrega de valor ao cliente (ROTHER & SHOOK, 2003).	Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
Apoio às decisões estratégicas (priorização de *kaizens*) através de uma visão holística dos processos agregadores e não agregadores de valor. "Um bom mapa é aquele capaz de tornar possível vislumbrar claramente a mudança" (FERRO, 2005).	Art. 5º Para os fins desta Lei, considera-se: XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
Representação gráfica da linha do tempo. Relatório final do tempo total de atravessamento que está diretamente relacionado aos tempos de agregação de valor e tempos de não agregação de valor (ROTHER; SHOOK, 2003).	Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. I - Implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.

Fonte: Elaborado pelo autor.

Diante do referencial teórico exposto, que considera o dado pessoal como ativo das organizações contemporâneas, ao confrontar os conceitos da GI e as técnicas de modelagem de fluxo informacional com os conceitos do *Lean* e LIM, foi possível inferir que o MFV, se adaptado de forma adequada, pode contribuir para o mapeamento de fluxo de informação.

De forma a tratar dados e informação como um ativo patrimonial e, consequentemente, sua vulnerabilidade como um desperdício, a grande maioria das modelagens de fluxo informacional, apresentadas anteriormente, não correspondem a essa necessidade.

Sendo assim, existem evidências de que a utilização dos conceitos e parâmetros do MFV, sendo bastante abrangente em estudos de caráter econômico, social e ambiental, pode ser utilizado também, quando adaptado, em diversas áreas de negócio e áreas de conhecimento, incluindo gestão da informação com o foco na vulnerabilidade dos dados.

3 METODOLOGIA

Esta pesquisa é classificada como exploratória e quali-quantitativa, tendo em vista que o trabalho propõe um método de mapeamento e avaliação de processos, focado nos requisitos da LGPD, através do processo de coleta e análise de dados numéricos, passando por teste e avaliação do método proposto, por meio de 3 estudos de casos. Gil (2008) defende que a característica central de estudos exploratórios é desenvolver, esclarecer e modificar conceitos, ideias e fenômenos, proporcionando nova visão de um determinado fato. A ideia deste trabalho é explorar uma questão específica, ao buscar a resposta para a possibilidade de se utilizar os conceitos do MFV para análise da segurança da informação à luz dos requisitos da LGPD. Triviños (1987) explica que estudos exploratórios são utilizados em situações de pesquisas relativamente novas, com poucas informações sobre o assunto, permitindo aumentar o conhecimento sobre determinado problema. Já a pesquisa quantitativa propicia ao pesquisador a mensuração de hábitos, atitudes e opiniões, por meio de uma amostra estatística representativa (TERENCE, ESCRIVÃO FILHO, 2006). De forma processual, este trabalho foi dividido em quatro fases, objetivando elucidar a problemática proposta. A primeira fase consistiu em uma revisão bibliográfica, com o objetivo de desbravar os conceitos e aplicações práticas da literatura, navegando entre os elementos de contextualização desta pesquisa.

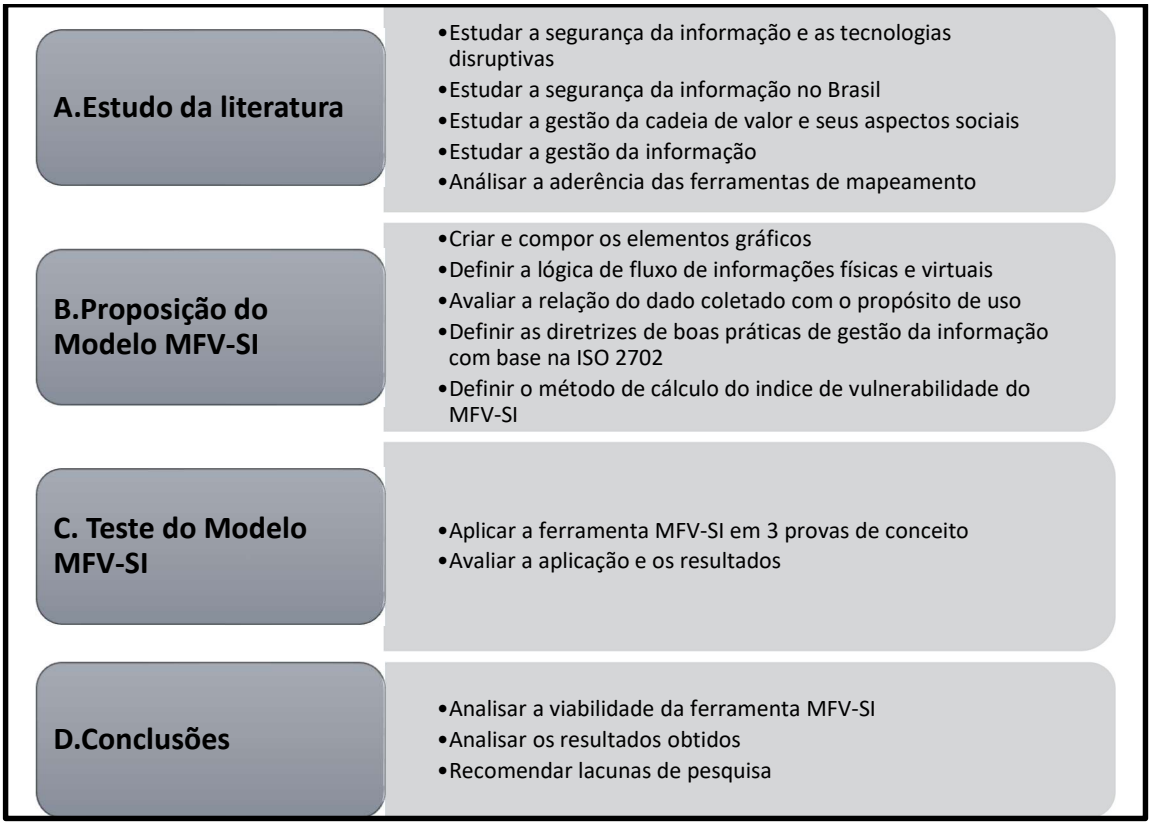
A segunda fase trata da formulação do modelo MFV-SI, focado no gerenciamento da cadeia de valor voltado para a segurança dos dados pessoais. Esta formulação passa por uma adequação das representações gráficas do MFV tradicional, bem como pelo dimensionamento da métrica de vulnerabilidade do fluxo informacional.

A terceira fase trata do processo de teste da ferramenta proposta em três empresas, por meio da aplicação de três estudos de caso.

A quarta, e última fase, consiste na elaboração dos resultados, análises e conclusões obtidas nos estudos de caso a fim de avaliar seus resultados.

A Figura 7 apresenta um desdobramento das quatro fases apresentadas anteriormente e o detalhamento das atividades a serem realizadas em cada uma delas.

Figura 7 - As fases de Pesquisa



Fonte: Elaborador pelo autor.

3.1 Concepção do método MFV-SI

A releitura do MFV, propondo o MFV-SI, tem por objetivo criar uma nova ferramenta de auxílio à jornada de adequação aos requisitos da LGPD, contribuindo para a gestão da informação de uma forma inédita, pois se diferencia do MFV tradicional ou *manufacturing* em três elementos: aquisição e tratamento de dados vinculados ao **propósito do fluxo de valor**, o **consentimento do usuário** para aquisição de dado baseado na real necessidade do seu uso e a mensuração do nível de **vulnerabilidade** ao longo da cadeia de valor.

Utilizar o MFV, uma ferramenta originalmente concebida para aplicação do conceito *Just-in-Time* (JIT), que foca basicamente no gerenciamento de estoque, pode parecer, a princípio, não fazer sentido para mapeamento do tratamento dos dados pessoais. No entanto, ao entender que novos modelos de negócio, atribuídos principalmente à coleta e ao tratamento de dados pessoais, geram um novo tipo de produto ou valor, deparamo-nos com a necessidade de gerenciamento da vulnerabilidade dos dados, observando sua integridade, confidencialidade e disponibilidade.

De acordo com os termos e definições estabelecidos na ABNT NBR ISO/IEC 27000, a integridade pode ser entendida como a garantia de que as informações não sofram qualquer

modificação, a não ser quando autorizado, da sua origem ao seu destino, a confidencialidade trata sobre a disponibilização de informações a somente pessoas autorizadas, e a disponibilidade trata a possibilidade de acesso àquela informação. O processo de disponibilidade está relacionado à manutenção da estrutura de trafego da informação de forma confiável e íntegra, possibilitando as ações de consulta e inserção de novas informações.

No conceito JIT, em que, entre outras coisas, o foco está na busca por estoque zero, os estoques são considerados ao mesmo tempo a razão e a consequência de ineficiências operacionais, como transportes, esperas e problemas de qualidade, por exemplo. Quanto mais estoque existe ao longo da cadeia de valor, mais desperdícios serão gerados. Em contrapartida, enquanto os processos *Kaizen* não solucionam por definitivo as causas geradoras dos desperdícios, os estoques podem proporcionar uma relativa estabilidade e uma aparente conexão entre processos desordenados.

No MFV *Manufacturing*, essa relação entre estoques e desperdícios é representada através do elemento gráfico chamado de "linha do tempo". Em seu livro, *O Sistema Toyota de Produção*, além da produção em larga escala, Ohno (1997) escreveu: "Tudo o que estamos fazendo é olhar para a linha do tempo, desde o momento em que o cliente nos dá um pedido até o momento em que coletamos o dinheiro […] E estamos reduzindo essa linha do tempo removendo os desperdícios sem valor agregado". Tal linha representa o cálculo do tempo de atravessamento de um produto ao longo da cadeia de valor, adotando basicamente quantidades de estoques iniciais, intermediários e finais, como o indicador dos desperdícios.

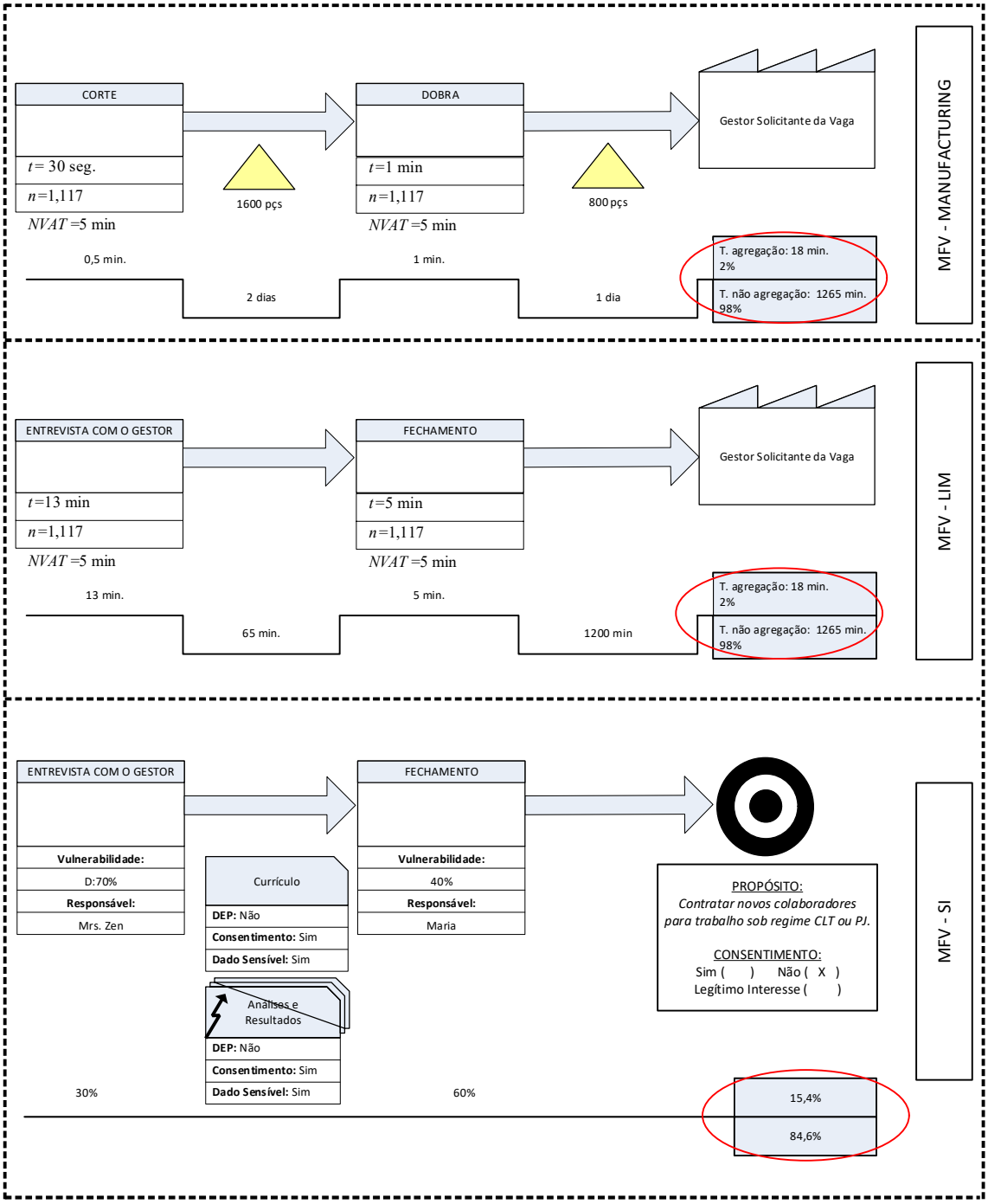
No MFV, adaptado para o LIM, a linha do tempo traduz os tempos de espera pela informação entre cada etapa e, no caso do MFV-SI, em que o ativo focal é o dado pessoal, essa linha do tempo passa a ser compreendida como a linha que representa a relação de vulnerabilidade do dado pessoal tratado.

De forma análoga à linha do tempo do MFV *Manufacturing* e do MFV adaptado ao LIM, o MFV-SI apresentará a linha de vulnerabilidade, que ponderará as atividades de agregação de valor e não agregação de valor, agora apoiada em novos desperdícios: a confidencialidade, a integridade e a disponibilidade. Com o advento da LGPD, a vulnerabilidade dos dados pessoais passa a ser, também, razão e consequência pela qual novos desperdícios poderão acontecer ao longo de uma cadeia de valor.

A partir da existência da nova lei, novos valores ao cliente serão incorporados ao longo da cadeia. Permitir um determinado grau vulnerabilidade dos dados pessoais, gerará desperdícios associados às novas exigências da lei, como privacidade e segurança (razão), e outros desperdícios, como, por exemplo, movimentação de dados em excesso, espera,

problemas de acesso e perda de informação, gerarão vulnerabilidade (consequência). A Figura 8 apresenta um exemplo comparativo entre a linha do tempo do MFV *manufacturing*, MFV-LIM e a linha do tempo do MFV-SI.

Figura 8 - Linha do tempo para o MFV-Manufacturing x MFV-LIM x MFV-SI

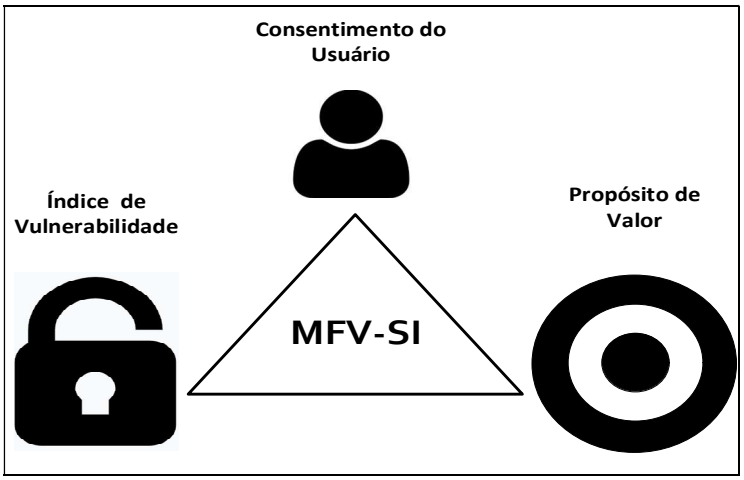


Fonte: Elaborado pelo autor.

Além da nova metodologia de mensuração da linha do tempo, outros elementos inéditos do MFV-SI são estabelecidos para atendimento ao **propósito do fluxo de valor** e o

consentimento do usuário, compondo a tríade de elementos inéditos do MFV-SI, que está representada na Figura 9.

Figura 9 - Tríade de elementos inéditos do MFV-SI



Fonte: Elaborado pelo autor.

Os tópicos, a seguir, detalharão os métodos propostos pelo modelo, para a definição do propósito do fluxo de valor e para a avaliação do consentimento necessário ou da utilização do artifício do legítimo interesse na obtenção e tratamento dos dados pessoais.

3.1.1 Definição do Propósito e do Consentimento

Para obter assertividade na definição do propósito de fluxo de valor, é necessário que se busque o alinhamento com as exigências da LGPD. Para tanto, o Quadro 5 serve como guia e apoia o mapeador na análise e definição do propósito do MFV-SI.

Ao responder "Sim" para todas as perguntas, o mapeador atenderá aos oito princípios estabelecidos pela LGPD, em seu artigo 6º, que estabelece os princípios para que um dado seja tratado, sendo: finalidade, necessidade, adequação, livre acesso, qualidade, transparência, prevenção e não discriminação. O Quadro 5 apresenta uma explicação por princípios da lei.

Quadro 5 - Avaliação do Propósito de Valor Baseado no Consentimento do Usuário

Princípios para o tratamento de dados pessoais - Art. 6º da LGPD	
Finalidade	A coleta do dado deve seguir interesses específicos, legítimos e explícitos ao titular.
Necessidade	Quantidade mínima necessária para a realização da finalidade requerida.
Adequação	Coerência e compatibilidade do tratamento realizado com a finalidade informada ao titular.
Livre acesso	Garantia da possibilidade de consulta integral e facilitada, por parte do titular, de seus dados pessoais.
Qualidade	Garantia da integridade e confidencialidade dos dados dos titulares.

Transparência	Informações claras, assertivas e acessíveis sobre os aspectos do tratamento de dados.
Prevenção	Mitigação de riscos de dados derivados do tratamento de dados.
Não discriminação	Veto da possibilidade de tratamento de dados para fins discriminatórios, abusivos ou ilícitos.

Fonte: Adaptado da Lei 13.709 (BRASIL, 2018a), LGPD.

A LGPD é clara na exigência da definição do propósito do tratamento do dado pessoal coletado, em teoria, não sendo possível a utilização do mesmo consentimento para várias finalidades de utilização. O MFV, neste aspecto, pode ter grande valor, uma vez que ele foi projetado para ser aplicado em agrupamentos de famílias de produtos, ou seja, um MFV para cada fluxo de valor, com seus processos comuns e propósito de valor bem definido pelo cliente.

Dessa forma, cada fluxo de valor no MFV-SI, pode ser projetado a partir de um consentimento adquirido ou cada fluxo de valor deverá adequar seus processos de coleta, tratamento, armazenamento e uso de dados ao propósito do consentimento especificado para tanto.

O segundo elemento se refere ao consentimento por parte do usuário, onde deverá referenciar de forma clara e objetiva a finalidade e propósito de uso dos dados. A lei elucida em seu Art. 7º, nos parágrafos 3º e 4º, respectivamente, que: "É vedado o tratamento de dados pessoais mediante vício de consentimento" e "O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas" (BRASIL, 2018a). Rother e Shook (2003) explicam que os mapas devem ser desenhados de acordo com cada família de produto ou serviço. O que caracteriza uma família de produtos é a similaridade operacional e o propósito de entrega de valor ao cliente. A interatividade e a clareza na definição de toda a cadeia, por onde o dado possa trafegar, proporciona o conhecimento do fluxo por parte de todos os envolvidos e a priorização de investimentos em melhorias.

O consentimento deve ser claro e vinculado diretamente ao propósito explicitado. No entanto, a possibilidade da justificativa de obtenção dos dados através do legítimo interesse, perante a ausência de consentimento, exigirá maiores responsabilidades. Tal alternativa, por exemplo, jamais poderá ser feita quando houver o uso de dados sensíveis.

As questões do Quadro 6 auxiliam na tomada de decisão para a justificativa de tratamento de dados pessoais, baseado em legítimo interesse. Se para pelo menos uma das perguntas listadas, no Quadro 6, a resposta for "não", ou se existirem dúvidas sobre alguma afirmação positiva, é sugerido, então, que se obtenha o consentimento do titular antes do tratamento dos dados.

Quadro 6 - Avaliação do Propósito de Valor Baseado no Legítimo Interesse

Nº	QUESTÃO
1	Processo somente dados não sensíveis ou de pessoas maiores de idade?
2	A finalidade de tratamento dos dados está explícita?
2.1	Os dados coletados são estritamente necessários para atingimento da finalidade?
2.2	É possível justificar o tratamento do dado coletado?
2.3	A utilização do seu dado atende às expectativas do titular?
3	A privacidade, os direitos e liberdades serão preservados?
4	É possível garantir a transparência e o acesso ao tratamento de dados?
5	Possuo técnicas de gerenciamento de risco?

Fonte: Elaborado pelo autor.

3.1.2 Cálculo do índice de vulnerabilidade do MFV-SI

Apoiado na norma ISO/IEC 27002, Poepjes (2015) desenvolveu uma classificação de importância das 39 principais categorias de segurança e seus objetivos de controle associados. Através de um questionário respondido por um grupo de 80 pessoas, composto por técnicos em tecnologia da informação, alta administração e usuários finais, seu trabalho classificou as 10 medidas mais relevantes, através do cálculo da média das respostas dos três grupos de respondentes. As medidas de segurança da informação classificadas pelo autor são apresentadas no Quadro 7.

A primeira coluna da tabela é referente às cláusulas de controle apontadas pela norma, a segunda coluna, às principais categorias de cada cláusula e a terceira, à pontuação obtida em pesquisa. Vale destacar que a versão brasileira da norma apresenta duas cláusulas a mais que as 11 cláusulas da norma internacional: “Criptografia” e “Segurança nas Comunicações”.

O Quadro 7 traz em ordem decrescente as principais categorias de segurança escolhidas pelos respondentes da pesquisa.

Quadro 7 – Classificação de importância das categorias de segurança da ISO/IEC 27002

ISO/IEC 27002		
CLÁUSULAS DE CONTROLE DE SEGURANÇA	**PRINCIPAIS CATEGORIAS DE SEGURANÇA**	**AI**
Controle de Acesso	Responsabilidades do Usuário	5.36
Gestão de Incidentes de Segurança da Informação	Relatório de eventos de segurança da informação e pontos fracos	5.28
Controle de Acesso	Computação móvel e teletrabalho	5.27
Gestão de comunicações e operações	Intercâmbio de informações	5.23
Gestão de comunicações e operações	Uso de Mídias	4.94

Gestão de Ativos	Classificação da Informação	4.89
Controle de Acesso	Requisitos de negócios para controle de acesso	4.75
Conformidade	Conformidade com os requisites legais	4.69
Gestão de Ativos	Responsabilidade pelos ativos	4.65
Segurança Física e Ambiental	Segurança do Equipamento	4.62

Fonte: Adaptado de Poepjes (2015).

Das 11 cláusulas contidas na norma e avaliadas por Poepjes (2015), seis aparecem entre as escolhidas. As outras cinco cláusulas de controle que não estiveram entre as questões mais importantes foram: *"Security Policy", "Organization of Information Security", "Human Resources Security", "Business Continuity Management" e "Compliance".*

A partir da seleção das mais importantes cláusulas da norma ISO/IEC 27002, estabelecidas através do estudo de Poepjes (2015), foi possível estruturar um questionário por meio da seleção das principais categorias de segurança da informação, para que o mapeador do processo, ou o aplicador MFV-SI, calcule o índice de vulnerabilidade.

O cálculo do índice de vulnerabilidade baseia-se na porcentagem de respostas positivas para cada categoria de segurança respondida como "sim". O Quadro 8 correlaciona as diretrizes estabelecidas pela NBR ISO 27002 para cada uma das mais importantes cláusulas, segundo Poepjes (2015).

Quadro 8 – Diretrizes da NBR ISO 27002 X 6 cláusulas de Poepjes (2015) X Questões para Índice de Vulnerabilidade

CAP. ISO 27002	**QUESTÃO DA REFERÊNCIA** Poepjes (2015)	**DIRETRIZES NBR ISO 27002**	**QUESTÕES**
8	4 - Quão conscientes da necessidade de propriedade e responsabilização dos ativos, os grupos de *stakeholders* precisam estar, a fim de manter a proteção adequada dos ativos organizacionais?	Convém que os ativos associados com informação e com os recursos de processamento da informação sejam identificados e um **inventário destes ativos** seja estruturado e mantido.	C.6; I.9
		Convém que os ativos mantidos no inventário tenham um proprietário.	C.6; I.9
		Convém que regras para o uso aceitável das informações, dos **ativos** associados com a informação e dos recursos de processamento da informação, sejam identificadas, documentadas e implementadas.	C.6; I.9
		Convém que todos os funcionários e partes externas devolvam todos os ativos da organização que estejam em sua posse, após o **encerramento de suas atividades**, do contrato ou acordo.	I.11
		Convém que a **informação seja classificada** em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.	C.5
	5 - Quão conscientes da necessidade de classificar as informações os grupos de *stakeholders* precisam estar, para que as informações recebam um	Convém que um conjunto apropriado de procedimentos para **rotular e tratar** a informação seja desenvolvido e implementado de acordo com o esquema de **classificação da informação** adotado pela organização.	C.5
		Convém que procedimentos para o tratamento dos ativos sejam desenvolvidos e implementados de acordo com o esquema de **classificação da informação** adotada pela organização.	C.5

	nível adequado de proteção?	Convém que existam procedimentos implementados para o gerenciamento de **mídias removíveis**, de acordo com o esquema de classificação adotado pela organização.	C.8
		Convém que as **mídias sejam descartadas** de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.	C.8
		Convém que **mídias** contendo informações sejam **protegidas** contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte.	C.8; C.9
11	10 - Quão conscientes das ameaças físicas e ambientais os grupos de *stakeholders* precisam estar, para evitar perdas, danos, roubos ou comprometimento de ativos e interrupção das atividades da organização?	Convém que **perímetros de segurança** sejam definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação, como as informações críticas ou sensíveis.	C.10; I.9
		Convém que as **áreas seguras** sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham **acesso permitido.**	C.12; I.9
		Convém que seja projetada e aplicada **segurança física** para escritórios, salas e instalações.	C.10; I.9
		Convém que sejam projetadas e aplicadas proteção física contra **desastres naturais, ataques maliciosos ou acidentes.**	C.13; C.14; D.1
		Convém que seja projetado e aplicado procedimentos para o trabalho em **áreas seguras.**	C.13; C.14; D.1
		Convém que **pontos de acesso**, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.	C.11; D.1
		Convém que os **equipamentos** sejam colocados no local ou **protegidos** para reduzir os riscos de ameaças e perigos do meio-ambiente, bem como as oportunidades de acesso não autorizado.	D.5; D.1
		Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.	D.9
		Convém que o **cabeamento de energia e de telecomunicações** que transporta dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos.	D.9
		Convém que os equipamentos tenham um **controle de entrada e saída** do local para assegurar sua disponibilidade e integridade permanente.	I.8
	17 - Quão conscientes das técnicas necessárias para proteger as mídias removíveis os grupos de *stakeholders* precisam estar, a fim de minimizar a divulgação, modificação, remoção ou destruição de ativos não autorizados?	Convém que equipamentos, informações ou *software* não sejam **retirados do local** sem autorização prévia.	C.8
		Convém que sejam tomadas medidas de segurança para ativos que operem **fora do local**, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.	I.11
		Convém que todos os equipamentos que contenham **mídias de armazenamento** de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido removidos ou sobre-gravados com segurança, antes do descarte ou do seu uso.	I.11 I.7
		Convém que os usuários assegurem que os **equipamentos** não monitorados tenham proteção adequada.	D.9; D.1; I.8
		Convém que seja adotada uma política de **mesa limpa** de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.	C.14
12	18 - Quão conscientes das políticas e procedimentos de troca de informações os grupos de *stakeholders* precisam ser, para preservar a segurança de qualquer informação ou software trocado dentro de uma organização ou com qualquer entidade externa?	Convém que os **procedimentos de operação** sejam documentados e disponibilizados a todos os usuários que necessitem deles.	Todas
		Convém que **mudanças na organização**, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam controladas.	Todas
		Convém que a **utilização dos recursos** seja monitorada e ajustada e as projeções sejam feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema.	Todas
		Convém que ambientes de **desenvolvimento, teste e produção** sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.	Desenvolvedores de Software

		Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra **códigos maliciosos**, combinado com um adequado programa de conscientização do usuário.	C.3; C.4
		Convém que **cópias de segurança** das informações, *softwares* e das imagens do sistema, sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.	D.2; I.2; I..4
		Convém que **registros (*log*)** de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares.	I.1
		Convém que as informações dos registros de **eventos (*log*)** e seus recursos sejam protegidas contra acesso não autorizado e adulteração	I.1; I.2
		Convém que as atividades dos administradores e operadores do sistema sejam registradas e **os registros (*logs*)** protegidos e analisados criticamente, a intervalos regulares.	I.1
		Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma única **fonte de tempo precisa**.	I.6
		Convém que procedimentos para controlar a **instalação de *software*** em sistemas operacionais sejam implementados.	I.3
		Convém que informações sobre **vulnerabilidades técnicas** dos sistemas de informação em uso sejam obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados.	C.7
		Convém que sejam estabelecidas e implementadas regras, definindo critérios para a **instalação de *software*** pelos usuários.	I.3
		Convém que os requisitos e atividades de **auditoria** envolvendo verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio.	C.7
9	21 - Qual a consciência das políticas e requisitos de negócios para disseminação e autorização de informações os grupos de *stakeholders* precisam ter, para controlar o acesso à informação?	Convém que uma política de **controle de acesso** seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.	C.1; C.2
		Convém que os usuários somente recebam **acesso às redes** e aos serviços de rede que tenham sido especificamente autorizados a usar.	C.3
		Convém que um processo formal de **registro e cancelamento** de usuário seja implementado para permitir atribuição de direitos de acesso.	I.11
		Convém que um processo formal de provisionamento de acesso do usuário seja implementado para conceder ou revogar os **direitos de acesso** do usuário para todos os tipos de usuários em todos os tipos de sistemas e serviços.	
		Convém que a concessão e uso de direitos de **acesso privilegiado** sejam restritos e controlados.	C.12
	23 - Quão conscientes das responsabilidades dos usuários, para manter controles eficazes de acesso, os grupos de *stakeholders* precisam ser, para impedir o acesso não autorizado ao usuário e comprometer ou roubar instalações de processamento de informações e informações?	Convém que a concessão de informação de **autenticação secreta** seja controlada por meio de um processo de gerenciamento formal.	C.9; C.1; C.2; I.11
		Convém que os proprietários de ativos **analisem criticamente** os direitos de acesso dos usuários, a intervalos regulares.	I.11; C.5
		Convém que os **direitos de acesso** de todos os funcionários e partes externas às informações e aos recursos de processamento da informação sejam retirados logo após o encerramento de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades.	I.11
		Convém que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de **autenticação secreta.**	C.5
	27 - Quão conscientes dos riscos associados à computação móvel e ao	Convém que o acesso à informação e às **funções dos sistemas de aplicações** seja restrito, de acordo com a política de controle de acesso.	C.9

	teletrabalho, em um ambiente desprotegido, os grupos de *stakeholders* precisam estar?	Convém que, onde aplicável pela **política de controle de acesso**, o acesso aos sistemas e aplicações sejam controlados por um procedimento seguro de entrada no sistema (*log-on*)	C.9
		Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade.	C.1; C.2
		Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações sejam restritos e estritamente controlados.	I.3
14	31 - Quão conscientes da segurança dos arquivos do sistema e do código fonte, os grupos de *stakeholders* precisam ser?	Convém que o acesso ao código-fonte de programa seja restrito.	Somente para Fabricantes de *Software*
		Convém que os requisitos relacionados com segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.	Somente para Fabricantes de *Software*
		Convém que as informações envolvidas nos serviços de aplicação que transitam sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.	Somente para Fabricantes de *Software*
		Convém que informações envolvidas em transações nos aplicativos de serviços sejam protegidas para prevenir transmissões incompletas, erros de roteamento, alteração não autorizada da mensagem, divulgação não autorizada, duplicação ou reapresentação da mensagem não autorizada.	Somente para Fabricantes de *Software*
		Convém que regras para o desenvolvimento de sistemas e software sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.	Somente para Fabricantes de *Software*
		Convém que as mudanças em sistemas no ciclo de vida de desenvolvimento sejam controladas utilizando procedimentos formais de controle de mudanças.	Somente para Fabricantes de *Software*
		Quando plataformas operacionais forem modificadas, convém que as aplicações críticas de negócio sejam analisadas criticamente e testadas para assegurar que não ocorreu nenhum impacto adverso nas operações da organização ou na segurança.	Somente para Fabricantes de *Software*
		Convém que modificações em pacotes de software sejam desencorajadas e estejam limitadas às mudanças necessárias, e todas as mudanças sejam estritamente controladas.	Somente para Fabricantes de *Software*
		Convém que princípios para projetar sistemas seguros sejam estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação.	Somente para Fabricantes de *Software*
		Convém que as organizações estabeleçam e protejam adequadamente ambientes de desenvolvimento seguros para os esforços de desenvolvimento e integração de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema.	Somente para Fabricantes de *Software*
		Convém que a organização supervisione e monitore as atividades de desenvolvimento de sistemas terceirizado.	Somente para Fabricantes de *Software*
		Convém que os testes de funcionalidades de segurança sejam realizados durante o desenvolvimento de sistemas.	Somente para Fabricantes de *Software*
		Convém que programas de testes de aceitação e critérios relacionados sejam estabelecidos para novos sistemas de informação, atualizações e novas versões.	Somente para Fabricantes de *Software*
		Convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados.	Somente para Fabricantes de *Software*
16	34 - Qual a necessidade de relatórios oportunos de eventos e fraquezas de segurança da informação, os grupos de *stakeholders* precisam ter, para permitir que medidas corretivas oportunas sejam tomadas?	Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a **incidentes de segurança da informação.**	C.7; D.4
		Convém que os **eventos de segurança** da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível.	C.7; D.4
		Convém que os funcionários e partes externas que usam os sistemas e serviços de informação da organização, sejam instruídos a registrar e notificar quaisquer **fragilidades de segurança da informação**, suspeita ou observada, nos sistemas ou serviços.	C.7; D.4

		Convém que os **eventos de segurança da informação** sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação.	C.7; D.4
		Convém que **incidentes de segurança da informação** sejam reportados de acordo com procedimentos documentados.	C.7; D.4
		Convém que os conhecimentos obtidos da análise e resolução dos **incidentes de segurança da informação** sejam usados para reduzir a probabilidade ou o impacto de incidentes futuros.	C.7; D.4
		Convém que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como **evidências.**	C.7; D.4
18	37 - Qual a consciência do cumprimento dos requisitos legais os grupos de *stakeholders* precisam estar, a fim de evitar violações de quaisquer obrigações legais, legais, regulatórias ou contratuais, e de quaisquer requisitos de segurança relacionados?	Convém que todos **os requisitos legislativos estatutários**, regulamentares e contratuais pertinentes, e o enfoque da organização para atender a esses requisitos, sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.	D.3
		Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os **requisitos legislativos**, **regulamentares e contratuais** relacionados com os direitos de propriedade intelectual, e sobre o uso de produtos de softwares proprietários.	D.3
		Convém que **registros** sejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.	Todas
		Convém que a privacidade e proteção das **informações de identificação pessoal** sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.	Todas
		Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.	I.5
		Convém que o **enfoque da organização** para gerenciar a segurança da informação e a sua implementação (por exemplo, controles, objetivo dos controles, políticas, processos e procedimentos para a segurança da informação) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas.	D.3
		Convém que os gestores **analisem criticamente**, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.	D.3
		Convém que os sistemas de informação sejam **analisados criticamente**, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização.	D.3

Fonte: Elaborado pelo autor.

A correlação apresentada no Quadro 8 resultou em 81 diretrizes da segurança da informação. A partir disso, foi possível atribuir uma ou mais boas práticas para pelo menos uma das diretrizes. A escolha de tais boas práticas proporcionou o agrupamento de uma ou mais diretrizes de segurança, gerando 30 atividades capazes de serem avaliadas presencialmente.

As correlações entre diretrizes e boas práticas foram apresentadas no Quadro 8, na coluna “Questões”. Cada uma das 30 boas práticas possui um código de referência composto por uma letra e um número sequencial, onde a letra poderá ser “C”; “I” ou “D”, correspondendo

respectivamente a boas práticas de confidencialidade, integridade e disponibilidade. O Quadro 9 apresenta as 30 questões de apoio para a avaliação do índice de vulnerabilidade.

Quadro 9 – Boas práticas para avaliação de vulnerabilidade

Nº	Código	Boas práticas
1	C.1	As senhas expiram periodicamente (por exemplo, a cada XX dias)?
2	C.2	Existe duplo critério de autenticação?
3	C.3	Existe o mínimo de *stateful firewalls* implantados em todas as conexões externas (por exemplo, Internet)?
4	C.4	Existe um processo / critério para avaliar o risco de protocolos / portas antes de implementá-los nos *firewalls*?
5	C.5	A informação crítica é classificada de acordo com uma diretriz de classificação (por exemplo, seguro, confidencial, público etc.)?
6	C.6	Existe um inventário dos ativos em posse da Empresa? Todos os dados críticos da empresa têm um proprietário?
7	C.7	Existe um processo de gestão auditoria e comunicado de vulnerabilidades técnicas ocorridas?
8	C.8	Existe uma política para tratar da segurança de dispositivos móveis (*PDAs*, *laptops*, *smartphones*, *pen drive*)?
9	C.9	Existe um controle de acesso nos sistemas de informações utilizados que garante que cada colaborador veja somente os dados pertinentes a ele?
10	C.10	Existem áreas seguras que protegem informações confidenciais?
11	C.11	Existe controle de acesso em áreas seguras? A entrada para áreas seguras é protegida?
12	C.12	Os acessos privilégios são restritos?
13	C.13	As áreas seguras estão localizadas de maneira protegida?
14	C.14	Existe orientação para os usuários sobre o que fazer quando não estão presentes em suas estações de trabalho ou contra desastres naturais ou atentados?
15	C.15	Existe uma prática de ambiente de trabalho, com mesa limpa de papéis, mídias móveis e tela limpa?
16	I.1	O *log* está ativado em todos os *firewalls*, roteadores e servidores *proxy*? Existe um processo para revisar os *logs* regularmente?
17	I.2	Existe uma auditoria regular realizada para contabilizar todas as fitas de *backup*?
18	I.3	Existe procedimento para controle bem como regras para instalação de *softwares* pelos usuários?
19	I.4	Periodicamente restaura informações de fitas de *backup* para garantir a integridade dos dados?
20	I.5	Os dados armazenados nos discos rígidos estão criptografados?
21	I.6	Existe uma fonte (relógio) de tempo precisa e sincronizada para os sistemas de processamento relevantes?
22	I.7	As informações são removidas adequadamente da mídia ou equipamento que serão descartados?
23	I.8	A remoção de informações e equipamentos para fora das instalações da organização é controlada?
24	I.9	Os alarmes, proteção contra incêndio e outros sistemas estão instalados?
25	I.10	Existe procedimentos e controles de contratação e desligamento de funcionários, bem como suas permissões de acesso durante o período empregado?
26	D.1	Existem instalações de recuperação de desastres para sistemas críticos, localizados em uma área geograficamente independente?
27	D.2	Os *backups* de dados críticos de negócios são feitos regularmente (pelo menos semanalmente)?
28	D.3	Uma análise de impacto nos negócios foi realizada em todos os aplicativos e sistemas dos clientes?
29	D.4	Existem planos de recuperação de desastres escritos formalmente (DRPs), cobrindo a perda parcial ou total de servidores, aplicações críticas, instalações físicas?
30	D.5	Os cabos de energia e telecomunicações e equipamentos, em geral, estão adequadamente protegidos? Os equipamentos essenciais estão protegidos contra a falta de energia?

Fonte: Elaborado pelo autor.

Para o cálculo do índice de vulnerabilidade, será necessário que o mapeador responda, para todas as etapas da cadeia de valor, as 30 questões listadas no Quadro 9. Após a obtenção das respostas, o mapeador deverá somar as respostas positivas e dividir a soma pelo total de 30 questões, obtendo o índice de vulnerabilidade individual de cada processo. Em seguida, deverá multiplicar os índices individuais de toda a cadeia de valor para obter o índice de vulnerabilidade geral, uma vez que as vulnerabilidades ao longo da cadeia são acumulativas, ou seja, um problema pode acontecer na etapa 1 e na etapa 5, por exemplo.

Supondo um fluxo de valor, com o propósito de contratação de colaboradores, com quatro etapas. Após a coleta das respostas do Quadro 9, para cada uma das quatro etapas obtivemos: cinco respostas positivas para etapa 1, cinco respostas positivas para etapa 2, oito respostas positivas para etapa 3, 10 respostas positivas para etapa 4. Dessa forma, o cálculo do índice de vulnerabilidade por etapa é dado por: 5/30=0,1666; 5/30=0,1666; 8/30=0,2666 e 10/30=0,3333 respectivamente.

Por fim, para obter o índice de vulnerabilidade geral desta cadeia de valor, basta subtrair de 1 a multiplicação das porcentagens obtidas em cada etapa, o que nos levaria ao resultado: [1-(0,1666*0,1666*0,2666*0,3333)] = 99,75% de vulnerabilidade.

Supondo que, após um processo de melhoria implementado, em que as quantidades de respostas positivas para as quatro etapas do fluxo foram, respectivamente, 23, 23, 24 e 26, teremos um novo índice de vulnerabilidade, que refletiria tais melhorias com o valor de [1-(0,767*0,767*0,8*0,867)] = 60,6%.

3.1.3 Padrões gráficos do MFV-SI

O terceiro desafio, na elaboração do modelo MFV-SI, após a definição das diretrizes de propósito/consentimento e do cálculo do índice de vulnerabilidade, consiste na criação dos padrões gráficos e suas regras de preenchimento.

Para tanto, foi elaborado um quadro comparativo da abrangência da aplicação do MFV-SI, no que diz respeito aos três elementos inéditos abordados pelo modelo, o Quadro 10. O quadro comparativo avalia as abordagens de maior e menor relevância entre tratamento de materiais, tratamento de informações, as particularidades das métricas da linha do tempo e o enfoque dos ativos tratados em cada um dos modelos MFV – *Lean Manufacturing*, MFV- *Lean Information Management* e MFV- SI. Após a comparação das abrangências e aplicabilidade de cada modelo, o Quadro 10 apresenta os novos elementos de controle, que serão representados graficamente no modelo MFV-SI.

Quadro 10 - Comparativo de abrangência e aplicabilidade dos 3 tipos de MFV

VALOR PARA A ORGANIZAÇÃO	MFV – LEAN MANUFACTURING (LM)	MFV- LEAN INFORMATION MANAGEMENT (LIM)	MFV- SI
ATIVO FOCAL	Materiais e Tempo	Informação e Tempo	Informação e Vulnerabilidade
TRATAMENTO DOS MATERIAIS	***Maior Relevância***. O Mapeamento no fluxo de material, baseado no *Just-in-Time* (Quantidade certa na hora certa). Busca pela eliminação dos desperdícios relacionados ao processo. Produtos com zero defeitos.	***Menor Relevância.*** Mapeamento dos tipos de documentos físicos e métodos de armazenamento e transferência no processo de apoio à entrega do serviço.	***Menor Relevância.*** Mapeamento dos tipos de documentos físicos e métodos de armazenamento e transferência no processo de apoio à entrega do serviço.
TRATAMENTO DAS INFORMAÇÕES	***Menor Relevância.*** Mapeamento do fluxo de informação atrelados à produção do produto. Geralmente vinculados aos departamentos de PCP, Compras, Comercial e Expedição.	***Maior Relevância.*** Mapeamento do trafego dos dados **SOLICITADOS** ou **FORNECIDOS** pelos agentes do fluxo de valor, sem vínculo ao propósito estabelecido para uso do dado. A quantidade de dados bem como seu tratamento é determinado pelo gerente do fluxo de valor	***Maior Relevância.*** Mapeamento do trafego dos dados **SOLICITADOS** ou **FORNECIDOS** pelos agentes do fluxo de valor, **com vínculo ao propósito** estabelecido para uso do dado. A quantidade de dados passa a ser vinculada ao propósito. A vulnerabilidade dos dados pessoais passa a ser um valor para a empresa.
MÉTRICA GERAL DA LINHA DO TEMPO	FOCADO NOS **ESTOQUES** INTERMEDIARIOS, PRODUTOS ACABADOS E DE MATÉRIA PRIMA. Dias de estoque, lead time de atravessamento do pedido.	**ESPERA** ENTRE OS PROCESSOS E INDICE DE COMPLETO E CORRETO (De acordo com o solicitado ou fornecido). Dias para conclusão do serviço ou entrega da informação.	**VULNERABILIDADE** ENTRE AS TRASAÇÕES POR PROCESSOS, (De acordo com o propósito de existência do fluxo de valor em questão. Porcentagem de vulnerabilidade da cadeia de valor.
NOVOS ELEMENTOS DO MFV-SI	--	--	1 - A quantidade certa de dados passa a ser limitada pela **FINALIDADE DO FLUXO DE VALOR,** exigida pela lei. 2 - O dado correto passa por um novo elemento. O **CONSENTIMENTO** do usuário, que permite o devido uso do dado para o devido propósito estabelecido pelo fluxo de valor. 3 - A **VULNERABILIDADE** traduz o índice de controle do fluxo de valor minimamente necessário para proporcionar a Integridade, a Disponibilidade e a Confidencialidade, mostrando sua evolução ao se comparar os mapas do estado atual e futuro.

Fonte: Elaborado pelo autor.

Graficamente o MFV-SI utilizará em grande parte os mesmos elementos gráficos adotados pelo MFV desenvolvido para a manufatura e o MFV do LIM.

Como elementos novos, podemos destacar três representações: a “caixa de análise”, “bloco de dados físicos” e “bloco de dados virtuais”.

No MFV *manufacturing*, a “caixa de análise”, também conhecida como “caixa de dados”, é adotada por processo. Cada processo passa a ter seus parâmetros analisados, como o

índice OEE, número de funcionários e tempo de ciclo, por exemplo. No MFV-SI, a "caixa de análise" será aplicada por bloco de dados e não por processo, como no MFV *manufacturing*.

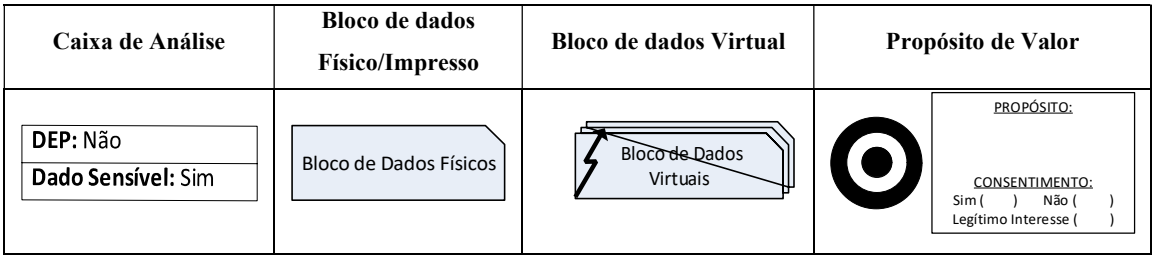
Os "blocos de dados" devem ser entendidos como um documento ou um processo cadastral que contenha dados pessoais em seu conteúdo. Esses "blocos de dados" devem ser classificados de acordo com uma macro atividade do processo mapeado, como, por exemplo, cadastro de cliente, cadastro de funcionário ou um pedido médico.

Tanto "caixa de análise", quanto os "blocos de dados" dependerão de um certo grau de arbitrariedade e experiência do mapeador, no entanto, três elementos são fundamentais e exigidos para o atingimento do propósito da ferramenta: a classificação de "Dados Extra Propósito" (DEP), de "Consentimento" e de "Dado Sensível". Todos eles deverão receber uma resposta binária (sim ou não).

Quando apontado como "sim", o DEP representará que aquele bloco de dados apresenta informações desvinculadas ao propósito do fluxo mapeado, ou seja, aquele dado pessoal aumenta o risco e não atende ao requisito da lei.

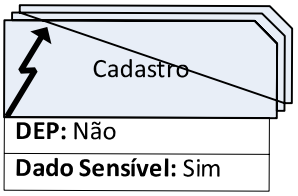
O outro elemento obrigatório para a "caixa de análise" é o "Dado Sensível". Este campo serve de alerta para o aumento de severidade, caso um vazamento ocorra. Caso os dados coletados estejam dentro do seu propósito de tratamento, bem como com seu consentimento de uso correto, o campo "Dado Sensível" destacará uma maior importância para a redução da vulnerabilidade daquela etapa da cadeia. Na Figura 10, são apresentados a "caixa de análise", o "bloco de dados" e logo em seguida, na Figura 11, terá a representação gráfica conjunta dos 2 elementos.

Figura 10 - Novos elementos Gráficos do MFV-SI



Fonte: Elaborado pelo autor.

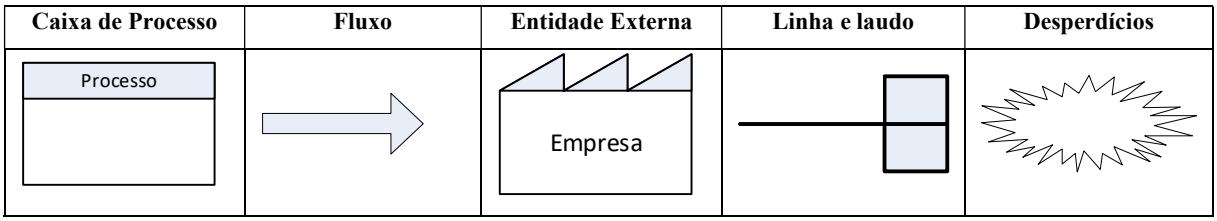
Figura 11 - Exemplo de aplicação conjunta dos elementos Gráficos do MFV-SI



Fonte: Elaborado pelo autor.

Apresentados os novos elementos, a Figura 12 apresenta os elementos gráficos em comum entre o MFV e o MFV-SI.

Figura 12 - Elementos Gráficos comum entre MFV e MFV-SI



Fonte: Elaborado pelo autor.

Após a definição dos elementos gráficos, bem como do método de cálculo do índice de vulnerabilidade, expostos acima, é possível propor um exemplo do modelo MFV-SI. A próximo seção apresentará um exemplo hipotético de um processo mapeado através do modelo MFV-SI.

3.1.4 Exemplificação do modelo MFV-SI

Podemos exemplificar o modelo MFV-SI para um processo de contratação de novos colaboradores em uma empresa hipotética.

A leitura do MFV-SI deve ser feita da esquerda para a direita, em que, no exemplo, inicia-se pela captação de candidatos através de uma entidade externa. Nesta etapa, devemos destacar a importância da corresponsabilidade dos termos de consentimento, armazenamento e tratamento dos currículos cadastrados entre o tratador dos dados e seus fornecedores de serviços.

Na primeira etapa, é possível observar a existência de dados pessoais em forma física, indicadores de desempenho dos candidatos em gestão a vista, permitindo que todos os visitantes da sala tenham acesso ao desempenho dos candidatos nas entrevistas. Observa-se que o elemento gráfico para o bloco de dados físico é diferente do virtual.

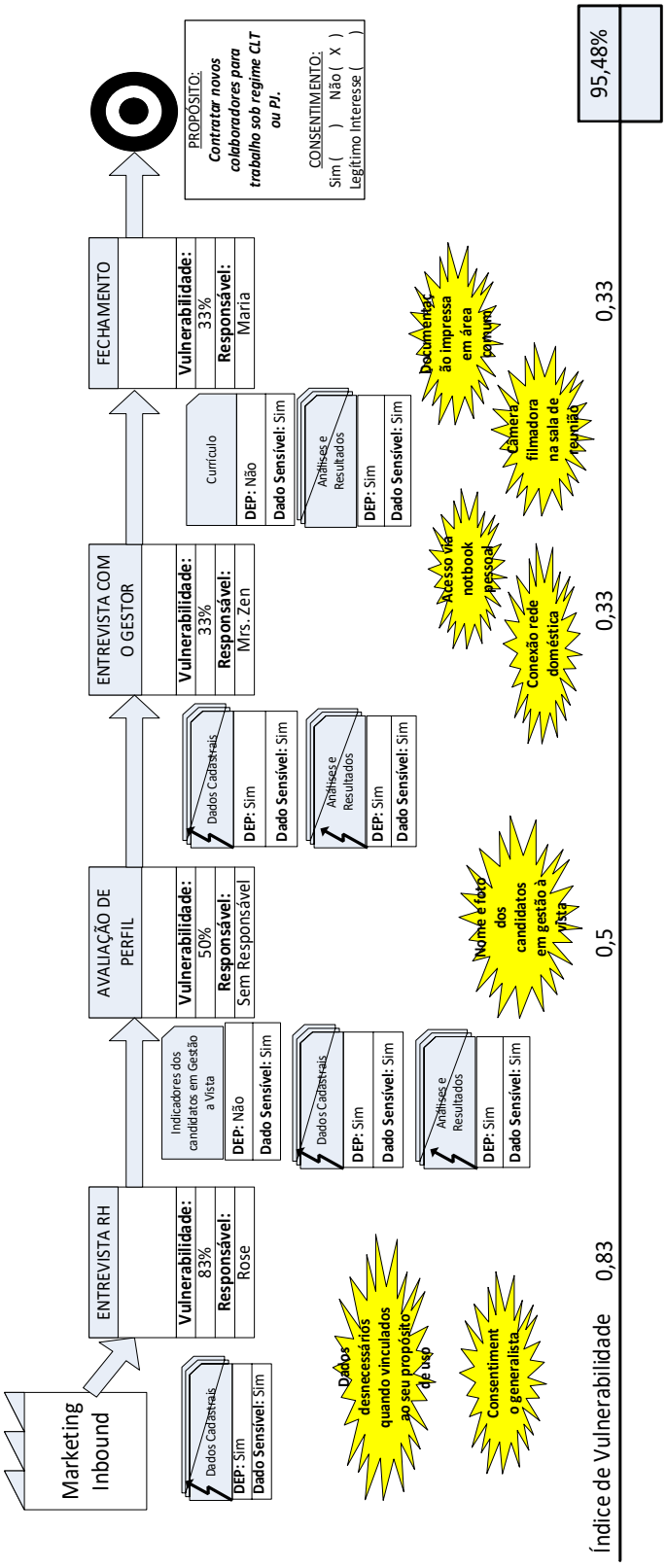
Na segunda etapa, “análise de perfil”, são geradas análises dos resultados obtidos na etapa anterior, caracterizando o que a LGPD chama de tratamento de dados, ou seja, quando, na posse de dados pessoais, a empresa processa esses dados e gera novos dados relacionados ao indivíduo, como nesse caso, por exemplo, traço de perfil comportamental ou uma nota de desempenho em uma prova técnica.

A terceira etapa exemplifica processos remotos com equipamentos pessoais compartilhados em processos corporativos, muito comum nas atividades de *home office*.

Por fim, a quarta etapa demonstra situações de exposição de documentações pessoais, em ambientes de escritórios com pouca ou nenhuma preocupação com seu sigilo. É o caso representado pelo currículo impresso sobre a mesa, em uma sala de reunião compartilhada.

A Figura 13 apresenta o MFV-SI atual de um processo hipotético do departamento de recursos humanos para a contratação de colaboradores descrito acima.

Figura 13 - MFV-SI para um processo hipotético de contratação de colaboradores



Fonte: Elaborado pelo autor.

3.1.5 Etapas da implementação do modelo MFV-SI

De forma didática, Rother e Shook (2003) criaram um manual para uso empresarial, estabelecendo diretrizes práticas e um sequenciamento lógico para a aplicação dos conceitos do MFV. Esse roteiro tem sido amplamente utilizado para coleta e análise de dados em pesquisas acadêmicas, como se pode observar, por exemplo, nos trabalhos de Abdulmalek e Rajgopal (2007), Lian e Van Landeghem (2007) e Singh e Sharma (2009).

Para este estudo, o roteiro estabelecido por Rother e Shook (2003) serviu de base para a elaboração de um manual de implementação do MFV-SI.

O primeiro passo para a elaboração do MFV-SI é a escolha da família de produtos. Para o MFV, os critérios adotados para essa fase são, geralmente, a similaridade dos processos que determinados produtos são submetidos. No MFV-SI, o critério adotado deverá estar relacionado ao propósito da coleta e tratamento dos dados pessoais. O mapeador deverá estar a tento ao novo elemento gráfico estabelecido por este estudo. É através dele que as especificações do propósito do fluxo de valor devem ser estabelecidas.

A segunda etapa trata de desenhar o estado atual do fluxo de valor. Esta etapa deve, obrigatoriamente, conter as representações gráficas das etapas bem como sua ordenação, os blocos de dados e sua caixa de análise (DEP, Consentimento, Dados Sensíveis), a especificação do propósito do fluxo de valor, o índice de vulnerabilidade, bem como os desperdícios explícitos em seus respectivos elementos gráficos estabelecidos anteriormente.

A terceira etapa consiste na projeção de um fluxo de valor optimizado, chamado de MFV-SI-Futuro. Suas representações gráficas são coincidentes com a do MFV-SI-Atual, com a diferença obrigatória de pelo menos a redução do índice de vulnerabilidade e a redução dos destaques apontados para os desperdícios do estado atual.

Por fim, na quarta etapa o mapeador deverá elaborar, de forma prática, um plano de ação com prazos e responsáveis capazes de serem monitorados a fim de se atingir as diretrizes estabelecidas no MFV-SI-Futuro.

O Quadro 11 apresenta as correlações entre as etapas estabelecidas por Rother e Shook (2003) para a elaboração do MFV tradicional comparando-as com as etapas estabelecidas para o desenvolvimento do MFV-SI:

Quadro 11 - Etapas e características da implementação do MFV e MFV-SI

ETAPAS PARA IMPLEMENTAÇÃO MFV (ROTHER E SHOOK, 2003)	CARACTERÍSTICAS DAS ETAPAS MFV(ROTHER E SHOOK, 2003)	CARACTERÍSTICAS DAS ETAPAS MFV-SI
(1) Seleção do fluxo de valor	A definição das famílias utiliza o critério de compartilhamento de processos agrupando produtos que passam por etapas de processamento semelhantes, sendo necessária quando a empresa possui grande *mix* de produtos em seu portfólio. Quais processos compartilham produtos diferentes? Quais produtos?	A seleção das famílias passa a ser feita levando em conta o propósito do trafego do dado diante do fluxo de valor mapeado, não eliminando, mas levando para segundo plano o agrupamento de produtos/serviços considerando a similaridade dos processos. Para quais propósitos comerciais eu coleto e/ou trato dados pessoais?
(2) Mapeamento do estado atual	O mapa do estado atual tem o intuito de se obter uma visão global do fluxo de valor representando suas atividades de agregação e não agregação de valor. Seus elementos gráficos devem ser utilizados de modo que seus pontos de melhoria sejam perceptíveis para futura adequação.	O mapa do estado atual com os objetivos associados a uma visão global do fluxo de valor e às representações de atividades de agregação e não agregação de valor. Seus elementos gráficos foram adaptados destacando-se os novos elementos da "caixa de análise", e a diferenciação entre dado virtual e físico. Devem ser utilizados de modo que seus pontos de melhoria sejam perceptíveis para futura adequação.
(3) Mapeamento do estado futuro	O mapeamento do estado futuro sucede a elaboração do mapa atual projetando uma melhoria de processo. A construção do mapa futuro norteia-se pela melhoria dos valores da linha do tempo, bem como pela implantação práticas de redução de desperdícios.	O mapeamento do estado futuro sucede a elaboração do mapa atual projetando uma melhoria de processo. A construção do mapa futuro norteia-se pela melhoria dos valores do índice de vulnerabilidade bem como pela implantação das boas práticas de segurança da informação fisicamente e virtualmente expostas.
(4) Plano de trabalho e implementação	Designação de prazos e responsáveis para a execução de um plano de tarefas.	Designação de prazos e responsáveis para a execução de um plano de tarefas.

Fonte: Elaborado pelo autor.

4 DESENVOLVIMENTO

A próxima seção, deste trabalho, caracteriza-se pelo processo de avaliação do modelo proposto MFV-SI. Tal avaliação será feita em três diferentes segmentos empresariais, segmento da saúde, indústria alimentícia e comércio e distribuição, através da aplicação de três provas de conceito, seguindo o protocolo de implementação descrito na seção 3.1.

As provas de conceitos (PoC) tem por característica ser um modelo prático capaz de verificar que um conceito é suscetível, quando explorado em prática. Para Silva (2014), o objetivo da prova de conceito é "provar a viabilidade de um projeto ou conceito em escala reduzida", possibilitando uma avaliação prática por parte de organizações acerca de um produto ou serviço, além de diminuir custos e riscos.

4.1 As unidades de análises

A escolha das unidades de análise levou em consideração, inicialmente, a carência de processos estruturados e pessoas qualificadas e dedicadas para o gerenciamento da segurança da informação em pequenas e médias empresas brasileiras. Netto e Silveira (2007) verificaram que as Pequenas e Médias Empresas (PMEs), em sua maioria, não possuem infraestrutura para implantar segurança da informação (SI), tão pouco conhecimento técnico e pessoal com dedicação integral às atividades necessárias de segurança da informação.

As empresas, onde foram aplicadas as provas de conceito, situam-se no estado do Paraná, sendo um Laboratório de Análises Clínicas, na cidade de Umuarama, uma indústria de rótulos e etiquetas, na cidade de Marialva, e uma montadora de mini computadores, localizada na cidade de Maringá.

O Laboratório de Análises clínicas se destaca pela sua longevidade, atuando desde 1970. Em 2019, a empresa realizou, uma média de 40 mil exames por mês e, desde 2012, opera sob o regime de duas normas de gestão da qualidade, o Sistema Nacional de Acreditação de Laboratórios-DICQ e o Sistema de Gestão da Qualidade (ABNT NRB ISO 9001, 2015).

A indústria de rótulos e etiquetas tem como característica de destaque atender grandes *players* dos segmentos alimentícios, bebidas, higiene, limpeza, cosméticos, entre outros. O grupo possui três unidades fabris no Brasil, e a unidade de análise em questão possui uma área de 12.500m², equipamentos de alta tecnologia, empregando em torno de 215 funcionários, alocados em dois turnos diariamente. A montadora de minicomputadores atua no mercado de hardware desde 2015, é composta por 10 funcionários, também possui certificação ABNT NRB ISO 9001 (2015), destacando-se pela venda de produtos personalizados com suporte ao cliente.

4.2 Prova de conceito 1: laboratório de análises clínicas

A primeira prova de conceito ocorreu em um laboratório de análises clinicas, situado na cidade de Umuarama, no interior do estado do Paraná, com aproximadamente 200 mil habitantes.

Fundado em 1970, através da fusão de outros quatro laboratórios, a unidade de análise contava, em dezembro de 2019, com 60 funcionários, atuando em uma área construída de 1000mª, na realização de exames nas especialidades de Bioquímica, Hematologia, Imunologia, Hormônios, Microbiologia, Citologia, Parasitologia e Urinálise, e aplicação de vacinas. Em 2019, a empresa realizou, em média, 40 mil exames por mês e, desde 2012, atua sob o regime de duas normas de gestão da qualidade, o Sistema Nacional de Acreditação de Laboratórios (DICQ) e a ABNT NRB ISO 9001 (2015). O laboratório se destaca pela inovação e qualidade do atendimento, sendo o primeiro a implementar o sistema de *drive thru* para coleta de material em pacientes com dificuldades de locomoção, e disponibilizar uma sala e realidade virtual para humanizar o processo de coleta de material de análise ou aplicação de vacinas em crianças.

Outro fator importante para a escolha desta unidade é o fato de se tratar de um tipo de negócio que manipula um grande volume de dados pessoais, dentre eles dados pessoais, considerados sensíveis pela legislação.

Dessa forma, a escolha da unidade de análise, em questão, pretende expor o modelo proposto a uma ampla gama de desafios enfrentados por pequenas e médias empresas brasileiras no que se refere ao tratamento e segurança de dados pessoais, uma vez que este fluxo de valor realiza o tratamento de dados sensíveis, de dados de pessoas menores de idade, por meios físicos e virtual.

Seguindo as etapas de implementação apresentadas no Quadro 11, a seguir são apresentadas quatro subseções, uma para cada etapa, a fim de apresentar a prova de conceito.

4.2.1 Seleção do Fluxo de Valor

Em uma vista presencial à unidade de análise em questão, onde foram adotadas medidas de observação dos processos em execução e entrevista com o gerente administrativo, o supervisor da aplicação e a supervisora de atendimento. Essa etapa tinha como objetivo entender o fluxo operacional, produzindo um esboço do MFV-SI, entender e constatar evidências do tráfego de dados, formas de armazenamento, proteção e propósito de obtenção.

Como resultado prévio, foram observadas cinco etapas: recepção virtual ou recepção

presencial, recepção interna, coleta de material, análise técnica e arquivamento. Em seguida, para cada etapa do fluxo de valor, foram levantadas as entradas de informações, representadas pelos chamados Blocos de Dados.

Para cada Bloco de Dados, foram aplicadas oito questões, apresentadas no Quadro 6, a fim de avaliar se o propósito do tratamento dos dados pode ou não ser baseado no legítimo interesse, ou se necessita de consentimento do usuário.

O Quadro 12 apresenta a avaliação do legítimo interesse e mostra que tal artifício não poderá ser adotado, uma vez que pelo menos uma das respostas foi negativa, como mostrado a seguir. Sendo assim, esse fluxo de valor deverá obter o consentimento para o propósito estabelecido, que foi descrito como: realizar exames laboratoriais e seus tramites financeiros nas especialidades de Bioquímica, Hematologia, Imunologia, Hormônios, Microbiologia, Citologia, Parasitologia e Urinálise e aplicação e vacinas.

Quadro 12 – Caso 1: Avaliação de Propósito e Legítimo Interesse

BLOCOS/QUESTÕES	**1**	**2**	**2.1**	**2.2**	**2.3**	**3**	**4**	**5**
Cadastro de clientes	N	N	S	S	S	S	N	S
Capa de exames	N	N	S	S	S	S	N	S
Identificação da Amostra	S	N	S	S	S	S	N	S
Análises e Resultados	N	N	S	S	S	S	N	S
Mapa de trabalho	N	N	S	S	S	S	N	S
Pedido médico	S	S	S	S	S	S	N	S
Protocolo de entrega	N	N	S	S	S	S	N	S

BLOCO DE DADOS	**DETALHAMENTO DOS BLOCOS DE INFORMAÇÕES.**
Cadastro de clientes	Nome, sexo, nascimento, nome da mãe, informações clínicas, medicação, CPF, RG, telefones, e-mail e endereço.
Capa de exames	Nome, sexo, nascimento, solicitantes, convênio e exames.
Identificação da Amostra	Nome, nascimento e exames.
Análises e Resultados	Nome, solicitante, idade, convênio, exames e resultados.
Mapa de trabalho	Nome, idade, sexo, solicitante, informações clínicas, medicação, exames e resultados.
Pedido médico	Nome, solicitante e exames.
Protocolo de entrega	Nome, convênio, solicitante, idade, sexo, exames, informações financeiras e dados para acesso online, exceto data de nascimento.

Fonte: Elaborado pelo autor.

A propósito da escolha do "produto" ou família de produto a ser mapeado, a escolha foi pelo fluxo de valor de exames laboratoriais, pela sua representatividade financeira e volume de operações, quando comparado com o fluxo de valor de aplicação de vacinas.

4.2.2 Mapeamento do Estado Atual

Após a coleta das respostas apresentadas no Quadro 13, obtivemos: sete respostas positivas para etapa 1, sete respostas positivas para etapa 2, seis respostas positivas para etapa 3, quatro respostas positivas para etapa 4 e uma resposta positiva para a etapa 5. Dessa forma, o cálculo do índice de vulnerabilidade por etapa é dado por: 7/30=0,2333; 7/30=0,2333; 6/30=0,20; 4/30=0,13 e 1/30=0,0333 respectivamente.

O Quadro 14 apresenta as respostas obtidas para as questões de vulnerabilidade do estado atual.

Quadro 13 – Caso 1: Cálculo de Vulnerabilidade

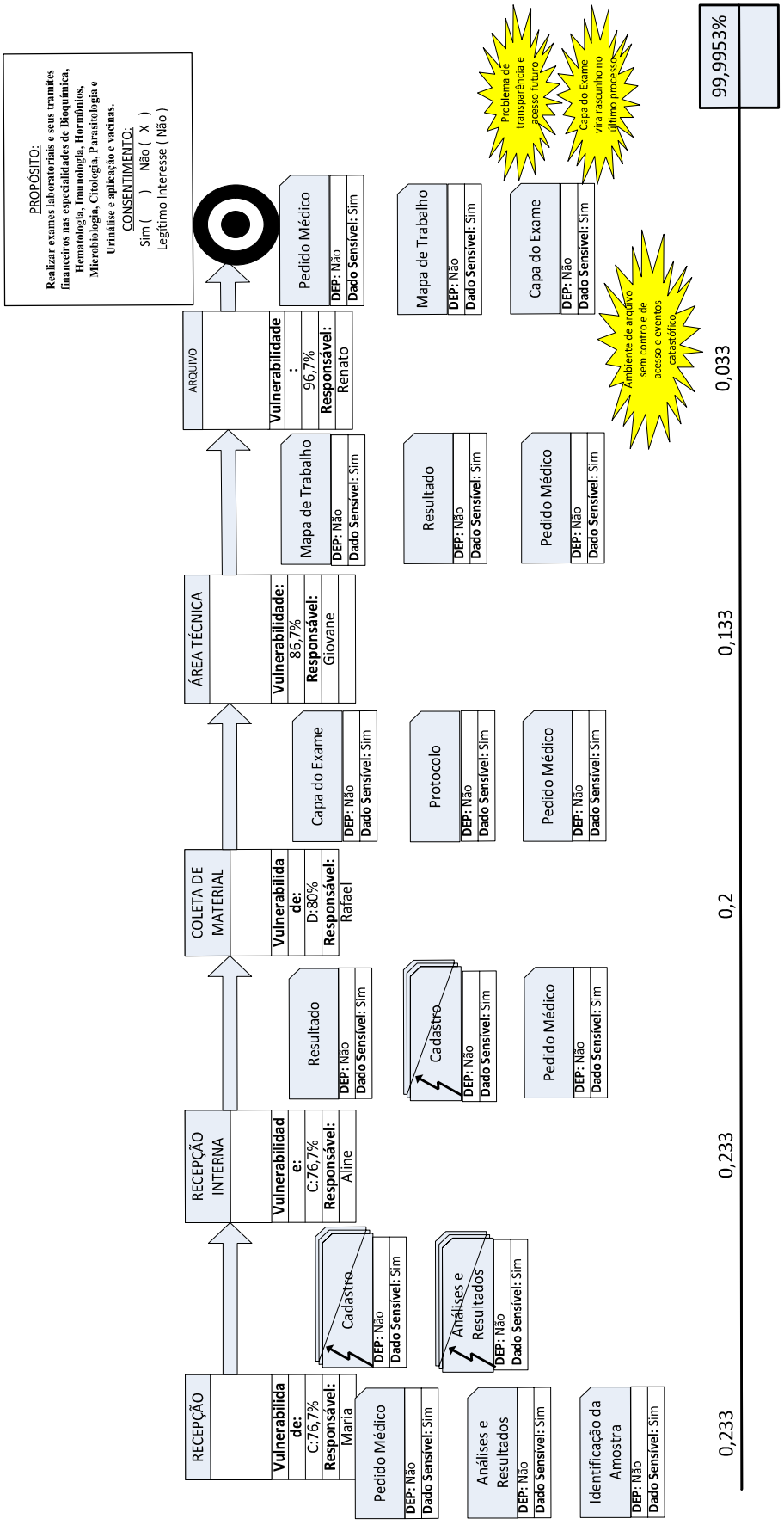
Nº	Código	Boas práticas	E1	E2	E3	E4	E5
1	C.1	As senhas expiram periodicamente (por exemplo, a cada XX dias)?	N	S	N	N	S
2	C.2	Existe duplo critério de autenticação?	N	N	N	N	N
3	C.3	Existe o mínimo de *firewalls* implantados em todas as conexões externas (por exemplo, Internet)?	S	S	N	N	N
4	C.4	Existe um processo / critério para avaliar o risco de protocolos / portas antes de implementá-los nos firewalls?	N	N	N	N	N
5	C.5	A informação crítica é classificada de acordo com uma diretriz de classificação (por exemplo, seguro, confidencial, público etc.)?	N	N	S	N	N
6	C.6	Existe um inventário dos ativos em posse da Empresa? Todos os dados críticos da empresa têm um proprietário?	S	N	N	S	N
7	C.7	Existe um processo de gestão auditoria e comunicado de vulnerabilidades técnicas ocorridas?	N	N	N	N	N
8	C.8	Existe uma política para tratar da segurança de dispositivos móveis (*PDAs, laptops, smartphones, pen drive*)?	S	N	S	N	N
9	C.9	Existe um controle de acesso nos sistemas de informações utilizados que garante que cada colaborador veja somente os dados pertinentes a ele?	N	N	N	N	N
10	C.10	Existem áreas seguras que protegem informações confidenciais?	N	S	S	N	N
11	C.11	Existe controle de acesso em áreas seguras? A entrada para áreas seguras é protegida?	N	N	N	N	N
12	C.12	Os acessos privilégios são restritos?	N	N	N	N	N
13	C.13	As áreas seguras estão localizadas de maneira protegida?	S	N	N	N	N
14	C.14	Existe orientação para os usuários sobre o que fazer quando não estão presentes em suas estações de trabalho ou contra desastres naturais ou atentados?	N	S	N	S	N
15	C.15	Existe uma prática de ambiente de trabalho, com mesa limpa de papéis, mídias móveis e tela limpa?	S	S	S	N	N
16	I.1	O *log* está ativado em todos os *firewalls*, roteadores e servidores *proxy*? Existe um processo para revisar os logs regularmente?	N	N	N	N	N
17	I.2	Existe uma auditoria regular realizada para contabilizar todas as fitas de *backup*?	N	N	N	N	N

18	I.3	Existe procedimento para controle bem como regras para instalação de softwares pelos usuários?	S	S	S	N	N
19	I.4	Periodicamente restaura informações de fitas de *backup* para garantir a integridade dos dados?	S	S	S	S	N
20	I.5	Os dados armazenados nos discos rígidos estão criptografados?	N	N	N	N	N
21	I.6	Existe uma fonte (relógio) de tempo precisa e sincronizada para os sistemas de processamento relevantes?	N	N	N	N	N
22	I.7	As informações são removidas adequadamente da mídia ou equipamento que serão descartados?	N	N	N	N	N
23	I.8	A remoção de informações e equipamentos para fora das instalações da organização é controlada?	N	N	N	N	N
24	I.9	Os alarmes, proteção contra incêndio e outros sistemas estão instalados?	N	N	N	N	N
25	I.10	Existe procedimentos e controles de contratação e desligamento de funcionários bem como suas permissões de acesso durante o período empregado?	N	N	N	N	N
26	D.1	Existem instalações de recuperação de desastres para sistemas críticos localizados em uma área geograficamente independente?	N	N	N	S	N
27	D.2	Os *backups* de dados críticos de negócios são feitos regularmente (pelo menos semanalmente)?	N	N	N	N	N
28	D.3	Uma análise de impacto nos negócios foi realizada em todos os aplicativos e sistemas dos clientes?	N	N	N	N	N
29	D.4	Existem planos de recuperação de desastres escritos formalmente (DRPs), cobrindo a perda parcial ou total de servidores, aplicações críticas, instalações físicas?	N	N	N	N	N
30	D.5	Os cabos de energia e telecomunicações e equipamentos em geral, estão adequadamente protegidos? Os equipamentos essenciais estão protegidos contra a falta de energia?	N	N	N	N	N
Índice de Vulnerabilidade			**23.3%**	**23.3%**	**20%**	**13.3%**	**3.3%**

Fonte: Elaborado pelo autor.

Por fim, para obter o índice de vulnerabilidade geral desta cadeia de valor, foi subtraído de 1 a multiplicação das porcentagens obtidas em cada etapa, o que nos resultou em: [1-(0,2333*0,2333*0,20*0,1333*0.0333)] = 99,995% de vulnerabilidade. A Figura 14 apresenta o MFV-SI-Atual.

Figura 14 - Caso 1: MFV-SI-Atual



Fonte: Elaborado pelo autor.

4.2.3 Mapeamento do Estado Futuro

Com o objetivo de projetar o estado futuro, a equipe envolvida no mapeamento da prova de conceito em questão, focou no desenvolvimento da tríade oferecida pelo modelo MFV-SI apresentada na Figura 9.

Em se tratando da melhoria dos valores do índice de vulnerabilidade, foram avaliadas as medidas de baixa e média complexidade de implementação no intuito de adotar medidas de boas práticas de segurança da informação física e virtualmente expostas. A ideia foi aproveitar o movimento positivo causado pelo mapeamento do estado atual bem como a mobilização da média e alta gerência.

Ao avaliar o propósito de valor do fluxo de trabalho, foi necessário adequar uma sistemática para divulgação do propósito da coleta de dados perante aos clientes, uma vez que, a empresa não o especificava clara e individualmente. Consequentemente o consentimento do fornecedor dos dados sobre o propósito em questão também passou a ser coletado para o atendimento do estado futuro projetado.

Já o dispositivo do legítimo interesse não pode ser usado para a dispensa do consentimento dos fornecedores de dados, pois ao responder as questões estabelecidas no Quadro 6, as questões 1 e 2 foram negativadas.

O Quadro 14 apresenta, com destaque em cor diferente, os pontos de melhoria escolhidos para a evolução do índice de vulnerabilidade.

Quadro 14 – Caso 1: Pontos de Melhoria do Índice de Vulnerabilidade

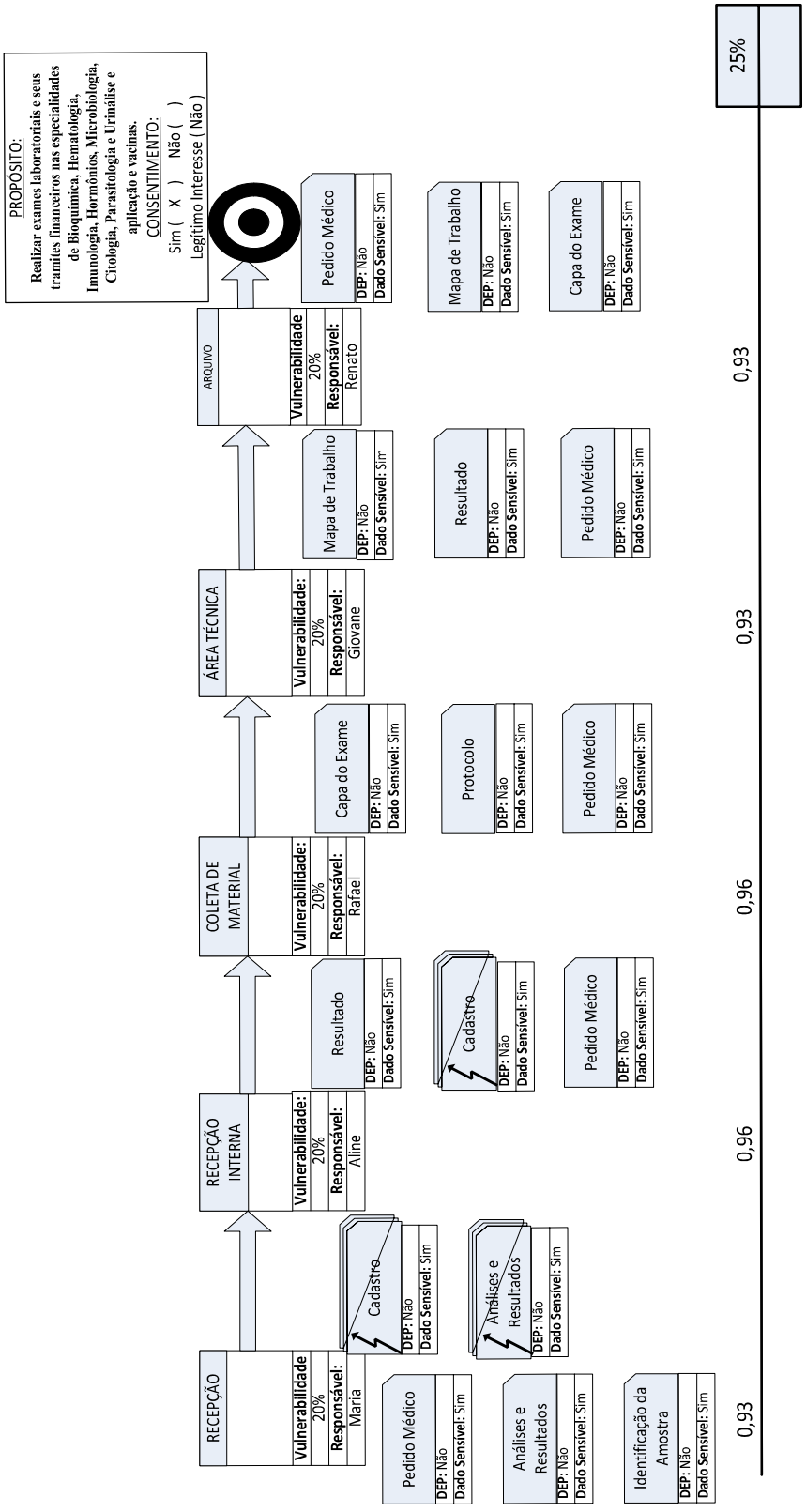
Nº	Código	P1	P2	P3	P4	P5
1	C.1	S	S	S	S	S
2	C.2	S	S	S	S	S
3	C.3	S	S	S	S	S
4	C.4	S	S	S	S	S
5	C.5	S	S	S	S	S
6	C.6	S	S	S	S	S
7	C.7	S	S	S	S	S
8	C.8	S	S	S	S	S
9	C.9	S	S	S	S	S
10	C.10	S	S	S	S	S
11	C.11	S	S	S	S	S
12	C.12	N	N	N	S	S
13	C.13	S	S	S	N	N
14	C.14	S	S	S	S	S
15	C.15	S	S	S	S	S
16	I.1	S	S	S	S	S
17	I.2	N	S	S	N	N

18	I.3	S	S	S	S	S
19	I.4	S	S	S	S	S
20	I.5	S	S	S	S	S
21	I.6	S	S	S	S	S
22	I.7	S	S	S	S	S
23	I.8	S	S	S	S	S
24	I.9	S	S	S	S	S
25	I.10	S	S	S	S	S
26	D.1	S	S	S	S	S
27	D.2	S	S	S	S	S
28	D.3	S	S	S	S	S
29	D.4	S	S	S	S	S
30	D.5	S	S	S	S	S
Índice Futuro		**93,3%**	**96,7%**	**96,7%**	**93,3%**	**93,3%**

Fonte: Elaborado pelo autor.

O índice de vulnerabilidade final proposto foi de 25,00% de vulnerabilidade, mediante ao cumprimento das ações estabelecidas pelo plano de ação. A partir de então, foi possível projetar o MFV-SI Futuro com as representações dos processos da forma como planejado. A Figura 15 apresenta o MFV-SI Futuro para o caso 1.

Figura 15 - Caso 1: MFV-SI-Futuro



Fonte: Elaborado pelo autor.

4.2.4 Plano de Ação

A construção do mapa futuro, desta prova de conceito, baseou-se na melhoria dos valores do índice de vulnerabilidade, pela implantação das boas práticas de segurança da informação bem como pelo estabelecimento do propósito do fluxo de valor ou do propósito da coleta do dado do indivíduo e da análise do consentimento de uso do dado obtido.

Na elaboração do plano de ação do caso 1, destaca-se as tratativas no processo de arquivamento no que diz respeito à proteção dos arquivos físicos, uma vez que não existe controle de acesso ou contra eventos catastróficos no setor de arquivamento.

Outro destaque é a reutilização da "Capa de Exame" como rascunho após o arquivamento do atendimento em questão. Ao utilizar o verso do papel como rascunho, os processos do fluxo de valor acabam gerando exposição do indivíduo através da circulação de dados de pacientes com os protocolos de atendimento encerrados.

Com a projeção do estado futuro concretizada, é possível traçar um plano de ação para alcança-lo. O Quadro 15 apresenta as ações necessárias para o alcance do estado futuro proposto, bem como seus respectivos prazos e responsáveis.

Quadro 15 – Caso 1: Plano de Ação

Ação	Prazo	Responsável
Digitalizar documentação de arquivo morto.	Out/2021	Arquivo
Implementar controle de acesso em arquivo morto.	Abr/2021	Direção
Implementar dispositivo contra incêndio em arquivo morto.	Mai/2021	Direção
Destruir e descartar capas de Exame pós arquivamento do processo.	Imediato	Área Técnica
Reduzir o índice de vulnerabilidade para 85%.	Jun/2021	TI
Coletar registro de consentimento para uso dos dados pessoais atrelado ao propósito do fluxo de valor.	Mar/2021	TI

Fonte: Elaborado pelo autor.

4.3 Prova de conceito 2: processo de contratação de colaboradores em uma indústria etiquetas e rótulos

A segunda prova de conceito ocorreu em uma indústria de etiqueta e rótulos adesivos, situada em uma cidade do interior do estado do Paraná, com aproximadamente 80 mil habitantes. A empresa pertence a um grupo de três unidades fabris no Brasil, e a unidade de análise, em questão, possui uma área de 12.500m² equipada com máquinas e processos de alta tecnologia, empregando em torno de 215 funcionários alocados em dois turnos diários. Atende

nacional e internacionalmente grandes *players* dos segmentos alimentícios, bebidas, higiene, limpeza, cosméticos, entre outros.

A escolha da unidade de análise, em questão, pretende avaliar um processo muito comum entre as pequenas e grandes empresas, o processo de contratação de colaboradores.

Seguindo as etapas de implementação apresentadas no Quadro 11, a seguir, são apresentadas a seleção da família do fluxo de valor e a avaliação do alinhamento do propósito do fluxo em questão, seguido pelos mapas do estado atual, futuro e o plano de ação.

4.3.1 Seleção da Família de Produtos

Em uma visita presencial à unidade de análise em questão, onde foram adotadas medidas de observação dos processos em execução e entrevista não estruturada com o gerente de TI e com o supervisor de recrutamento e seleção, foi discutido o fluxo operacional do processo de recrutamento e seleção de novos colaboradores, a partir de uma solicitação do gestor. O objetivo foi entender e constatar evidências do tráfego de dados, formas de armazenamento, proteção e propósito de obtenção.

Como resultado prévio, foram observadas seis etapas: alinhamento de demanda com gestor, captação de currículo, *check-in* portaria, entrevista com RH, validação com gestor e fechamento. Em seguida, para cada etapa do fluxo de valor, foram levantadas as entradas de informações representadas pelos chamados Blocos de Dados.

Para cada Bloco de Dados, foram aplicadas oito questões, apresentadas no Quadro 6, a fim de avaliar se o propósito do tratamento dos dados pode ou não ser baseado no legítimo interesse, ou se necessita de consentimento do usuário. O resultado foi negativo, uma vez que pelo menos uma das respostas foi negativa, necessitando a solicitação do consentimento do proprietário dos dados, conforme é possível avaliar no Quadro 16 abaixo.

Quadro 16 – Caso 2: Avaliação de Propósito e Legítimo Interesse

BLOCOS DE DADOS	**QUESTÕES DE AVALIAÇÃO DO PROPÓSITO/LEGÍTIMO INTERESSE**							
	1	**2**	**2.1**	**2.2**	**2.3**	**3**	**4**	**5**
Formulário de Abertura de Vaga	N	N	N	N	S	N	S	S
Currículo	S	N	S	S	S	N	S	S
Parecer Recrutamento e Seleção	N	N	N	N	S	N	S	S
Parecer Entrevista - Avaliações	N	N	N	N	S	N	S	S
Planilha de Controle de Entrada e Saída	S	N	N	N	S	N	S	S

Ficha de Contratação	N	N	N	N	S	N	S	S

BLOCO DE DADOS	**DETALHAMENTO DOS BLOCOS DE INFORMAÇÕES.**
Formulário de Abertura de Vaga	Data da solicitação, Tipo da Vaga, Motivo Contratação, Setor, Solicitante, Descr. Vaga, Benefícios, Horário de trab., Salário, Escolaridade, Experiência, Requisitos Técnicos, Conhecimentos técnicos, Perfil Comportamental, Idade e Sexo.
Currículo	Foto, Histórico de Trabalho, Idade, e-mail, Data Nascimento, Telefone, Histórico Acadêmico, Endereço.
Parecer Recrutamento e Seleção	Parecer do Psicólogo, Nome do Colaborador, Vaga, Escolaridade, Pretensão Salarial, Data Entrevista, Histórico Familiar, Experiência Profissional, Socioeconômico e Social.
Parecer Entrevista - Avaliações	Parecer do Psicólogo, Nome, Idade, Sexo, CPF, Local de Nascimento, Escolaridade.
Planilha de Controle de Entrada e Saída	Nome, CPG ou RG, Convidado por.
Ficha de Contratação	Data, Tipo Contratação, Filial, Gestor, Cargo, Setor, Nome Candidato, Data Nascimento, Rg, CPF, Telefones, Estado Civil, Filhos (Sim/Não/qtde/idade), Escolaridade, Salário, Horário de Trabalho, Meio de Transporte, Nº calçado, tamanho calça e camisa, assinatura.

Fonte: Elaborado pelo autor.

Dessa forma, esse fluxo de valor deverá obter o consentimento para o propósito estabelecido, que foi descrito como: contratar novos colaboradores para trabalho sob regime CLT ou PJ.

4.3.2 Mapeamento do Estado Atual

Após a coleta das respostas referentes às perguntas apresentadas no Quadro 17, obtivemos: 18 respostas positivas para etapa 1, 18 respostas positivas para etapa 2, 17 respostas positivas para etapa 3, 18 respostas positivas para etapa 4, 19 respostas positivas para a etapa 5 e 19 respostas positivas para a etapa 6. Dessa forma, o cálculo do índice de vulnerabilidade por etapa é dado por: 19/30=0,63; 19/30=0,63; 18/30=0,60; 19/30=0,63, 20/30=0,67 e 20/30=0,67 respectivamente.

O Quadro 17 apresenta as respostas obtidas para as questões de vulnerabilidade do estado atual.

Quadro 17 – Caso 2: Cálculo de Vulnerabilidade

Nº	**Código**	**Boas práticas**	**E1**	**E2**	**E3**	**E4**	**E5**	**E6**
1	C.1	As senhas expiram periodicamente (por exemplo, a cada XX dias)?	N	N	N	N	S	S
2	C.2	Existe duplo critério de autenticação?	N	N	N	N	N	N

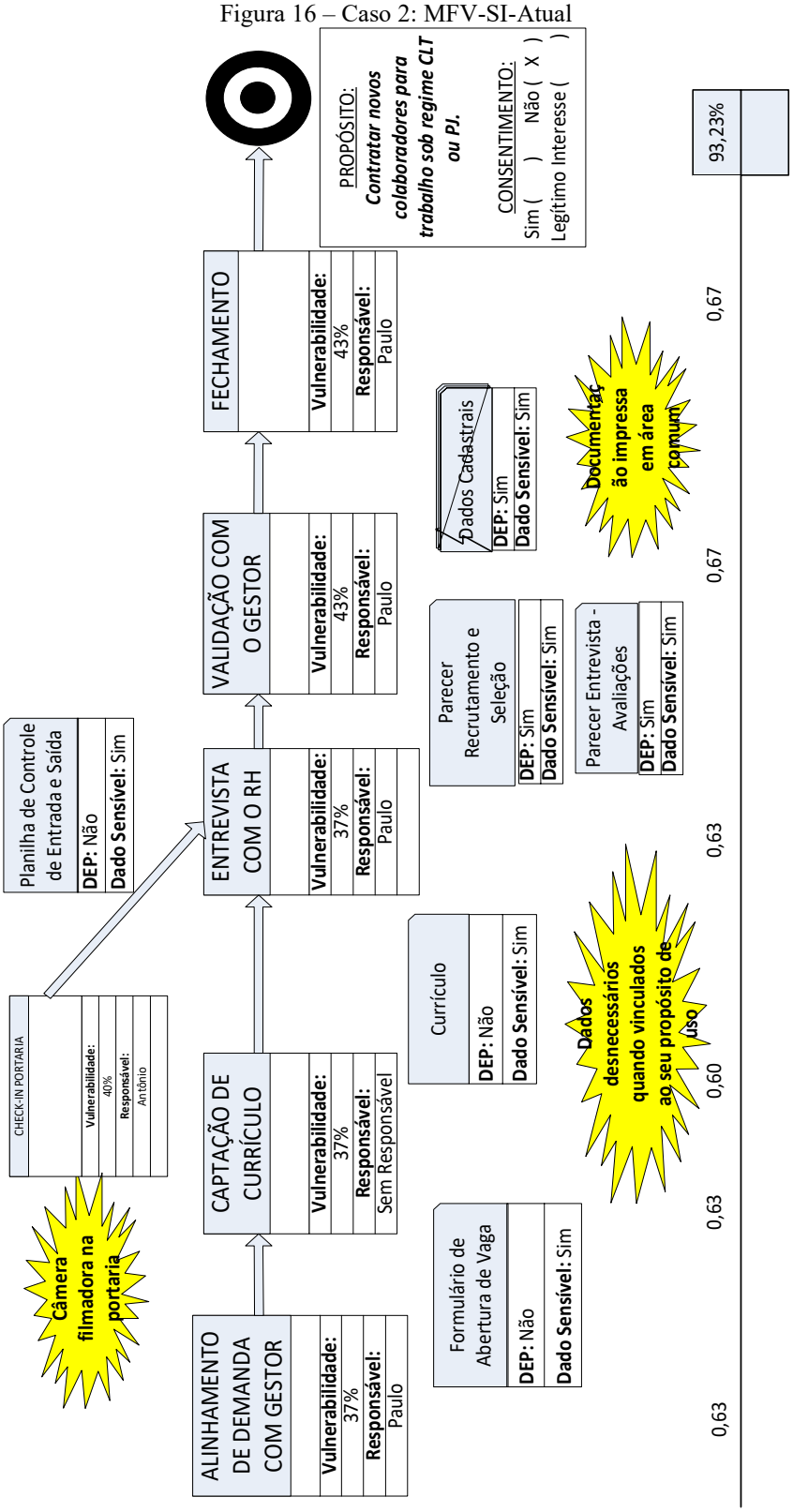
3	C.3	Existe o mínimo de *stateful firewalls* implantados em todas as conexões externas (por exemplo, Internet)?	S	S	N	S	S	S
4	C.4	Existe um processo / critério para avaliar o risco de protocolos / portas antes de implementá-los nos firewalls?	S	S	S	S	S	S
5	C.5	A informação crítica é classificada de acordo com uma diretriz de classificação (por exemplo, seguro, confidencial, público etc.)?	N	N	N	N	N	N
6	C.6	Existe um inventário dos ativos em posse da Empresa? Todos os dados críticos da empresa têm um proprietário?	N	N	N	N	N	N
7	C.7	Existe um processo de gestão auditoria e comunicado de vulnerabilidades técnicas ocorridas?	S	S	S	S	S	S
8	C.8	Existe uma política para tratar da segurança de dispositivos móveis (*PDAs*, *laptops, smartphones, pen drive)?*	N	N	N	N	N	N
9	C.9	Existe um controle de acesso nos sistemas de informações utilizados que garante que cada colaborador veja somente os dados pertinentes a ele?	S	S	S	S	S	S
10	C.10	Existem áreas seguras que protegem informações confidenciais?	S	S	S	S	S	S
11	C.11	Existe controle de acesso em áreas seguras? A entrada para áreas seguras é protegida?	S	S	S	S	S	S
12	C.12	Os acessos privilégios são restritos?	S	S	S	S	S	S
13	C.13	As áreas seguras estão localizadas de maneira protegida?	S	S	S	S	S	S
14	C.14	Existe orientação para os usuários sobre o que fazer quando não estão presentes em suas estações de trabalho ou contra desastres naturais ou atentados?	N	N	N	N	N	N
15	C.15	Existe uma prática de ambiente de trabalho, com mesa limpa de papéis, mídias móveis e tela limpa?	S	S	S	S	S	S
16	I.1	O log está ativado em todos os *firewalls,* roteadores e servidores *proxy*? Existe um processo para revisar os *logs* regularmente?	S	S	S	S	S	S
17	I.2	Existe uma auditoria regular realizada para contabilizar todas as fitas de *backup*?	N	N	N	N	N	N
18	I.3	Existe procedimento para controle bem como regras para instalação de *softwares* pelos usuários?	S	S	S	S	S	S
19	I.4	Periodicamente restaura informações de fitas de *backup* para garantir a integridade dos dados?	N	N	N	N	N	N
20	I.5	Os dados armazenados nos discos rígidos estão criptografados?	N	N	N	N	N	N
21	I.6	Existe uma fonte (relógio) de tempo precisa e sincronizada para os sistemas de processamento relevantes?	S	S	S	S	S	S
22	I.7	As informações são removidas adequadamente da mídia ou equipamento que serão descartados?	N	N	N	N	N	N
23	I.8	A remoção de informações e equipamentos para fora das instalações da organização é controlada?	N	N	N	N	N	N
24	I.9	Os alarmes, proteção contra incêndio e outros sistemas estão instalados?	S	S	S	S	S	S
25	I.10	Existe procedimentos e controles de contratação e desligamento de funcionários bem como suas permissões de acesso durante o período empregado?	S	S	S	S	S	S
26	D.1	Existem instalações de recuperação de desastres para sistemas críticos localizados em uma área geograficamente independente?	S	S	S	S	S	S
27	D.2	Os *backups* de dados críticos de negócios são feitos regularmente (pelo menos semanalmente)?	S	S	S	S	S	S

28	D.3	Uma análise de impacto nos negócios foi realizada em todos os aplicativos e sistemas dos clientes?	S	S	S	S	S	S
29	D.4	Existem planos de recuperação de desastres escritos formalmente (DRPs), cobrindo a perda parcial ou total de servidores, aplicações críticas, instalações físicas?	S	S	S	S	S	S
30	D.5	Os cabos de energia e telecomunicações e equipamentos em geral, estão adequadamente protegidos? Os equipamentos essenciais estão protegidos contra a falta de energia?	S	S	S	S	S	S
Índice de Vulnerabilidade			**0,63**	**0,63**	**0,60**	**0,63**	**0,67**	**0,67**

Fonte: Elaborado pelo autor.

Por fim, para obter o índice de vulnerabilidade geral desta cadeia de valor, foi subtraído de 1 a multiplicação das porcentagens obtidas em cada etapa, o que nos resultou em: [1-(0,63*0,63*0,60*0,670,67*0,67)] = 93,23% de vulnerabilidade. A Figura 14 apresenta o MFV-SI-Atual.

Figura 16 – Caso 2: MFV-SI-Atual



Fonte: Elaborado pelo autor.

4.3.3 Mapeamento do Estado Futuro

O mapeamento do estado futuro sucede a elaboração do mapa atual projetando uma melhoria de processo.

Baseado na tríade oferecida pelo modelo MFV-SI apresentada na Figura 9, foi possível projetar o estado futuro. Em se tratando da melhoria dos valores do índice de vulnerabilidade foram avaliadas as de maior impacto e menor dificuldade de implementação. A ideia foi aproveitar o engajamento causado pelo mapeamento do estado atual bem como a mobilização da média e alta gerência.

Em se tratando do propósito da coleta do dado, o mesmo não estava estabelecido e divulgado aos candidatos. Fez se necessário adequar uma sistemática para divulgação do propósito da coleta de dados. O consentimento do fornecedor dos dados, no caso candidatos à um vaga de trabalho, também passou a ser coletado para o atendimento do estado futuro projetado. Neste sentido uma situação crítica era estabelecida no memento de ingresso do candidato nas dependências da empresa para a realização das entrevistas. Ao passar pela portaria, o processo estabelecia a obrigatoriedade da coleta do nome, CPF e a captura de uma foto, sem qualquer justificativa para coleta de tais dados.

Já o dispositivo do legitimo interesse não pode ser usado para a dispensa do consentimento dos usuários, pois ao responder as questões estabelecidas no Quadro 6, as questões 2; 2.1; 2.3 e 4 foram negativadas.

Outro ponto de destaque nas resoluções encontradas, diz respeito à coleta e tratamento de dados além do propósito estabelecido, mesmo este impreciso, não divulgado e não consentido, foi possível identificar dados que não seriam necessários para o processo de contratação. Tais dados extra propósito foram encontrados nos blocos de dados “Dados Cadastrais”, “Parecer Recrutamento e Seleção” e “Parecer Entrevista- Avaliações”.

O Quadro 18 apresenta, com destaque em cor diferente, os pontos de melhoria escolhidos para a evolução do índice de vulnerabilidade.

Quadro 18 - Caso 2: Pontos de Melhoria do Índice de Vulnerabilidade

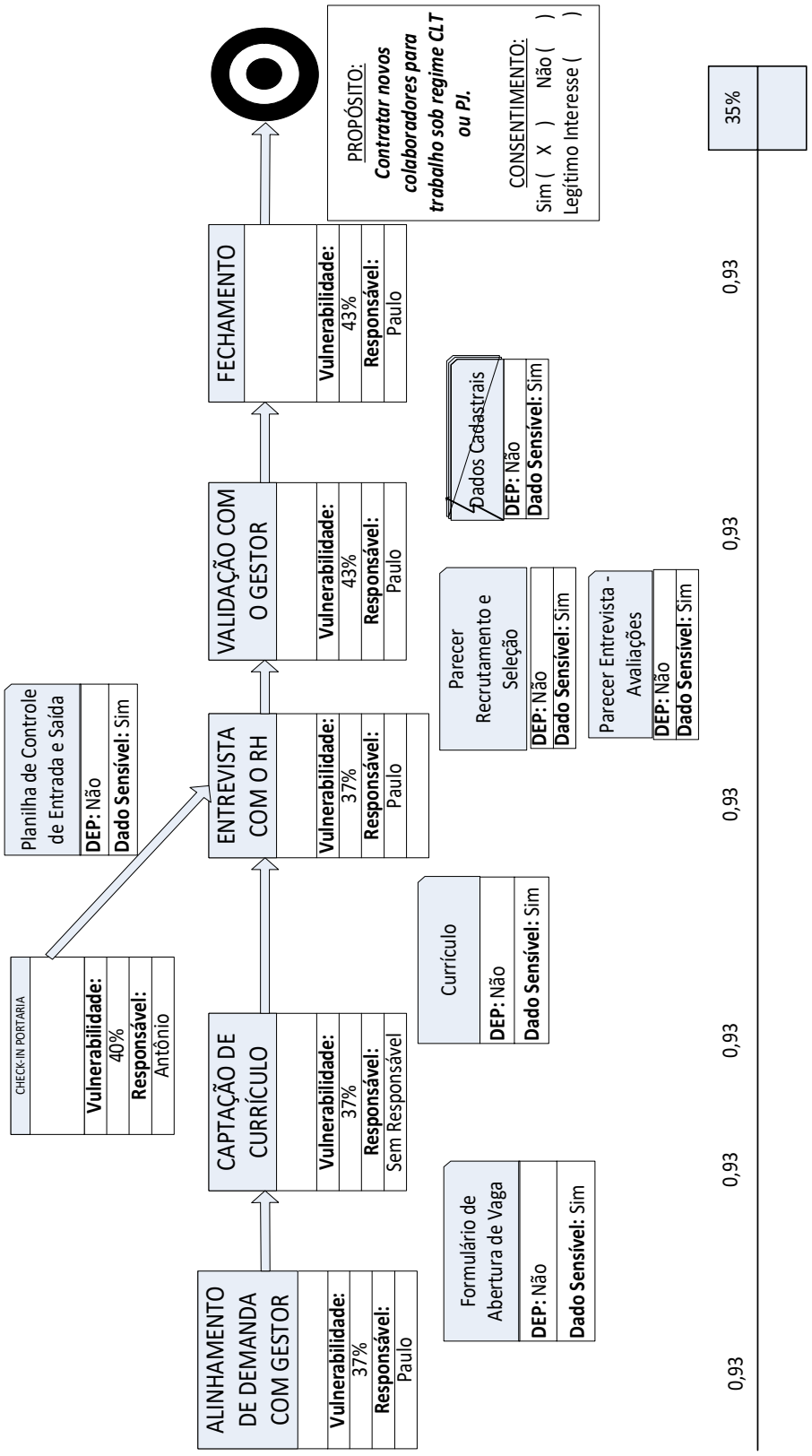
Nº	Código	E1	E2	E3	E4	E5	E6
1	C.1	S	S	S	S	S	S
2	C.2	S	S	S	S	S	S
3	C.3	S	S	S	S	S	S
4	C.4	S	S	S	S	S	S
5	C.5	S	S	S	S	S	S
6	C.6	S	S	S	S	S	S
7	C.7	S	S	S	S	S	S

8	C.8	S	S	S	S	S	S
9	C.9	S	S	S	S	S	S
10	C.10	S	S	S	S	S	S
11	C.11	S	S	S	S	S	S
12	C.12	S	S	S	S	S	S
13	C.13	S	S	S	S	S	S
14	C.14	S	S	S	S	S	S
15	C.15	S	S	S	S	S	S
16	I.1	S	S	S	S	S	S
17	I.2	N	N	N	N	N	N
18	I.3	S	S	S	S	S	S
19	I.4	N	N	N	N	N	N
20	I.5	S	S	S	S	S	S
21	I.6	S	S	S	S	S	S
22	I.7	S	S	S	S	S	S
23	I.8	S	S	S	S	S	S
24	I.9	S	S	S	S	S	S
25	I.10	S	S	S	S	S	S
26	D.1	S	S	S	S	S	S
27	D.2	S	S	S	S	S	S
28	D.3	S	S	S	S	S	S
29	D.4	S	S	S	S	S	S
30	D.5	S	S	S	S	S	S
Índice Futuro		**0,93**	**0,93**	**0,93**	**0,93**	**0,93**	**0,93**

Fonte: Elaborado pelo autor.

O índice de vulnerabilidade final proposto foi de 35,00% de vulnerabilidade, mediante ao cumprimento das ações estabelecidas pelo plano de ação. A partir de então, foi possível projetar o MFV-SI Futuro com as representações dos processos da forma como planejado. A Figura 17 apresenta o MFV-SI Futuro para o caso 2.

Figura 17 - Caso 2: MFV-SI-Futuro



Fonte: Elaborado pelo autor.

4.3.4 Plano de Ação

A construção do mapa futuro norteou-se pela melhoria dos valores do índice de vulnerabilidade e pela implantação das boas práticas de segurança da informação.

Na prova de conceito 2, colocou-se em destaque duas situações: a obtenção de imagens das câmeras de segurança na portaria sem consentimento, e a coleta e tratamento de dados pessoais além do propósito estabelecido, encontrados nos blocos de dados “Dados Cadastrais”, “Parecer Recrutamento e Seleção” e “Parecer Entrevista- Avaliações”.

Sobre o índice de vulnerabilidade o valor final proposto foi de 35% de vulnerabilidade, mediante ao cumprimento das ações estabelecidas. Com a projeção do estado futuro concretizada, é possível traçar um plano de ação para alcançá-lo. O Quadro 19 apresenta as ações necessárias para o alcance do estado futuro proposto, bem como seus respectivos prazos e responsáveis.

Quadro 19 - Caso 2: Plano de Ação

Ação	Prazo	Responsável
Obter consentimento do candidato para a coleta e tratamento de dados e imagem.	Abr/2021	RH
Simplificar e eliminar dados extra propósito dos blocos de dados “Dados Cadastrais”, “Parecer Recrutamento e Seleção” e “Parecer Entrevista - Avaliações”	Abr/2021	RH
Reduzir o índice de vulnerabilidade para 35%.	Jun/2021	TI

Fonte: Elaborado pelo autor.

4.4 Prova de conceito 3: processo de manutenção e garantia em uma montadora de computadores

A terceira prova de conceito ocorreu em uma indústria montadora de minicomputadores e *apliance* de *firewall.* Situada na cidade de Maringá, no interior do estado do Paraná, com aproximadamente 380 mil habitantes, a empresa possui uma área de 2.500m² e emprega atualmente 13 funcionários.

A escolha da unidade de análise, em questão, pretende avaliar um processo suporte e garantia de produtos vendidos, processo esse exigido por lei para a indústria de computadores. Seguindo o roteiro de implementação do MFV-SI, apresentadas no Quadro 11, as subseções posteriores apresentarão a seleção do fluxo de valor, a avaliação do propósito do fluxo, seguido pelos mapas do estado atual, futuro e o plano de ação.

4.4.1 Seleção da Família de Produtos

Em uma visita presencial à unidade de análise em questão, onde foram adotadas medidas de observação dos processos em execução e realizada entrevista não estruturada com o gerente de produção e com o técnico em análise de *hardware*, foi possível entender o fluxo operacional, produzindo um esboço do MFV-SI, e constatar evidências do tráfego de dados, formas de armazenamento, proteção e propósito de obtenção.

Para a aplicação do MFV-SI, foi escolhida a cadeia de valor de RMA, processo responsável de tratar as manutenções de equipamentos dentro e fora de garantia, composta por cinco etapas, sendo: entrada de mercadoria, diagnóstico, orçamento/aprovação, reparo/testes e faturamento/expedição. Em seguida, para cada etapa do fluxo de valor foi levantado as entradas de informações, representadas pelos chamados Blocos de Dados.

Para cada Bloco de Dados, foram aplicadas oito questões apresentadas no Quadro 6, a fim de avaliar se o propósito do tratamento dos dados pode ou não ser baseado no legítimo interesse, ou se necessita de consentimento do usuário. Após a aplicação das questões para avaliação da proposição do legítimo interesse apresentadas no Quadro 20, foi possível observar que todas as respostas foram positivas, ou seja, este fluxo de valor poderá lançar mão do legítimo interesse no tratamento de dados, uma vez que os mesmos atendem aos requisitos elementares.

Sendo assim, esse fluxo de valor não necessitará obter o consentimento do dono do dado para que a empresa o utilize para o propósito estabelecido, como: solucionar as exigências legais relacionadas à garantia de equipamentos de informática e às manutenções fora de garantia aprovadas pelo cliente.

Quadro 20 – Caso 3: Avaliação de Propósito e Legítimo Interesse

BLOCOS DE DADOS	**QUESTÕES DE AVALIAÇÃO DO PROPÓSITO/LEGÍTIMO INTERESSE**							
	1	**2**	**2.1**	**2.2**	**2.3**	**3**	**4**	**5**
Declaração de Isenção de I.E.	S	S	S	S	S	S	S	S
Ordem de Serviço	S	S	S	S	S	S	S	S
Análise e Parecer Técnico	S	S	S	S	S	S	S	S
E-mail de aceite ou recusa	S	S	S	S	S	S	S	S
Minuta de Despacho	S	S	S	S	S	S	S	S
NF	S	S	S	S	S	S	S	S
BLOCO DE DADOS	**DETALHAMENTO DOS BLOCOS DE INFORMAÇÕES.**							

Declaração de Isenção de I.E.	Nome, CPF, RG, telefones, e-mail e endereço.
Ordem de Serviço	Nº Ordem, Data da Emissão, Cidade, Nome, CPF, RG, telefones, e-mail e endereço, descrição do prod., quantidade do prod. e valor do produto.
Análise e Parecer Técnico	Nº Ordem, Data da Emissão, Cidade, Nome, CPF, RG, telefones, e-mail e endereço, descrição do prod., quantidade do prod. e valor do prod., Defeito Relatado.
E-mail de aceite ou recusa	Nome, e-mail.
Minuta de Despacho	Nº Ordem, Data da Emissão, Cidade, Nome, CPF, RG, telefones, e-mail e endereço, descrição do prod., quantidade do prod. e valor do produto.
NF	Nº Ordem, Data da Emissão, Cidade, Nome, CPF, RG, telefones, e-mail e endereço, descrição do prod., quantidade do prod. e valor do produto.

Fonte: Elaborado pelo autor.

4.4.2 Mapeamento do Estado Atual

O processo do mapeamento do estado atual iniciou-se com as respostas das perguntas estabelecidas no Quadro 21, onde obtivemos: seis respostas positivas para etapa 1, quatro respostas positivas para etapa 2, quatro respostas positivas para etapa 3, quatro respostas positivas para etapa 4 e seis respostas positiva para a etapa 5.

Dessa forma, o cálculo do índice de vulnerabilidade por etapa é dado por: 6/30=0,20; 4/30=0,13; 4/30=0,13; 4/30=0,13 e 6/30=0,20 respectivamente.

O Quadro 21 apresenta as respostas obtidas para as questões de vulnerabilidade do estado atual.

Quadro 21 – Caso 3: Cálculo de Vulnerabilidade

Nº	**Cód.**	**Boas práticas**	**P1**	**P2**	**P3**	**P4**	**P5**
1	C.1	As senhas expiram periodicamente (por exemplo, a cada XX dias)?	N	N	N	N	N
2	C.2	Existe duplo critério de autenticação?	N	N	N	N	N
3	C.3	Existe o mínimo de stateful *firewalls* implantados em todas as conexões externas (por exemplo, Internet)?	S	S	S	S	S
4	C.4	Existe um processo / critério para avaliar o risco de protocolos / portas antes de implementá-los nos firewalls?	S	N	N	N	S
5	C.5	A informação crítica é classificada de acordo com uma diretriz de classificação (por exemplo, seguro, confidencial, público etc.)?	N	N	N	N	N
6	C.6	Existe um inventário dos ativos em posse da Empresa? Todos os dados críticos da empresa têm um proprietário?	N	N	N	N	N
7	C.7	Existe um processo de gestão auditoria e comunicado de vulnerabilidades técnicas ocorridas?	N	N	N	N	N

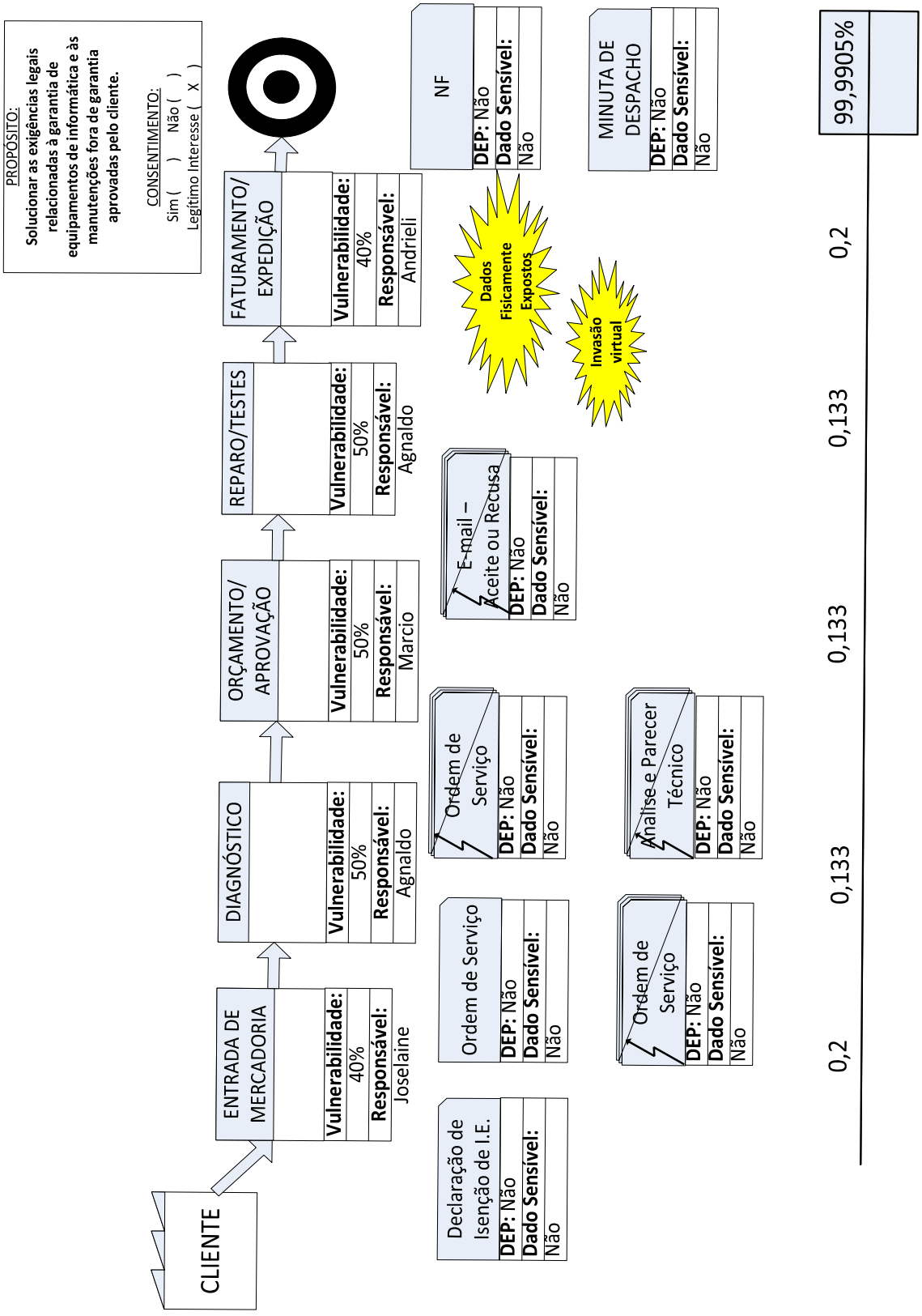
8	C.8	Existe uma política para tratar da segurança de dispositivos móveis (*PDAs, laptops, smartphones, pen drive*)?	N	N	N	N	N
9	C.9	Existe um controle de acesso nos sistemas de informações utilizados que garante que cada colaborador veja somente os dados pertinentes a ele?	S	S	S	S	S
10	C.10	Existem áreas seguras que protegem informações confidenciais?	N	N	N	N	N
11	C.11	Existe controle de acesso em áreas seguras? A entrada para áreas seguras é protegida?	N	N	N	N	N
12	C.12	Os acessos privilegiados são restritos?	S	S	S	S	S
13	C.13	As áreas seguras estão localizadas de maneira protegida?	N	N	N	N	N
14	C.14	Existe orientação para os usuários sobre o que fazer quando não estão presentes em suas estações de trabalho ou contra desastres naturais ou atentados?	N	N	N	N	N
15	C.15	Existe uma prática de ambiente de trabalho com mesa limpa de papéis, mídias móveis e tela limpa?	N	N	N	N	N
16	I.1	O log está ativado em todos os *firewalls*, roteadores e servidores *proxy*? Existe um processo para revisar os logs regularmente?	S	N	N	N	s
17	I.2	Existe uma auditoria regular realizada para contabilizar todas as fitas de *backup*?	N	N	N	N	N
18	I.3	Existe procedimento para controle bem como regras para instalação de *softwares* pelos usuários?	N	N	N	N	N
19	I.4	Periodicamente restaura informações de fitas de *backup* para garantir a integridade dos dados?	N	N	N	N	N
20	I.5	Os dados armazenados nos discos rígidos estão criptografados?	N	N	N	N	N
21	I.6	Existe uma fonte (relógio) de tempo precisa e sincronizada para os sistemas de processamento relevantes?	N	N	N	N	N
22	I.7	As informações são removidas adequadamente da mídia ou equipamento que serão descartados?	N	N	N	N	N
23	I.8	A remoção de informações e equipamentos para fora das instalações da organização é controlada?	N	N	N	N	N
24	I.9	Os alarmes, proteção contra incêndio e outros sistemas estão instalados?	N	N	N	N	N
25	I.10	Existe procedimentos e controles de contratação e desligamento de funcionários, bem como suas permissões de acesso durante o período empregado?	N	N	N	N	N
26	D.1	Existem instalações de recuperação de desastres para sistemas críticos localizados em uma área geograficamente independente?	N	N	N	N	N
27	D.2	Os *backups* de dados críticos de negócios são feitos regularmente (pelo menos semanalmente)?	S	S	S	S	S
28	D.3	Uma análise de impacto nos negócios foi realizada em todos os aplicativos e sistemas dos clientes?	N	N	N	N	N
29	D.4	Existem planos de recuperação de desastres escritos formalmente (DRPs), cobrindo a perda	N	N	N	N	N

		parcial ou total de servidores, aplicações críticas, instalações físicas?					
30	D.5	Os cabos de energia e telecomunicações e equipamentos em geral, estão adequadamente protegidos? Os equipamentos essenciais estão protegidos contra a falta de energia?	N	N	N	N	N
Índice de Vulnerabilidade			**20,0%**	**13,3%**	**13,3%**	**13,3%**	**20,0%**

Fonte: Elabora pelo autor.

Por fim, para obter o índice de vulnerabilidade geral desta cadeia de valor, foi subtraído de 1 a multiplicação das porcentagens obtidas em cada etapa, o que nos resultou em: [1-(0,20*0,13*0,13*0,13*0,20)] = 99,9905% de vulnerabilidade. A Figura 18 apresenta o MFV-SI-Atual.

Figura 18 – Caso 3: MFV-SI Estado Atual



Fonte: Elaborado pelo autor.

4.4.3 Mapeamento do Estado Futuro

Da mesma forma a modelagem do estado futuro da terceira prova de conceito baseou-se na tríade oferecida pelo modelo MFV-SI apresentada na Figura 9.

Em se tratando da melhoria dos valores do índice de vulnerabilidade foi realizada uma força tarefa no intuito que implementar boa parte das medidas de boas práticas de segurança da informação fisicamente e virtualmente expostas. A ação foi motivada pela visão da alta direção em se adequar à lei vigente, antevendo possíveis danos aos clientes e à empresa.

Ao avaliar o propósito de valor do fluxo de trabalho, foi necessário adequar uma sistemática para divulgação do propósito da coleta de dados para os clientes, uma vez que, a empresa não o especificava claramente. Já consentimento do fornecedor dos dados sobre o propósito em questão foi, justificadamente, desprezado, uma vez que o dispositivo do legítimo interesse pode ser acionado para sua dispensa. Todas as questões estabelecidas no Quadro 6, foram positivadas.

O Quadro 22 apresenta com destaque em cor diferente, os pontos de melhoria escolhidos para a evolução do índice de vulnerabilidade.

Quadro 22 - Caso 3: Pontos de Melhoria do Índice de Vulnerabilidade

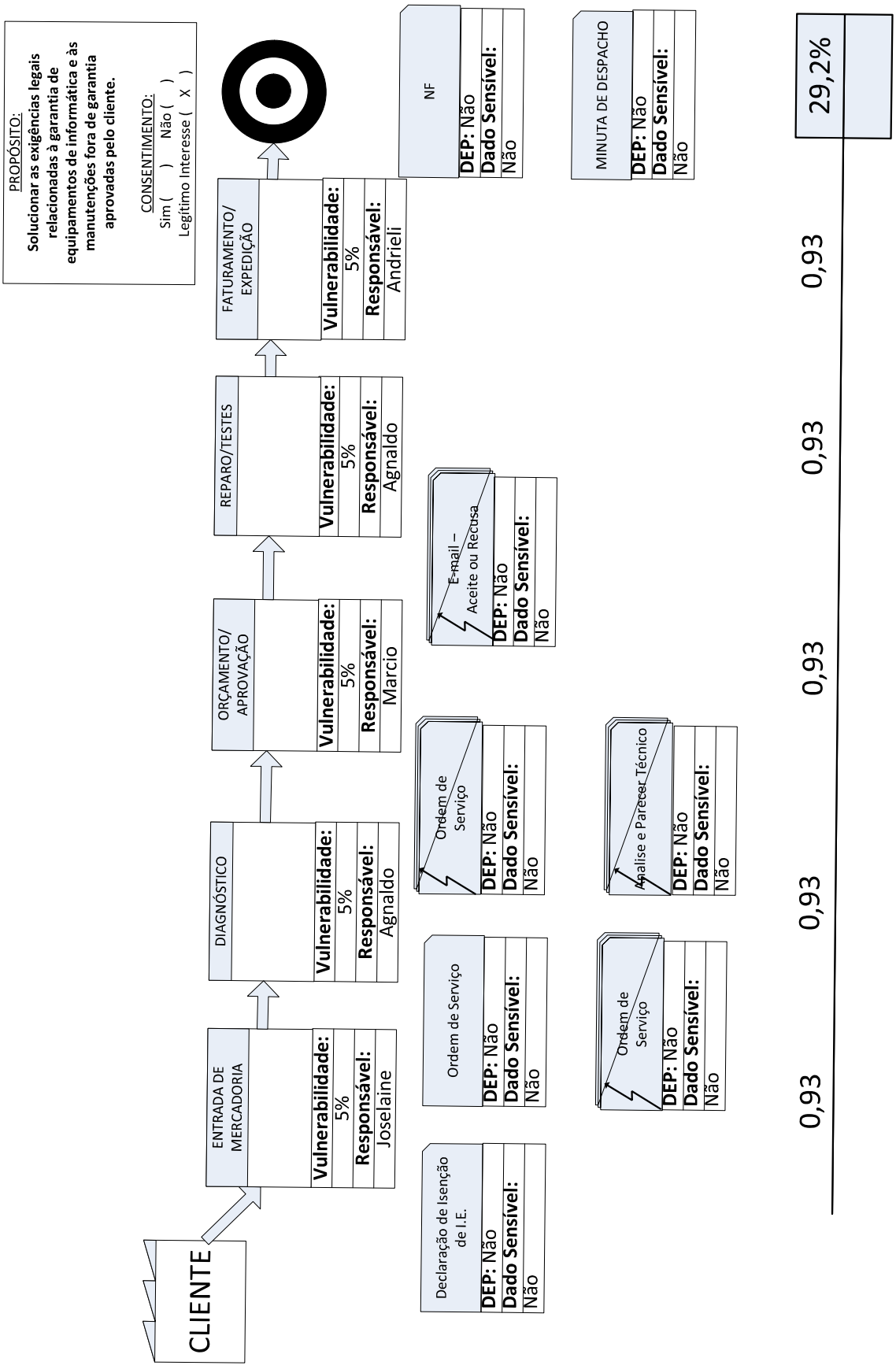
Nº	Código	P1	P2	P3	P4	P5
1	C.1	S	S	S	S	S
2	C.2	S	S	S	S	S
3	C.3	S	S	S	S	S
4	C.4	S	S	S	S	S
5	C.5	S	S	S	S	S
6	C.6	S	S	S	S	S
7	C.7	S	S	S	S	S
8	C.8	S	S	S	S	S
9	C.9	S	S	S	S	S
10	C.10	S	S	S	S	S
11	C.11	S	S	S	S	S
12	C.12	S	S	S	S	S
13	C.13	S	S	S	S	S
14	C.14	S	S	S	S	S
15	C.15	S	S	S	S	S
16	I.1	s	S	S	S	s
17	I.2	S	S	S	S	S
18	I.3	S	S	S	S	S
19	I.4	S	S	S	S	S
20	I.5	S	S	S	S	S
21	I.6	S	S	S	S	S
22	I.7	S	S	S	S	S
23	I.8	N	N	N	N	N
24	I.9	N	N	N	N	N
25	I.10	S	S	S	S	S

26	D.1	S	S	S	S	S
27	D.2	S	S	S	S	S
28	D.3	S	S	S	S	S
29	D.4	S	S	S	S	S
30	D.5	S	S	S	S	S
Índice Futuro		**93,3%**	**93,3%**	**93,3%**	**93,3%**	**93,3%**

Fonte: Elaborado pelo autor.

O índice de vulnerabilidade final proposto foi de 29,20% de vulnerabilidade, mediante ao cumprimento das ações estabelecidas pelo plano de ação. A partir de então, foi possível projetar o MFV-SI Futuro com as representações dos processos da forma como planejado. A Figura 19 apresenta o MFV-SI Futuro para o caso 3.

Figura 19 – Caso 3: MFV-SI Estado Futuro



Fonte: Elaborado pelo autor.

4.4.4 Plano de Ação

O mapeamento do estado futuro sucede a elaboração do mapa atual projetando uma melhoria de processo. A construção do mapa futuro norteou-se pela melhoria do índice de vulnerabilidade e pela implantação das boas práticas de segurança da informação.

No plano de ação do caso 3 destaca-se a existência do legítimo interesse pela coleta de dados, fomentado por sua vez, pelo baixo volume de dados coletados e pela execução de uma atividade, a garantia dos produtos, legalmente estabelecida. Ao cumprir com a obrigação legal de atender às solicitações de reparo dentro da garantia, a empresa em questão precisa e coleta os dados necessários para a realização do conserto ou troca.

Sobre o índice de vulnerabilidade o valor final proposto foi de 29.20% de vulnerabilidade, mediante ao cumprimento das ações no plano de ação.

Com a projeção do estado futuro concretizada, é possível traçar um plano de ação para alcançá-lo. O Quadro 23 apresenta as ações necessárias para o alcance do estado futuro proposto, bem como seus respectivos prazos e responsáveis.

Quadro 23 - Caso 3: Plano de Ação

Ação	Prazo	Responsável
Adotar política de mesa limpa e organização dos departamentos envolvidos	Abr/2021	RMA
Eliminar Ordem de Serviço no modelo impresso.	Abr/2021	RMA
Reduzir o índice de vulnerabilidade para 22%.	Jun/2021	TI

Fonte: Elaborado pelo autor.

4.5 Análise dos resultados

Declarado o objetivo geral desta pesquisa como a elaboração o Mapa de Fluxo de Valor – Segurança da Informação (MFV-SI), à luz dos requisitos da LGPD, a primeira contribuição, a ser pontuada, está relacionada aos aspectos sociais da gestão de cadeia de valor. Nesse sentido a análise realizada pelo Quadro 2, Relações entre GI, requisitos da LGPD e desperdícios no LIM, ajuda a entender que mediante ao surgimento de uma nova Lei a LGPD, surge então a necessidade de se classificar uma nova classe de desperdício, o desperdício da vulnerabilidade dos dados pessoais.

Uma das contribuições do estudo está relacionada à adaptação do MFV aos requisitos da LGPD. O Quadro 3, Ferramentas de modelagem de processos x requisitos da LGPD, auxiliou

na análise de sete requisitos considerados básicos para que qualquer modelo de mapeamento de processo estivesse pré-condicionado a contribuir com os aspectos sociais atrelados à nova lei. Nessa análise, o MFV se posicionou como a ferramenta de maior potencialidade entre todas as avaliadas, uma vez que, a princípio, apenas dois cenários não seriam atendidos pelo MFV: o de garantia do tratar somente dados essenciais para a realização de sua(s) finalidade(s) e a análise quantitativa de riscos. Vale ressaltar que nenhuma das outras 12 ferramentas de mapeamento contemplavam esses dois requisitos. No entanto, ao aplicar os estudos de caso, as novas representações gráficas, propostas pelo modelo MFV-SI, proporcionaram o atendimento dos requisitos anteriormente não atendidos. Tais representações gráficas, apresentadas na Figura 10, mostraram-se práticas no momento do mapeamento e intuitivas em sua compreensão.

Sobre os fundamentos do MFV, o Quadro 4, Fundamentos do MFV e os requisitos da LGPD, foi posto à prova nas provas de conceito. Em todos os estudos, os fundamentos do MFV se mostraram sólidos, perpetuando seu propósito de mapear a percepção de valor. Já o nível de detalhamento de desenho do mapa, que em grande parte depende da experiência do mapeador, uma vez que "Olhar muito de longe significa não ser capaz de enxergar precisamente o estado atual e não ter visão de futuro. Olhar muito de perto implica enxergar apenas melhorias pontuais e não sistêmicas" (FERRO, 2005), foi de certa forma balizado pela escrita do propósito do fluxo de valor em questão. Nos três estudos, por mais óbvio que parecesse ser, nenhuma das empresas possuíam um consenso estabelecido e claramente declarado sobre o porquê e para que tais dados estariam sendo tratados. Tal fato pode ser comprovado pela frequência dos chamados "Dados Extra Propósito" explicitados no MFV-SI-Atual dos casos 1 e 2.

Para cada um dos requisitos da lei apontados pelo Quadro 4, é possível identificar uma contribuição concreta após a aplicação do modelo MFV-SI.

Sobre o Art. 37, que diz que "O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse" (BRASIL, 2018a), podemos evidenciar a importância da análise do legítimo interesse, feita através da aplicação das oito questões elaboradas e apresentadas no Quadro 14. Durante a aplicação dos estudos de caso, foi possível perceber o aumento da confiança dos gestores e controladores de dados em se apoiar nessas evidências como argumento do declínio na obtenção do consentimento dos usuários.

Já os artigos 5 e 38 da lei, que tratam sobre a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), onde explicam que a autoridade nacional poderá solicitar documentação ao controlador, e que tal relatório deverá descrever como os processos de tratamento podem gerar riscos às liberdades civis e aos direitos fundamentais, medidas,

salvaguardas e mecanismos de mitigação de risco, também foram abordados de supridos organicamente pelo novo modelo. Com o apoio do procedimento estabelecidos no Quadro 11, nos três estudos de caso foi possível observar a contribuição do MFV-SI para o RIPD, na comparação dos índices de vulnerabilidade entre o estado atual e o futuro, na descrição graficamente simples e intuitiva das etapas, a expliciticidade do propósito de coleta dos dados e a definição dos dados coletados. Como disposto, o MFV-SI contribuiu com o relatório contendo a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Com as aplicações das provas de conceito foi possível constatar que, as aplicações do MFV-SI, apontaram ações causadoras algum tipo de vulnerabilidade diretamente ligada ao propósito estabelecido pelo fluxo em questão, potencialmente capaz de expor o indivíduo. Academicamente, este trabalho contribui ao adicionar à lista de desperdícios do LIM uma nova classificação de desperdício, o desperdício da vulnerabilidade. No processo de aquisição de dados, por exemplo, a obtenção de dados, além do propósito estabelecido, gerou maiores volumes de dados, sem necessariamente, ter sido tomado maiores cuidados com possível exposição social. Dessa forma, o modelo proposto se mostrou capaz em contribuir com o viés social , através da estruturação de processos de negócio, baseado na redução ou eliminação de desperdícios relacionados ao direito de privacidade.

No aspecto quantitativo, o índice de vulnerabilidade se mostrou capaz de diferenciar o risco inerente entre cadeias de valores com diferentes tamanhos, assim, mostrou-se uma ferramenta convergente aos artigos 46, parágrafo segundo, que explicita que as medidas de segurança do dado pessoal deverão ser observadas desde a fase de concepção do produto ou serviço até a sua execução, e o artigo 50, parágrafo segundo, inciso I – C, que trata que um programa de governança em privacidade deve levar em conta a estrutura, a escala e o volume de suas operações. Comparando os três estudos, foi possível perceber que quanto maior a cadeia de valor e maior o tráfego percorrido pelos dados, maiores são as situações de exposições a ataques ou interferência humana, intencional ou não, aumentando, assim, o valor do índice.

Por fim, outra contribuição observada ao longo das três jornadas de testagem do modelo, foi atribuída à objetividade das questões estudadas no Quadro 9, boas práticas para avaliação de vulnerabilidade. A seleção das principais diretrizes da ISO 27002 e sua conversão em 30 questões objetivas, contribuíram para um processo ágil de coleta e análise das vulnerabilidades da cadeia, uma vez que a lista de questões estabelecidas permitiu a condução de uma análise binária. Nesse contexto, as questões escolhidas se mostraram coerentes tanto para a empresa da

prova de conceito 2, que possuía departamento de TI estruturado e um total de 215 colaboradores, quanto para as empresas dos estudos 1 e 3, que não possuíam pessoas dedicadas à segurança da informação, tão pouco departamento de TI. Essa afirmação pode ser corroborada pelo número de respostas positivas relativamente baixo, encontrado no MFV-SI-Atual das três empresas testadas. Por fim, a listagem de 30 questões de boas práticas, serviu de apoio para o estabelecimento do plano de ação em busca do estado futuro, projetado pelo MFV-SI-Futuro, uma vez que os estudos apontaram que a maior parte das ações necessárias para a redução da vulnerabilidade estavam contempladas na lista.

5 CONCLUSÕES

Neste tópico, foram apresentadas as conclusões finais acerca dos fatores motivadores dos objetivos de pesquisa, sobre a contribuição do modelo para o atendimento aos requisitos da LGPD e as limitações e proposições para pesquisas futuras.

5.1 Sobre os objetivos de pesquisa

O desenvolvimento do trabalho mostrou uma forte correlação entre as técnicas de gerenciamento e a redução dos desperdícios, oferecidas pela filosofia *Lean* com a gestão de dados pessoais, principalmente quando o dado pessoal passa a ser analisado como ativo empresarial e sua vulnerabilidade como um desperdício que deve ser combatido.

Nesse espectro, os princípios elementares que compõe MFV convencional mostraram-se satisfatórios balizadores na elaboração de um novo modelo de análise da segurança da informação à luz dos requisitos da LGPD, o MFV-SI.

Dessa forma, o objetivo geral da pesquisa, de elaborar o Mapa de Fluxo de Valor – Segurança da Informação (MFV-SI) – à luz dos requisitos da LGPD, por meio da releitura das funcionalidades do MFV convencional, contribuiu como uma ferramenta de auxílio na melhoria de processos de negócios focado em aspectos sociais relacionados à privacidade do indivíduo.

5.2 Sobre as contribuições do modelo MFV-SI

As composições inéditas, que diferenciam o MFV-SI do MFV tradicional, giram em torno da nova metodologia de mensuração da linha do tempo, **a vulnerabilidade**, o atendimento ao **propósito do fluxo de valor** e o **consentimento** do usuário.

O índice de vulnerabilidade se mostrou eficaz na proposição de um valor quantitativo para análise dos riscos da cadeia de valor. No entanto, novos estudos podem propor novas metodologias de análise da vulnerabilidade, como, por exemplo, a escolha de outras questões práticas, ou a ponderação das questões estabelecidas através da análise dos níveis de severidade, ocorrência e detecção de cada uma delas.

A análise do propósito do fluxo de valor se mostrou capaz de promover uma discussão sobre as razões e consequências em se adotar uma determinada sequência de processos, em questionar a quantidade de etapas do processo bem como o conteúdo dos blocos de dados processados pela cadeia de valor. O MFV-SI contribui para que, dinamicamente, seja feita uma análise correlacional entre o propósito estabelecido e os dados adquiridos, proporcionando uma visão dos desperdícios relacionados a transporte de informações, espera, excesso de

informações, atraso em alterações de informações e número excessivo de sistemas e vulnerabilidade, por exemplo.

Não menos importante, a análise do consentimento se mostrou eficiente como balizador para a tomada de decisão de se tratar ou não determinado dado pessoal, e principalmente para a avaliação da necessidade de estruturação ou adaptação dos processos de negócio para a obtenção, sem vícios, de consentimento do proprietário dos dados.

Por fim, o estudo mostrou que o MFV continua sendo uma ferramenta atual e acessível a adaptações, possibilitando o vasto cenário de aplicações, como já proposto por outros autores. Não diferente, quando adaptado para as novas exigências da LGPD, o MFV-SI se mostrou um caminho viável na **proposição de valor ao indivíduo**, seja ele trabalhador ou cliente, seja ela empresa com algum nível de segurança, ou iniciando sua jornada.

5.3 Sobre as limitações do modelo MFV-SI e proposições futuras

Apesar dos resultados satisfatórios, algumas oportunidades de desdobramento deste estudo merecem destaque. O estudo sobre as ferramentas de mapeamento de processos à luz dos critérios da LGPD pode evoluir na adoção de outros critérios da lei nacional e/ou critérios associados a outras leis internacionais correlatas, como o caso da GDPR.

Já a metodologia proposta para o cálculo do índice de vulnerabilidade pode ser recolocada sob novos prismas, abordando novas práticas de segurança da informação.

Por fim, novos estudos abordando um número maior de organizações irá contribuir para uma análise mais robusta a respeito da aderência do índice de vulnerabilidade, das representações gráficas e da tríade do ineditismo contemplados pelo modelo MFV-SI.

REFERÊNCIAS

ABDULMALEK, F. A.; RAJGOPAL, J. Analyzing the benefits of lean manufacturing and value stream mapping via simulation: a process sector case study. **International Journal of Production Economics**, v. 107, n. 1, p. 223-236, 2007.

AHLSTROM, P. Lean service operations: translating lean production principles to service operations. **International Journal of Service Technology and Management**, v. 5, no. 5/6, p. 545-566, 2004.

ALCOCK, J. R; DURUGBO, C.; TIWARI, A. Modelling information flow for organisations: A review of approaches and future challenges. **International Journal of Information Management**, v. 33, n. 3, p. 597-610, 2013.

ALVANDI, S.; LI, W.; SCHÖNEMANN, M.; KARA, S.; HERRMANN, C. Economic and environmental value stream map (E2VSM) simulation for multi-product manufacturing systems. **International Journal of Sustainable Engineering**, 9(6), p. 354-362, 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**: Tecnologia da informação: Técnicas de segurança: Sistemas de gestão de segurança da informação: Requisito. Rio de Janeiro: ABNT, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002**: Tecnologia da Informação: Técnicas de Segurança: Código de Prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005**: Tecnologia da Informação: Técnicas de segurança: Gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2011.

BARBOSA, R. R. Gestão da Informação e Gestão do Conhecimento: origens, polêmicas e perspectivas. **Informação & Informação**, v. 13, no. esp., p. 1-25, 2008.

BEAL, A. **Conceitos e Princípios Básicos da Informaçã***o*: Segurança da Informação. São Paulo: Atlas, 2005.

BEAL, A. **Gestão estratégica da informação**: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas, 2009.

BEZERRA, T.; NETO, E.; MORAIS, J. L. O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data: o fenômeno da *dataveillance* em relação à utilização de metadados e seu impacto nos direitos humanos. **Direito e Mundo digital,** 7 (3), p. 185-199, 2017.

BHARADWAJ, A.; EL SAWY, O.; PAVLOU, P.; VENKATRAMAN, N. Digital business strategy*: Toward a next generation of insights*. **MIS Quarterly**, 37(2), p. 471-482, 2013.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 01 mar. 2020.

BRASIL. Decreto-lei nº 12.527, de 18 de Novembro de 2011. **Congresso Nacional**. Disponível em: <http://bit.ly/2HPS1Di>. Acesso em: 10 mar. 2020.

BRASIL. Decreto-lei nº 12.965, de 23 de Abril de 2014. **Congresso Nacional**. Disponível em: <http://bit.ly/2CBJrVk>. Acesso em: 10 mar. 2020.

BRASIL. Decreto-lei nº 13.709, de 14 de Agosto de 2018a. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Congresso Nacional**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 12 mar. 2020.

BRASIL. Medida provisória no. 869, de 27 de Dezembro de 2018b. **Congresso Nacional**. Disponível em: <http://bit.ly/2TvhsMy>. Acesso em: 12 mar. 2020.

BRESCIANI, S.; SCUOTTO, V.; SANTORO, G.; DEL GIUDICE, M. Mudando os processos de inovação intra e interorganizacional para os negócios digitais: uma análise empírica das PME. **Gestão da Criatividade e Inovação**, 26 (3), p. 247-255, 2017.

BRESCIANI, S.; FERRARIS, A.; DEL GIUDICE, M. O gerenciamento da ambidestidade organizacional por meio de alianças em um novo contexto de análise*:* projetos de cidades inteligentes na Internet das Coisas (IoT). **Previsão tecnológica e mudança social**, v. 136, p. 331-338, 2018.

BUBICZ, M. E.; DIAS, A. P. F.; PÓVOA, B.; CARVALHO, A. Incorporating social aspects in sustainable supply chains: Trends and future directions. **Journal of Cleaner Production**, v. 237, 2019.

CEA (THE COUNCIL OF ECONOMIC ADVISERS). **The Cost of Malicious Cyber Activity to th U.S Economy**. Washington, Feb, 2018. Disponível em: <https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-MaliciousCyber-Activity-to-the-U.S.-Economy.pdf>. Acesso em: 18 jul. 2018.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Estatísticas dos Incidentes Reportados ao CERT.br por ano**. Brasil, 2019. Disponível em:<https://cert.br/stats/incidentes/>. Acesso em: 26 fev. 2020.

CHAABANE, A., RAMUDHIN, A.; PAQUET, M. Designing supply chains with sustainability considerations, **Production Planning & Control**: The Management of Operations. Vol. 22, no. 8, p. 727-741, 2012. Disponível em: <http://dx.doi.org/10.1080/09537287.2010.543554>. Acesso em: 12 mar. 2020.

CHOO, C. W. **Gestão de informação para a organização inteligente**: a arte de explorar o meio ambiente. Lisboa: Editorial Caminho, 2003.

COMISSÃO EUROPEIA. **Corporate Social Responsibility & Responsible Business Conduct***,* 2011. Disponível em:

<https://ec.europa.eu/growth/industry/sustainability/corporate-social-responsibility_pt>. Acesso em: 10 mar. 2020.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Declaração americana dos direitos e deveres do homem**. Aprovada na Nona Conferência Internacional Americana, Bogotá, 1948. Disponível em: <https://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htm>. Acesso em: 01 mar. 2020.

DASGUPTA, A.; GILL, A. Q.; HUSSAIN, F. **A Review of General Data Protection Regulation for Supply Chain Ecosystem**. University of Technology Sydney, Sydney, Austrália, 2020.

DAVENPORT, T. H. **Ecologia da informação**: por que só a tecnologia não basta para o sucesso na era da informação. 5ª ed. São Paulo: Futura, 1998.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. Adotada e proclamada pela Assembleia Geral das Nações Unidas. **Resolução 217 a III**, **em 10 de dezembro 1948**. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 02 mar. 2020.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Revista Espaço Jurídico**, vol. 12, no. 2. Joaçaba: Unoesc, 2011.

DÜES, C.M.; TAN, K. H.; LIM, M. Green as the new Lean: how to use Lean practices as a catalyst to greening your supply chain. **Journal of Cleaner Production**, v. 40, p. 93-100, 2013. Disponível em: <https://doi.org/10.1016/j.jclepro.2011.12.023>. Acesso em: 10 jan. 2020.

EDWARDS, L.; MCAULEY, D.; DIVER, L. From privacy impact assessment to social impact assessment. **Security and Privacy Workshops (SPW)**, IEEE, p. 53-57, May, 2016.

ELKINGTON, J. **Cannibals with forks – Triple bottom line of 21st century business.** Stoney Creek, CT: New Society Publishers, 1997.

ERNST&YOUNG. **Metodologia PER para implantação SAP.** Manual da empresa Ernst & Young, 1997.

FAULKNER, W.; BADURDEEN, F. Sustainable Value Stream Mapping (Sus-VSM): methodology to visualize and assess manufacturing sustainability performance. **Journal of Cleaner Production**, v. 85, p. 8-18, 2014.

FENG, Y.; ZHU, Q.; LAI, K-H. Corporate social responsibility for supply chain management: A literature review and bibliometric analysis. **Journal of Cleaner Production**, n. 158, 2017.

FERREIRA, M. A. **Maturidade em gestão ambiental e adoção de práticas de Green Supply Chain Management:** proposta de um framework integrador à luz da análise de múltiplos casos em cadeias de alto impacto ambiental. Ribeirão Preto. Tese de Doutorado, apresentada à faculdade de Medicina de Ribeirão Preto/USP, 2014.

FERREIRA, M. A.; JABBOUR, C. J. C.; JABBOUR, A. B. L. S. **Maturity levels of material cycles and waste management in a context of green supply chain management**: an innovative framework and its application to Brazilian cases. Mater Cycles Waste Manag. Received: 17 March 2015 / Accepted: 23 June 2015 / Published online: 17 July 2015. Springer Japan, 2015.

FERREIRA, M. A.; JABBOUR, C. J. C. Relacionando níveis de maturidade em gestão ambiental e a adoção de práticas de Green Supply Chain Management: convergência teórica e estudo de múltiplos casos. **Gestão e Produção**, São Carlos, v. 26, n. 1, e1822, 2019. Disponível em: <https://doi.org/10.1590/0104-530X1822-19>. Acesso em: 10 jan. 2021.

FERRO, J. R. **A essência da ferramenta Mapeamento do Fluxo de Valor.** Lean Institute Brasil. Brasil, 2005. Disponível em: <https://www.lean.org.br/artigos/61/a-essencia-da-ferramenta-mapeamento-do-fluxo-de-valor.aspx>. Acesso em 24 mai. 2020.

FONSECA, J. J. S. **Metodologia da pesquisa científica.** Fortaleza: UEC, 2012.

FONTES, E. **Segurança da informação**: O usuário faz a diferença. 1. ed. São Paulo: Editora Saraiva, v. 1, 2006.

GIL, A. C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2008.

GODOY, A. S. Estudo de Caso Qualitativo. *In*: SILVA, A. B. da; GODOI, C. K.; BANDEIRA-DE-MELLO, R. **Pesquisa Qualitativa em estudos organizacionais**: paradigmas, estratégias e métodos. São Paulo: Saraiva, p. 115-146, 2006.

HARRINGTON, James. **Aperfeiçoando processos empresariais.** São Paulo: Makron Books, 1993.

HEDIGER, W. Welfare and capital-theoretic foundations of corporate social responsibility and corporate sustainability. **The Journal of Socio-Economics**, v. 39, p. 518-526, 2010.

HELLENO, A. L.; MORAES, A. J. I.; SIMON, A. T. Integrating sustainability indicators and Lean Manufacturing to assess manufacturing processes: Application case studies in Brazilian industry. **Journal of Cleaner Production**, p. 1-12, 2016.

HICKS, B J. Lean information management: Understanding and eliminating waste. **International Journal of Information Management**, vol. 27, n. 4, p. 233-249, 2007.

HÖLTTÄ, K.; MAHLAMÄKI, T.; EISTO, M.; STRÖM. **Lean information management model for engineering changes**. World Academy of Science, Engineering and Technology, 2010.

HOWELLS, J. R. Going global: The use of ICT networks in research and development. **Research Policy**, 24(2), p. 169-184. 1995.

HUARNG, K. H; YU, T. H. K.; LAI, W. Inovação e difusão de produtos, serviços e sistemas de alta tecnologia. **Journal of Business research**, 2015.

ILIC, J. Cybersecurity Software Revenue to Reach $27 bn by 2023. **Precise Security**. 2020. Disponível em: <https://www.precisesecurity.com/articles/cybersecurity-software-revenue-to-reach-27-bn-by-2023/>. Acesso em: 10 maio 2020.

IUGA, M.V.; KIFOR, C.V.; ROSCA L. Lean Information Management: Criteria For Selecting Key Performance Indicators At Shop Floor. **Acta Universitatis Cibiniensis**. Technical 66(1), 2014.

JAREBRANT, C.; WINKEL, J.; JOHANSSON HANSE, J.; MATHIASSEN, S. E.; ÖJMERTZ, B. ErgoVSM: A Tool for Integrating Value Stream Mapping and Ergonomics in Manufacturing. **Human Factors and Ergonomics In Manufacturing**, 26(2), p. 191-204, 2016.

KOPALLE, P. Why Amazon's Anticipatory Shipping is Pure Genius. **Forbes**. January 218, 2014.

KÜHNEN, M.; HAHN, R. Systemic social performance measurement: Systematic literature review and explanations on the academic status quo from a product life-cycle perspective. **Journal of Cleaner Production**, v. 205, p. 690-705, 2018.

LASTRI, H.; ALBAGLI, S. **Informação e Globalização na Era do Conhecimento.** Rio de Janeiro: Editora Campus Ltda, 1999.

LEAL, F. **Um diagnóstico do Processo de atendimento a clientes em uma agencia bancária através de mapeamento do processo e simulação computacional**. Dissertação de Mestrado. Programa de Pós-Graduação em Engenharia de Produção, Universidade Federal de Itajubá, MG, 2003.

LEE, H. L. Radically reinvent your Supply Chain - Don't Tweak Your Supply Chain Rethink It End to End. **Harvard Business Review**, v. 88, n. 10, p. 62-70, 2010.

LIAN, Y. H.; VAN LANDEGHEM, H. Analysing the effects of lean manufacturing using a value stream mappingbased simulation generator. **International Journal of Production Research**, v. 45, n. 13, p. 3037-3058, 2007.

LIKER, J. K. **The Toyota Way:** 14 Management Principles from the World's Greatest Manufacturer. New York: McGraw Hill, 2004.

LOTT, D. Relembre os principais vazamentos de dados de brasileiros em 2018. **Folha UOL**, 2019. Disponível: <https://www1.folha.uol.com.br/tec/2019/01/relembre-os-principais-vazamentos-de-dados-de-brasileiros-em-2018.shtml>. Acesso em: 01 mar. 2020.

MALIN, A. M. B. Gestão da informação governamental: em direção a uma metodologia de avaliação. **DataGramaZero**, v. 7, n. 5, out. 2006.

MARTINEZ-JURADO, P. J.; MOYANO-FUENTES, J. **Lean management, supply chain management and sustainability: A literature review. Journal of Cleaner Production**, 85, p. 134–150, 2014.

MARTINS, G. A.; THEÓPHILO, C. R. **Metodologia da investigação científica para ciências sociais aplicadas**. São Paulo: Editora Atlas, 2009.

McGEE, James V.; PRUSAK, Laurence. **Gerenciamento estratégico da informação:** aumento a competitividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. Rio de Janeiro: Campus, 1994.

MILLER, G.; PAWLOSKI, J.; STANDRIDGE, C. A case study of lean, sustainable manufacturing. **Journal of Industrial Engineering and Management**, vol. 3, n. 1, p. 11-32, 2013.

MITNICK, K. D.; SIMON, W. L. The Art of Intrusion: **The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers** (English Edition). Wiley Publishing, Indianapolis, Indiana, 1ª Edição, eBook Kindle, 2005.

MONTEIRO, R. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?. **Instituto Igarapé, Artigo Estratégico 39**. Rio de Janeiro, Brasil, 2018.

MOOR, J. H. Why we need better ethics for emerging technologies. **Ethics and Information Technology 7**, p. 111-119. 2005. Disponível em: <https://doi.org/10.1007/s10676-006-0008-0>. Acesso em: 23 abr. 2021.

MOSTAFA, S.; DUMRAK, J. Waste Elimination for Manufacturing Sustainability. **Procedia Manufacturing**, 2, 11-16, 2015.

MOURA, J. N. D. A. H. P. D. **Implantando a Gestão de Serviços de TI:** Uma abordagem horizontal baseada no catalogo de serviços de TI. Recife, 2007. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/sbsi/2008/0016.pdf >. Acesso em: 10 abr. 2020.

MOROZOV Evgeny. (2019), "Capitalism's New Clothes. Shoshana Zuboff's new book on 'surveillance capitalism' emphasizes the former at the expense of the later". **The Baffler**, 4 fev. Disponível em: <https://thebaffler.com/latest/capitalisms-new-clothes-morozov>. Acesso em: 23 abr. 2021.

NETTO, A. S.; SILVEIRA, M. A. P. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **JISTEM-Journal of Information Systems and Technology Management**, v. 4, n. 3, p. 375-397, 2007.

NORTON LIFE LOCK. **Norton Cyber Security Insights Report.** United States, 2017. Disponível em: <https://www.nortonlifelock.com/about/newsroom/press-kits/ncsir-2017>. Acesso em: 26 fev. 2020.

OHNO, T. **O Sistema Toyota de Produção: além da produção em larga escala.** Bookman, Porto Alegre, 1997.

PAGELL, M.; SHEVCHENKO, A. Why Research In Sustainable Supply Chain Managemant Should Have No Future. **Journal of Supply Chain Management**, v. 50, n. 1, 2014.

PARDOLESI, R. **Dalla riservatezza alla protezione dei dati personali:** una storia di evoluzione e discontinuità. Diritto alla riservatezza e circolazione dei dati personali. Milano: Giuffrè, 2003.

PIERCY, N.; RICH, N. The relationship between lean operations and sustainable operations. **International Journal of Operations & Production Management**, vol. 35, n. 2, p. 282-315, 2015.

POEPJES, R. **The development and evaluation of na Information Security Awareness Capability Model:** Linking ISO/IEC 27002 controls with Awareness Importance, Capability and Risk. School of Management and Enterprise. Faculty of Business, Education, Laws and Arts. The University of Southern Queensland, 2015.

PÓVOA, B. A. P; SILVA, C.; CARVALHO, A. Opportunities and Challenges in Sustainable Supply Chain: An Operations Research Perspective. **European Journal of Operational Research**, v. 268, 2018.

RAMINELLI, F.; RODEGHERI, L. **Proteção de Dados Pessoais na Internet no Brasil: Análise de Decisões Proferidas pelo Supremo Tribunal Federal.** Cadernos do Programa de Pós-Graduação em Direito PPGDir./UFRGS XI (2), p. 89-119, 2016.

RHODES-OUSLEY, M. **Information Security The Complete Reference.** 2th. The McGraw-Hill Companies, 2013.

ROGERS, K.; HUDSON, B. The triple bottom line: The synergies of transformative perceptions and practices of sustainability. OD Practitioner, 4(43), 3-9, 2011.
SOARES, S.; TEIXEIRA, L. Lean Information Management in Industrial Context: an Experience Based on a Practical Case. **International Journal of Industrial Engineering and Management (IJIEM)**, v. 5, n. 2, p. 107- 114, 2014.

ROTHER, M.; SHOOK, J. **Aprendendo a Enxergar:** mapeando o fluxo de valor para agregar valor e eliminar o desperdício. São Paulo: Lean Institute Brasil, 2003.

ROTHER, T.; PLISHKA, C.; LAWAL, A.; HARRISON, L.; SARI, N.; GOODRIDGE, D.; FLYNN, R; CHAN, J.; FIANDER, M.; POKSINSKA, B.; WILLOUGHBY, K.; KINSMAN L.; What Is Lean Management in Health Care? Development of an Operational Definition for a Cochrane Systematic Review. **Sage Journals,** vol. 42, Issue 3, 2019.

SHUKER, T.; TAPPING, D. **Value Stream Management for the Lean Office: 8 steps to planning, mapping, and sustaining lean improvements in administrative areas.** Primeira Edição, Nova Iorque, 2003.

SILVA, M. A. **Prova de Conceito (PoC) em Projetos.** Project Management Knowledge Base. 24 de junho de 2014. Disponível em: <http://pmkb.com.br/artigo/prova-de-conceitopoc-em-projetos/>. Acesso em: 03 de jan. 2021.

SINGH, B.; SHARMA, S. K. Value stream mapping as a versatile tool for lean implementation: an Indian case study of a manufacturing firm. **Measuring Business Excellence**, v. 13, n. 3, p. 58-68, 2009.

STARCK, K. R. **Gestão da informação no ambiente de projetos: Identificando sua relação com o desempenho dos Projetos empresariais.** Santa Catarina, 2011. 255f. Dissertação (mestrado em Ciência da Informação). Universidade Federal de Santa Catarina, 2011.

SUNDQVIST, A.; SVÄRD, P. Information culture and records management: a suitable match? Conceptualizations of information culture and their application on records management. **International Journal of Information Management**, v. 36, n. 1, p. 9-15, 2016.

SZCZERBICKI, E. Structuring an information flow for autonomous systems. **International Journal of Systems Science**, 22(12), p. 2599-2609, 1991.

TANNER, A. Never Give Stores Your ZIP Code. Here's Why. **Revista Forbes**, 2013. Disponível em: <http://bit.ly/2UWih2w>. Acesso em: 10 mar. 2020.

TERENCE, A. C. F.; ESCRIVÃO-FILHO, E. Abordagem quantitativa, qualitativa e a utilização da pesquisa-ação nos estudos organizacionais. *In*: Encontro Nacional de Administração, 26, 2006, Fortaleza. **Anais**. Fortaleza: ENEGEP, 2006.

THE ECONOMIST. **The world's most valuable resource is no longer oil, but data.** May, 6th 2017 edition. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 27 dez. 2020.

TRIVIÑOS, A, N, S. **Introdução à pesquisa em ciências sociais**. São Paulo: Atlas, 1987.

UNIÃO EUROPEIA. Regulation (eu) 2016/679 of the european parliament and of the council. **Official journal of the european union**. 27 de abril de 2016. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 10 mar. 2020.

VERMA, R.; GUSTAFSSON, A.; KRISTENSSON, P.; WITELL, L. Cocriação de clientes em inovação de serviços: uma questão de comunicação?. **Journal of service management**, 23 (3), p. 311-327, 2012.

WOMACK, J. E.; JONES, D.; DANIEL, T. **Lean Thinking**: Banish Waste and Create Wealth in Yout Corporation. 2 ed. New York, 1996.

WORTH, J.; SHUKER, T.; KEYTE, B.; OHAUS, K.; LUCKMAN, J.; VERBLE, D.; PALUSKA, K.; NICKEL, T. **Aperfeiçoando a jornada do paciente**: melhorando a segurança do paciente, a qualidade e a satisfação enquanto desenvolvimentos habilidades para resolver problemas. São Paulo: Lean Institute Brasil, 2013.

WORLD ECONOMIC FORUM. **Relatório Global de Riscos do Fórum Econômico Mundial de 2020.** 2020. Disponível em: < https://www.weforum.org/reports>. Acesso em: 26 fev. 2020.

WORLD ECONOMIC FORUM (WEF). **The Global Risks Report 2018**, 13th Edition. Geneva: 2018. ISBN: 978-1-944835-15-6. Disponível em: <http://www3.weforum.org/docs/WEF_GRR18_Report.pdf>. Acesso em: 15 ago. 2018.

YAWAR, A.S.; SEURING, S. Management of Social Issues in Supply Chains: A Literature Review Exploring Social Issues, Actions and Performance Outcomes. **Journal Business Ethics**, v. 141, p. 621-643, 2017.