UNIVERSIDADE NOVE DE JULHO - UNINOVE
PROGRAMA DE PÓS GRADUAÇÃO EM INFORMÁTICA E GESTÃO DO CONHECIMENTO - PPGI

EDUARDO STEFANI

FRAMEWORK DE RISCOS DA SEGURANÇA DA INFORMAÇÃO NO USO DAS TECNOLOGIAS DA TRANSFORMAÇÃO DIGITAL NAS EMPRESAS

São Paulo
2022

EDUARDO STEFANI

FRAMEWORK DE RISCOS DA SEGURANÇA DA INFORMAÇÃO NO USO DAS TECNOLOGIAS DA TRANSFORMAÇÃO DIGITAL NAS EMPRESAS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática e Gestão do Conhecimento da Universidade Nove de Julho - UNINOVE, como requisito para a obtenção do título de Mestre em Informática e Gestão do Conhecimento.

Prof. Orientador: Dr. Ivanir Costa

São Paulo
2022

Stefani, Eduardo.
Framework de riscos da segurança da informação no uso das tecnologias da Transformação Digital nas empresas. / Eduardo Stefani. 2022.
189 f.
Dissertação (Mestrado) - Universidade Nove de Julho - UNINOVE, São Paulo, 2022.
Orientador (a): Prof. Dr. Ivanir Costa.
1. Transformação Digital. 2. Tecnologias Digitais. 3. Risco. 4. Identificação de Risco. 5. Classificação de Risco.
I. Costa, Ivanir. II. Título.
CDU 004

UNINOVE
Universidade Nove de Julho

ATA DE DEFESA DA DISSERTAÇÃO

Ao vigésimo segundo dia do mês de fevereiro de dois mil e vinte e dois, às 14h30, do programa de Pós-Graduação, desta Universidade, reuniu-se em sessão pública a Comissão Julgadora da dissertação de Mestrado de Eduardo Corrêa Stefani sob o título "Framework de Riscos no Uso de Tecnologias da Transformação Digital nas Empresas".

Integraram a comissão os professores: Prof. Dr. Ivanir Costa (PPGI/UNINOVE), o Prof. Dr. Aguinaldo Aragon Fernandes (FIA), e o Prof. Dr. Fellipe Silva Martins sob a presidência do primeiro, orientador da dissertação. A banca examinadora, tendo decidido aceitar a dissertação, passou à argüição pública do candidato. Encerrados os trabalhos, os examinadores deram parecer final sobre a dissertação.

	Parecer
Prof. Dr. Ivanir Costa	Aprovado
Prof. Dr. Aguinaldo Aragon Fernandes	Aprovado
Prof. Dr. Fellipe Silva Martins	Aprovado

Parecer:

A aluno deverá incorporar no texto final as correções e sugestões solicitadas pela banca examinadora.

Em conclusão, o candidato foi considerado aprovado, no grau de Mestre em Informática e Gestão do Conhecimento. E, para constar, eu, Prof. Dr. André Felipe Henriques Librantz, diretor do Programa de Mestrado e Doutorado em Informática e Gestão do Conhecimento, lavrei a presente ata que assino juntamente com os membros da banca examinadora.

São Paulo, 22 de fevereiro de 2022.

Prof. Dr. Ivanir Costa

Prof. Dr. Aguinaldo Aragon Fernandes

Prof. Dr. Fellipe Silva Martins

Prof. Dr. André Felipe Henriques Librantz

DEDICATÓRIA

Luciana e Valentina

Esposa e filha que apoio e paciência tornaram este trabalho possível.

AGRADECIMENTOS

Agradecimento especial aos meus pais Jair e Marisa, por terem proporcionado todas as condições para o meu desenvolvimento desde os primeiros estágios da minha educação. Sem esse apoio inicial eu não teria os instrumentos necessários para um empreendimento como este.

Agradeço ao meu orientador, Prof. Dr. Ivanir Costa, por me apoiar e incentivar desde as conversas preliminares, pelo direcionamento e incansáveis revisões deste trabalho. A sua lucidez e disposição de compartilhar um vasto conhecimento acadêmico e profissional me dão uma grande honra de tê-lo como orientador.

Agradeço ao Prof. Dr. Fellipe Silva Martins e Prof. Dr. Aguinaldo Aragon Fernandes, por terem aceitado o convite para as bancas de qualificação e defesa, e pelo tempo investido ao contribuir com valiosos comentários e direcionamentos. As contribuições excederam o aperfeiçoamento deste trabalho e resultaram em perspectivas a serem aplicadas em outros trabalhos acadêmicos, bem como na atuação profissional. Ao Prof. Dr. Fellipe Silva Martins que com o seu rigor acadêmico me inspirou a observar todas as possibilidades metodológicas, e a sonhar com outras produções intelectuais.

Agradeço ao Prof. Dr. Marcos Antonio Gaspar, pelo tempo investido ao contribuir com comentários que me ajudaram no aperfeiçoamento da ideia deste trabalho na disciplina de seminários.

Agradeço aos meus amigos do programa e mestrandos Jorge Alonso e Vinicius Rodrigues Pereira dos Santos. Ao Jorge por me acompanhar a desbravar as ferramentas bibliométricas com paciência e com a visão de quem escreve sobre simulações, e por compartilhar o completo desespero quando os prazos estavam curtos. Ao Vinicius pelos esclarecimentos oportunos sobre como aplicar corretamente as desafiadoras normas ABNT.

Agradeço ao meu caro amigo Prof. Amaro Terto, que com olhar de fora e atento me ajudou a revisar o texto quando eu já não identificava as sutilizas de um trabalho acadêmico.

Agradeço ao PPGI pela experiência proporcionada por este programa de mestrado que acolhe e permite que profissionais de mercado iniciem a vida acadêmica, e a estabelecer contato com professores e estudantes inspiradores. São programas assim que mudam carreiras e vidas, e que me fazem acreditar no futuro.

Agradeço à CAPES e à Universidade Nove de Julho, pela bolsa de estudos que proporcionou condições de eu percorrer esse caminho. Iniciativas que contribuem para o desenvolvimento acadêmico do Brasil.

RESUMO

O crescente impacto das tecnologias digitais na sociedade, bem como as mudanças rápidas e disruptivas que provocam, com a busca por processos eficientes e modernos, pressiona as empresas a utilizarem soluções digitais. Todavia, elas têm pouco espaço para escolhas e raramente conseguem se prevenir da velocidade e dos desafios trazidos pelo uso intenso das tecnologias digitais. Por outro lado, os pesquisadores desse tema indicam que há uma face desse percurso que é o risco da segurança da informação no uso dessas tecnologias o qual não está completamente visível, mesmo com os ganhos obtidos com o uso das tecnologias digitais. Nesse contexto, esta pesquisa tem o objetivo de revelar os riscos mais relevantes envolvidos no uso das tecnologias da Transformação Digital que podem trazer efeitos adversos às expectativas iniciais. Como metodologia de pesquisa foi realizada uma revisão sistemática da literatura, na busca por artigos científicos em bases de dados acadêmicas, que deu visibilidade aos tipos de riscos que estão presentes ao adotar as tecnologias digitais e que permitiu a composição de um *framework* que as contempla. Esses riscos foram avaliados por especialistas de Tecnologia da Informação de mercado, por meio do instrumento de pesquisa do tipo questionário. Os resultados desse estudo permitiram identificar, organizar e classificar os riscos que as empresas estão sujeitas no uso das tecnologias da Transformação Digital. Como contribuição para o mercado e para a academia, esta pesquisa disponibiliza um instrumento que é o *framework* para apoiar as empresas na jornada da Transformação Digital e no reconhecimento dos riscos da segurança da informação inerentes ao uso das tecnologias digitais. Como trabalho futuro que esta pesquisa proporciona, sugere-se a criação de um modelo para priorização e para mitigação de riscos com o *framework* proposto e validado nesse estudo como um ponto de partida.

Palavras-chave: Transformação Digital. Tecnologias Digitais. Risco. Identificação de Risco. Classificação de Risco.

ABSTRACT

The increasing impact of digital technologies in society, with rapid and disruptive changes, including more efficient and modern processes, press companies to use digital solutions. However, companies have limited choices, and they rarely can avoid being affected by the speed and challenges of digital technologies. Researchers have noticed a perspective that the cybersecurity risk of using those technologies is not completely visible, even with the advantages of this phenomenon. In this context, this research aims to reveal the associated risks of using Digital Transformation technologies that can cause unfavorable effects compared to initial expectations. As a research methodology, a systematic literature review was carried out, searching for scientific articles in academic databases. It provided visibility of the risks when adopting digital technologies and provided a framework that highlights the most relevant risks involved. IT specialists evaluated those risks through a questionnaire, and its results allowed the identification, organization and classification of the risks that companies are subjected to when using digital technologies. As a contribution to the market and the academic settings, this research provides a framework to support companies in their Digital Transformation journey and recognize the cybersecurity risks associated with digital technologies. Future works suggest creating a model for risk prioritization and mitigation with the proposed framework as a starting point.

Keywords: Digital Transformation. Digital Technology. Risk. Risk Identification. Risk Classification.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

CAPÍTULO 1

INTRODUÇÃO

Neste capítulo é apresentada a contextualização, os objetivos, a justificativa, a delimitação do tema e a estrutura do trabalho.

1.1 CONTEXTUALIZAÇÃO

As tecnologias digitais que representam a combinação e a conectividade de um disperso volume de informação, de comunicação e de tecnologias de computação (BHARADWAJ *et al.*, 2013), passaram a ter um impacto crescente na vida das pessoas, nos negócios e nas empresas (SCHNEIDER; KOKSHAGINA, 2020). A evolução delas resultou em modelos comerciais baseados em plataformas digitais, o que impactou a maneira como as empresas se estruturam e como a gestão delas é conduzida (FERNANDES *et al.*, 2019). Isso inclui alterações no comportamento das empresas, pressionando-as de um modo que elas raramente conseguem se prevenir da crescente competição e dos desafios trazidos pelas tecnologias digitais (AL-DEBEI; AVISON, 2010).

A Transformação Digital (TD) como um processo que contempla a digitalização das empresas, incluindo produtos, serviços e a criação de valor a partir da implementação de várias tecnologias (SCHNASSE; MENZEFRICKE; DUMITRESCU, 2021), resultou em um cenário de mudanças, que inclui a evolução das tecnologias da informação, a busca por processos eficientes e a modernização (VIAL, 2019). A TD se transformou em um componente crítico para o sucesso e para a sobrevivência das empresas, por permitir a identificação e a criação de oportunidades para fortalecerem as suas vantagens competitivas (EL-HADDADEH, 2020).

Embora esse tema venha sendo alvo de interesse crescente pela academia e pelo mercado (HANELT *et al.*, 2021), um entendimento conjunto sobre o que é TD e o que ela significa ainda está faltando (MORAKANYANE; GRACE; O'REILLY, 2017). Pode-se defini-la, de acordo com a literatura, como um processo que aperfeiçoa uma entidade específica, desencadeando muitas mudanças, por meio da informação, da computação, da comunicação e da conectividade (VIAL, 2019). Pode-se também, compreender a TD como uma mudança organizacional desencadeada a partir da difusão das tecnologias digitais (HANELT *et al.*, 2021).

As tecnologias digitais estão transformando o modo como as empresas e os mercados interagem (LAMBERTON; STEPHEN, 2016; VERHOEF *et al.*, 2017). À medida que elas passam a estar presentes em todas as áreas, as empresas estão nomeando executivos para liderarem as suas agendas digitais e para ressaltarem a importância que as tecnologias digitais desempenham no contexto atual, pois elas estão diante da necessidade de usá-las da maneira mais eficiente possível (SCHNEIDER; KOKSHAGINA, 2020), visto que estão em todo lugar, desempenhando um papel cada vez mais importante na vida das pessoas (COLBERT; YEE; GEORGE, 2016). As tecnologias digitais são usadas para incrementar o desempenho e as capacidades de um usuá-

rio, sistema ou processo (GUILBAUD; HAYES; HAMED, 2019). Elas são empregadas para permitir a conectividade entre os componentes, bem como buscar informações, transformar e armazenar dados. No contexto da integração mútua e de otimização das tecnologias digitais, isso torna mais simples e conveniente a produção, o processamento e a moldagem de produtos (XIA *et al.*, 2013).

Dentre as tecnologias que impactam o processo de TD das empresas, os autores Costa *et al.* (2022) apontam que *Internet* das coisas (IoT), *big data* e *analytics*, inteligência artificial (IA), computação em nuvem, sistemas ciber-físicos e impressão 3D são as mais relevantes na atualidade. De acordo com a literatura, não há um conjunto específico e estático de tecnologias da TD. Elas variam de acordo com o negócio de uma empresa e da disponibilidade tecnológica em um momento histórico ou lugar específico.

O desafio é como as empresas vão conduzir a velocidade crescente e os riscos impostos pelas novas e disruptivas tecnologias (VIAL, 2019). Trata-se de considerar o efeito que o uso das tecnologias digitais exercem na sociedade, as quais enfrentam uma disrupção viral que impacta a noção de prosperidade a qualquer custo, bem como os fundamentos da confiança nas instituições e em um futuro melhor (CARAYANNIS *et al.*, 2021). Risco pode ser entendido como a possibilidade de um evento ter resultados inesperados, a incerteza do desconhecido ou como os seus efeitos são percebidos (LEMOS, 2020). Ele é a probabilidade de variação de um resultado esperado (SPEKMAN; DAVIS, 2004). Adiciona-se ainda o fato das empresas estarem expostas a riscos que podem causar interrupções inesperadas em razão de greves, desastres naturais ou falhas com fornecedores (LIBRANTZ *et al.*, 2021). Com um aumento na complexidade, a TD elevou esse tema a um novo patamar, com a inserção de riscos sistêmicos e estruturais (GAIVORONSKAYA *et al.*, 2020).

1.2 SITUAÇÃO-PROBLEMA

O progresso e o desenvolvimento tecnológico acumulado desde a revolução das tecnologias da informação, resultaram na integração de tecnologias digitais que estão mudando o modo como as empresas se organizam e interagem entre si (LAMBERTON; STEPHEN, 2016; ARAUJO; OLIVEIRA *et al.*, 2017; VERHOEF *et al.*, 2017). Em um contexto de mudanças disruptivas, a busca por eficiência e modernização trouxe a TD para as empresas (VIAL, 2019), o que afeta direta e indiretamente a vida das pessoas.

Com a globalização das atividades das empresas e a difusão das tecnologias digitais, pessoas e empresas estão se tornando conectadas, com a troca e o compartilhamento de dados entre elas, incrementando os riscos no uso das tecnologias (MIYAZAWA *et al.*, 2020).

Diante desse cenário, a computação em nuvem, por exemplo, contém o risco associado ao poder de mercado de poucos fornecedores (NUCCIO; GUERZONI, 2019), ao passo que *IoT*, com milhares de sensores espalhados pelas cidades, põe em risco a privacidade e a liberdade individual (CARAYANNIS *et al.*, 2021). Já a IA pode transportar ideias preconcebidas para

dentro dos algoritmos, ou seja, agir como uma extensão de valores, ou de preconceitos humanos (PERES *et al.*, 2020). Há ainda, do ponto de vista de uma nação, a probabilidade de dependência tecnológica diante da compra de tecnologia de outros países, o que compromete a autonomia e a soberania nacionais (AL-ALI, 1991). No contexto da TD, a literatura afirma que os riscos percorrem vários setores, incluindo as empresas, a sociedade e os próprios países (BIRKEL *et al.*, 2019). Adiciona-se a isso a preocupação com restrições legais sobre privacidade com o uso de dados de empresas e de consumidores por algorítimos de IA e o aprendizado de máquina, os quais podem desencadear riscos como roubo ou vazamento de dados (MIYAZAWA *et al.*, 2020).

Todavia, à medida que os são gerenciados, é possível que a TD seja um instrumento que aumente o desenvolvimento econômico, social e que não abale a confiança nas instituições e um futuro próspero (CARAYANNIS *et al.*, 2021).

Neste contexto, o problema de pesquisa a ser tratado nesta dissertação é identificar e classificar os riscos mais relevantes que as empresas estão sujeitas com o uso das tecnologias digitais. Não se trata somente do uso de uma tecnologia específica, mas sim da integração de várias delas no contexto da TD, e o que eleva o tema risco a um novo patamar.

1.3 Questão de Pesquisa

A partir da revisão da literatura e a situação problema apresentada para atender o propósito da pesquisa com suporte dos autores pesquisados, a seguinte questão de pesquisa é colocada: Como propor um *framework* para a identificação e a classificação dos riscos da segurança da informação associados ao uso de tecnologias da TD nas empresas?

1.4 Objetivos

1.4.0.1 Objetivo Geral

A partir da problemática estabelecida para o tema risco da segurança da informação no uso das tecnologias da TD, o seguinte objetivo geral foi estabelecido.

- **Desenvolver e validar um *framework* de riscos da segurança da informação que permita a orientação das empresas quanto aos desafios no uso das tecnologias da TD.**

1.4.0.2 Objetivos Específicos

De modo a viabilizar o atendimento deste objetivo geral, os seguintes objetivos específicos foram estabelecidos:

- **Identificar os riscos da segurança da informação das tecnologias digitais;**

- **Classificar os riscos da segurança da informação das tecnologias digitais;**
- **Desenvolver um *framework* de riscos da segurança da informação das tecnologias digitais;**
- **Validar o *framework* de riscos da segurança da informação das tecnologias digitais.**

1.5 JUSTIFICATIVA

Esta pesquisa se justifica devido ao fato de que nenhum setor ou área das empresas está fora dos efeitos da TD e esta se tornou uma resposta para essa pressão da economia digital, ganhando o *status* de prioridade estratégica (HESS *et al.*, 2016).

Alguns fatos corroboram essa percepção de urgência com relação ao tema riscos no uso das tecnologias da TD, pois de acordo com Cisco (2020) por meio do Relatório Anual da *Internet*, em 2023 o mundo terá por volta de 5.3 bilhões de usuários conectados à *Internet*, ou seja, 66% da população global, incluindo aproximadamente 4 dispositivos conectados por cidadão, um número que chegará próximo de 29 bilhões de dispositivos, com 50% destes conectados entre eles por meio de conexões *Machine-To-Machine* (M2M). Ainda de acordo com esse relatório, 70% da população mundial terá conexão móvel por volta de 2023, incluindo 10% desses dispositivos com a tecnologia 5G.

Já o IDC (2020) prevê que em 2025 os dados gerados pelos dispositivos de *IoT* serão de aproximadamente 73 zettabytes, partindo de 18 zettabytes em 2019 (e grande parte desses dados serão oriundos de vídeos), porém as aplicações industriais de *IoT* terão uma representação significativa desses dados.

De acordo com Gartner (2021), leis modernas de privacidade cobrirão 75% da população mundial, e por volta de 2025, 60% das empresas usarão algum critério de risco de segurança como determinante para conduzir negócios com terceiros. Ainda de acordo com Gartner (2021), até o final de 2025 haverá um aumento de 30% nas nações que terão legislações para regulamentar pagamentos em razão de ataques de *ransomware*.

Dessa forma, identificar e classificar os riscos inerentes às tecnologias da TD é um fator relevante para as empresas que poderão implementar estratégias de proteção e de segurança cibernética. Vale ressaltar ainda que o mundo está presenciando a transição de uma sociedade industrial para uma de informação, com as tecnologias impondo desafios que requerem soluções efetivas e de qualidade (GAIVORONSKAYA *et al.*, 2020).

1.6 DELIMITAÇÃO DO TEMA

Esta dissertação tem como proposta a validação, por meio de um *framework*, dos riscos que as empresas estão sujeitas no uso das tecnologias digitais. No entanto, a TD envolve ainda

outros elementos, como: estratégias, processos, pessoas, comportamentos, cultura, mercado, clientes, etc, porém este trabalho se concentrará nas tecnologias. Destina-se exclusivamente às empresas, não sendo avaliados os riscos da TD dentro de instituições públicas, governos, órgãos governamentais, e de organizações não governamentais, nem mesmo cidadãos ou mesmo a sociedade como um todo. Por outro lado, o *framework* proposto neste trabalho pode ser aplicado em empresas privadas de diferentes setores, desde que estejam enquadradas em um contexto de uso de tecnologias digitais.

1.7 Estrutura da Dissertação

Esta dissertação está organizada da seguinte forma: o Capítulo 2 apresenta uma revisão sistemática da literatura. Já o Capítulo 3 trata do referencial teórico, ao passo que o Capítulo 4 apresenta a metodologia de pesquisa, incluindo a construção e validação do *framework* proposto. O Capítulo 5 expressa as considerações finais, expondo as contribuições para a área, as limitações da pesquisa e os trabalhos futuros.

CAPÍTULO 2

REVISÃO SISTEMÁTICA DA LITERATURA

Como forma de proporcionar uma coleta de dados neutra em uma situação na qual os resultados são imprevisíveis (BRYMAN, 2006), esta pesquisa é estruturada com uma revisão sistemática da literatura – a qual foi realizada com buscas nas bases de dados digitais *Web of Science* e *SCOPUS*, o que constitui o embasamento teórico da pesquisa, com o estado da arte sobre os riscos que o uso das tecnologias da TD trazem às empresas. Ela é estruturada a partir do método *PRISMA* (*Preferred Reporting Items for Systematic review and Meta-Analysis*), baseado em Moher *et al.* (2010), que divide a condução da pesquisa entre os seguintes passos: identificação, triagem, elegibilidade e inclusão. A fim de assegurar que todo o material analisado seja consistente e com o mínimo de perspectivas subjetivas, o item elegibilidade contempla os critérios de inclusão e de exclusão apresentados por Liao *et al.* (2017). Eles permitem um modo objetivo de identificar se os trabalhos resultantes das buscas são aderentes ao tema central da pesquisa e situam o presente estudo nas discussões que já vêm ocorrendo a partir da literatura existente.

2.1 BUSCAS NAS BASES DE DADOS DIGITAIS

A revisão sistemática da literatura se deu por meio de uma busca de trabalhos científicos nas bases de dados digitais *Web of Science* e *SCOPUS*. O **Quadro 2.1** apresenta os termos usados na expressão de busca.

Quadro 2.1: *Termos usados na expressão de busca*

Termo	**Operador Lógico**
Digital Transformation	AND
*Risk**	OR
Privacy	OR
*Breach**	OR
*Leak**	OR
*Mitigati**	OR
Security	OR

Fonte: autor

Os termos de busca foram acomodados de modo a proporcionar uma pesquisa que envolva a TD com o risco das tecnologias digitais, portanto o termo riscos é mandatório. As palavras privacidade, brecha, vazamento, mitigação e segurança ampliam a busca, já que são relacionadas a riscos. Vale notar que o termo tecnologias digitais não aparece no **Quadro 2.1**, pois observou-se que a procura por TD inclui automaticamente o conceito das tecnologias digitais.

O **Quadro 2.2** apresenta a expressão final utilizada nas pesquisas.

Quadro 2.2: *Expressão utilizada nas buscas*

"digital transformation"AND (risk* OR privacy OR breach* OR leak* OR mitigati* OR security)

Fonte: autor

As buscas forneceram o resultado bruto que pode ser observado no **Quadro 2.3**, sem ainda ter os critérios de inclusão e de exclusão aplicados, bem como contemplam eventuais duplicidades.

Quadro 2.3: *Resultado bruto*

Bases de Dados	**Número de Trabalhos**	**Data da Busca**
Web of Science	475	20 de outubro de 2021
SCOPUS	999	20 de outubro de 2021
Total de Estudos	1474	

Fonte: autor

O universo total retornado com as buscas nas bases de dados acadêmicas foi de 1474 trabalhos acadêmicos. O **Apêndice A** apresenta as expressões de busca e as condições específicas de cada base de dados.

2.2 CRITÉRIOS DE INCLUSÃO E DE EXCLUSÃO

A partir do resultado bruto obtido com a expressão de busca nas bases de dados digitais mencionadas, os critérios de inclusão e de exclusão apresentados por Liao *et al.* (2017) foram aplicados nos trabalhos. O **Quadro 2.4** apresenta os critérios de inclusão e de exclusão, com comentários.

Quadro 2.4: *Critérios de inclusão e de exclusão, com comentários*

I/E	Critérios	Comentários
E	RFB (em Razão da Ferramenta de Busca)	O artigo tem somente o título, *abstract* e palavras-chaves em inglês, mas sem o texto completo.
E	STC (Sem Texto Completo)	Texto completo inacessível.
E	NR (Não Relacionado)	NR-1: o trabalho não é um artigo acadêmico; NR-2: a definição de risco não está relacionada com TD.
I	VR (Vagamente Relacionado)	VR-1: Risco e TD são usados como exemplos; VR-2: Risco e TD são utilizados para trabalhos futuros; VR-3: Risco e TD são empregados como expressões; VR-4: Risco e TD estão presentes como palavras-chaves.
I	PR (Parcialmente Relacionado)	PR-1: Risco e TD são utilizados como desafios ou tendências; PR-2: Risco e TD são um dos tópicos revisados ou discutidos.
I	TR (Totalmente Relacionado)	Os esforços da pesquisa são explicitamente dedicados a Risco e à TD.

Fonte: adaptado de Liao *et al.* (2017)

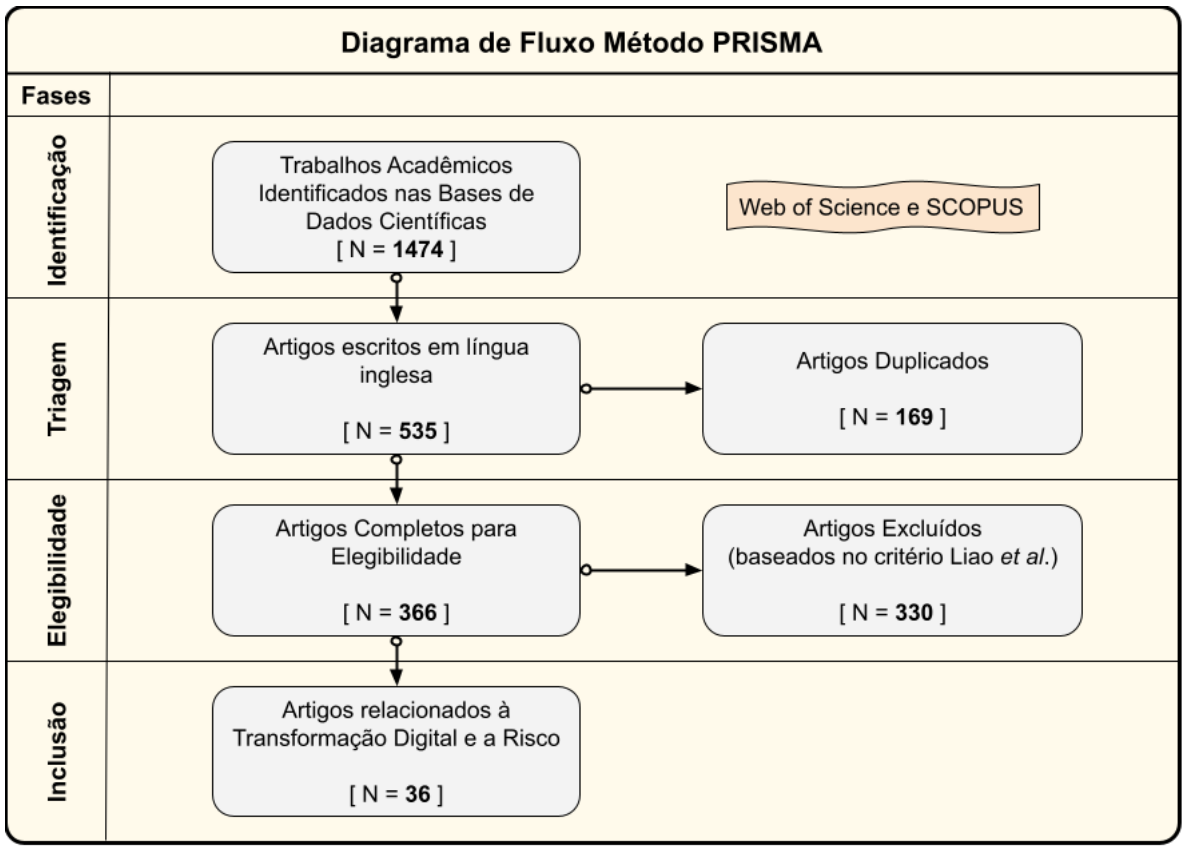
Dois princípios nortearam a revisão da literatura desse estudo:

- Revisão Objetiva: cada trabalho coletado foi revisado para determinar a sua inclusão ou exclusão. O *abstract* e as palavras-chaves foram analisados inicialmente, de modo a verificar objetivamente se o trabalho era aderente aos critérios estabelecidos;
- Coleta de dados com evidências: à medida que se observou que o trabalho era aderente aos critérios estabelecidos, dados relevantes foram capturados, incluindo anotações para fundamentar elementos importantes da pesquisa.

2.3 MÉTODO PRISMA

Com a aplicação do método *PRISMA* (*Preferred Reporting Items for Systematic review and Meta-Analysis*), baseado em Moher *et al.* (2010), a revisão sistemática da literatura resultou na amostra apresentada na **Figura 2.1**.

Figura 2.1: *Aplicação do Método PRISMA*



Fonte: autor

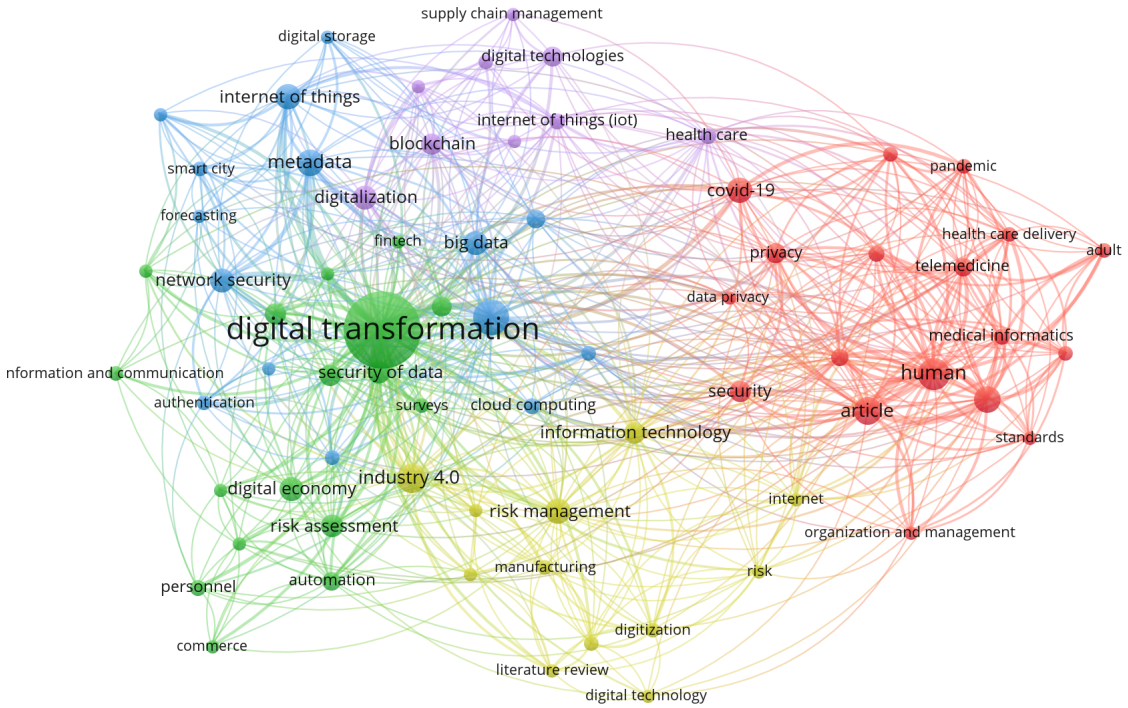
Os trinta e seis estudos selecionados da base científica estão relacionados no **Apêndice B**. Para cada um deles foi atribuída uma identificação do número um até o número trinta e seis, tendo como critério a ordem da descoberta do estudo.

2.4 ANÁLISE BIBLIOMÉTRICA

A revisão sistemática da literatura foi acompanhada de uma análise bibliométrica que fizeram uso das ferramentas *VosViewer* e *Biblioshiny*. As análises foram realizadas durante as buscas iniciais com testes das palavras chaves, e posteriormente já com os dados consolidados para entender o nível de estudo sobre o tema pela academia.

A **Figura 2.2** apresenta o gráfico de correlação de palavras chaves gerado pelo *VosViewer*.

Figura 2.2: *Correlação das Palavras Chaves*

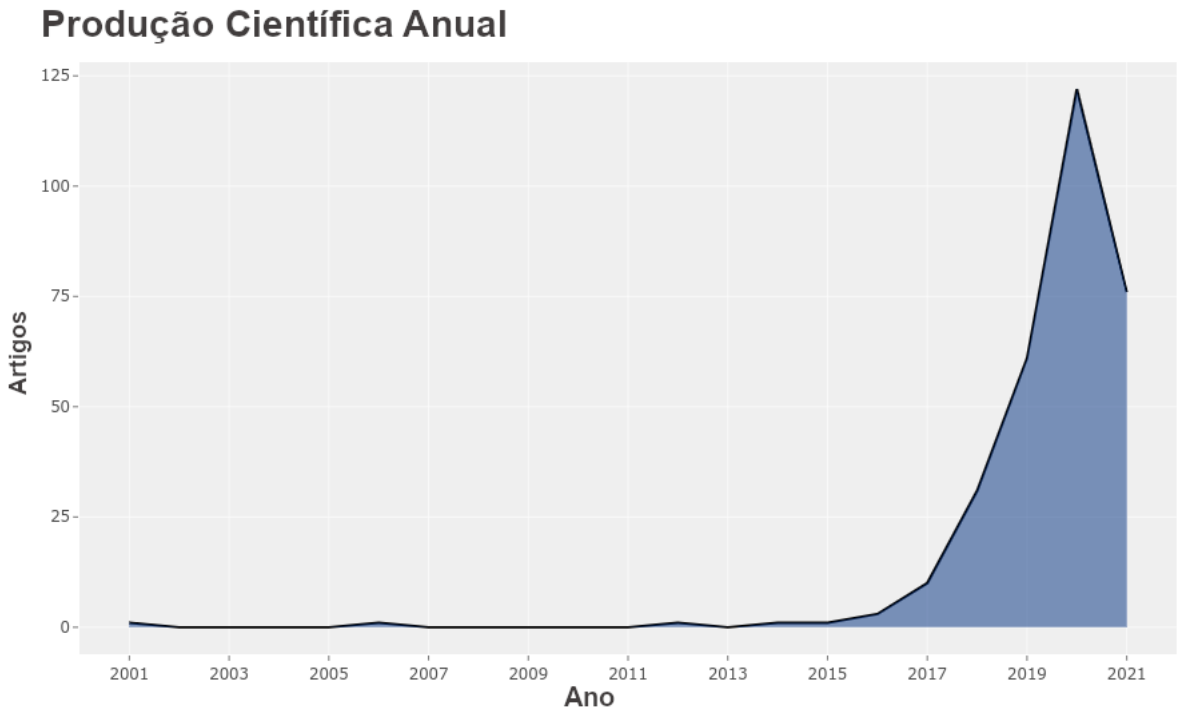


Fonte: autor

É possível observar na **Figura 2.2** a existência de 5 (cinco) *clusters* em que o primeiro na cor verde reúne a TD com os termos economia digital, comércio, automação, segurança de dados e avaliação de riscos. O segundo na cor azul reúne as tecnologias da TD como *IoT*, *big data*, computação em nuvem, armazenamento digital e conceitos mais gerais como digitalização e cidades inteligentes. O terceiro *cluster* na cor lilás também indica *IoT*, adiciona *blockchain* e traz o termo tecnologias digitais. O quarto no cor vermelha traz o contexto humano que inclui o termo pandemia, telemedicina e adiciona o termo privacidade de dados. O quinto *cluster* traz os termos gerenciamento de riscos, TI e Indústria 4.0 (I4.0). Vale notar que o termo risco foi citado em dois *clusters*. Isso ajuda a entender a razão pela qual os riscos não aparecem como protagonistas, mas como um efeito de todas as tecnologias e conceitos ligados à TD que são apresentados.

A **Figura 2.3** apresenta o gráfico gerado pelo *Biblioshiny* do crescimento anual de produções científicas sobre o tema.

Figura 2.3: *Produção Científica Anual*

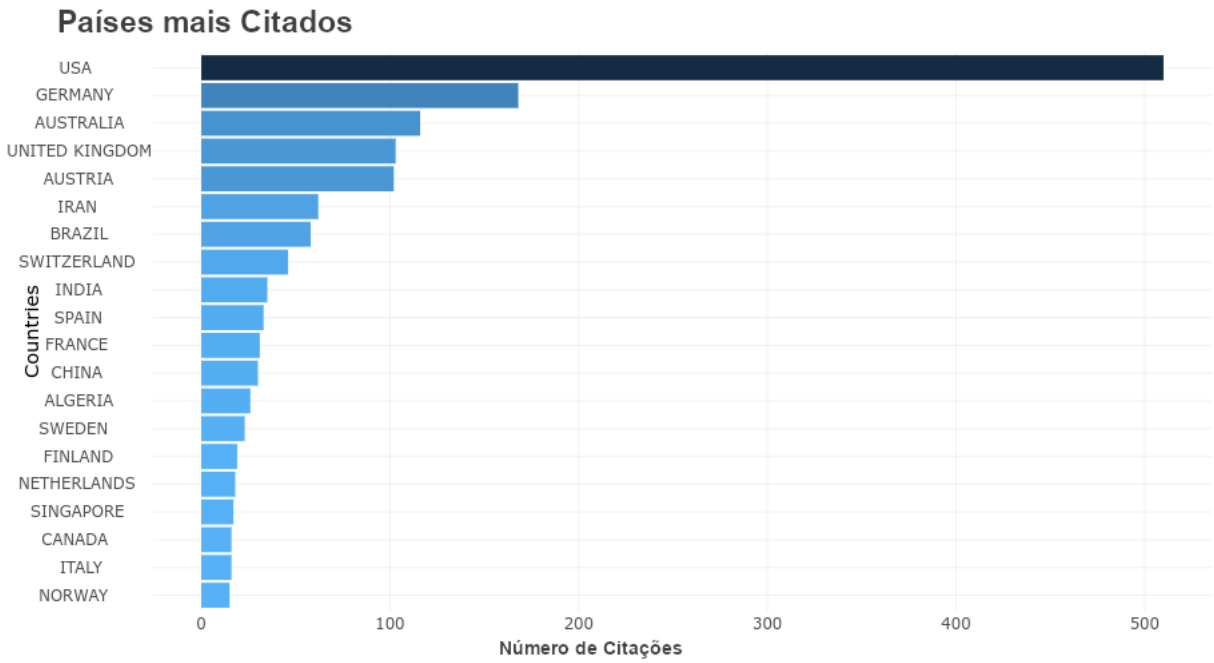


Fonte: autor

Como a **Figura 2.3** apresenta, observa-se que não havia pesquisas expressivas sobre o tema até 2015, quando começou a ocorrer um crescimento acentuado. Isso revela a novidade do tema e a necessidade de tratá-lo em razão do crescimento acelerado no uso das tecnologias digitais.

A **Figura 2.4** apresenta o gráfico gerado pelo *Biblioshiny* dos países com mais citações.

Figura 2.4: *Países mais Citados*

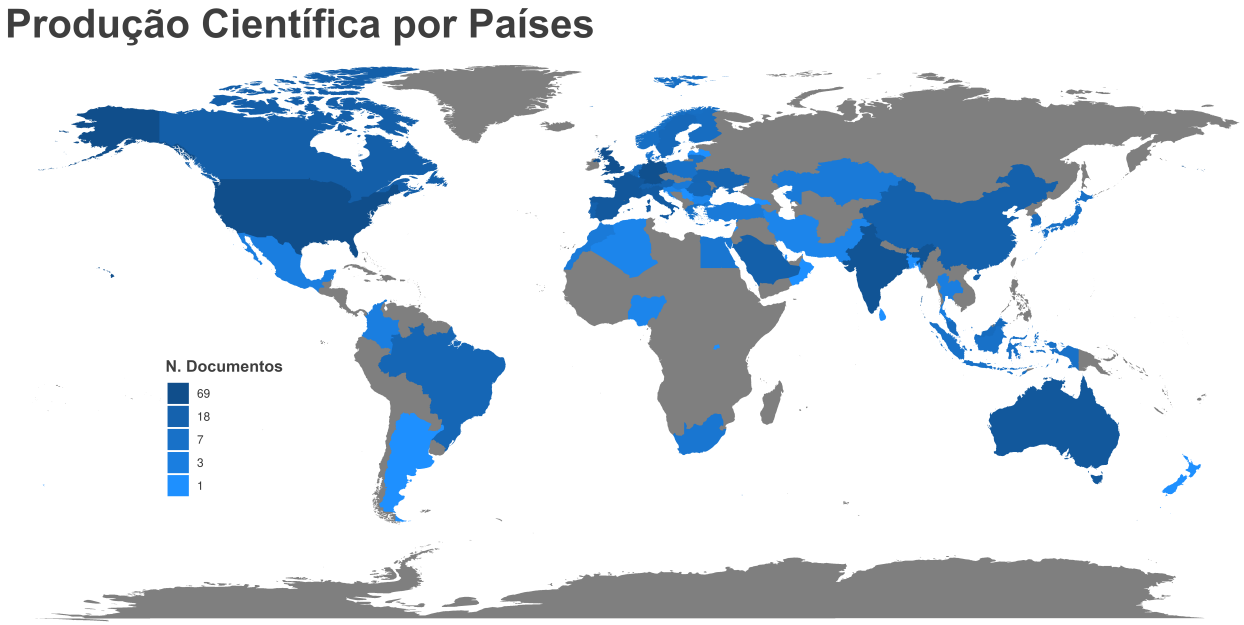


Fonte: autor

No gráfico com os países mais citados, como apresenta a **Figura 2.4**, o Brasil está em sétimo lugar com aproximadamente 80 (oitenta) citações. Os Estados Unidos lideram com mais de 500 (quinhentas) citações. Há uma diferença expressiva com a Alemanha que é a segunda na lista, com aproximadamente 200 citações. Esse gráfico revela o foco dados pelos Estados Unidos ao tema estudado. Vale notar que a China aparece em décimo segundo lugar. Embora seja um país com uma robusta produção acadêmica, não apresentou um volume de citações expressiva para o tema.

A **Figura 2.5** apresenta o gráfico gerado pelo *Biblioshiny* com o volume de produção acadêmica dos países.

Figura 2.5: *Produção Academica dos Países*



Fonte: autor

Como mostra a Figura 2.5, a produção acadêmica mostra um resultado diferente quanto comparado com as citações. É possível observar os Estados Unidos, partes da Europa e Índia com uma densa produção acadêmica, tendo a China com uma expressiva contribuição. Vale observar que o Brasil está situando com a produção de 7 (sete) trabalhos acadêmicos.

CAPÍTULO 3

FUNDAMENTAÇÃO TEÓRICA

Esta seção apresenta a plataforma teórica prevista para o desenvolvimento da pesquisa, apresentando os conceitos relacionados com a TD, as tecnologias da TD e os riscos no uso das tecnologias digitais.

3.1 TRANSFORMAÇÃO DIGITAL

O tema TD tornou-se alvo de atenção do mundo corporativo e acadêmico, mas ainda é um desafio ter uma definição clara, precisa e conjunta sobre ele (MORAKANYANE; GRACE; O'REILLY, 2017). Grande parte da dificuldade em ter um significado exato quanto a esse tópico é o fato de a TD ter uma perspectiva multidisciplinar (HAUSBERG *et al.*, 2018). Uma característica importante dela é o uso integrado de tecnologias que alcançam e impactam os processos dentro das empresas e que têm a particularidade de impactar as sociedades e as pessoas (URBINATI *et al.*, 2020).

Nesse prisma, como afirmam Hausberg *et al.* (2018), o componente humano é um aspecto da TD, seja nos meios, seja nos objetivos. O uso integrado dessas tecnologias digitais altera o modo como os indivíduos trabalham e tem o objetivo final de aperfeiçoar as condições materiais da sociedade (URBINATI *et al.*, 2020).

Para Schneider e Kokshagina (2020), em entrevistas com executivos, há uma confusão ao definir o termo digital, pois se trata de algo bastante saturado e que pode ter diversos significados. Ainda de acordo com esses autores, embora existam definições que enfatizam a tecnologia em si, os aspectos transformadores, as estratégias e os modelos de negócios foram incorporados a essa palavra.

Já de acordo com Carayannis *et al.* (2021), a perspectiva multidisciplinar da Transformação Digital leva em consideração o ponto de vista da sociedade. Dessa forma, as oportunidades que acompanham essa revolução são importantes, mas vêm acompanhadas de riscos que afetam diretamente as pessoas. Para O'Leary e Armfield (2020), a TD é descrita como o uso de tecnologias para aperfeiçoar radicalmente as empresas e para repensar como elas se utilizam desse recurso, bem como de pessoas e de processos para alterar o desempenho dos negócios.

Diante dos conceitos e das definições expostos aqui, é possível observar que a TD não tem uma significação unificada. As perspectivas são diferentes, de acordo com os autores e seus campos de estudos, mas todos eles são capazes de elaborar uma definição própria para esse evento que está revolucionando as sociedades.

3.2 TECNOLOGIAS DA TRANSFORMAÇÃO DIGITAL

Bharadwaj *et al.* (2013) e Vial (2019) identificam que a inovação por trás da TD é a combinação da informação, computação, comunicação e tecnologias de conectividade. Como afirmou Hausberg *et al.* (2018), muitas das tecnologias que estão diretamente ligadas à TD não são novas, porém, como observaram Araujo, Oliveira *et al.* (2017), o processo evolutivo que ocorreu nas últimas décadas, partindo da informática até a sociedade da informação, pavimentou o caminho que viabilizou um evento com a intensidade que tem a TD.

Com os exemplos de Cheng *et al.* (2016), é possível listar algumas tecnologias, como *internet* das coisas, computação em nuvem, *big data*, sistemas ciberfísicos, realidade virtual e aumentada e, finalmente, a IA. Esta especificamente reserva alguns desafios. Como observaram O'Leary e Armfield (2020), o objetivo final dela é a criação de um algoritmo que seja capaz de resolver problemas e realizar tarefas cognitivas de modo apropriado ou melhor que os humanos.

Já a robotização de processos é uma tecnologia que merece atenção e como ressaltou Siderska (2020), não substitui a IA ou o aprendizado de máquina, mas é capaz de desempenhar tarefas automáticas e repetitivas, como, por exemplo, a mineração de dados.

Como pontuaram Yang, Xiong e Ren (2020) em relação à tecnologia de nuvem, outros mecanismos, como a *IoT*, depositam dados e dependem da nuvem para alcançarem a integração que a TD vem proporcionando, a qual permeia os cidadãos e as empresas.

Como é possível notar, o universo das tecnologias disponíveis é muito amplo, por isso uma definição estática delas seria de certo modo incompleta. É importante notar que as que hoje causam preocupação, em poucos anos estarão incorporadas aos cidadãos e às empresas, assim não mais representando uma ameaça. Do mesmo modo como Gaivoronskaya *et al.* (2020) identificou riscos hipotéticos de tecnologias como a IA, a qual será um potencial risco à humanidade daqui a alguns anos, as que no passado proporcionaram inovações e riscos, hoje estão completamente incorporadas à sociedade.

3.3 RISCOS NO USO DAS TECNOLOGIAS DIGITAIS

Como afirma El-Haddadeh (2020), as tecnologias se tornaram um requisito para uma empresa ter vantagens competitivas. Por outro lado, como observou Hausberg *et al.* (2018), mesmo com os ganhos da TD, pesquisadores estão começando a discutir os efeitos negativos da digitalização. Nesse viés, o esforço a ser empreendido aqui é relacionar o uso das tecnologias digitais com os riscos inerentes a esse processo. Embora os benefícios sejam relevantes, não é possível ignorar os riscos que estão associados a eles.

Como identificou Carayannis *et al.* (2021), o risco sempre acompanhou a humanidade, porém, de certo modo, foi gerenciado. No tocante à TD, Gaivoronskaya *et al.* (2020) identifica que ela traz riscos sistêmicos e estruturais, como a segurança econômica, que reside na dependência de tecnologias de outros países, e a falta de suas bases elementares para a construção delas. Já

Panda e Bower (2020) citam a integração desse processo com tecnologias de terceiros como uma fonte de perigo. Isso aumenta os riscos de cibersegurança e a sua complexidade, pois uma vulnerabilidade pode estar associada justamente a um elemento externo (esse tipo de dependência foi identificada pelo Parlamento Europeu em 2019). Hoje, o mundo está globalizado, com as sociedades profundamente integradas. Nesse cenário, as tecnologias dão uma velocidade que impõem um desafio importante, pois ainda de acordo com Carayannis *et al.* (2021), é preciso melhorar a condição das pessoas e reforçar a expectativa em um futuro melhor.

Adicionalmente, Gaivoronskaya *et al.* (2020) pontuam que a IA pode trazer riscos e desafios difíceis de serem calculados, os quais podem causar incertezas sem precedentes. Em suma, trata-se da dificuldade em predizer claramente os riscos envolvidos com o uso de IA nos diversos setores das sociedades. É possível desenhar cenários drásticos, como a perda do controle de sistemas militares, mas há horizontes mais simples que contemplam a dificuldade em se ter leis e regulações para o uso adequado de tecnologias dessa natureza, sem que se transformem em um risco.

Panda e Bower (2020) afirmam que a TD adicionou uma nova camada de risco, que é a cibernética, a qual pode sofrer um efeito cascata a partir de um evento natural, como um desastre, que pode desencadear efeitos inesperados na infraestrutura que suporta as tecnologias digitais. Por exemplo, uma indisponibilidade prolongada de energia elétrica pode afetar diretamente a continuidade dos centros de dados.

Nesse cenário, a possibilidade da ocorrência de um efeito cascata traz um termo antes reservado à literatura sobre ciberguerra e ciberterrorismo. Trata-se da infraestrutura crítica que representa os sistemas e os ativos, que podem ser físicos ou virtuais. Se eles estiverem destruídos ou comprometidos, podem causar um impacto debilitador na segurança nacional, na segurança econômica, na saúde pública ou em todos os itens combinados (HR3162, 2001). É importante ressaltar que o ciberespaço compõe a infraestrutura crítica, aos passo que o DHS (2003) define-o como computadores, servidores, roteadores e cabos que viabilizam o funcionamento daquela.

Owen (2007) lista alguns itens que fornecem uma dimensão mais doméstica da infraestrutura crítica, como energia, alimentação, transporte, sistema bancário e comunicação. Já Zarzuelo (2021) inclui os portos como parte integrante dela, em razão de uma cadeia global de suprimentos que inclui a integração com as redes de transporte, de energia e de telecomunicações. Como observou Zarzuelo (2021), a *IoT* e o gerenciamento de uma grande quantidade de dados disponíveis na nuvem criam uma importante dependência da infraestrutura crítica. Para Yang, Xiong e Ren (2020), à medida que a nuvem hospeda um volume maior de dados, incluindo os sensíveis, aumenta a preocupação com relação a potenciais ataques cibernéticos, os quais têm os dados como alvo.

Dessa maneira, é possível observar que esses exemplos contemplam indústrias de naturezas distintas, mas há pontos em comum, como a busca por competitividade e a TD (meio pelo qual elas estão trabalhando para atingir esse objetivo). O risco surge quando áreas sensíveis

alcançadas pela TD sofrem um evento inesperado. Como pontuou Panda e Bower (2020), um evento súbito pode ser um desastre ou mesmo uma ação humana com o propósito de causar danos.

Fekete e Rhyner (2020) observam que o uso intensivo de tecnologias digitais pode aumentar o risco humano e a vulnerabilidade social. Trata-se de reconhecer que países, empresas e cidadãos não são iguais. Segundo esses autores, nem todos os seres humanos estão conectados à *Internet*, pois isso depende da infraestrutura de telecomunicação, da renda e da localização da pessoa. Isso resulta nas desigualdades digitais ou em diferentes formas de igualdade. Essa visão é relevante para cidadãos e empresas de regiões menos desenvolvidas, as quais sofrem pressão para a adoção e para a implantação da TD, porém sem estarem em paridade, no ponto de partida, com outras mais desenvolvidas. Ainda de acordo com Fekete e Rhyner (2020), essa vulnerabilidade social pode marginalizar localidades e empresas inteiras, de modo que tenham grande dificuldade em acompanhar o ritmo de adoção de tecnologias avançadas, criando então o que se chama de divisão digital.

Já Nuccio e Guerzoni (2019) pontuam que o risco pode existir no processo de concentração das plataformas digitais e no alto investimento em inovação que essas indústrias requerem, como, por exemplo, computação em nuvem. No entanto, somente empresas que alcançam um certo poder de mercado conseguem viabilizar o elevado aporte necessário para inovação das plataformas digitais. Esse poder de mercado e de concentração podem dificultar a entrada de novos participantes e, por fim, prejudicar todo o sistema.

CAPÍTULO 4

METODOLOGIA DE PESQUISA APLICADA

As seções seguintes apresentam e descrevem os métodos adotados na condução desta dissertação.

4.1 FUNDAMENTOS METODOLÓGICOS

Esta dissertação é exploratória e qualitativa, pois emprende-se uma identificação e classificação dos riscos envolvidos no uso das tecnologias digitais da TD nas empresas, por meio de uma revisão sistemática da literatura, o que fundamentou a criação de um *framework*, com a aplicação de um questionário como instrumento de pesquisa para a coleta de dados. A perspectiva quantitativa deste trabalho é a validação do *framework* por meio da escala *Likert* do questionário.

O resultado deste trabalho é a construção de um *framework* de riscos validados inerentes ao uso das tecnologias digitais da TD. Isso permitirá às empresas implementar estratégias de proteção e de segurança cibernética.

4.2 IDENTIFICAÇÃO DOS RISCOS

A revisão sistemática da literatura empreendida na condução desta dissertação permitiu identificar riscos que permeiam o uso das tecnologias digitais. Sabe-se que eles existem, mas a revisão de literatura permitiu a seleção de riscos conectados à realidade, preocupação de outros pesquisadores, que embora otimistas com a revolução tecnológica que está em curso, começam a dar atenção aos efeitos negativos dessa mudança rápida (HAUSBERG *et al.*, 2018).

Os critérios de inclusão e de exclusão do método *PRISMA* selecionaram 36 (trinta e seis) artigos acadêmicos que se encontram como completamente relacionados, ou seja, os esforços da pesquisa são diretamente dedicados a riscos da TD. Foram identificados 21 (vinte e um) riscos que permeiam o uso das tecnologias digitais e que podem ser observados no **Quadro 4.1**, em ordem de ocorrência.

Quadro 4.1: *Riscos Identificados*

Identificação	Risco	Ocorrências
a	Privacidade	18
b	*Malware*	8
c	*Ransonware*	8
d	Vazamento de Informação	7
e	Roubo e Manipulação de Dados	5
f	Acesso não Autorizado	5
g	*Phishing*	4
h	Divulgação de Informação	4
i	*DoS*	3
j	*Data Breach*	3
k	*Spoofing*	3
l	*Spyware*	2
m	Vírus	2
n	*Tampering*	2
o	*Sniffing*	2
p	*Worms*	1
q	*Bombs*	1
r	*Trojans*	1
s	*MitM attacks*	1
t	*Repudiation*	1
u	Elevação de Privilégios	1

Fonte: autor

Os riscos, a partir da coluna Identificação, são classificados por letras que vão de "a"até "u", reunindo deste modo os 21 (vinte e um) riscos observados na revisão sistemática e que auxiliará na leitura do **Quadro 4.2**, o qual relaciona os riscos e seus respectivos autores.

Quadro 4.2: *Autores* versus *Riscos*

Autores	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**
Nuccio e Guerzoni (2019)	x																				
Riyana e Natwichai (2018)	x																				
Vasil'ev, Zegzhda e Poltavtseva (2018)						x															
Tokody *et al.* (2018)	x																				
Rossi, Rubattino e Viscusi (2019)	x																				
Birkel *et al.* (2019)	x																				
Khanboubi e Boulmakoul (2019)					x	x															
Mendhurwar e Mishra (2021)	x			x		x	x		x				x		x	x	x	x			
Baghdasarin (2019)														x							
Eckhart *et al.* (2019)		x	x																		
Shi, Jin e Li (2019)	x	x				x									x						
Alharbi (2020)		x																			
Popescu *et al.* (2020)	x																				
Park, Li e Hong (2020)				x																	
O'Leary e Armfield (2020)	x																				
Puraite *et al.* (2020)	x																				
Kabbas, Alharthi e Munshi (2020)		x																			
Panda e Bower (2020)		x																			
Zarzuelo (2021)			x																		
Yang, Xiong e Ren (2020)	x			x		x		x													
El-Haddadeh (2020)	x																				
Fard *et al.* (2020)		x																			
Oliveira *et al.* (2020)											x								x		
Sestino *et al.* (2020)	x			x																	
Kavallieratos e Katsikas (2020)								x			x			x						x	x
Bhattacharjee, Chen e Dasgupta (2020)	x							x		x											
Elizaveta e Tjasa (2020)	x																				
Tech (2020)		x	x				x		x			x									
Gaivoronskaya *et al.* (2020)			x	x	x																
Bocayuva (2021)			x																		
Lee (2021)	x		x		x		x		x		x	x	x								
Krafft *et al.* (2021)	x			x				x		x											
Dobrolyubova (2021)	x			x																	
Chalyuk *et al.* (2021)			x																		
Spivakovskyy *et al.* (2021)					x																
Creazza *et al.* (2021)		x	x		x		x			x											
Total	**18**	**8**	**8**	**7**	**5**	**5**	**4**	**4**	**3**	**3**	**3**	**2**	**2**	**2**	**2**	**1**	**1**	**1**	**1**	**1**	**1**

Fonte: autor

Diante dos riscos identificados e para selecionar aqueles mais relevantes, recorre-se ao autor Ballou (1993), o qual observa que o conceito de Curva ABC é largamente utilizado em empresas para classificação de informações de diversas origens. Esse instrumento é importante porque perante todos os riscos identificados, há aqueles com um baixo número de ocorrências nos artigos percorridos, indicando que são de baixa relevância. Por outro lado, há aqueles que foram muito citados e que merecem uma análise mais aprofundada. Para diferenciá-los, a classificação foi feita da seguinte forma: os itens de maior relevância são categorizados com A, os de média importância são classificados como B e finalmente os de baixa importância são classificados como C. Vale notar que o conceito de classificação ABC é utilizado em diversas aplicações tanto na perspectiva profissional como na pessoal (ALVARENGA; NOVAES, 2000).

Já de acordo com Pacchini *et al.* (2019), um aspecto da Curva ABC que deve ser observado é que os percentuais para classificação não seguem uma regra matemática fixa para todos os casos, com valores de corte diferentes para cada uma das faixas de categorização (A, B e C). Ainda segundo Pacchini *et al.* (2019), diante dessa falta de uniformidade e da ausência de referências sobre o tema na literatura, o seguinte critério de classificação foi utilizado: 70% das citações compõem os itens A, 17% os B e finalmente 9% os C.

O **Quadro 4.3** apresenta a classificação dos riscos mais citados, o que levou a um resultado de oito riscos mais relevantes, classificados como A, com representatividade de 70% do total de oitenta e duas citações nos artigos acadêmicos pesquisados e selecionados.

Quadro 4.3: *Indicação dos Riscos Relevantes com uso da Curva ABC*

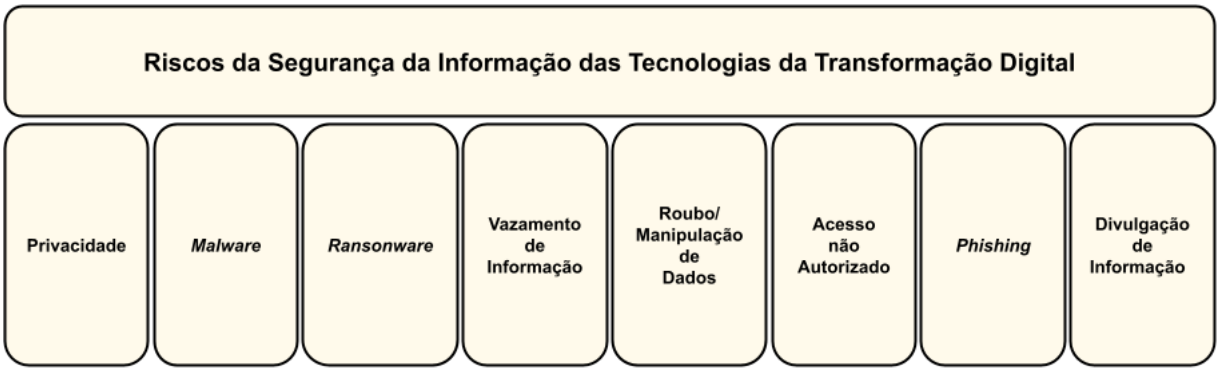
Risco	# Citações	% Citações	% Total	ABC	Descrição
a	18	21,43%	21,43%	A	Privacidade
b	8	9,52%	30,95%	A	*Malware*
c	8	9,52%	40,48%	A	*Ransonware*
d	7	8,33%	48,81%	A	Vazamento de Informação
e	5	5,95%	54,76%	A	Roubo e Manipulação de Dados
f	5	5,95%	60,71%	A	Acesso não Autorizado
g	4	4,76%	65,48%	A	*Phishing*
h	4	4,76%	70,24%	A	Divulgação de Informação
i	3	3,57%	73,81%	B	*DoS*
j	3	3,57%	77,38%	B	*Data Breach*
k	3	3,57%	80,95%	B	*Spoofing*
l	2	2,38%	83,33%	B	*Spyware*
m	2	2,38%	85,71%	B	Vírus
n	2	2,38%	88,10%	B	*Tampering*
o	2	2,38%	90,48%	C	*Sniffing*
p	1	1,19%	91,67%	C	*Worms*
q	1	1,19%	92,86%	C	*Bombs*
r	1	1,19%	94,05%	C	*Trojans*
s	1	1,19%	95,24%	C	*MitM attacks*
t	1	1,19%	96,43%	C	*Repudiation*
u	1	1,19%	97,62%	C	Elevação de Privilégios

Fonte: autor

4.3 *Framework* PROPOSTO

Com base no critério de seleção adotado e para efeito desta dissertação, o *framework* será composto dos riscos considerados como mais relevantes e que foram classificados pela Curva ABC como tal. A **Figura 4.1** representa graficamente o *framework* proposto.

Figura 4.1: *Representação Gráfica do Framework*



Fonte: autor

Esses são os riscos da segurança da informação mais relevantes oriundos do uso das tecnologias da TD:

a. **Privacidade:** a preservação da privacidade se tornou uma antítese para a ideia de uma era digital. Seja nos dispositivos inteligentes utilizados, nos serviços digitais ou mesmo os lugares visitados, os dados sobre as atividades, os hábitos e as preferências dos usuários estão sendo coletados em uma escala sem precedentes. No entanto, privacidade é um direito humano fundamental, e também é considerado um efeito colateral dos serviços personalizados e monetizados oferecidos às pessoas (BHATTACHARJEE; CHEN; DASGUPTA, 2020).

b. ***Malware*:** é a ferramenta principal dos cibercriminosos para atacar sistemas digitais. Trata-se de um programa de computador malicioso que inclui vírus, *worms*, *trojans*, *backdoors* e *rootkits* (FARD *et al.*, 2020).

c. ***Ransomware*:** o mundo conectado proporciona novas oportunidades para cibercriminosos que coletam dados pessoais para transações fraudulentas ou para introduzir um *ransomware* – um programa de computador malicioso que bloqueia ou encripta dispositivos, sendo pedido dinheiro como troca pela chave de decriptação (CHALYUK *et al.*, 2021).

d. **Vazamento de Informação:** trata-se da propagação descontrolada de informação para fora de uma empresa, dos limites físicos ou territoriais, bem como de um círculo de pessoas que tem acesso à informação (GAIVORONSKAYA *et al.*, 2020).

e. **Roubo e Manipulação de Dados:** um usuário tem dados sensíveis armazenados em uma solução de nuvem que consiste em vários servidores. Um invasor pode agir para ter acesso não autorizado às informações dele, como, por exemplo, roubo de dados, destruir ou corrompê-los de modo que sejam inutilizáveis pelo usuário (XING; LEVITIN, 2017).

f. **Acesso não Autorizado:** em uma conta bancária, somente o proprietário dela deveria acessá-la, ou o funcionário de um banco que auxilia o proprietário com transações específicas, ninguém mais deveria ter acesso a ela. Uma vez que é acessada por outros, a confidencialidade dos dados é comprometida, a qual é irreversível (YANG; XIONG; REN, 2020).

g. ***Phishing*:** há várias definições do termo *phishing* propostas e discutidas por especialistas, por pesquisadores e pelas instituições. Embora não exista uma acepção definitiva em razão da sua constante evolução, esse termo foi definido de diversas formas, de acordo com o uso e o contexto. Trata-se de forjar o beneficiário de modo que o invasor alcance uma ação desejada (ALKHALIL *et al.*, 2021), como, por exemplo, o envio de mensagens eletrônicas a alvos específicos.

h. **Divulgação de Informação:** é a ação conjunta entre plataformas, provedores e consumidores para revelar a informação dos usuários, de produtos e dos serviços por meio de uma plataforma digital (XU; ZENG; HE, 2021).

Com um *framework* que sintetiza os riscos relevantes encontrados na revisão da literatura, juntamente com a identificação e classificação desses riscos, torna-se necessário uma ferramenta que permita uma pesquisa de campo para validar se o *framework* corresponde à realidade das empresas. No caso específico do *framework* construído neste trabalho, a tarefa é validar com especialistas de TI a aderência dos riscos identificados à realidade das empresas. De modo a cumprir essa etapa, a ferramenta questionário foi escolhida para a pesquisa de campo a ser empreendida.

Como afirma Rugg e Petre (2006), questionários são uma ferramenta útil para entender o quão difundido é um tema, como quando é preciso ter a percepção dos respondentes sobre um determinado assunto. Ainda de acordo com Rugg e Petre (2006), os questionários são úteis para investigar a correlação entre dois temas, como a opinião sobre quão relevante é um tema em relação a um outro.

4.4 QUESTIONÁRIO

Tendo em vista que a revisão sistemática da literatura permitiu a construção de um *framework* a partir dos riscos identificados nos artigos selecionados, o questionário é um instrumento determinante para validar os riscos inerentes ao uso das tecnologias digitais da TD. Lucato *et al.* (2012), em seu estudo sobre competitividade, construiu um questionário que acomoda dimensões e afirmativas que permitem medir o nível de maturidade baseado em respostas como maturidade inexistente ou totalmente presente. Já o questionário apresentado aqui e adaptado de Lucato *et al.* (2012) e acomoda os 8 (oito) riscos identificados na revisão da literatura, com quatro afirmativas sobre cada risco.

O questionário passou por duas rodadas. Uma chamada de piloto para obter a validação e aprovação do questionário, a partir da percepção de 5 (cinco) especialistas em TI sobre os riscos, as afirmativas e a escala *Likert*. Já o questionário publicado foi disponibilizado a 35 (trinta e cinco) especialistas em TI que responderam cada afirmativa por meio da escala *Likert*, juntamente com a percepção deles sobre os riscos.

Adaptado de El-Haddadeh (2020), as afirmativas de cada risco serão medidas com uma escala *Likert* de cinco pontos, com a pontuação cinco indicando concorda totalmente e a pontuação um indicando que discorda totalmente. No trabalho de El-Haddadeh (2020), o autor aplicou uma escala de sete pontos, a qual foi descartada para este questionário. O questionário desenvolvido para esta pesquisa é semelhante ao apresentado por Creazza *et al.* (2021), o qual também utiliza um escala de cinco pontos, porém com outras nomenclaturas. Os dois estudos mencionados medem o risco cibernético por meio da escala *Likert*.

4.5 PILOTO

As seções seguintes exploram os comentários e as validações dos respondentes, incluindo uma avaliação dos resultados alcançados e os itens que podem ser melhorados no questionário.

4.5.1 AFIRMATIVAS DA LITERATURA

O questionário construído possuí as pontuações a seguir:

5. Concordo totalmente
4. Concordo
3. Neutro
2. Não concordo
1. Discordo totalmente

O questionário foi acomodado com as seguintes afirmativas de cada risco identificado:

a. Privacidade

a.1 As pessoas estão cada vez mais preocupadas com o modo como as empresas usam os seus dados pessoais (SESTINO *et al.*, 2020);

a.2 Impactos negativos na privacidade podem comprometer temas fundamentais, como liberdade de expressão e formas de discriminação (PURAITE *et al.*, 2020);

a.3 O uso de dados abre precedentes legais que requerem direções claras de políticas e de instituições (BIRKEL *et al.*, 2019);

a.4 Incidentes com privacidade podem impactar o uso e a adoção de novas tecnologias (MENDHURWAR; MISHRA, 2021).

b. *Malware*

b.1 O risco de um ataque com *malware* é identificado como alto (CREAZZA *et al.*, 2021);

b.2 Ataques com *malware* têm apresentado uma escalada, a qual impõe desafios para os benefícios da atual revolução tecnológica (FARD *et al.*, 2020);

b.3 Identificar a presença de um *malware* tem se tornado mais difícil (KABBAS; ALHARTHI; MUNSHI, 2020);

b.4 Uma vez que as tecnologias digitais alcançam setores críticos, a disseminação do *malware* pode causar uma cibercatástrofe mundial (ECKHART *et al.*, 2019).

c. *Ransomware*

c.1 Especialistas reconhecem que *ransomware* é um dos maiores riscos à segurança da informação atualmente (GAIVORONSKAYA *et al.*, 2020);

c.2 Ataques com *ransomware* têm atingindo vários setores, como fabricantes de automóveis, empresas de logística, serviços de saúde e agências governamentais (CREAZZA *et al.*, 2021);

c.3 Um ataque com *ransomware* pode causar perdas financeiras, multas, sanções e danos à reputação de uma empresa (LEE, 2021);

c.4 Um ataque com *ransomware* compromete e causa disrupções em serviços importantes à sociedade (BOCAYUVA, 2021).

d. Vazamento de Informação

d.1 A comunicação de dados locais para a nuvem pode resultar em perda de informação (YANG; XIONG; REN, 2020);

d.2 Segurança insuficiente em sistemas governamentais pode aumentar os custos da interação digital (DOBROLYUBOVA, 2021);

d.3 Propagandas que não são administradas bem podem resultar na percepção de perda de controle das informações pessoais (KRAFFT *et al.*, 2021);

d.4 As empresas devem proteger os dados dos consumidores para evitar a perda de confiança no progresso tecnológico (SESTINO *et al.*, 2020).

e. Roubo e Manipulação de Dados

e.1 Roubo e manipulação ocorrem com empresas e cidadãos individuais (SPIVAKOVSKYY *et al.*, 2021);

e.2 Sistemas digitalizados interconectados são explorados por criminosos cibernéticos (LEE, 2021);

e.3 Ataques podem incluir adversários e invasores motivados por ganhos econômicos (LEE, 2021);

e.4 Roubo e manipulação de informação afeta indivíduos e a segurança econômica de mercados e de seus participantes (GAIVORONSKAYA *et al.*, 2020).

f. Acesso não Autorizado

f.1 Acesso não autorizado pode ser tratado com a detecção de comportamentos anormais (SHI; JIN; LI, 2019);

f.2 Autorização e controle de acesso são problemas urgentes de ambientes virtualizados na nuvem (VASIL'EV; ZEGZHDA; POLTAVTSEVA, 2018);

f.3 A digitalização do sistema bancário eleva o risco de acesso não autorizado (KHANBOUBI; BOULMAKOUL, 2019);

f.4 Dados podem ser distribuídos em múltiplos servidores e cada servidor acessado por múltiplos usuários (YANG; XIONG; REN, 2020).

g. *Phishing*

g.1 *Phishing* pode ser considerado um dos riscos cibernéticos (CREAZZA *et al.*, 2021);

g.2 *Phishing* é das das principais técnicas de ataque (TECH, 2020);

g.3 *Phishing* é um risco crescente na segurança de dispositivos móveis (LEE, 2021);

g.4 *Phishing* atinge a camada da aplicação, juntamente com a injeção maliciosa de código e de ataques *DoS* (MENDHURWAR; MISHRA, 2021).

h. Divulgação de Informação

h.1 Permitir que vendedores digitais analisem dados pessoais como esforço para recomendações personalizadas, o que pode ser entendido como um acordo entre empresas e consumidores (KRAFFT *et al.*, 2021);

h.2 A conveniência e a escalabilidade dos serviços digitais atraem usuários e empresas a terceirizarem os dados para provedores externos (YANG; XIONG; REN, 2020);

h.3 A divulgação de informação à medida que isso é necessário para melhores decisões (incremental), reduz o risco da privacidade (BHATTACHARJEE; CHEN; DASGUPTA, 2020);

h.4 A divulgação de informação revela informação confidencial para entidades não autorizadas (KAVALLIERATOS; KATSIKAS, 2020).

4.5.2 Revisão dos comentários dos respondentes

O questionário construído a partir do *framework* foi objeto de um piloto realizado entre os dias 14 e 27 de setembro de 2021 por meio de um *Google Form*. O formulário foi enviado por correio eletrônico a cinco profissionais de TI, incluindo dois especialistas em segurança,

um arquiteto e dois engenheiros. O perfil completo dos respondentes pode ser observado no **Apêndice C.1**.

A seleção dos respondentes seguiu três critérios: eles devem ser especialistas de TI de mercado e que possam proporcionar percepções de regiões geográficas diferentes. Inicialmente pensou-se em restringir a pesquisa à cidade de São Paulo para delimitar a pesquisa a uma região específica, mas o argumento contra essa perspectiva foi de que em um momento de completa integração global, em razão do trabalho remoto, não haveria razão de restringir o estudo a uma localidade.

Deste modo, decidiu-se por convidar respondentes de regiões diferentes. Dois respondentes do Brasil, um do Canadá e dois dos Estados Unidos foram convidados. O questionário foi disponibilizado em língua inglesa, permitindo respostas em português, espanhol e inglês. Os convites foram realizados por meio de mensagens privadas no *Linkedin*, seguidas de um correio eletrônico formal enviado pelo *Google Forms*, incluindo uma carta-convite explicando os objetivos da pesquisa. Os respondentes aceitaram-na prontamente e responderam ao piloto em poucos dias. Ela pode ser observada no **Apêndice C.3**.

A característica principal do questionário para o piloto foi a inserção de um campo obrigatório para comentários e para validação de cada risco do *framework*. Isso permitiu obter a perceção dos respondentes sobre os riscos e as afirmativas, e não as respostas específicas de cada peso da escala Likert. O objetivo foi ter uma percepção sobre os textos e as opções da escala Likert. Deste modo há análises dos 5 (cinco) respondentes para os oito riscos identificados.

Isso deu visibilidade à validade do questionário e a sua aderência à realidade das empresas. Segue uma revisão dos comentários e da validação dos respondentes sobre cada risco:

a. Privacidade

Como a Curva ABC no **Quadro 4.3** revela, o tema privacidade permeia as discussões sobre cibersegurança e sobre riscos das tecnologias digitais. Partindo do princípio que ela é um direito humano fundamental (BHATTACHARJEE; CHEN; DASGUPTA, 2020), a construção, a implantação e o uso da tecnologia não têm efeito se a privacidade não é preservada. Na validação deste tema, os respondentes se dividiram em dois extremos. De um lado e de acordo com o Respondente 1, há a constatação de que as pessoas não estão preocupadas com privacidade e que essa questão reside nas mãos de profissionais que se encarregam de analisar os desafios relacionados com identidade e com segurança. Adicionalmente e ainda nesse extremo, o Respondente 3 aponta que privacidade é uma preocupação restrita a alguns grupos e que é preciso educar as pessoas sobre o que ela significa e como isso pode impactar ou danificar os direitos fundamentais delas. Por outro lado, o Respondente 4 deposita o risco privacidade nas empresas que estão ficando cada vez mais interessadas nos dados dos consumidores e usando técnicas sofisticadas de coleta e de tratamento. Adiciona-se também, como ressalta o Respondente 5, que grandes empresas de tecnologia e que proveem serviços digitais perdem os dados individuais ou os monetizam. Ainda de acordo com esse respondente, é preciso políticas mais robustas para

proteger dispositivos pessoais que são críticos para a privacidade. É importante notar que ele afirma que não é contra as tecnologias digitais, mas que é necessário mais segurança quando essas tecnologias são usadas. Já o Respondente 2 age como um ponderador, pois de acordo com a sua perspectiva, leis como GDPR *(General Data Protection Regulation)* e LGPD (Lei Geral de Proteção de Dados) estão causando um tratamento mais cuidadoso dos dados pessoais e que sistemas têm sido redesenhados para dar mais garantia à privacidade.

As quatro afirmativas foram capazes de revelar essas três dimensões sobre privacidade que percorrem as pessoas, as empresas e as leis. Os indivíduos, não se preocupam com esse tema, pois querem ter o conforto das novas funcionalidades oferecidas pelos provedores de serviços digitais, porém as empresas acabam por tirar vantagem desses dados e os monetizam. Finalmente, restam as leis que podem garantir a privacidade a partir de boas práticas e de eventuais penalidades no caso de violações.

b. Malware

O tópico *malware* proporcionou uma discussão que ultrapassa o escopo de um risco cibernético. O Respondente 1 aponta que os consumidores não punem as empresas que perderam os seus dados em razão de um ataque com *malware*, independente do quão severo ele foi. Esse é um ponto de vista que merece ser analisado com cuidado, pois a percepção por parte das empresas que os consumidores não vão puni-las, pode resultar na falta de investimento ou na negligência diante da certeza de que incidentes não vão causar danos ou punições. Já o Respondente 2 adota a perspectiva da prevenção e que as empresas investem muita atenção nos antivírus, porém essa não é a melhor tecnologia para prevenir um ataque com *malware* e que o mais adequado seria as tecnologias de *Endpoint Detection and Response*. O ponto de vista do Respondente 3 é que *malware* existe e que o risco é crescente, porém para evitar uma cibercatástrofe, será necessário que as tecnologias de prevenção atinjam um público maior. O Respondente 4 adota uma perspectiva que ultrapassa a tecnologia em si e questiona como e quem é capaz de criar um conteúdo como um *malware*. O verdadeiro desafio é combater esse risco em outros ambientes, como, por exemplo, identificar grupos que são capazes de desenvolver tais programas maliciosos. O Respondente 5 provê uma visão mais sistêmica, em que países estão preocupados com dispositivos móveis importados de outras nações e que são capazes de rastrear dados pessoais e os enviar para fora, alguns incluindo filtros que podem alterar os resultados de consultas realizas em sistemas de busca. Essa última perspectiva pode ir um pouco além de uma preocupação de uma empresa, por envolver preocupações de governos e de países, mas disponibiliza uma dimensão de risco que ultrapassa grupos autônomos de cibercriminosos e eleva o patamar a ações de Estado.

As afirmativas com relação ao risco *malware* proporcionaram dimensões importantes que percorrem a falta de punição às empresas por parte dos consumidores, as tecnologias que podem detectar e prevenir esse risco, a necessidade de atingir uma audiência maior para evitar uma cibercatástrofe, a necessidade de identificar os grupos que são capazes de produzir tais códigos

e finalmente países que produzem dispositivos que podem ser usados para ações maliciosas.

c. Ransomware

O ataque de *ransomware* é o que mais tem chamado a atenção do público, pois atingiu o noticiário com empresas que perderam dados ou que estão com os sistemas indisponíveis em razão desse tipo de ataque. O Respondente 1 basicamente reconheceu que os ataques com *ransomware* têm sido documentados nos noticiários e confirmados pelas empresas que foram atingidas. O Respondente 2 provê os mesmos comentários providos sobre os ataques com *malware*. Trata-se da importância das empresas adotarem outras formas de prevenção, além de antivírus que já não são mais eficientes. O Respondente 3 adota uma perspectiva da infraestrutura necessária para permitir uma recuperação rápida no caso de um ataque com *ransomware*, especialmente no quesito cópia de segurança, que deve ser testada e eficiente. A perspectiva é que as técnicas de prevenção podem eventualmente falhar e um ataque acontecer, portanto, diante disso, resta identificar o que é preciso para permitir uma recuperação rápida e eficiente. Ainda de acordo com o Respondente 3 e agora com uma perspectiva de prevenção, as pessoas devem ser educadas para evitar a propagação de *ransomware* e as empresas devem implementar tecnologias como *Extended Detection and Response*, *Network Detection and Response*, *Security Information and Event Management* e *Security Orchestration, Automation and Response*. O Respondente 4 traz uma visão realista do tema ao assumir que depois que um ataque com *ransomware* ocorrer, é muito difícil uma solução. O que acontece basicamente é uma recuperação dos sistemas por meio da restauração das cópias de segurança, mas isso requer investimento e bons hábitos que em geral as empresas não têm os recursos necessários para tal. O Respondente 5 reconhece que o ataque com *ransomware* está em crescimento e cita um evento em uma empresa que precisou desligar os seus sistemas para evitar a disseminação de um ataque.

As afirmativas foram capazes de estimular uma discussão sobre o reconhecimento que *ransomware* é um risco latente, com os noticiários documentando ocorrências e as empresas assumindo que foram alvos. Adiciona-se ainda formas de prevenção com o uso de diversas tecnologias, incluindo investimento em bons hábitos para proporcionar uma rápida recuperação.

d. Vazamento de Informação

Embora o risco vazamento de informação tenha proximidade com de privacidade, há uma diferença importante. Não se trata necessariamente de uma ação intencional para violar a privacidade, mas do vazamento de informação em razão de más práticas ou da negligência. O Respondente 1 percorreu novamente o desinteresse dos consumidores com o tema e afirmou que é pouco provável que uma empresa seja penalizada em razão da perda ou do vazamento de informação. É uma perspectiva que novamente pode resultar em empresas que ignoram os riscos diante da certeza que poucos danos financeiros ou à imagem podem ocorrer. O Respondente 2 afirma que o fato dos dados serem levados para a nuvem, não deveria ter como efeito colateral o vazamento de informação. De acordo com esse respondente, controles fracos de segurança

podem estar em qualquer ambiente e a má implementação da tecnologia nuvem pode causar o vazamento, não a tecnologia em si. O Respondente 3 observa que vazamento de informação é especialmente crítico quando empresas que coletam os dados possuem parcerias com empresas menores, que não possuem os mesmos critérios ou investimentos em segurança. Ele usa como exemplo o escândalo da *Cambridge Analytica* e *Facebook*. Já o Respondente 4 afirma que os dados são um dos ativos de maior valor de uma empresa e que a prioridade máxima deveria ser protegê-los. O Respondente 5 também deposita nas empresas a responsabilidade da proteção dos dados. O padrão deveria ser a proteção dos dados dos consumidores e não o seu uso sem permissão.

As afirmativas desse risco revelaram os extremos entre o desinteresse dos consumidores com o tema e a responsabilidade das empresas de protegerem os dados de modo que vazamentos sejam evitados. O Respondente 3 trouxe um item muito importante que é a parceria com outras empresas. À medida que os mercados estão mais integrados e muitos dos serviços são terceirizados por meio de parcerias estreitas entre as empresas, o risco de vazamento de informação é um grande desafio.

e. Roubo e Manipulação de Dados

De acordo com os respondentes, o roubo e a manipulação de dados são um novo meio de vida para os cibercriminosos. O Respondente 1 concordou com todas as afirmativas. Como bem apontou o Respondente 2, dados são roubados e seguidos de pedidos de resgate e até de extorsões, incluindo por exemplo, a venda de dados para concorrentes da empresa afetada. Aqui, ele cita o ataque com *ransomware* como um meio para concretizar o roubo de dados. Já o Respondente 5 estende o roubo de dados a cripto moedas, em que pessoas perdem dinheiro em razão de ataques dessa natureza. Como observou o Respondente 3, empresas e cidadãos podem demorar para se darem conta que um ataque está ocorrendo e, por isso, pode ser tarde demais quando uma iniciativa é tomada. Ele cita a necessidade de soluções de defesa especializadas para prevenir ataques. O Respondente 4 combina a anonimidade da *Internet* e o desconhecimento dos usuários em relação a práticas inseguras como modos para a concretização desse risco.

As afirmativas trouxeram um olhar novo para o roubo e para a manipulação de dados por relacioná-los como um meio inovador de vida para os criminosos. Não é somente mais um risco, mas um negócio original que usa a fragilidade de sistemas para movimentar uma quantia grande de recursos financeiros.

f. Acesso não Autorizado

Todos os respondentes percorreram a necessidade de configurações adequadas e de modos de detectar anomalias para prevenir acessos não autorizados. Esse é um risco que proporcionou respostas bem homogêneas e sem a apresentação de opiniões opostas. O Respondente 1 observa que provedores de nuvem vivem basicamente da distribuição de dados, porém o acesso não autorizado não é causado por provedores inseguros, mas por configurações inadequadas. O

Respondente 2 percorre o mesmo caminho enfatizando que a ausência de revisões de acessos, permite que um sistema sofra acessos indevidos. Adicionalmente, ele observa que em razão de falhas na implementação, um invasor consegue fazer uso de credenciais legítimas ao burlar as regras de negócio. Já o Respondente 3 aponta que os acessos não autorizados são um problema antigo e relacionado com a necessidade de senha nos sistemas. Esse respondente cita o movimento ou corrente para sistemas sem senhas como um modo mais moderno de autenticação, mas que isso ainda está longe de ser concretizado. O Respondente 4 coloca uma relação de causa e feito com o uso de nuvem. Ao mesmo tempo em que o maior benefício da nuvem é a sua resiliência, esse mesmo benefício aumenta a vulnerabilidade de algumas áreas. Como solução, o Respondente 5 afirma que sistemas para detecção de anomalias é um modo de fortalecer a segurança dos sistemas.

As afirmativas resultaram em pontos de vista mais homogêneos, indicando que os respondentes não confundiram os riscos, embora alguns possuam certa similaridade, como, por exemplo, acesso não autorizado e roubo de informação.

g. Phishing

Embora a definição de *phishing* não seja definitiva (ALKHALIL *et al.*, 2021), trata-se de uma técnica clássica e que não envolve força bruta. Com o uso em massa de correio eletrônico e a inserção de *web links* no corpo das mensagens, tem se tornado simples criar conteúdos que inspiram legitimidade, mas que na verdade direcionam os usuários a destinos falsos. No entanto, o Respondente 1 fez uma afirmação aposta ao consenso entre os outros respondentes. De acordo com o ele, o risco *phishing* está se tornando menos relevante em razão das autenticações baseadas em multiplos fatores, citando ainda sistemas sem senhas que podem impedir os ataques. O fato é que se o objetivo for a obtenção de uma senha, essa afirmação pode fazer sentido, porém se a finalidade for outra, como a obtenção de dados específicos, como o número de um cartão de crédito, o risco *phishing* continua a ser relevante. O Respondente 2 relaciona o aumento dos acessos remotos em razão da pandemia com ataques mais efetivos. O Respondente 3 observa que este tipo de ataque é o mais fácil e efetivo para atingir uma empresa e sem o uso de força bruta. Todavia, usuários distraídos podem abrir as portas aos invasores. O Respondente 4 observa o baixo esforço que é necessário para um ataque com *phishing*. Dessa forma, invasores enviam mensagens eletrônicas a uma grande audiência e o sucesso é obtido mesmo quando poucos alvos são atingidos. O Respondente 5 aponta que sistemas avançados de IA não são capazes de bloquear ataques, com *phishing*, e, assim, embora seja um modo clássico de ataque, o risco de ataque *phishing* ainda é muito alto.

As afirmativas trouxeram consenso entre os respondentes, com exceção do Respondente 1, ao afirmar que os ataques são menos eficientes em razão de sistemas mais complexos de autenticação.

h. Divulgação de Informação

Os comentários dos respondentes mostram que o risco de divulgação de informação pode ser mal interpretado. Trata-se do compartilhamento consciente de informação pelos usuários diante de benefícios com serviços personalizados. O Respondente 1 pondera que as afirmativas dependem do ambiente no qual os dados são coletados. O Respondente 2 afirma que novas regulamentações estão mudando o modo como os dados dos usuários são publicados. Já o Respondente 3 assegura que essa é uma área cinzenta, porque os usuários concordam em fornecer alguns dados com o entendimento de que eles serão protegidos, porém, poucos leem os termos de uso e os aceitam, permitindo que os dados sejam divulgados. Isso é algo incerto, pois se um termo de uso não for aceito, não há um outro modo de utilizar um serviço, visto que os termos de uso não são negociáveis. O Respondente 4 afirma que o desafio é ter um entendimento claro das regras e se elas serão atendidas. A divulgação de informação está muito próxima da confidencialidade e a chave é definir quem tem acesso aos dados. O Respondente 5 cita o exemplo comum de buscas que imediatamente resultam em propagandas relacionadas com os termos mencionados. Isso abre um precedente muito claro do que é feito com a informação à medida que ela é divulgada. As afirmativas relevaram o caráter contraditório da divulgação da informação, pois, por um lado, essa é uma ação consciente dos consumidores e, por outro, os termos de uso dos dados não são claros ou são negligenciados por esses consumidores. Esse é um risco que não se traduz em forma de ataque, mas no modo paradoxal como consumidores e provedores se relacionam.

4.5.3 Análise das respostas dos respondentes

A partir da revisão dos comentários retornados pelo piloto, é possível afirmar que o questionário apresentou um resultado satisfatório e superou as expectativas iniciais. Embora a revisão sistemática tenha proporcionado sólidas bases para a identificação dos riscos, havia uma preocupação sobre a similaridade de alguns deles e como isso poderia causar contradições para os respondentes, já que há similaridades entre roubo, manipulação, vazamento e divulgação de informação. Adiciona-se a isso, o risco privacidade que permeia os outros por se tratar de uma preocupação importante neste momento de adoção acelerada de tecnologias digitais. Vale também mencionar as similaridades entre *malware* e *ransomware*.

O fato positivo é que as contradições não se concretizaram e de acordo com os comentários, os respondentes diferenciaram os riscos com clareza. Isso revela que já existe um consenso quanto aos termos junto aos profissionais consultados, porém isso será confirmado na pesquisa mais abrangente a ser realizada. Embora muito similares, os riscos representam assuntos distintos, pois roubo e manipulação de informação são ações intencionais. Contudo, o vazamento pode ocorrer acidentalmente em razão de procedimentos frágeis de segurança ou mesmo por negligência. Já a divulgação é um ato consciente de um consumidor de compartilhar dados ao aceitar os termos de uso de uma plataforma digital. Apesar de *malware* poder ser um vírus, *ransomware* é legitimamente um novo negócio para os cibercriminosos.

Por um lado, os respondentes não encontraram problemas nas questões colocadas no documento e dessa forma o questionário está aprovado para uma busca mais abrangente no mercado corporativo. Entende-se que o questionário é viável para ser submetido a uma audiência mais ampla, o que permitirá uma análise quantitativa com estatísticas básicas nos próximos passos.

Por outro, os itens a seguir devem ser aperfeiçoados para submissão mais ampla do questionário:

1. Inserir mais opções para a área ou departamento dos respondentes. Para evitar respostas abertas, esse item faz uso de um campo de múltipla escolha, mas as opções são insuficientes, pois dois respondentes selecionaram a opção "Outra". A próxima versão do questionário deve incluir alternativas mais abrangentes e a remoção da opção "Outra".

2. Tornar o campo "Quanto tempo trabalha nessa empresa?" múltipla escolha, com opções mais restritas. No piloto, esse campo foi uma resposta aberta que pode causar dificuldades para analisar as de uma audiência maior.

3. Revisar a relação entre pontuação e as cores dos gráficos no *Google Form*. A maneira como elas foram dispostas pode causar contradições, pois a cor verde representa "Não Concordo" e a vermelha "Concordo". De modo natural, assumimos a cor verde como aceitação e a vermelha como negação.

4.6 Consulta aos Especialistas

O questionário contendo as alterações oriundas do piloto foi publicado e respondido por 35 especialistas entre os dias 18 e 25 de janeiro de 2022 por meio de um *Google Form* e o perfil completo deles pode ser observado no **Apêndice D.1**. Os respondentes são especialistas de TI de mercado que proporcionaram percepções de regiões geográficas diferentes, em razão de uma completa integração global com o trabalho remoto.

Foi disponibilizado em língua inglesa, permitindo respostas em português, espanhol e inglês. Os convites foram realizados por meio de mensagens privadas no *Linkedin*, incluindo uma carta-convite explicando os objetivos da pesquisa. Os respondentes aceitaram prontamente e responderam o questionário em poucos dias. A carta-convite pode ser observada no **Apêndice D.3**.

4.6.1 Afirmativas da Literatura

As afirmativas do questionário publicado e enviado aos especialistas sofreram alterações em comparação com o piloto. Tratam-se do atendimento dos itens da Seção **4.5.3** que apresentam aperfeiçoamentos a serem incorporados a partir do resultado do piloto.

As pontuações da escala *Likert* foram modificadas para serem apresentadas na ordem inversa. Na nova versão o primeiro item é "Discordo totalmente". Na versão do piloto o primeiro item foi o "Concordo totalmente". Essa modificação foi realizada para ter o questionário mais aderente a questionários que especialistas de TI recebem e respondem de pesquisas corporativas. De acordo com buscas de questionários semelhantes, observou-se que o primeiro item é o "Discordo totalmente".

As pontuações foram acomodadas da seguinte forma:

1. Discordo totalmente;
2. Não concordo;
3. Neutro;
4. Concordo;
5. Concordo totalmente.

De modo a atender o **Item 1** da **Seção 4.5.3**, novas áreas ou departamentos foram adicionados para permitir que os respondentes tenham mais opções ao responder o questionário. As novas áreas ou departamentos são: pesquisa e desenvolvimento, desenvolvimento de produtos e serviços de TI, em adição a vendas, pré-vendas, *marketing*, engenharia e suporte. Vale notar que vendas e pré-vendas foram separadas, pois na versão piloto estavam unificadas como vendas/pré-vendas. Essas modificações permitiram maior aderência às áreas internas das empresas, especialmente ao separar vendas e pré-vendas.

O **Item 2** da **Seção 4.5.3** não foi atendido. Decidiu-se por permitir que os especialistas respondessem o tempo de atuação na área ou posição com texto livre. Observou-se que um campo de múltipla escolha tiraria a precisão dessa informação.

O **Item 3** da **Seção 4.5.3** não foi atendido porque os gráficos do *Google Form* não foram usados. Os gráficos utilizados neste documento foram elaborados a partir de um arquivo texto gerado pelo *Google Form* e plotado no *Jupyter Notebook*. Essa mudança de estratégia solucionou contradições com as cores observadas nos gráficos do *Google Form* no piloto.

O campo comentários foi preservado como obrigatório. Alguns respondentes disseram que não tinham comentários a adicionar, mas a maior parte colaborou com comentários sobre as perpeções de risco.

A carta-convite inserida no questionário foi modificada para evitar *priming* ou apelo à autoridade. *Priming* é fenômeno onde um estímulo influencia o comportamento subsequente sem intenção ou sem guiá-lo (SHERMAN; RIVERS, 2021). Decidiu-se por incorporar essa modificação para não influenciar as respostas dos especialistas com esses tipos de comportamentos sociais. A nova versão da carta-convite pode ser observada no **Apêndice D.3**.

As afirmativas foram ajustadas de modo a evitar confusão com os termos usados, como por exemplo, cidadão, indivíduo, usuário, ou consumidor. O mesmo ocorreu com os termos empresas, organizações, corporações ou instituições. Os ajustes tiveram o objetivo de uniformizar os

termos e evitar potenciais confusões.

O questionário foi acomodado com as seguintes alterações:

a. Privacidade

a.1 Os consumidores estão cada vez mais preocupados com o modo como as empresas usam os seus dados pessoais (SESTINO *et al.*, 2020);

d. Vazamento de Informação

d.3 Propagandas que não são administradas bem podem resultar na percepção de perda de controle dos dados dos consumidores (KRAFFT *et al.*, 2021);

e. Roubo e Manipulação de Dados

e.4 Roubo e manipulação de dados afeta consumidores e a segurança econômica de mercados e seus participantes (GAIVORONSKAYA *et al.*, 2020).

h. Divulgação de Informação

h.2 A conveniência e a escalabilidade dos serviços digitais atraem consumidores e empresas a terceirizarem os dados para provedores externos (YANG; XIONG; REN, 2020);

4.6.2 VALIDAÇÃO DO *framework*

Esta seção apresenta uma revisão das repostas de cada afirmativa do questionário e empreende a validação do *framework* de riscos a partir dos resultados da escala *Likert*. Adiciona-se os comentários que são textos livres tecidos pelos respondentes e que são consolidados, comentados e fornecem perspectivas relevantes sobre os riscos. São de grande valia porque trazem as percepções dos especialistas sobre o tema. É válido ressaltar que o *framework* de riscos foi construído a partir de uma revisão sistemática da literatura e que a validação pelos especialistas assegura que o *framework* está aderente à realidade do mercado, com a percepção desses especialistas em relação aos riscos no uso das tecnologias digitais. Essa validação proporciona uma contribuição mútua entre academia e mercado. De um lado a academia contribui com uma revisão sistemática da literatura que identifica e classifica os riscos mais relevantes. Por outro lado, os especialistas de mercado contribuem com a percepção da aderência desses riscos à realidade das empresas, ou seja, percorre a validação do *framework* como uma contribuição para as empresas na jornada da TD.

O questionário com a aplicação da escala *Likert* proporcionou dados brutos que permitem identificar quantos respondentes escolheram uma escala específica para cada afirmativa, como

por exemplo, quantos escolheram concordo ou discordo para as afirmativas. A partir desses dados, é possível determinar um percentual das respostas para cada afirmativa. Tendo em mãos esses números, o próximo passo é determinar as respostas que revelam a aderência do *framework* à realidade do mercado. Assumiu-se como critério de pesquisa que "Concordo" e "Concordo Totalmente" definem essa aderência, portanto essas duas escalas são medidas. Trata-se de ter dois resultados que proporcionam condições de análise. Optou-se pela média simples de cada reposta, portanto ocorre a soma dos percentuais de cada escala, e calcula-se a média simples. Como define Cazorla, Santana e Utsumi (2019), quando há uma porção de dados brutos, apresentados em tabelas ou gráficos, soma-se os valores e os divide pelo número de dados. Isso denomina o que é uma média simples.

Há duas médias, pois o mesmo ocorre para "Concordo" e "Concordo Totalmente". Com as duas médias em mãos, assume-se que a média final a ser considerada para a validação é a soma das médias dessas duas escalas. Por critério deste trabalho, assume-se que se a média (resultado da soma das duas) final for acima de 70%, o risco foi validado pelos especialistas. Isso significa que o risco tem aderência ao mercado e à realidade das empresas, e que reflete os achados da revisão sistemática da literatura consolidada por meio da Curva ABC que pode ser observada no **Quadro 4.3**.

A menção à Curva ABC é oportuna porque os riscos classificados como relevantes são aqueles que compõem 70% do universo de citações para cada risco, e isso permitiu classificar os 8 (oito) riscos mais relevantes. Este trabalho adotou como critério que a validação dos riscos pelo questionário ocorre quando a soma das médias de "Concordo Totalmente" e "Concordo" é igual ou maior a 70%, pois isso preserva uma uniformidade na análise.

Para cada risco foram gerados gráficos cujas cores mostram o número de respondentes que optaram por uma das alternativas de cada afirmativa que compõe o risco, e que foram convertidas em percentuais para efeito de cálculo das médias que permitiram uma discussão quantitativa. Esses gráficos são apresentados para cada um dos riscos discorridos na validação do *framework*.

a. Privacidade

O tema privacidade ganhou preponderância nos últimos anos em razão das leis de proteção de dados e influencia o modo como as tecnologias são adotadas. O piloto realizado em meados de setembro de 2021 revelou opiniões opostas e o questionário publicado em janeiro de 2022 reproduziu o mesmo comportamento. O Respondente 6 afirma que as pessoas não sabem a serventia dos seus dados e que estão alheias a qualquer risco envolvido. Por isso, assume-se que a preocupação com privacidade é menor enquanto os dados são usados exclusivamente para o oferecimento de produtos alinhados às preferências pessoais. De acordo com esse respondente, quem está preocupado acaba por influenciar todos os outros, porém isso não significa que há uma preocupação generalizada sobre esse tema. O risco reside exatamente na confusão entre quem está preocupado ou não e a frágil fronteira entre o uso dos dados para oferecimento de

produtos ou para utilização indevida.

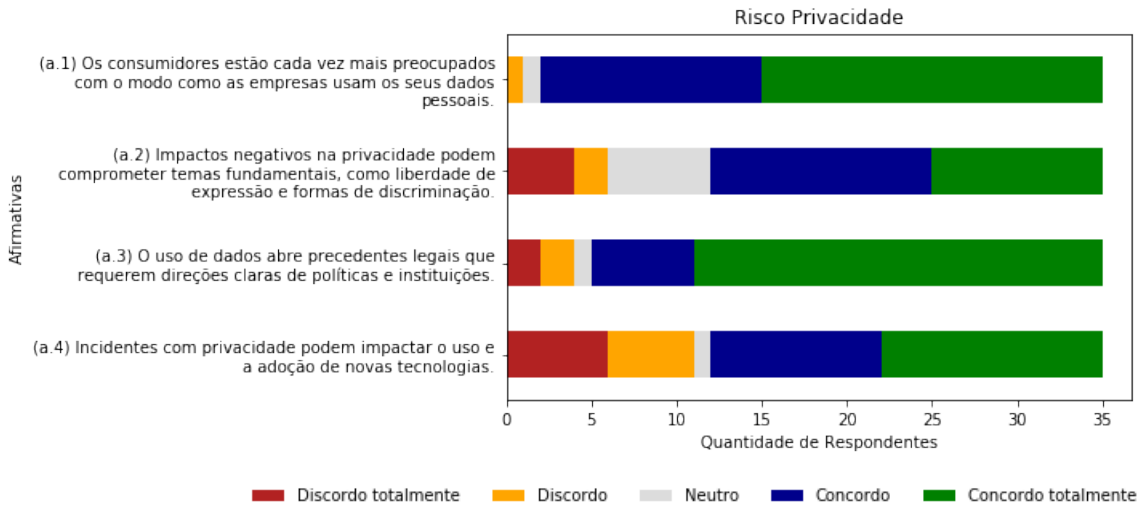
Apesar de o Respondente 2 fazer menção às leis de proteção de dados, ele afirma elas não impactam a adoção de novas tecnologias, porém exigem um tratamento e utilização corretos dos dados pessoais. Já o Respondente 21 cita os processos como importantes para suportar a privacidade. Em geral a preocupação se limita às tecnologias e subestima o poder dos processos para a viabilização de uma completa aderência. Todavia, o Respondente 16 não acredita que o tema pode dificultar ou evitar a utilização de tecnologias, mas, que causará um esforço adicional para acomodar os requerimentos de privacidade. Por outro lado, o Respondente 11 pondera que as tecnologias essencialmente não comprometem a privacidade, porém, em verdade o uso delas contribui para proporcionar mais segurança.

O Respondente 3 apresenta uma perspectiva que traz os aspectos comportamentais e cognitivos da privacidade. Ele cita, por exemplo os incidentes com as empresas *Cambridge Analytics* e *Facebook* como uma guerra cognitiva. Trata-se do corrompimento da privacidade de milhões de indivíduos para permitir o entendimento e a previsão do comportamento coletivo. A perspectiva trazida pelo Respondente 3 tem impactos na sociedade, diante do uso dos dados pessoais como uma arma.

Em contrapartida, o Respondente 25 sintetiza que a privacidade não impacta ou reduz a velocidade da adoção de novas tecnologias. Ele afirma que as novas tecnologias são adotadas rapidamente, e somente após a adoção completa é que se tem a dimensão do impacto sobre a privacidade. Cita ainda o *Facebook* como um exemplo claro de crescimento acelerado sem o ter a perspectiva da privacidade como uma preocupação legítima desde o início.

O Respondente 14 ressalta que embora as leis e regulamentações tenham crescido e colaborado nos últimos anos, as tecnologias estão evoluindo em um ritmo superior, resultando em riscos não previstos. O gráfico da **Figura 4.2** apresenta as respostas de acordo com a escala *Likert* das respectivas afirmativas.

Figura 4.2: *Escala Likert Privacidade*



Fonte: autor

Como apresenta o gráfico da **Figura 4.2**, na afirmativa (a.1) 94% dos respondentes responderam entre concordo e concordo totalmente, com 37% e 57% respectivamente. Neutro e discordo apresentam 6%, com 3% cada. Não houve respostas para discordo totalmente. A afirmativa (a.2) apresenta 66% das respostas entre concordo e concordo totalmente. Os 34% restantes reúnem as respostas discordo totalmente, discordo e neutro, com 11%, 6% e 17% respectivamente. A afirmativa (a.3) apresenta 6%, 6%, 3%, 17% e 69% para discordo totalmente, discordo, neutro, concordo e concordo totalmente. A afirmativa (a.4) é a que apresenta mais respostas com discordo totalmente e discordo somando 31%, com 17% e 14% cada. Neutro com 3%, com concordo e concordo totalmente com 66%, com 29% e 37% respectivamente.

A escala concordo tem a média de 30%, juntamente com a média de 48% para concordo totalmente. A soma das duas médias resulta em 78%. Na curva ABC o risco foi classificado como relevante com 21,43% das citações e na escala *Likert* os respondentes indicam 78% de concordância com o risco, desta forma ele foi validado junto aos especialistas.

As afirmativas sobre privacidade permitiram comentários que expressam a urgência e as contradições inerentes ao acelerando crescimento das tecnologias digitais. No entanto, não há um consenso sobre como definir e mitigar o risco da privacidade, visto que é impossível evitar uma ação proposital para o comprometimento da privacidade, mesmo com todos os processos, leis e tecnologias.

b. Malware

No piloto o tema *malware* proporcionou uma discussão que excedeu o escopo de um risco cibernético no sentido da segurança da informação, e trouxe a perspectiva do risco da importação de equipamentos de outros países que contém *software* embarcado e sujeitos a falhas. Isso excede porque entra em um campo de preocupação de governos e de países, não necessaria-

mente de uma empresa, salvo se for objeto de competição entre as empresas. O questionário publicado trouxe mais duas perspectivas que merecem atenção, embora também possam ser alvo de preocupação de governos e de países, empresas privadas podem ocupar o espaço que será descrito a seguir.

O Respondente 3 afirma que *malware* por si próprio é um armamento. Essa afirmação abre um precedente por tirar o *malware* do contexto de segurança da informação e inseri-lo na circunstância de uma das armas táticas a serem usadas em conflitos entre países ou na competição e na concorrência entre empresas. Nesse sentido, não se trata somente de um vírus, mas sim de códigos direcionados a alvos e a propósitos específicos.

O Respondente 19 explora o termo cibercatástrofe citada em uma das afirmativas. Do ponto de vista dele, esse é um evento possível, mas exagerado, pois o investimento de atacantes e de defensores está em relativo equilíbrio. Isso está ligado ao conceito de armamento citado pelo Respondente 3. É comum em conflitos tradicionais, o equilíbrio em razão de armas específicas, ou seja, em um conflito real com o uso vasto de *malware*, uma cibercatástrofe afetaria os atacantes e os defensores. O Respondente 2 adiciona a isso que dependendo do tipo de *malware* e os cuidados tomados pelas empresas, uma cibercatástrofe pode ser possível. Essa situação seria algo mais dentro da normalidade, um evento em decorrência da negligência acompanhado de um *malware* eficiente.

O Respondente 4 traz a perspectiva da integração. Nesse viés, parte-se do princípio de que se governos e empresas de grande porte têm sido vítimas de *malware*, há o precedente de despreparo para enfrentar tal risco, o, que, diante da integração dos sistemas, torna uma cibercatástrofe possível.

Embora essas duas perspectivas não estejam aderentes à realidade da segurança da informação das empresas, contribui para o desenho de cenários possíveis, como a utilização do *malware* na competição entre duas ou mais empresas.

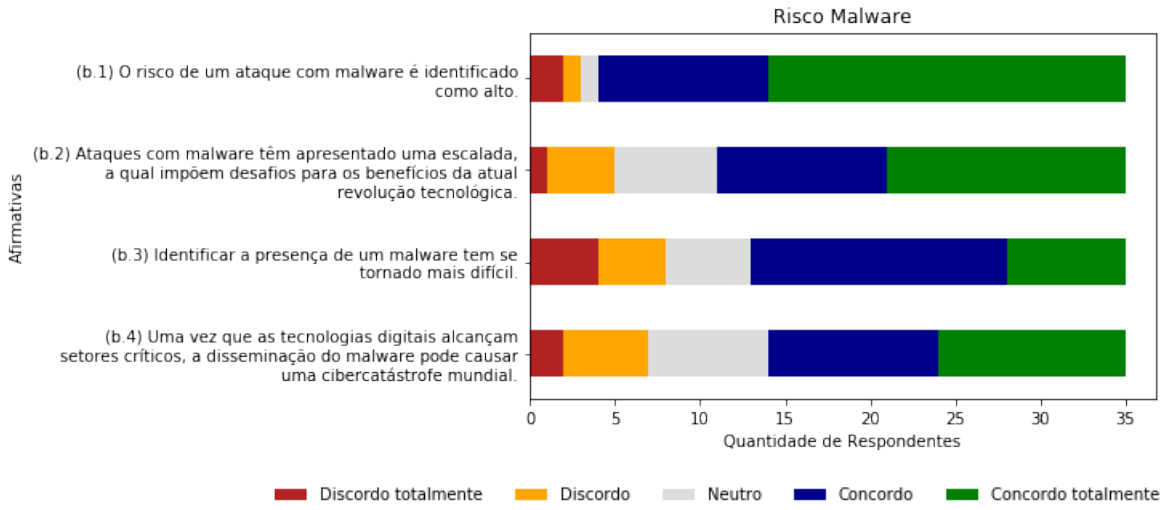
No entando, o Respondente 10 indica que atacantes estão escolhendo sequestrar um sistema, de modo a não danificá-lo. Em decorrência disso, somente o pagamento de um resgate permite o acesso àquele. Essa situação remete novamente à escolha de armas táticas. Se o objetivo não for a destruição de sistemas, o *malware* pode não ser a arma certa.

O Respondente 15 colocou um ponto de vista que merece análise. Segundo ele, os sistemas estão se tornando mais descentralizados, assim o risco de uma cibercatástrofe é menor. É possível que essa afirmação não seja acurada, pois o nível de integração entre os sistemas é maior. Possivelmente estão mais descentralizados, mas seguramente mais integrados. É justamente a integração de sistemas que eleva o risco.

O Respondente 16 por outro lado afirma que o elo mais fraco da segurança que permite ataques de *malware* são as pessoas, e que por isso o investimento em treinamentos e em processos é importante. Essa é uma perspectiva não acurada, visto que os sistemas estão mais integrados e autônomos. Por conta disso, o *malware* pode ter como alvos aqueles que não dependem de um elo humano determinado.

O gráfico da **Figura 4.3** apresenta as respostas de acordo com a escala *Likert* das respectivas afirmativas.

Figura 4.3: *Escala Likert Malware*



Fonte: autor

Como apresenta o gráfico da **Figura 4.3**, na afirmativa (b.1) 89% dos respondentes situam-se entre concordo e concordo totalmente, com 29% e 60% respectivamente. Discordo totalmente, discordo e neutro somam 11%, com 6%, 3% e 3% cada. Já a afirmativa (b.2) apresenta 69% para concordo e concordo totalmente, com 29% e 40% cada. 17% se situam em neutro, e 14% entre discordo totalmente e discordo, com 3% e 11% cada. A afirmativa (b.3) soma 63% para concordo e discordo totalmente, com 43% e 20% cada. 14% em neutro, com 11% para discordo totalmente e 11% para discordo. A afirmativa (b.4) soma 60% para concordo e concordo totalmente, com 29% e 31% cada. Discordo totalmente, discordo e neutro apresentam 6%, 14% e 20% respectivamente.

A escala concordo tem a média de 32%, juntamente com a média de 38% para concordo totalmente. A soma das duas médias resulta em 70%. Na curva ABC o risco foi classificado como relevante com 9,52% das citações e na escala *Likert* os respondentes indicam 70% de concordância com o risco, desta forma ele foi validado junto aos especialistas.

Em suma, o tema *malware* trouxe discussões que contribuem para o desenho de possíveis cenários. A perspectiva de que ele é em verdade, uma arma, muda a forma como os defensores veem o risco. Desse modo, é possível imaginar que uma empresa, além de um alvo potencial de um ataque em massa, pode também ser um objetivo específico diante de uma condição particular, como a concorrência por exemplo.

c. Ransomware

O ataque de *ransomware* se tornou popular em razão dos noticiários para o público em geral que cobrem esse tema, com empresas e órgãos governamentais impactados com esse tipo de

ataque. Vale notar que esse é um ataque que tem conexão com o mundo físico, pois se trata de um sequestro, cujo objetivo não é causar danos, mas ter o pagamento de um regaste como benefício.

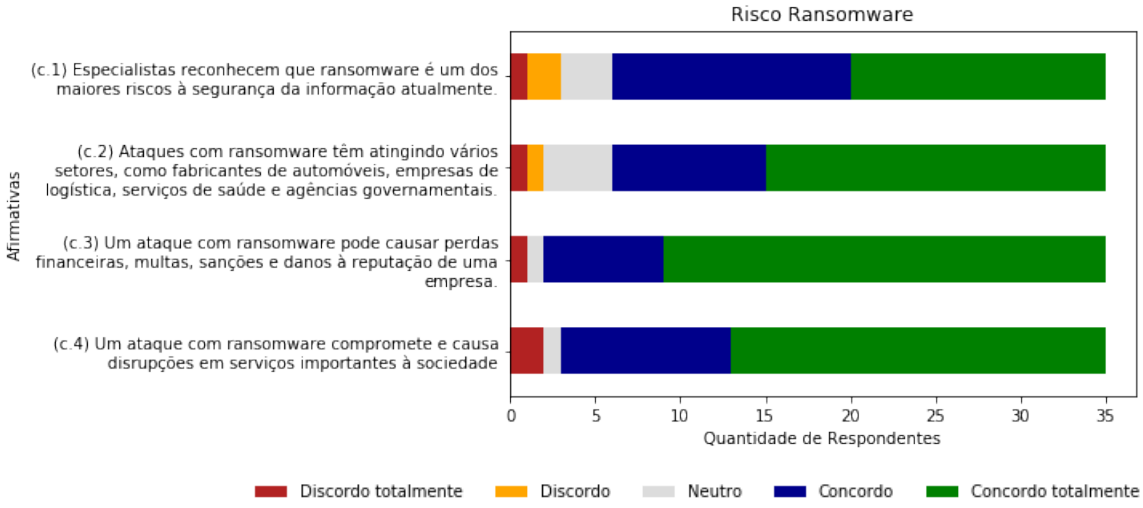
O Respondente 26 afirma que o ataque de *ransomware* tem sido explorado mais amplamente em razão das formas de transferência de recursos de modo anônimo, como as cripto moedas. Essa afirmação abre o precedente de que o *ransomware* está além da segurança da informação, o que permite discussões sobre a capacidade do sistema financeiro de monitorar transações dessa natureza.

O Respondente 23 adiciona a isso que além do dano financeiro para as empresas, efeitos colaterais podem acontecer, especialmente na sociedade. Como o Respondente 7 observou, exemplos como o Ministério da Saúde do Brasil que teve seus sistemas impactados em dezembro de 2021, exercem efeito direto na sociedade. O Respondente 8 acrescenta que as perdas além das financeiras, compromete a reputação das empresas e a confiança dos consumidores. Ademais, o Respondente 21 afirma que ataques de *ransomware* podem afetar a posição de uma empresa no mercado.

Já o Respondente 16 compara os setores público e privado, ressaltando a defasagem do setor público no quesito proteção. Essa perspectiva remete à integração dos sistemas, pois o todo pode ser comprometido se uma das partes é mais vulnerável, exatamente pelo nível de integração dos sistemas. Um banco público com os sistemas indisponíveis, pode impactar uma parcela da iniciativa privada em razão das interdependências. É nesse tipo de dependência que pode residir uma cibercatástrofe, porque as partes integradas não estão no mesmo ritmo de investimento e de prevenção.

O gráfico da **Figura 4.4** apresenta as respostas de acordo com a escala *Likert* das respectivas afirmativas.

Figura 4.4: *Escala Likert Ransomware*



Fonte: autor

De acordo com o gráfico da **Figura 4.4**, a afirmativa (c.1) apresenta 83% dos respondestes entre concordo e concordo totalmente, com 40% e 43% cada. Discordo totalmente, discordo e neutro somam 17%, com 3%, 6% e 9% respectivamente. A afirmativa (c.2) com resultados semelhantes apresenta 83% para concordo e concordo total, com 26% e 57% cada. Discordo totalmente, discordo e neutro somam 17%, com 3%, 3% e 11% respectivamente. A afirmativa (c.3) resultou em 94% dos respondentes entre concordo e concordo totalmente, com 20% e 74% cada. Discordo totalmente e neutro reúnem 6%, com 3% cada. Não há respostas para discordo. A afirmativa (c.4) reúne 91% dos respondentes entre concordo e concordo totalmente, com 29% e 63% cada. Discordo totalmente e neutro reúnem 6% e 3% respectivamente.

A escala concordo tem a média de 29%, juntamente com a média de 59% para concordo totalmente. A soma das duas médias resulta em 88%. Na curva ABC o risco foi classificado como relevante com 9,52% das citações e na escala *Likert* os respondentes indicaram 88% de concordância com o risco, desta forma ele foi validado junto aos especialistas.

De acordo com os achados da literatura e os comentários dos especialistas, depois que um ataque dessa natureza se concretiza, as opções são limitadas. Tratam-se basicamente de pagar um resgate ou de reconstruir os sistemas. O fato é que independente da opção, o dano já foi feito e afeta a imagem da empresa no mercado. Dessa maneira, essa questão ultrapassa o contexto da segurança da informação e entra na percepção dos consumidores sobre uma marca ou empresa.

d. Vazamento de Informação

Ao mencionar o tema vazamento de informação é importante lembrar da pequena introdução feita sobre essa questão no piloto. Privacidade e vazamento de informação andam muito próximas, porém a segunda ocorre em razão de más práticas ou negligência. Trata-se de vazamento e não da invasão de privacidade em um sentido mais amplo. Esse é um tema que provoca opiniões divergentes. Por isso, vale começar pelo Respondente 7, que afirma que o uso indevido e pontual de personalização não impacta a confiança na evolução tecnológica, mas a desgasta. Essa é uma perspectiva que abre os precedentes de segurança, pois embora ocorra uma queda de confiança nas tecnologias, há um grau de tolerância quanto ao uso indevido de personalização. Pode-se entender que isso é algo como uma troca, isto é, que em razão de algumas facilidades, tolera-se um eventual uso indevido.

O Respondente 2 reforça a promulgação das leis de proteção de dados que criaram uma exigência legal de adequação das empresas no quesito proteção dos dados dos indivíduos. As legislações existem, porém como o Respondente 14 ressaltou, há uma defasagem entre as iniciativas privada e estatal. Por conta disso, ocorre o já mencionado risco de integração. Assim, embora uma instituição privada esteja aderente às leis de proteção de dados, no momento em que uma transação atinge uma instituição estatal, riscos em razão da defasagem tecnológica podem ocorrer. Nesse sentido, eventos como os ataques ao Ministério da Saúde do Brasil ocorrido em dezembro de 2021, bem como o vazamento de dados pessoias do Banco Central do Brasil que aconteceu em janeiro de 2022 reforçam a sensação de uma defasagem tecnológica

da iniciativa estatal.

A partir de um outro extremo, o Respondente 3 afirma que os dados só serão invioláveis se bem armazenados, desconectados das redes e com os dispositivos desligados. Essa é uma perspectiva que se aproximada do Respondente 7 e revela certa tolerância com incidentes de segurança em razão do uso intenso de dados, com seus benefícios e facilidades. Trata-se de assumir riscos depois que os sistemas estão conectados e integrados.

Por outro lado, o Respondente 4 traz uma perspectiva dos lucros inerentes ao vazamento de dados. Segundo ele, os dados refletem o consumo e o perfil dos indivíduos. Entretanto, se os dados não estão seguros, qualquer atacante que venha a ter acesso a eles, tentará faturar com isso incondicionalmente. Essa é uma lógica da qual não se pode ter dúvida.

Já o Respondente 16 afirma que o uso da tecnologia nuvem não aumenta necessariamente o risco de vazamento de dados, e que os cuidados com os dados devem ser os mesmos quando hospedados *on-premises*. Essa é uma afirmação que merece análise, pois em um ambiente em nuvem a complexidade de acesso é maior. Todavia, em uma nuvem pública, acessos são realizados por milhares de usuário e a segurança está baseada em políticas bem definidas, não sendo trivial compará-la com ambientes *on-premises* nos quais os acessos são basicamente realizados por um limitado número de usuários. No entanto, quando *on-premises*, a responsabilidade de se adotar políticas de segurança adequadas, e de atualização dos sistemas, é toda do proprietário do ambiente. Nesse sentido, não há um compartilhamento da responsabilidade como ocorre em ambientes de hospedagem na nuvem. O Respondente 21 chama a atenção para os processos que bem conduzidos, podem minimizar o risco de segurança. Essa é uma perspectiva que tira a ênfase depositada exclusivamente na tecnologia.

O Respondente 25 afirma que embora as empresas devam proteger os dados dos indivíduos, perda de confiança não é o foco. O argumento dele é que muitos perderam a confiança, mas não é possível saber se é quem perdeu ou em quem vendeu os dados pessoais. Essa é uma perspectiva que releva a complexidade dos sistemas integrados, pois quando há um vazamento não é trivial entender quem foi o responsável para ter essa perda de confiança.

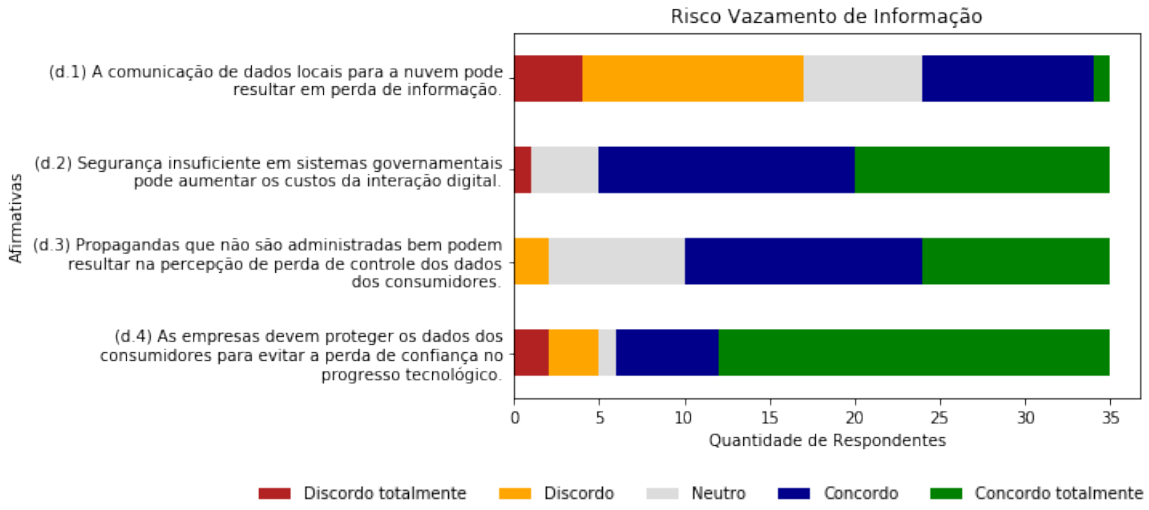
Adicionalmente, a perspectiva trazida pelo Respondente 26 inclui os algorítimos de IA na equação. Ele cita que as tecnologias para predizer e influenciar as pessoas está além do que qualquer resultado desejado, apontando os anúncios personalizados que foram criados com boas intenções, mas que agora há uma tentativa de influenciar e controlar as preferências dos consumidores. Essa perspectiva tem uma relação de causa e feito, visto que o uso de IA para analisar dados não revela um vazamento de informação, mas quando esses algorítimos são executados em dados nos quais não se sabe a procedência, eventualmente resulta no vazamento de informação.

Por fim, o Respondente 27 afirma que pequenas e médias empresas não têm um especialista para garantir políticas apropriadas para a segurança dos dados. Entretanto, depositar a responsabilidade da elaboração de políticas dessa dimensão em um especialista remete à perspectiva trazida pelo Respondente 21, que cita os processos como um fator relevante para a segurança

da informação.

O gráfico da **Figura 4.5** apresenta as respostas de acordo com a escala *Likert* das respectivas afirmativas.

Figura 4.5: *Escala Likert Vazamento de Informação*



Fonte: autor

Como apresenta o gráfico da **Figura 4.5**, a afirmativa (d.1), 31% dos respondentes reúnem-se entre concordo e concordo totalmente, com 29% e 3% cada. Discordo totalmente, discordo e neutro reúnem 69% dos respondentes, com 11%, 37% e 20% respectivamente. A afirmativa (d.2) apresenta 86% dos respondentes entre concordo e discordo totalmente. Discordo totalmente e neutro reúnem 14% dos respondentes, com 3% e 11% cada. Já a afirmativa (d.3) soma 71% dos respondentes entre concordo e concordo totalmente, com 40% e 31% cada. Discordo e neutro somam 29%, com 6% e 23% respectivamente. A afirmativa (d.4) soma 83% dos respondentes entre concordo e concordo totalmente, com 40% e 31% respectivamente. Discordo totalmente discordo e neutro reúnem 17%, com 6%, 9% e 3% cada.

A escala concordo tem a média de 32%, juntamente com a média de 36% para concordo totalmente. A soma das duas médias resulta em 68%. Na curva ABC o risco foi classificado como relevante com 8,33% das citações e na escala *Likert* os respondentes indicaram 68% de concordância com o risco. Este risco se situa abaixo do corte de 70% para elegibilidade de relevância do risco, porém os comentários dos especialistas que trazem uma perspectiva qualitativa, revelam que o risco em questão é objeto de atenção pelas empresas, deste modo o pesquisador considera que ele foi validado junto aos especialistas.

e. Roubo e Manipulação de Dados

Os comentários dos respondentes sobre o tema roubo e manipulação de dados trouxeram perspectivas que revelam que o benefício ou ganho por traz de uma ação é um fator preponderante. Todavia, o Respondente 3 afirma que esse evento ocorre se o dado tem um valor legítimo,

pois um sem importância não seria alvo de um roubo. Mesmo que tenha algum tipo de importância, seria pequeno o suficiente para não motivar o roubo e a eventual manipulação. O Respondentes 14 e 30 teceram comentários semelhantes e afirmam que o mencionado ganho é econômico. Isso revela que os cibercriminosos, como quaisquer criminosos em outras esferas, agem baseados em interesses e ganhos específicos. Essas afirmações trazem luz à importância da priorização quando o tema é segurança da informação, pois se a motivação de um ataque é o ganho financeiro em razão do valor de um dado, o investimento em segurança não precisa ser o mesmo para o universo total de dados de um indivíduo ou de uma empresa. É nesse quesito que pode ocorrer a separação dos dados, de modo que os mais importantes tenham camadas de segurança maiores.

Já o Respondente 4 observou que os dados de um único cidadão não têm tanto poder em comparação com os de um grupo. Ao obter dados deste, decisões importantes podem ser influenciadas. Um evento dessa natureza pode ocorrer em momentos de eleições ou de plebiscitos nacionais, quando os dados de uma parcela da população pode favorecer uma das partes em razão da possibilidade de prever comportamentos.

O Respondente 10 afirma que os dados não precisam ser necessariamente roubados, pois há muitos deles disponíveis na *Internet*, o que possibilita às pessoas sofrerem ataques. Essa é uma afirmação que se relaciona ao tema vazamento de dados. Um dado que é vazado e vendido, fica disponível de um modo que o roubo não é mais necessário.

Por fim, o Respondente 23 observa a relação entre o roubo de dados e os incidentes de segurança com equipamentos conectados à *Internet*. Para ele, uma parcela significativa dos equipamentos eletrônicos possuem *software* embarcado que está sujeito a falhas de segurança, as quais podem ser exploradas.

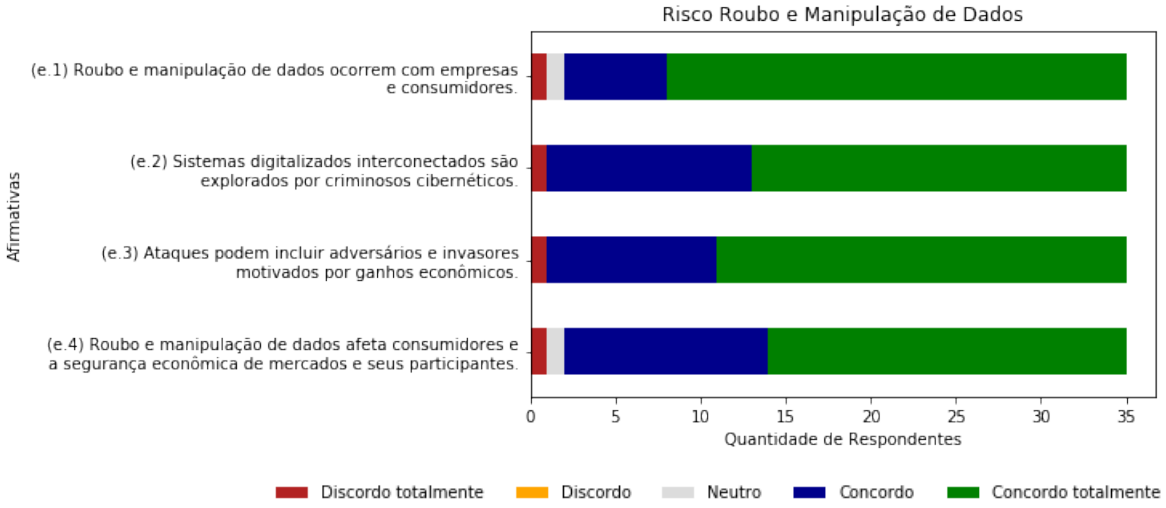
O gráfico da **Figura 4.6** apresenta as respostas de acordo com a escala *Likert* das respectivas afirmativas.

De acordo com o gráfico da **Figura 4.6**, a afirmativa (e.1) soma 94% dos respondentes entre concordo e concordo totalmente, com 17% e 77% respectivamente. Discordo totalmente e neutro somam 6%, com 3% cada. A afirmativa (e.2) reúne 97% dos respondentes entre concordo e concordo totalmente, com 34% e 63% cada. Discordo totalmente resume 3% dos respondentes. A afirmativa (e.3) soma 97% para concordo e concordo totalmente, com 29% e 69% cada. Discordo totalmente resume 3% dos respondentes. A afirmativa (e.4) soma 94% entre concordo e concordo totalmente, com 34% e 60% respectivamente. Discordo totalmente e neutro somam 6%, com 3% cada.

A escala concordo tem a média de 29%, juntamente com a média de 67% para concordo totalmente. A soma das duas médias resulta em 96%. Na curva ABC o risco foi classificado como relevante com 5,95% das citações e na escala *Likert* os respondentes indicaram 96% de concordância com o risco, desta forma o risco foi validado junto aos especialistas.

O risco em questão foi validado com uma margem signiticativa de respondentes se situando entre concordo e concordo totalmente. Isso revela que é um risco legítimo e alcança a esfera

Figura 4.6: *Escala Likert Roubo e Manipulação de Dados*



Fonte: autor

dos interesses dos cibercriminosos por um objeto diante do seu valor.

f. Acesso não Autorizado

Sobre o tema acesso não autorizado, o Respondente 26 afirma que a engenharia social pode detectar o comportamento normal não anômalo, de modo que um acesso não autorizado não seja detectado. Em outras palavras, isso indica que mesmo com um investimento em soluções de prevenção, a engenharia social é capaz de reproduzir um comportamento que é reconhecido como normal por tecnologias de proteção. Esse mesmo respondente observa que grande parte dos acessos não autorizados ocorrem dentro de uma empresa. Isso revela que a transferência de dados para a nuvem não é em si um aumento do risco de acessos não autorizados.

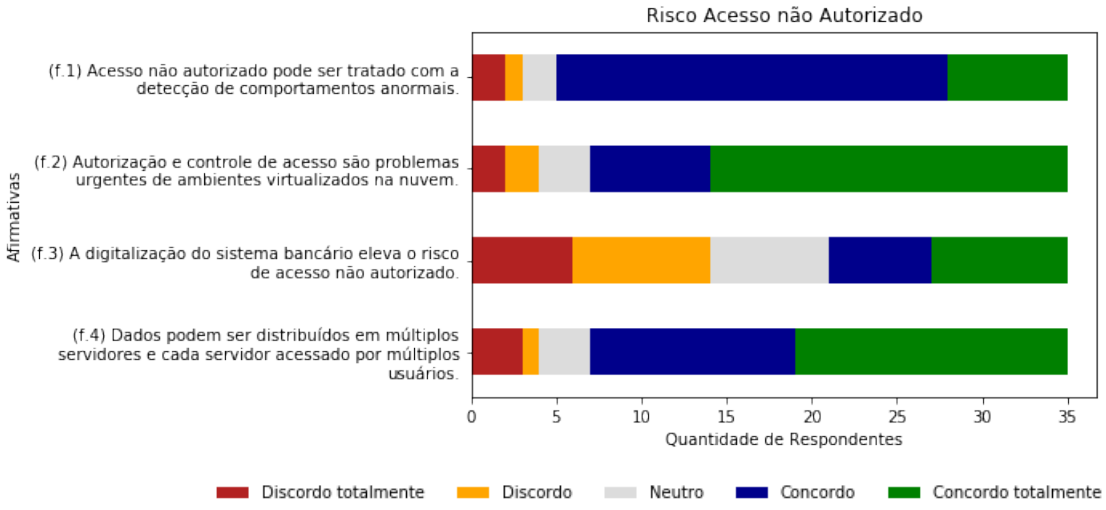
Já o Respondente 30 cita a necessidade de treinamento para evitar que ataques de engenharia social resultem em acesso não autorizado. A monitoração é importante, mas este tema é relacionado com a maneira como as pessoas lidam com a segurança da informação. Investimento em prevenção pode ser realizado, porém se as pessoas dentro do processo não resistirem a ataques de engenharia social, acessos não autorizados podem ocorrer facilmente.

Todavia, o Respondente 27 considera os bancos brasileiros como um exemplo no quesito controle de acesso, mas mesmo assim essas instituições permanecem investindo em novas tecnologias. Ainda com relação aos bancos, o Respondente 16 indica que os setores bancário e financeiro foram digitalizados há muito tempo e que mesmo hoje, com o uso de infraestrutura em nuvem, os controles são eficientes.

Finalmente, o Respondente 3 afirma que acesso não autorizado é um crime antigo e que o aspecto humano é preponderante. Isso explica a ocorrência de acessos não autorizados dentro das empresas, bem como o sucesso das técnicas de engenharia social para se obter acesso tanto físico como cibernéticos da infraestrutura e dos dados sensíveis.

O gráfico da **Figura 4.7** apresenta as respostas de acordo com a escala *Likert* das respectivas afirmativas.

Figura 4.7: *Escala Likert Acesso não Autorizado*



Fonte: autor

Como apresenta o gráfico da **Figura 4.7**, a afirmativa (f.1) reúne 86% dos respondentes entre concordo e concordo totalmente, com 66% e 20% cada. Discordo totalmente, discordo e neutro reúnem 14%, com 6%, 3% e 6% respectivamente. A afirmativa (f.2) reúne 80% entre concordo e concordo totalmente, com 20% e 60% cada. Discordo totalmente, discordo e neutro reúnem 20%, com 6%, 6% e 9% respectivamente. A afirmativa (f.3) reúne 40% entre concordo e concordo totalmente, com 17% e 23% cada. Discordo totalmente, discordo e neutro somam 60%, com 17%, 23% e 20% cada. Já a afirmativa (f.4) reúne 80% dos respondentes entre concordo e concordo totalmente, com 34% e 46% respectivamente. Discordo totalmente, discordo e neutro somam 20%, com 9%, 3% e 9% cada.

A escala concordo tem a média de 34%, juntamente com a média de 37% para concordo totalmente. A soma das duas médias resulta em 71%. Na curva ABC o risco foi classificado como relevante com 5,95% das citações e na escala *Likert* os respondentes indicaram 71% de concordância com o risco, desta forma ele foi validado junto aos especialistas.

Este risco revelou a importância da engenharia social. Revela que investimentos podem ser neutralizados pela possibilidade dos usuários causarem acesso não autorizado por meio da engenharia social como estratégia inicial dos invasores.

g. Phishing

Como os respondentes 2, 17 e 21 reconhecem, o ataque *phising* é amplamente empregado pelos atacantes e como indicou o Respondente 11, causa danos porque o usuário é o elo fraco da cadeia e de algum modo é conduzindo a esse tipo de ataque.

No entando, o Respondente 31 indica que ataque *phishing* é a porta de entrada para ataques mais robustos, já que usuários regulares podem intencionalmente ou por acidente abrir uma página suspeita. Adicionalmente, como ressalta o Respondente 27, a partir de um ataque *phishing*, ataques de *malware* e de *ransomware* podem ser desencadeados.

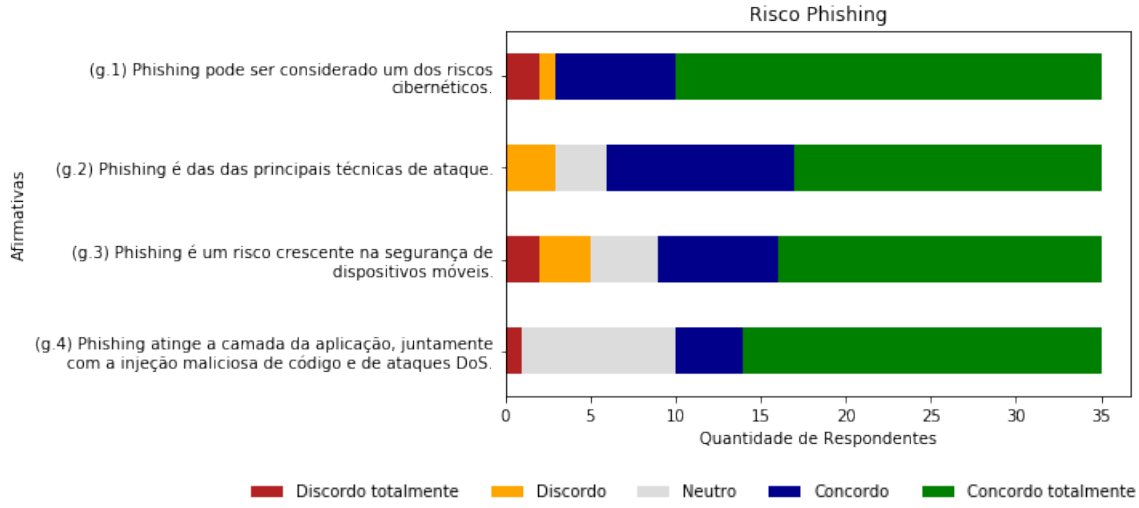
Como o Respondente 10 ressalta, o ataque *phishing* é empreendido não somente por correio eletrônico, mas também por mensagens em dispositivos móveis ou mesmo por aplicativos de mensagens. Vale notar que esse tipo de ataque também ocorre nas redes sociais, com a criação de perfis falsos e com propagandas que levam os usuários a abrirem páginas suspeitas em busca de promoções ou de oportunidades únicas. Como afirma o Respondente 4 o ataque *phishing* é também empregado para a obtenção de dados pessoais por meio do envio em massa de mensagens falsas. Adiciona-se a isso como lembrou o Respondente 16, a exploração pelos atacantes da vulnerabilidade social de grupos particulares que estão mais propensos a abrir uma página falsa. Exemplos dessa vulnerabilidade pode ser o regaste de quantias em dinheiro de programas assistenciais, cadastros antecipados para vacinação em massa ou qualquer outra ação governamental que tenha um grupo particular como beneficiário.

Consequentemente, o Respondente 26 afirma que com o objetivo de tornar a vida dos usuários mais simples, o resultado é um aumento da vulnerabilidade. Esse respondente ressalta que usuários treinados e experientes também ficam em dúvida sobre a legitimidade de uma mensagem de modo a detectar um ataque *phishing*.

Por outro lado, como afirma o Respondente 25, as pessoas estão se tornando mais atentas às táticas empregadas pelo ataque *phishing*. Nesse sentido, treinamentos apropriados e testes randômicos estão contribuindo para a redução do sucesso desse tipo de ataque.

O gráfico da **Figura 4.8** apresenta as respostas de acordo com a escala *Likert* das respectivas afirmativas.

Figura 4.8: *Escala Likert Phishing*



Fonte: autor

De acordo com o gráfico da **Figura 4.8**, a afirmativa (g.1) reúne 91% dos respondentes entre concordo e concordo totalmente, com 20% e 71% cada. Discordo totalmente e discordo somam 9%, com 6% e 3% respectivamente. A afirmativa (g.2) reúne 82% entre concordo e concordo totalmente, com 31% e 51% cada. Discordo e neutro somam 18%, com 9% cada. A afirmativa (g.3) reúne 74% dos respondentes entre concordo e concordo totalmente, com 20% e 54% cada. Discordo totalmente, discordo e neutro somam 26%, com 6%, 9% e 11% respectivamente. Já a afirmativa (g.4) reúne 71% entre concordo e concordo totalmente, com 11% e 60% respectivamente. Discordo totalmente e neutro reúnem 29% dos respondentes, com 3% e 26% cada.

A escala concordo tem a média de 21%, juntamente com a média de 59% para concordo totalmente. A soma das duas médias resulta em 80%. Na curva ABC o risco foi classificado como relevante com 4,76% das citações e na escala *Likert* os respondentes indicaram na 80% de concordância com o risco, desta forma ele foi validado junto aos especialistas.

Phishing é uma técnica clássica para obter atenção dos usuários, e mesmo após décadas do surgimento dos sistemas de correio eletrônico, é uma técnica eficiente. Ela alcançou as redes sociais e aplicativos direcionados a grupos particulares para obter atenção e em seguida iniciar o ataque que pode desencadear outros.

h. Divulgação de Informação

O tema divulgação da informação se diferencia pelo fato de que os dados são conscientemente compartilhados pelos usuários. No entanto, o risco reside no mau uso dessa informação. O Respondente 3 afirma que um acordo para divulgação de informação está além da pessoa que o assinou. Desse modo um acordo ser bom para alguns não significa que é para todos. Adicionalmente, divulgar dados confidencialmente não significa que eles estão em boas mãos. Já o Respondente 7 afirma que a divulgação da informação não é essencialmente ruim, desde que os fundamentos das leis de proteção de dados sejam respeitados.

Entretanto, o Respondente 8 ressalta o incômodo de observar publicidade sobre um assunto que foi pesquisado nas ferramentas de buscas minutos antes. Ele afirma que nunca autorizou tal monitoração das buscas para oferecimento de publicidade, mas algo que deve ser levado em conta é justamente o acordo de privacidade quando um serviço é obtido. É importante destacar que são acordos extensos e de difícil leitura, porém é preciso ter conhecimento se a divulgação de informação que é da aqui prevista neles.

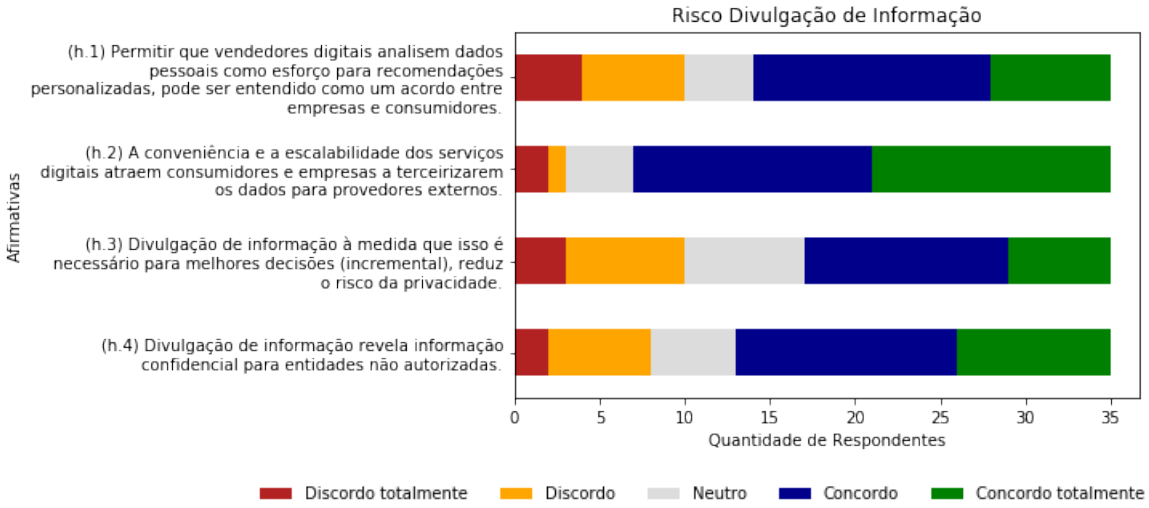
O Respondente 16 afirma que as preferências e os comportamentos de consumo são os itens mais explorados sem o completo consentimento dos usuários. Não se trata somente das preferências e dos consumos que são explorados no perfil do usuário, mas sim do uso desses dados para análises conjuntas para observar o perfil de consumo de grupos específicos, ou mesmo de regiões geográficas.

Já o Respondente 25 afirma que não tem reservas quanto ao uso de dados pessoais por lojas para a sugestão de produtos. Por outro lado, observa que essas sugestões raramente ajudam e

mostram como os dados pessoais e os *cookies* são usados facilmente.

O gráfico da **Figura 4.9** apresenta as respostas de acordo com a escala *Likert* das respectivas afirmativas.

Figura 4.9: *Escala Likert Divulgação de Informação*



Fonte: autor

Como apresenta o gráfico da **Figura 4.9**, a afirmativa (h.1) reúne 60% dos respondentes entre concordo e concordo totalmente, com 40% e 20% respectivamente. Discordo totalmente, discordo e neutro somam 40%, com 11%, 17% e 11% cada. A afirmativa (h.2) reúne 80% dos respondentes entre concordo e concordo totalmente, com 40% cada. Discordo totalmente, discordo e neutro reúnem 20%, com 6%, 3% e 11% respectivamente. A afirmativa (h.3) reúne 51% dos respondentes entre concordo e concordo totalmente, com 34% e 17% respectivamente. Discordo totalmente, discordo e neutro somam 49%, com 9%, 20% e 20% cada. Já a afirmativa (h.4) reúnem 63% dos respondentes entre concordo e concordo totalmente, com 37% e 26% respectivamente. Discordo totalmente, discordo e neutro reúnem 37%, com 6%, 17% e 14% cada.

A escala concordo tem a média de 38%, juntamente com a média de 26% para concordo totalmente. A soma das duas médias resulta em 64%. Na curva ABC o risco foi classificado como relevante com 4,76% das citações e na escala *Likert* os respondentes indicaram na 64% de concordância com tema. Este risco se situa abaixo do corte de 70% para elegibilidade de relevância do risco, porém os comentários dos especialistas que trazem uma perspectiva qualitativa, revelam que o risco em questão é objeto de atenção pelas empresas, deste modo o pesquisador considera que ele foi validado junto aos especialistas.

4.6.3 ANÁLISE DAS RESPOSTAS DOS RESPONDENTES

O *framework* construído e disponibilizado foi fundamentado em uma revisão sistemática da literatura que permitiu identificar e classificar os riscos mais relevantes inerentes ao uso das tecnologias digitais. Essa revisão proporcionou uma visão acadêmica sobre o tema a partir de artigos científicos publicados. Por outro lado, de modo a permitir uma contribuição ao mercado, a pesquisa foi a campo por meio de um questionário para capturar a percepção de especialistas de TI para validar o *framework*. Essa consulta proporcionou uma perspectiva mais pragmática sobre o tema por se conectar com o que ocorre nas empresas com as percepções dos especialistas. Permitiu validar o *framework* com essa perspectiva de mercado.

Foram identificados 21 (vinte um) riscos, porém 8 (oito) deles categorizados como mais relevantes pela Curva ABC **(Quadro 4.3)**. Esses 8 (oito) riscos totalizam 70% das citações observadas nos trabalhos acadêmicos resultado da revisão sistemática da literatura. Baseada nessa revisão, cada um dos riscos mais relevantes contou com 4 (quatro) afirmativas que foram acomodadas em um questionário de escala *Likert*, contando também com um campo para comentários livres.

O *framework* foi validado conforme as expectativas dos objetivos da pesquisa, pois a grande maioria dos riscos foi validado com sucesso. Como critério deste trabalho, assumiu-se que um risco é validado quando soma das médias das respostas para concordo totalmente e concordo são maiores que de 70% e isso aconteceu para 6 (seis) dos 8 (oito) riscos. Os 2 (dois) riscos que não atingiram esse percentual são Vazamento de Informação e Divulgação de Informação com valores finais de 68% e 64% respectivamente. De modo direto e baseado na escala *Likert*, é possível reconhecer que esses dois riscos não atingiram o percentual necessário para assumi-los como validados e aderentes à realidade das empresas, mas por outro lado, os comentários dos respondentes demonstram a faceta qualitativa do estudo que comprova uma preocupação legítima com o risco pelos respondentes. Esses comentários podem ser observados na **Seção 4.6.2** (Validação do *Framework*). Entende-se que essa contradição é uma contribuição relevante para a academia por dar visibilidade dessas percepções de especialistas de mercado. Vale mencionar que embora abaixo da linha corte, estão muito próximos e não foi uma diferença expressiva. Isso legitima a a importância dos riscos mencionados e valida o *framework* proposto.

Como foi discutido no piloto, embora a revisão sistemática tenha proporcionado sólidas bases para a identificação dos riscos, havia uma preocupação sobre a similaridade de alguns deles e que isso poderia causar alguma confusão para os respondentes. O fato positivo é que as confusões não se manifestaram e de acordo com os comentários, os respondentes diferenciaram os riscos com clareza.

Os riscos Vazamento de Informação e Divulgação de Informação não atingiram o percentual de corte estabelecido, mas os comentários dos respondentes revelam a legitimidade deles, como preocupação corrente das empresas diante de suas percepções. Esse resultado é relevante por de um modo dar visibilidade aos riscos que estão inerentes ao uso das tecnologias, e também

às contradições nesse entendimento, o qual é um gerador de risco que pode ser estudado em trabalhos futuros.

4.7 IMPLEMENTAÇÃO DO *framework* DE RISCOS

Como forma de apoiar as empresas na utilização do *framework* de riscos em segurança da informação, o **Capítulo 5** apresenta um conjunto de diretrizes que podem ser seguidas como orientação para as empresas. São diretrizes que apoiam as empresas no fortalecimento do gerenciamento dos riscos em segurança da informação identificados e classificados neste trabalho.

CAPÍTULO 5

DIRETRIZES PARA IMPLEMENTAÇÃO DO *framework* DE RISCOS

O presente capítulo apresenta um conjunto de diretrizes em forma de orientações para apoiar as empresas no gerenciamento de riscos a partir da identificação e classificação deles por relevância empreendida por este trabalho. O objetivo é que essas orientações apoiem as empresas a avaliar o estado atual no qual se encontram no quesito gerenciamento de riscos, bem como permitir estratégias para redução e mitigação deles na ocorrência de eventos de segurança. As orientações apresentadas são uma adaptação do *framework* Sendai para redução de riscos de desastres 2015-2030 (SENDAI, 2015) elaborado pelo Escritório das Nações Unidas para Redução de Desastres. É um *framework* que aborda perspectivas como gerenciamento de risco de desastres, governança, setor privado, identificação e avaliação de riscos e que auxilia na elaboração de estratégias a partir dos riscos identificados e classificados.

É importante ressaltar que as diretrizes que orientam as empresas a implementar o *framework* de riscos contempla todos os riscos identificados e classificados neste traballho. A possibilidade de contemplar todos os riscos ocorre em virtude da abrangência das diretrizes, as quais orientam as empresas a entender como os riscos podem ser gerenciados. As diretrizes alcançam fornecedores, parceiros e clientes, permitindo aderência no uso de um vasto conjunto de tecnologias digitais que implicam nos riscos discutidos neste trabalho.

5.1 ORIENTAÇÃO 1: ENTENDENDO A IDENTIFICAÇÃO E CLASSIFICAÇÃO DE RISCOS

Estratégias e práticas para o gerenciamento de riscos podem ser baseadas no entendimento dos riscos identificados e classificados, seguidos das dimensões de vulnerabilidade, capacidade e exposição de pessoas e sistemas. Tal conhecimento pode permitir a criação de uma avaliação do estado ou maturidade atual de uma empresa, como forma de apoio na prevenção, mitigação e o desenvolvimento do preparo adequado para respostas efetivas a possíveis ocorrências de um evento de segurança.

De modo a permitir o entendimento dos riscos identificados, é importante:

- Promover a coleta, análise, gerenciamento e uso de dados relevantes dos riscos identificados para assegurar a sua disseminação, levando em consideração as necessidades das diferentes categorias de usuários e sistemas;
- Encorajar e fortalecer o uso de dados estatísticos sobre eventos de segurança e avaliar o risco de novas ocorrências, incluindo as dimensões de vulnerabilidade, capacidade e exposição de pessoas e sistemas e os potenciais impactos nos fornecedores, parceiros e clientes;

- Desenvolver e disseminar periodicamente informações dos riscos identificados para os tomadores de decisões, incluindo um mapa dos riscos e o nível de exposição em um formato apropriado que possa ser usado pelas partes interessadas;
- Avaliar, registrar e compartilhar as perdas em decorrência dos eventos de segurança para ajudar no entendimento dos impactos nos fornecedores, parceiros e clientes no contexto da exposição às vulnerabilidades;
- Promover acesso em tempo real a dados confiáveis para aperfeiçoar as ferramentas de coleta, análise e disseminação deles;
- Promover a troca de experiências entre fornecedores, parceiros e clientes, incluindo as lições aprendidas, boas práticas, treinamento e educação para o gerenciamento de riscos, com o uso de treinamentos existentes e mecanismos de educação;
- Promover e aperfeiçoar o diálogo e cooperação entre a comunidade empresarial e científica, incluindo as partes interessadas e tomadores de decisões para ações efetivas no gerenciamento de riscos;
- Fortalecer o atual conhecimento técnico para consolidar o conhecimento existente;
- Promover investimento em inovação e tecnologias a longo prazo;
- Promover a incorporação de conhecimento sobre gerenciamento de riscos, incluindo a prevenção de eventos, mitigação, preparação, resposta, recuperação e reabilitação, com educação formal e informal das partes interessadas.

5.2 ORIENTAÇÃO 2: FORTALECENDO O GERENCIAMENTO DE RISCOS

O gerenciamento de riscos em todos os níveis das empresas, considerando fornecedores, parceiros e clientes é relevante para a redução de eventos de segurança. Visões claras, planos, competência e coordenação através de todas as áreas, bem como a participação das partes interessadas são necessárias. O fortalecimento do gerenciamento de riscos para prevenção, mitigação, preparo, resposta, recuperação e reabilitação é necessário para incentivar a colaboração entre os setores empresariais e científico.

De modo a fortalecer o gerenciamento de riscos, é importante:

- Adotar e implementar estratégias e planos para gerenciamento de riscos, com objetivos claros, indicadores e prazos;
- Realizar uma avaliação das capacidades técnicas, financeiras, administrativas e gerenciais das partes interessadas para lidar com os riscos identificados em todos os níveis;

- Encorajar o estabelecimento dos mecanismos necessários para assegurar a aderência aos setores legais e regulações, especialmente com relação às leis de proteção de dados para permitir um foco adequado no gerenciamento de riscos;
- Desenvolver e fortalecer os mecanismos apropriados para acompanhamento, avaliação periódica e publicação de relatórios sobre o progresso dos planos para gerenciamento de riscos, incluindo a promoção de debates internos sobre a efetividade das ações;
- Atribuir tarefas e responsabilidades para representantes das partes interessadas, com processos de tomada de decisão e consultas para o gerenciamento de riscos;
- Estimular e fortalecer representantes das partes interessadas para trabalhar e coordenar o gerenciamento de riscos entre fornecedores, parceiros e clientes;
- Promover padrões de qualidade para o gerenciamento de riscos, incluindo certificações e prêmios, com a participação da comunidade empresarial e científica.

5.3 ORIENTAÇÃO 3: INVESTINDO NA REDUÇÃO DE RISCOS

O investimento empresarial na prevenção de riscos é relevante para a preservação dos negócios e da confiança de fornecedores, parceiros e clientes. Pode ser um condutor de inovação, crescimento e lucratividade. Tal medida é efetiva para prevenir e reduzir perdas e assegurar a recuperação e reabilitação efetiva no caso de algum evento.

De modo a investir na redução de riscos, é importante:

- Alocar os recursos necessários, incluindo financeiros e logísticos a todas as áreas da empresa para a implantação de estratégias para a redução de riscos;
- Promover mecanismos para a transferência de riscos, seguro, compartilhamento de risco e proteção financeira para fornecedores, parceiros e clientes;
- Fortalecer os investimentos para a preservação e redução de riscos para instalações e sistemas críticos;
- Promover a preparação contra eventos de segurança;
- Promover a integração de medidas para a redução de riscos com medidas financeiras e legais;
- Promover e integrar a perspectiva de redução de riscos entre fornecedores, parceiros e clientes.

CAPÍTULO 6

CONSIDERAÇÕES FINAIS

A TD é, indiscutivelmente, um dos eventos mais impactantes que está ocorrendo na atualidade. Ela é resultado de uma evolução tecnológica gradual, que partiu da revolução das tecnologias da informação, ocorrida entre as décadas de 1980 e 1990, e alcançou rapidamente o estágio atual, com o uso maciço de tecnologia pelos cidadãos e pelas empresas. Não se trata de uma escolha que pode ser feita de acordo com um modo de vida, mas de um requisito básico para desempenhar tarefas diárias, como fazer compras, estudar, movimentar contas bancárias, assistir a filmes e conversar com amigos. Assim, tarefas que antes eram realizadas fisicamente, agora são predominantemente digitais.

Dessa maneira, espera-se mais lucro e vantagem competitiva para as empresas, preços melhores e produtos e serviços com mais qualidade para os consumidores, melhora da qualidade de vida e finalmente trabalho para as pessoas. Deposita-se esperança nisso, porque a partir do uso das tecnologias, tem-se a expectativa de mais conforto, segurança e de tempo livre para as atividades que dão prazer. Isso é algo que os indivíduos buscam com o uso da tecnologia, ao terceirizar para máquinas trabalhos repetitivos ou perigosos, o que proporciona condições para tarefas que agreguem mais valor, sejam no sentido de lazer ou de educação. Isso alimenta a expectativa em um futuro melhor.

Mesmo com essas expectativas, a realidade pode mostrar uma outra face. Em razão de uma mudança rápida e disruptiva que a TD está desencadeando, empresas não conseguem se adaptar. Entretanto, a vantagem competitiva não vem de modo incondicional somente pelo uso de tecnologias e as empresas desaparecem do mercado em poucos anos (HARARI, 2018). Em decorrência disso, as pessoas se frustram porque perdem os seus trabalhos e como consumidores, se sentem inseguras em razão dos problemas com privacidade, à medida que compartilham os seus dados pessoais com as empresas remanescentes. Assim, o risco toma o lugar da expectativa. Consequentemente, os cidadãos e as empresas se sentem ameaçados com esta revolução que deveria proporcionar otimismo.

De acordo com os resultados da presente pesquisa, o que ocorre é a subestimação de um elemento fundamental na ocorrência de uma revolução. Isso não é privilégio da TD, mas de todas as mudanças disruptivas que ocorreram no passado. Trata-se de subestimar o risco, isto é, a ameaça que uma modificação envolve. Esse é o perigo que a TD traz para cidadãos e para empresas, o qual deve ser considerado com mais atenção, de modo a obter o máximo proveito desta grande disrupção.

É importante salientar que o risco não é trivial e possui várias dimensões. Não se trata somente do risco de invasão a servidores de uma empresa ou a um roteador doméstico. Esse risco existe, porém já é bem tratado pelas ferramentas atuais. Há vários modelos e ferramentas que endereçam riscos em aplicações e equipamentos específicos.

Por fim, para responder a questão formulada neste trabalho, a revisão sistemática da litera-

tura permitiu a construção de um *framework* de riscos, o qual foi validado por especialistas de TI de mercado por meio de um questionário. Entrega um *framework* para apoiar as empresas na jornada da TD, e viabilizar mecanismos para os riscos serem priorizados e mitigados pelas empresas.

O *framework* proposto foi validado pelos especialistas e dessa forma os objetivos foram alcançados. Os objetivos específicos que são a identificação e classificação dos riscos, bem como o desenvolvimento e validação um *framework* de riscos foram atendidos. Esses objetivos alcançam a realização do objetivo geral que é o desenvolvimento e validação de um *framework* de riscos que apoia empresas quanto aos desafios no uso das tecnologias da TD. Deste modo a questão de pesquisa é respondida com precisão e a criação de um *framework* para identificação e classificação dos riscos pode ser empreendida por meio de uma revisão sistemática da literatura, em conjunto com a validação por especialistas de TI que trazem as percepções de mercado para os achados acadêmicos e assim legitimam a importância do tema que é percorrer os riscos inerentes ao uso das tecnologias digitais nas empresas.

Como todos os riscos foram validados pelos especialistas dentro dos critérios assumidos, tanto na análise quantitativa quanto nas opiniões qualitativas, o objetivo de se ter um *framework* de riscos validado foi atingido plenamente pela pesquisa.

6.1 CONTRIBUIÇÃO PARA A ÁREA

A contribuição desta pequisa tem três perspectivas. A primeira é uma contribuição imediata para academia, com a expansão da teoria sobre os riscos no uso das tecnologias digitais. O tema não é trivial porque facilmente ultrapassa os limites da pesquisa, pois os riscos percorrem várias áreas de conhecimento. Embora contradições possam acompanhar a identificação e classificação deles, a contribuição acadêmica é expandir este campo de estudo sobre os efeitos colaterais do uso das tecnologias digitais.

A segunda é disponibilizar uma revisão sistemática da literatura que proporciona o estado da arte acadêmico do tema riscos e tecnologias. É uma contribuição que disponibiliza um recorte do tema que pode ser comparado com outros estudos e com outros momentos no futuro.

A terceira contribuição é um instrumento que é o *framework*, que pode ser aplicado nas empresas, capaz de apoiá-las na jornada da TD, incluindo todas as referências e fundamentações que vão auxiliá-las a identificarem e classificarem os riscos associados. Trata-se de reconhecer os riscos de modo que sejam reduzidos e até mesmo prevenidos. Essa será a contribuição maior de toda a pesquisa, ao permitir que o uso das tecnologias digitais não acabe por gerar perdas em razão dos riscos discutidos aqui.

6.2 Limitações da Pesquisa

Esta pesquisa viabilizada a partir de uma revisão sistemática da literatura se concentra nos riscos das tecnologias digitais e nos seus efeitos nas empresas privadas, porém a pesquisa não contempla riscos sistêmicos, sociais, humanos ou que impactem a segurança nacional de países. A pesquisa também não contempla empresas públicas, governos, órgãos governamentais, e de organizações não governamentais, cidadãos individuais ou mesmo sociedade como um todo.

6.3 Trabalhos Futuros

O trabalho futuro que esta pesquisa proporciona, é criar um modelo para priorização e mitigação de riscos com o *framework* proposto e avaliado como um ponto de partida. Pode-se expandir a pesquisa para além das empresas privadas, incluindo empresas públicas ou mesmo governos, órgãos de governo ou organizações não governamentais. É uma expansão da pesquisa que permitirá apoiá-los na jornada da TD com a perspectiva dos riscos no contexto de governos e da sociedade. Adicionalmente, sugere-se como trabalho futuro, expandir a pesquisa para riscos de outras naturezas, como riscos sociais, humanos e que impactem a segurança nacional de países. Será uma expansão da pesquisa para além dos riscos das tecnologias digitais e contemplará os seus efeitos na sociedade ou na infraestrutura crítica de países. O tema risco é amplo e pode ser explorado em várias perspectivas nos trabalhos futuros que virão a ser empreendidos. Adiciona-se também como trabalho futuro, revisitar os riscos Vazamento de Informação e Divulgação de Informação, os quais apresentaram algumas contradições entre os respondentes na pesquisa de campo.

REFERÊNCIAS BIBLIOGRÁFICAS

AL-ALI, S. **Technological dependence in developing countries: A case study of Kuwait**. *Technology in Society*, Elsevier, v. 13, n. 3, p. 267–277, 1991. Citado na pág. 15.

AL-DEBEI, M. M.; AVISON, D. **Developing a unified framework of the business model concept**. *European journal of information systems*, Taylor and Francis, v. 19, n. 3, p. 359–376, 2010. Citado na pág. 13.

ALHARBI, S. A. **A qualitative study on security operations centers in Saudi Arabia: Challenges and Research directions**. *Journal of Theoretical and Applied Information Technology*, v. 98, n. 24, 2020. Citado na pág. 32, 82.

ALKHALIL, Z.; HEWAGE, C.; NAWAF, L.; KHAN, I. **Phishing Attacks: Recent Comprehensive Study and a New Anatomy**. *Frontiers in Computer Science*, Frontiers, v. 3, p. 6, 2021. Citado na pág. 35, 44.

ALVARENGA, A. C.; NOVAES, A. G. N. ***Logística aplicada: suprimento e distribuição física***. [S.l.]: Editora Blucher, 2000. Citado na pág. 33.

ARAUJO, R. F. de; OLIVEIRA, M. *et al.* **Da informática à tecnologia da informação: dependência, reserva de mercado e suas implicações político-econômicas From informatics to information technology: dependence, market reserve and its political and economic implications**. *Liinc em Revista*, Instituto Brasileiro de Informação em Ciência e Tecnologia, v. 13, n. 2, 2017. Citado na pág. 14, 27.

BAGHDASARIN, D. **MRO Cybersecurity SWOT**. *International Journal of Aviation, Aeronautics, and Aerospace*, v. 6, n. 1, p. 9, 2019. Citado na pág. 32, 82.

BALLOU, R. H. ***Logística empresarial: transportes, administração de materiais e distribuição física***. [S.l.]: Atlas, 1993. Citado na pág. 33.

BHARADWAJ, A.; SAWY, O. A. E.; PAVLOU, P. A.; VENKATRAMAN, N. **Digital business strategy: toward a next generation of insights**. *MIS quarterly*, JSTOR, p. 471–482, 2013. Citado na pág. 13, 27.

BHATTACHARJEE, K.; CHEN, M.; DASGUPTA, A. **Privacy-preserving data visualization: reflections on the state of the art and research opportunities**. In: WILEY ONLINE LIBRARY. *Computer Graphics Forum*. [S.l.], 2020. v. 39, n. 3, p. 675–692. Citado na pág. 32, 35, 39, 40, 83.

BIRKEL, H. S.; VEILE, J. W.; MüLLER, J. M.; HARTMANN, E.; VOIGT, K.-I. **Development of a risk framework for Industry 4.0 in the context of sustainability for established manufacturers**. *Sustainability*, Multidisciplinary Digital Publishing Institute, v. 11, n. 2, p. 384, 2019. Citado na pág. 15, 32, 37, 81.

BOCAYUVA, M. **Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic**. *WMU Journal of Maritime Affairs*, Springer, p. 1–20, 2021. Citado na pág. 32, 38, 84.

BRYMAN, A. **Integrating quantitative and qualitative research: how is it done?** *Qualitative research*, SAGE publications Sage CA: Thousand Oaks, CA, v. 6, n. 1, p. 97–113, 2006. Citado na pág. 18.

CARAYANNIS, E. G.; CHRISTODOULOU, K.; CHRISTODOULOU, P.; CHATZICHRISTOFIS, S. A.; ZINONOS, Z. **Known Unknowns in an Era of Technological and Viral Disruptions-Implications for Theory, Policy, and Practice**. *Journal of the Knowledge Economy*, Springer, p. 1–24, 2021. Citado na pág. 14, 15, 26, 27, 28.

CAZORLA, I. M.; SANTANA, E. R. dos S.; UTSUMI, M. C. O campo conceitual da média aritmética: uma primeira aproximação conceitual. *Revista Eletrônica de Educação Matemática*, 2019. Citado na pág. 49.

CHALYUK, Y.; DOVHANYK, N.; KURBALA, N.; KOMAROVA, K.; KOVALCHUK, N. **The digital economy in a global environment**. Akademické sdružení MAGNANIMITAS, 2021. Citado na pág. 32, 35, 84.

CHENG, G.-J.; LIU, L.-T.; QIANG, X.-J.; LIU, Y. **Industry 4.0 development and application of intelligent manufacturing**. In: IEEE. *2016 international conference on information system and artificial intelligence (ISAI)*. [S.l.], 2016. p. 407–410. Citado na pág. 27.

CISCO, U. Cisco annual internet report (2018–2023) white paper. *Cisco: San Jose, CA, USA*, 2020. Citado na pág. 16.

COLBERT, A.; YEE, N.; GEORGE, G. **The digital workforce and the workplace of the future**. Academy of Management Briarcliff Manor, NY, 2016. Citado na pág. 13.

COSTA, I.; RICCOTTA, R.; MONTINI, P.; STEFANI, E.; GOES, R. de S.; GASPAR, M. A.; MARTINS, F. S.; FERNANDES, A. A.; MACHADO, C.; LOçANO, R. *et al.* The degree of contribution of digital transformation technology on company sustainability areas. *Sustainability*, Multidisciplinary Digital Publishing Institute, v. 14, n. 1, p. 462, 2022. Citado na pág. 14.

CREAZZA, A.; COLICCHIA, C.; SPIEZIA, S.; DALLARI, F. **Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era**. *Supply Chain Management: An International Journal*, Emerald Publishing Limited, 2021. Citado na pág. 32, 36, 37, 38, 39, 84.

DHS. ***The National Strategy to Secure Cyberspace***. 2003. Citado na pág. 28.

DOBROLYUBOVA, E. **Measuring Outcomes of Digital Transformation in Public Administration: Literature Review and Possible Steps Forward**. *Network of Institutes and Schools of Public Administration in Central and Eastern Europe. The NISPAcee Journal of Public Administration and Policy*, De Gruyter Poland, v. 14, n. 1, p. 61–86, 2021. Citado na pág. 32, 38, 84.

ECKHART, M.; BRENNER, B.; EKELHART, A.; WEIPPL, E. R. **Quantitative Security Risk Assessment for Industrial Control Systems: Research Opportunities and Challenges.** *J. Internet Serv. Inf. Secur.*, v. 9, n. 3, p. 52–73, 2019. Citado na pág. 32, 37, 82.

EL-HADDADEH, R. **Digital innovation dynamics influence on organisational adoption: the case of cloud computing services**. *Information Systems Frontiers*, Springer, v. 22, n. 4, p. 985–999, 2020. Citado na pág. 13, 27, 32, 36, 83.

ELIZAVETA, G.; TJASA, I. **Regulatory sandboxes (experimental legal) regimes for digital innovations in Brics**. *BRICS Law Journal*, BRICS Law Journal, v. 7, n. 2, 2020. Citado na pág. 32, 84.

FARD, S. M. H.; KARIMIMPOUR, H.; DEHGHANTANHA, A.; JAHROMI, A. N.; SRIVASTAVA, G. **Ensemble sparse representation-based cyber threat hunting for security of smart cities**. *Computers & Electrical Engineering*, Elsevier, v. 88, p. 106825, 2020. Citado na pág. 32, 35, 37, 83.

FEKETE, A.; RHYNER, J. **Sustainable Digital Transformation of Disaster Risk-Integrating New Types of Digital Social Vulnerability and Interdependencies with Critical Infrastructure**. *Sustainability*, Multidisciplinary Digital Publishing Institute, v. 12, n. 22, p. 9324, 2020. Citado na pág. 29.

FERNANDES, A. A.; DINIZ, J. L.; ABREU VLADIMIR FERRAZ DE EMILIANO DE SOUZA, D.; TONON, D. H. P.; SILVA, E. Brito da; COSTA, I.; OLIVEIRA, J. Cardoso de; SEIXAS, J. Alberto de; LEãO, L.; FRANCISCO, M. C.; RODRIGUES, P. S. F.; BRITO, R.; RICCOTTA, R.; OLIVEIRA, S. Correia de; FERNANDES, T. C. M. **Governança Digital 4.0**. Brasport, Rio de Janeiro, 2019. Citado na pág. 13.

GAIVORONSKAYA, Y. V.; MAMYCHEV, A. Y.; PETROVA, D. A.; RUSANOVA, I. O. **Typology of Risks and Threats caused by Digitalization**. *Revista TURISMO: Estudos e Práticas*, n. 5, 2020. Citado na pág. 14, 16, 27, 28, 32, 35, 38, 48, 84.

GARTNER. *The Top 8 Cybersecurity Predictions for 2021-2022*. 2021. Acessado em 03/02/2022. Disponível em: <https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022-1>. Citado na pág. 16.

GUILBAUD, P.; HAYES, M.; HAMED, D. Use of enabling technology to enhance self-efficacy beliefs and social capital dispositions: Integrating arcgis in an upper level business course. In: ASSOCIATION FOR THE ADVANCEMENT OF COMPUTING IN EDUCATION (AACE). *Global Learn*. [S.l.], 2019. p. 130–143. Citado na pág. 14.

HANELT, A.; BOHNSACK, R.; MARZ, D.; MARANTE, C. A. A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. *Journal of Management Studies*, Wiley Online Library, v. 58, n. 5, p. 1159–1197, 2021. Citado na pág. 13.

HARARI, Y. N. ***21 Lessons for the 21st Century***. [S.l.]: Random House, 2018. Citado na pág. 69.

HAUSBERG, J.; LIERE-NETHELER, K.; PACKMOHR, S.; PAKURA, S.; VOGELSANG, K. **Digital transformation in business research: a systematic literature review and analysis**. *Proceedings of DRUID18*, 2018. Citado na pág. 26, 27, 30.

HESS, T.; MATT, C.; BENLIAN, A.; WIESBöCK, F. **Options for formulating a digital transformation strategy**. *MIS Quarterly Executive*, v. 15, n. 2, 2016. Citado na pág. 16.

HR3162. **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001**. 2001. Citado na pág. 28.

IDC. *IoT Growth Demands Rethink of Long-Term Storage Strategies*. 2020. Acessado em 03/02/2022. Disponível em: <https://www.idc.com/getdoc.jsp?containerId=prAP46737220#:~:text=IDC%20predicts%20that%20by%202025,from%2018.3%20ZB%20in%202019.> Citado na pág. 16.

KABBAS, A.; ALHARTHI, A.; MUNSHI, A. **Artificial Intelligence Applications in Cybersecurity**. *International Journal of Computer Science and Network Security*, v. 20, n. 2, p. 120–124, 2020. Citado na pág. 32, 37, 83.

KAVALLIERATOS, G.; KATSIKAS, S. **Managing Cyber Security Risks of the Cyber-Enabled Ship**. *Journal of Marine Science and Engineering*, Multidisciplinary Digital Publishing Institute, v. 8, n. 10, p. 768, 2020. Citado na pág. 32, 39, 83.

KHANBOUBI, F.; BOULMAKOUL, A. **Digital transformation in the banking sector: surveys exploration and analytics**. *International Journal of Information Systems and Change Management*, Inderscience Publishers (IEL), v. 11, n. 2, p. 93–127, 2019. Citado na pág. 32, 39, 81.

KRAFFT, M.; KUMAR, V.; HARMELING, C.; SINGH, S.; ZHU, T.; CHEN, J.; DUNCAN, T.; FORTIN, W.; ROSA, E. **Insight is power: Understanding the terms of the consumer-firm data exchange**. *Journal of Retailing*, Elsevier, v. 97, n. 1, p. 133–149, 2021. Citado na pág. 32, 38, 39, 48, 84.

LAMBERTON, C.; STEPHEN, A. T. **A thematic exploration of digital, social media, and mobile marketing: Research evolution from 2000 to 2015 and an agenda for future inquiry**. *Journal of Marketing*, SAGE Publications Sage CA: Los Angeles, CA, v. 80, n. 6, p. 146–172, 2016. Citado na pág. 13, 14.

LEE, I. **Cybersecurity: Risk management framework and investment cost analysis**. *Business Horizons*, Elsevier, 2021. Citado na pág. 32, 38, 39, 84.

LEMOS, F. On the definition of risk. *Journal of risk management in financial institutions*, Henry Stewart Publications, v. 13, n. 3, p. 266–278, 2020. Citado na pág. 14.

LIAO, Y.; DESCHAMPS, F.; LOURES, E. d. F. R.; RAMOS, L. F. P. **Past, present and future of Industry 4.0 - a systematic literature review and research agenda proposal**. *International journal of production research*, Taylor & Francis, v. 55, n. 12, p. 3609–3629, 2017. Citado na pág. 18, 19, 20.

LIBRANTZ, A. F. H.; COSTA, I.; SPINOLA, M. d. M.; NETO, G. C. de O.; ZERBINATTI, L. Risk assessment in software supply chains using the bayesian method. *International Journal of Production Research*, Taylor & Francis, v. 59, n. 22, p. 6758–6775, 2021. Citado na pág. 14.

LUCATO, W. C.; JúNIOR, M. V.; VANALLE, R. M.; SALLES, J. A. A. **Model to measure the degree of competitiveness for auto parts manufacturing companies**. *International Journal of Production Research*, Taylor & Francis, v. 50, n. 19, p. 5508–5522, 2012. Citado na pág. 36.

MENDHURWAR, S.; MISHRA, R. **Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges**. *Enterprise Information Systems*, Taylor & Francis, v. 15, n. 4, p. 565–584, 2021. Citado na pág. 32, 37, 39, 82.

MIYAZAWA, T.; FUKUNAGA, T.; TAKAHASHI, G.; KIKUCHI, R.; TAKAHASHI, S.; HASEGAWA, S. The future of data distribution and its security technology. *NTT Technical Review*, NTT, v. 18, n. 4, 2020. Citado na pág. 14, 15.

MOHER, D.; LIBERATI, A.; TETZLAFF, J.; ALTMAN, D. G. *et al.* **Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement**. *Int J Surg*, v. 8, n. 5, p. 336–341, 2010. Citado na pág. 18, 20.

MORAKANYANE, R.; GRACE, A. A.; O'REILLY, P. **Conceptualizing Digital Transformation in Business Organizations: A Systematic Review of Literature.** *Bled eConference*, v. 21, 2017. Citado na pág. 13, 26.

NUCCIO, M.; GUERZONI, M. **Big data: Hell or heaven? Digital platforms and market power in the data-driven economy**. *Competition and Change*, SAGE Publications Sage UK: London, England, v. 23, n. 3, p. 312–328, 2019. Citado na pág. 14, 29, 32, 81.

O'LEARY, T.; ARMFIELD, T. **Adapting to the Digital Transformation**. *Alta. L. Rev.*, HeinOnline, v. 58, p. 249, 2020. Citado na pág. 26, 27, 32, 82.

OLIVEIRA, J.; CARVALHO, G.; CABRAL, B.; BERNARDINO, J. **Failure Mode and Effect Analysis for Cyber-Physical Systems**. *Future Internet*, Multidisciplinary Digital Publishing Institute, v. 12, n. 11, p. 205, 2020. Citado na pág. 32, 83.

OWEN, R. S. **Infrastructures of cyber warfare**. In: *Cyber warfare and cyber terrorism*. [S.l.]: IGI Global, 2007. p. 35–41. Citado na pág. 28.

PACCHINI, A. P. T. *et al.* **O grau de prontidão das empresas industriais para implantação da indústria 4.0: um estudo no setor automotivo brasileiro.** Universidade Nove de Julho, 2019. Citado na pág. 33.

PANDA, A.; BOWER, A. **Cyber security and the disaster resilience framework**. *International Journal of Disaster Resilience in the Built Environment*, Emerald Publishing Limited, 2020. Citado na pág. 28, 29, 32, 83.

PARK, S.-T.; LI, G.; HONG, J.-C. **A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning**. *Journal of Ambient Intelligence and Humanized Computing*, Springer, v. 11, n. 4, p. 1405–1412, 2020. Citado na pág. 32, 82.

PERES, R. S.; JIA, X.; LEE, J.; SUN, K.; COLOMBO, A. W.; BARATA, J. **Industrial Artificial Intelligence in Industry 4.0-Systematic Review, Challenges and Outlook**. *IEEE Access*, IEEE, v. 8, p. 220121–220139, 2020. Citado na pág. 15.

POPESCU, S.; SANTA, R.; TELEABA, F.; ILESAN, H. **A structured framework for identifying risks sources related to human resources in a 4.0 working environment perspective**. *Human Systems Management*, IOS Press, n. Preprint, p. 1–17, 2020. Citado na pág. 32, 82.

PURAITE, A.; ZUZEVIčIūTė, V.; BEREIKIENė, D.; SKRYPKO, T.; SHMORGUN, L. **Algorithmic governance in public sector: is digitization a key to effective management**. 2020. Citado na pág. 32, 37, 82.

RIYANA, S.; NATWICHAI, J. **Privacy preservation for recommendation databases**. *Service Oriented Computing and Applications*, Springer, v. 12, n. 3, p. 259–273, 2018. Citado na pág. 32, 81.

ROSSI, E.; RUBATTINO, C.; VISCUSI, G. **Big data use and challenges: Insights from two internet-mediated surveys**. *Computers*, Multidisciplinary Digital Publishing Institute, v. 8, n. 4, p. 73, 2019. Citado na pág. 32, 81.

RUGG, G.; PETRE, M. *A gentle guide to research methods*. [S.l.]: McGraw-Hill Education (UK), 2006. Citado na pág. 36.

SCHNASSE, F.; MENZEFRICKE, J. S.; DUMITRESCU, R. Identification of socio-technical risks and their correlations in the context of digital transformation for the manufacturing sector. In: IEEE. *2021 IEEE 8th International Conference on Industrial Engineering and Applications (ICIEA)*. [S.l.], 2021. p. 159–166. Citado na pág. 13.

SCHNEIDER, S.; KOKSHAGINA, O. **Digital transformation: What we have learned (thus far) and what is next**. *Creativity and Innovation Management*, Wiley Online Library, 2020. Citado na pág. 13, 26.

SENDAI, J. Sendai framework for disaster risk reduction 2015–2030. *UN world conference on disaster risk reduction*, United Nations Office for Disaster Risk Reduction, v. 1, n. 1, p. 1–32, 2015. Citado na pág. 66.

SESTINO, A.; PRETE, M. I.; PIPER, L.; GUIDO, G. **Internet of Things and Big Data as enablers for business digitalization strategies**. *Technovation*, Elsevier, p. 102173, 2020. Citado na pág. 32, 37, 38, 48, 83.

SHERMAN, J. W.; RIVERS, A. M. There's nothing social about social priming: Derailing the "train wreck". *Psychological Inquiry*, Routledge, v. 32, n. 1, p. 1–11, 2021. Citado na pág. 47.

SHI, J.; JIN, L.; LI, J. **The integration of azure sphere and azure cloud services for internet of things**. *Applied Sciences*, Multidisciplinary Digital Publishing Institute, v. 9, n. 13, p. 2746, 2019. Citado na pág. 32, 39, 82.

SIDERSKA, J. **Robotic Process Automation - a driver of digital transformation?** *Engineering Management in Production and Services*, Walter de Gruyter GmbH, v. 12, n. 2, p. 21–31, jun. 2020. Citado na pág. 27.

SPEKMAN, R. E.; DAVIS, E. W. Risky business: expanding the discussion on risk and the extended enterprise. *International Journal of Physical Distribution & Logistics Management*, Emerald Group Publishing Limited, 2004. Citado na pág. 14.

SPIVAKOVSKYY, S.; KOCHUBEI, O.; SHEBANINA, O.; SOKHATSKA, O.; YAROSHENKO, I.; NYCH, T. *et al.* **The impact of digital transformation on the economic security of Ukraine**. 2021. Citado na pág. 32, 38, 84.

TECH, J. E. T. **Security in the age of digital disruption**. *Journal of Environmental Treatment Techniques*, v. 8, n. 1, p. 259–261, 2020. Citado na pág. 32, 39, 84.

TOKODY, D.; ALBINI, A.; ADY, L.; RAJNAI, Z.; PONGRáCZ, F. **Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city**. *Interdisciplinary Description of Complex Systems: INDECS*, Hrvatsko interdisciplinarno društvo, v. 16, n. 3-A, p. 384–396, 2018. Citado na pág. 32, 81.

URBINATI, A.; CHIARONI, D.; CHIESA, V.; FRATTINI, F. **The role of digital technologies in open innovation processes: an exploratory multiple case study analysis**. *R&D Management*, Wiley Online Library, v. 50, n. 1, p. 136–160, 2020. Citado na pág. 26.

VASIL'EV, Y. S.; ZEGZHDA, D. P.; POLTAVTSEVA, M. A. **Problems of security in digital production and its resistance to cyber threats**. *Automatic Control and Computer Sciences*, Springer, v. 52, n. 8, p. 1090–1100, 2018. Citado na pág. 32, 39, 81.

VERHOEF, P. C.; STEPHEN, A. T.; KANNAN, P.; LUO, X.; ABHISHEK, V.; ANDREWS, M.; BART, Y.; DATTA, H.; FONG, N.; HOFFMAN, D. L. *et al.* **Consumer connectivity in a complex, technology-enabled, and mobile-oriented world with smart products**. *Journal of Interactive Marketing*, Elsevier, v. 40, p. 1–8, 2017. Citado na pág. 13, 14.

VIAL, G. **Understanding digital transformation: A review and a research agenda**. *The Journal of Strategic Information Systems*, Elsevier, v. 28, n. 2, p. 118–144, 2019. Citado na pág. 13, 14, 27.

XIA, F.; LIU, L.; LI, J.; MA, J.; VASILAKOS, A. V. Socially aware networking: A survey. *IEEE Systems Journal*, IEEE, v. 9, n. 3, p. 904–921, 2013. Citado na pág. 14.

XING, L.; LEVITIN, G. **Balancing theft and corruption threats by data partition in cloud system with independent server protection**. *Reliability Engineering & System Safety*, v. 167, p. 248–254, 2017. ISSN 0951-8320. Citado na pág. 35.

XU, X.; ZENG, S.; HE, Y. **The impact of information disclosure on consumer purchase behavior on sharing economy platform Airbnb**. *International Journal of Production Economics*, Elsevier, v. 231, p. 107846, 2021. Citado na pág. 36.

YANG, P.; XIONG, N.; REN, J. **Data security and privacy protection for cloud storage: A survey**. *IEEE Access*, IEEE, v. 8, p. 131723–131740, 2020. Citado na pág. 27, 28, 32, 35, 38, 39, 48, 83.

ZARZUELO, I. de la P. **Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue**. *Transport Policy*, Elsevier, v. 100, p. 1–4, 2021. Citado na pág. 28, 32, 83.

Apêndices

APÊNDICE A

EXPRESSÕES DE BUSCA E CONDIÇÕES ESPECÍFICAS

–Scopus

999 document results

TITLE-ABS-KEY ("digital transformation"AND (security OR privacy OR breach* OR leak* OR mitigati* OR risk*))

353 document results

TITLE-ABS-KEY ("digital transformation"AND (security OR privacy OR breach* OR leak* OR mitigati* OR risk*)) AND (LIMIT-TO (DOCTYPE , "ar"))

308 document results

TITLE-ABS-KEY ("digital transformation"AND (security OR privacy OR breach* OR leak* OR mitigati* OR risk*)) AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English"))

–WoS

Results: 475

(from Web of Science Core Collection) You searched for: TOPIC: ("digital transformation"AND (security OR privacy OR breach OR leak OR mitigati OR risk)) Timespan: All years. Indexes: SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH, ESCI.

Results: 274

(from Web of Science Core Collection) You searched for: TOPIC: ("digital transformation"AND (security OR privacy OR breach* OR leak* OR mitigati* OR risk*)) Refined by: DOCUMENT TYPES: (ARTICLE) Timespan: All years. Indexes: SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH, ESCI.

Results: 227

(from Web of Science Core Collection) You searched for: TOPIC: ("digital transformation"AND (security OR privacy OR breach* OR leak* OR mitigati* OR risk*)) Refined by: LANGUAGES: (ENGLISH) AND DOCUMENT TYPES: (ARTICLE) Timespan: All years. Indexes: SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH, ESCI.

APÊNDICE B

ESTUDOS IDENTIFICADOS

Quadro B.1: *Estudos Identificados*

#	Autores	DOI	Título
01	Nuccio e Guerzoni (2019)	10.1177/1024529418816525	Big data: Hell or heaven? Digital platforms and market power in the data-driven economy
02	Riyana e Natwichai (2018)	10.1007/s11761-018-0248-y	Privacy preservation for recommendation databases
03	Vasil'ev, Zegzhda e Poltavtseva (2018)	10.3103/S0146411618080254	Problems of security in digital production and its resistance to cyber threats
04	Tokody *et al.* (2018)	10.7906/indecs.16.3.11	Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city
05	Rossi, Rubattino e Viscusi (2019)	10.3390/computers8040073	Big data use and challenges: Insights from two internet-mediated surveys
06	Birkel *et al.* (2019)	10.3390/su11020384	Development of a risk framework for Industry 4.0 in the context of sustainability for established manufacturers
07	Khanboubi e Boulmakoul (2019)		Digital transformation in the banking sector: surveys exploration and analytics

08	Mendhurwar e Mishra (2021)	10.1080/17517575.2019.1600041	Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges
09	Baghdasarin (2019)	10.15394/ijaaa.2019.1318	MRO cybersecurity swot
10	Eckhart *et al.* (2019)		Quantitative Security Risk Assessment for Industrial Control Systems: Research Opportunities and Challenges
11	Shi, Jin e Li (2019)	10.3390/app9132746	The integration of azure sphere and azure cloud services for internet of things
12	Alharbi (2020)		A qualitative study on security operations centers in Saudi Arabia: Challenges and research directions
13	Popescu *et al.* (2020)	10.3233/HSM-201034	A structured framework for identifying risks sources related to human resources in a 4.0 working environment perspective
14	Park, Li e Hong (2020)	10.1007/s12652-018-0998-6	A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning
15	O'Leary e Armfield (2020)		Adapting to the Digital Transformation
16	Puraite *et al.* (2020)	10.14807/ijmp.v11i9.1400	Algorithmic governance in public sector: is digitization a key to effective management

17	Kabbas, Alharthi e Munshi (2020)		Artificial Intelligence Applications in Cybersecurity
18	Panda e Bower (2020)	10.1108/IJDRBE-07-2019-0046	Cyber security and the disaster resilience framework
19	Zarzuelo (2021)	10.1016/j.tranpol.2020.10.001	Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue
20	Yang, Xiong e Ren (2020)	10.1109/ACCESS.2020.3009876	Data Security and Privacy Protection for Cloud Storage: A Survey
21	El-Haddadeh (2020)	10.1007/s10796-019-09912-2	Digital innovation dynamics influence on organisational adoption: the case of cloud computing services
22	Fard *et al.* (2020)	10.1016/j.compeleceng.2020.106825	Ensemble sparse representation-based cyber threat hunting for security of smart cities
23	Oliveira *et al.* (2020)	10.3390/fi12110205	Failure Mode and Effect Analysis for Cyber-Physical Systems
24	Sestino *et al.* (2020)	10.1016/j.technovation.2020.102173	Internet of Things and Big Data as enablers for business digitalization strategies
25	Kavallieratos e Katsikas (2020)	10.3390/jmse8100768	Managing cyber security risks of the cyber-enabled ship
26	Bhattacharjee, Chen e Dasgupta (2020)	10.1111/cgf.14032	Privacy-preserving data visualization: reflections on the state of the art and research opportunities

27	Elizaveta e Tjasa (2020)	10.21684/2412-2343-2020-7-2-10-36	Regulatory sandboxes (experimental legal regimes) for digital innovations in Brics
28	Tech (2020)		Security in the age of digital disruption
29	Gaivoronskaya *et al.* (2020)		Typology of risks and threats caused by digitalization
30	Bocayuva (2021)	10.1007/s13437-021-00240-4	Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic
31	Lee (2021)	10.1016/j.bushor.2021.02.022	Cybersecurity: Risk management framework and investment cost analysis
32	Krafft *et al.* (2021)	10.1016/j.jretai.2020.11.001	Insight is power: Understanding the terms of the consumer-firm data exchange
33	Dobrolyubova (2021)	10.2478/nispa-2021-0003	Measuring Outcomes of Digital Transformation in Public Administration: Literature Review and Possible Steps Forward
34	Chalyuk *et al.* (2021)		The digital economy in a global environment
35	Spivakovskyy *et al.* (2021)	10.25115/eea.v39i5.5040	The Impact of Digital Transformation on the Economic Security of Ukraine
36	Creazza *et al.* (2021)	10.1108/SCM-02-2020-0073	Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era

APÊNDICE C

QUESTIONÁRIO PILOTO

C.1 PERFIL DOS RESPONDENTES

Respondente #01

Quadro C.1: *Perfil Respondente #01*

Resposta	2021/09/14 1:50:20 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Engenharia
Posição	Diretor
Tempo na Posição	1 semana
País	Canadá

Fonte: autor

Respondente #02

Quadro C.2: *Perfil Respondente #02*

Resposta	2021/09/14 9:05:58 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Outra
Posição	Diretor
Tempo na Posição	5 anos
País	Brasil

Fonte: autor

Respondente #03

Quadro C.3: *Perfil Respondente #03*

Resposta	2021/09/14 6:31:08 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Vendas/Pré-Vendas
Posição	Engenheiro
Tempo na Posição	2 anos e meio
País	Brasil

Fonte: autor

Respondente #04

Quadro C.4: *Perfil Respondente #04*

Resposta	2021/09/25 4:35:29 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Outra
Posição	Arquiteto
Tempo na Posição	6 meses
País	EUA

Fonte: autor

Respondente #05

Quadro C.5: *Perfil Respondente #05*

Resposta	2021/09/27 10:06:31 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Suporte
Posição	Engenheiro
Tempo na Posição	1 ano
País	EUA

Fonte: autor

C.2 Resposta dos Respondentes

C.2.1 Respondente #01

a. Privacidade

a.1 Neutro

a.2 Neutro

a.3 Concordo totalmente

a.4 Neutro

In my experience private persons are somewhat less concerned about privacy issues than professionals in identity and security related software organizations.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo

b.3 Neutro

b.4 Concordo totalmente

No matter how severe cyberattacks have already been, consumers do not seem to "punish"companies that lost their personal data. And companies continue to, for example, collect data that are often not needed to full-fill services.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

All of these types of incidents have been documented in the news and been confirmed by harmed parties.

d. Vazamento de Informação

d.1 Concordo

d.2 Concordo

d.3 Concordo totalmente

d.4 Neutro

Especially the last bullet appear to be irrelevant for many consumers. I have yet to see a company that closes its business due to losing customers cause of data loss.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Everything listed is true as far as I can tell

f. Acesso não Autorizado

f.1 Neutro

f.2 Concordo totalmente

f.3 Concordo totalmente

f.4 Concordo totalmente

Especially cloud bases systems live through distribution of data. However, lost or insecure data is not caused by insecure cloud providers but due to the lack of proper configuration.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo

g.4 Concordo

Phishing becomes less successful the more systems such as multi-factor authentication (MFA) procedures are in place. Passwordless flows can also hinder phishing attacks

h. Divulgação de Informação

h.1 Neutro

h.2 Concordo totalmente

h.3 Concordo

h.4 Neutro

The last bullet depends very much on the environment in which data was collected.

C.2.2 RESPONDENTE #02

a. Privacidade

a.1 Concordo totalmente

a.2 Neutro

a.3 Concordo totalmente

a.4 Concordo totalmente

Após a adoção de leis como GDPR e LGPD, o tratamento de dados pessoais está sendo levado mais a sério. Muitos sistemas foram redesenhados para atender a privacidade dos dados pessoais.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Não concordo

b.4 Concordo totalmente

Apesar da grande disseminação de ataques de ransomware, as empresas não conseguem aumentar as barreiras para evitar os incidentes de segurança. Além disso, as empresas ainda não notaram que os tradicionais antivírus não são a proteção mais adequada. Atualmente a tecnologia EDR é muito mais eficaz, porém poucas empresas adotaram.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Mesmo comentário do item anterior

d. Vazamento de Informação

d.1 Discordo totalmente

d.2 Concordo

d.3 Neutro

d.4 Concordo totalmente

O fato de levarmos dados para nuvem, por si só, não causa vazamentos. A má implementação de controles de segurança, sim. Porém, controles fracos de segurança podem estar em qualquer ambiente.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Atualmente os criminosos cibernéticos utilizam as invasões e vazamentos para solicitar resgates, extorsões para não divulgar dados roubados e até mesmo para vender a concorrentes da empresa afetada. Ransomware se tornou um business de milhões de dólares e meio de vida para os criminosos.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Concordo totalmente

f.4 Concordo

A ausência de revisões de acesso a sistemas leva a possibilidade de um sistema ter acessos indevidos. Adicionalmente, é importante ressaltar que além do controle de autenticação, existem falhas de implementação de controles de autorização que apesar de utilizar uma credencial ser legítima, o atacante consegue burlar as regras de negócio e ter acesso indevido.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Neutro

g.4 Não concordo

A pandemia fez com que aumentasse a quantidade de acessos remotos. Desta maneira, os ataques de phishing se tornaram mais efetivos.

h. Divulgação de Informação

h.1 Concordo totalmente

h.2 Concordo totalmente

h.3 Não concordo

h.4 Concordo totalmente

Novamente, as novas regulamentações para dados pessoais estão mudando a maneira como esses dados estão sendo publicados.

C.2.3 RESPONDENTE #03

a. Privacidade

a.1 Concordo

a.2 Concordo totalmente

a.3 Concordo totalmente

a.4 Concordo

Although privacy is a growing concern among the "average Joe", there's still a urgent need to educate the people about what it means when we talk about privacy, the impacts and damages of getting it violated, and the rights.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Concordo

b.4 Concordo

The threat of malware is indeed growing and it is grave, but we have means to detect and respond to those incidents in a way to avoid a cyber catastrophe. the technology exists, just needs to reach a wider range.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Ransomware is a great example of why it's important to have properly configured backup infrastructure, tested and proven to be effective. Also, again the need to educate the people to avoid infections. The best defense is prevention. Also, it is vital to have deployed onto the organizations solutions like XDR, NDR, SIEM and SOAR.

d. Vazamento de Informação

d.1 Concordo

d.2 Concordo totalmente

d.3 Concordo totalmente

d.4 Concordo totalmente

Data leakage is a growing issue - specially when the company who collects the data has partnerships with smaller organizations that don't have the same security expertise nor budget - as happened with the Cambridge Analytica / Facebook scandal.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

A targeted attack aimed to a specific individual can grow and impact every person and organization who interacts with the targeted citizen. We saw this happen in many cases. What is more concerning is that, on a case of data theft attack, often the organizations and citizens fail to detect the attack until is too late - again the need for specialized cyber defense solutions.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Concordo

f.4 Concordo totalmente

This is an old issue. There's a movement to remove the need for passwords (passwordless environments) but it is still far away.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

It is the easiest and most effective way to target an organization: via the weakest link, which is the human being. You don't need to brute force a system to get in if the user opens a door for you...

h. Divulgação de Informação

h.1 Neutro

h.2 Concordo

h.3 Não concordo

h.4 Neutro

It is a gray area. You agree to disclose some information with a 3rd-party, under the understanding that they will protect your data but, most often, nobody reads the terms of usage and just accept it, leading to an unwanted authorization to disclosure of your data.

C.2.4 Respondente #04

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo totalmente

a.3 Concordo totalmente

a.4 Concordo totalmente

With more digitalization personal privacy a big question with smart phones being used by all over the world. Need stronger policy to safeguard personal devices which is lack and companies like Google, Facebook, Twitter missing using personal data and monetizing the data gathered from individual. Need more literacy for the public on digitalization. I am not against digitalization but needs to be more safer approach when doing it.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Concordo totalmente

b.4 Concordo totalmente

In recent time, you hear the news in India. The politician phone calls were hacked using software called pegasus. And many countries raised concern with China mad smart phones tracks personal information and sends it to outside country. Also filter many data when user search internet. Example tibet freedom, etc...

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

May 2021, biggest gasoline pipeline(Colonial Pipeline) in attacked by ransomeware and need to shutdown their system to avoid the spread. Ransomeware is a big threat and every industry try to transform their system to more digitalization, These type of threats percentage is increasing.

d. Vazamento de Informação

d.1 Não concordo

d.2 Concordo totalmente

d.3 Concordo totalmente

d.4 Concordo totalmente

The company who holds personal information are responsible for protecting them. With default settings it should protect the data and only the data owner can grant access to the data to whoever they like. But many companies default settings are collecting data from individual without asking their permission.

e. Roubo e Manipulação de Dados

e.1 Neutro

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Recent times, the cyber attacks are increasing and need stronger protection to avoid the attack. With Crypto currencies on the raise, few news came about crypto currencies exchanges are hacked and people have lost money.

f. Acesso não Autorizado

f.1 Concordo totalmente

f.2 Concordo totalmente

f.3 Neutro

f.4 Concordo totalmente

Knowing the risk and creating necessary preventive steps will avoid such unauthorized access. It doesn't mean that we should stop digitalization which will block the growth of economy and doesn't help the world. Only my ask is to do preventive and think about all possible scenarios. Like anomaly access detection and web app security scanning (static, dynamic, iast) frequently to strengthen security posture of your systems.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

Yes, Phishing is an big threat. Every organization is educating their employees on cyber security threat and phishing. Since worked on application security companies, we see that even with the latest AI based firewall system could not able to block all of phishing emails. Hence it is a risk.

h. Divulgação de Informação

h.1 Concordo totalmente

h.2 Concordo totalmente

h.3 Concordo totalmente

h.4 Concordo

Yes, If i search something in google. Immediately i get to see related adds in my facebook or in my TV. This is bad, because many company using google analytics to promote their product.

C.2.5 RESPONDENTE #05

a. Privacidade

a.1 Concordo

a.2 Concordo totalmente

a.3 Concordo

a.4 Concordo totalmente

We are currently seeing companies taking more interest in data about their customers. Some companies are using more and more sophisticated data gathering techniques.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo

b.3 Neutro

b.4 Concordo totalmente

When it comes to malware, the real trouble comes from those who are able to create their own original content. Identifying and defeating malware seen in other environments is a high priority of security companies of today.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Ransomware is a good example of the issues plaguing companies today. If an environment is infected with ransomeware it is notoriously difficult to resolve. Good IT practices like regular backups can save the day, but companies don't have the resources to implement these good habits. It may cost even more to handle the issue after the infection which digs an even deeper hole.

d. Vazamento de Informação

d.1 Concordo

d.2 Concordo totalmente

d.3 Concordo

d.4 Concordo totalmente

One of the most valuable assets for any company is their data. All company data must be protected at the utmost priority or else confidence in the holding company should rightfully be questioned.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo

e.3 Concordo totalmente

e.4 Concordo

The anonymity of the internet combined with many users ignorance of unsafe internet practices means the internet will unfortunately always have potential victims.

f. Acesso não Autorizado

f.1 Somewhat agree

f.2 Strongly agree

f.3 Strongly agree

f.4 Strongly agree

The resiliency of the cloud is one of the main benefits of using the cloud. The other side of that benefit is that it increases the potential vulnerable areas.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

Phishing is a low effort way for hackers to carry out their techniques. The hackers will cast a wide net and if they get a few bites, then it was a successful attempt.

h. Divulgação de Informação

h.1 Neutro

h.2 Concordo

h.3 Concordo

h.4 Não concordo

Confidently defining who is allowed to access data can go a long way to prevent data disclosure. The challenge is to ensure everyone understands the rules clearly and that the rules are defended strongly.

C.3 CARTA-CONVITE

Risks Evaluation on Implementing Digital Transformation (Pilot Survey)

Dear Invitee:

I am an MSc student at Universidade Nove de Julho's Information Technology and Knowledge Management program, with Prof. Dr. Ivanir Costa as my advisor. I am kindly requesting your participation in the research study that I am conducting entitled: Risk Evaluation on Implementing Digital Transformation. The intention is to assess how the rapid use and implementation of digital technology can get unfavorable effects compared to initial expectations.

As a contextualization, I can say that the increasing impact of digital technology in society, with rapid and disruptive changes, including more efficient and modern processes, press companies to implement Digital Transformation. However, companies have limited choices, and it's difficult to maintain the speed and competition brought on by digitization.

On the other hand, researchers have noticed a path that is not completely visible, even with companies taking advantage of this phenomenon. Therefore, researchers started discussing the adverse effects of this process. In this context, my research aims to evaluate the associated risks of implementing Digital Transformation.

A systematic literature review was carried out, searching for scientific articles in academic databases. As a result, it provided the risk dimensions present when executing this rapid change. Based on that, the expectation is to provide a framework that can highlight the risks involved.

An important step now is to validate those dimensions and risks through a pilot survey.

Based on your strong information technology background and skills, I would like to invite you to answer and validate this pilot survey. Your knowledge will be beneficial in allowing me to make sure there is no misconception in the dimensions and risks I am working on before sending this survey to a broader audience. If you could, please take 10 minutes reviewing 8 (eight) questions with 4 (four) statements each. Additional comments will be welcome to help me identify possible gaps.

As soon as I have accurate results, I will send you the results.

Sincerely,

Eduardo Stefani
Prof. Dr. Ivanir Costa (Advisor)
Information Technology and Knowledge Management
Universidade Nove de Julho
Sao Paulo
Brazil

APÊNDICE D

QUESTIONÁRIO PUBLICADO

D.1 PERFIL DOS RESPONDENTES

Respondente #01

Quadro D.1: *Perfil Respondente #01*

Resposta	2022/01/18 11:19:46 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Suporte
Posição	Consultor
Tempo na Posição	3 anos
País	Brasil

Fonte: autor

Respondente #02

Quadro D.2: *Perfil Respondente #02*

Resposta	2022/01/19 12:07:57 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Serviços de TI
Posição	Consultor de Dados
Tempo na Posição	3 anos
País	Brasil

Fonte: autor

Respondente #03

Quadro D.3: *Perfil Respondente #03*

Resposta	2022/01/19 2:46:13 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Serviços de TI
Posição	Especialista em Desenvolvimento Full Stack
Tempo na Posição	3 meses
País	Estados Unidos

Fonte: autor

Respondente #04

Quadro D.4: *Perfil Respondente #04*

Resposta	2022/01/19 8:55:50 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Serviços de TI
Posição	Consultor Técnico
Tempo na Posição	10 meses
País	Brasil

Fonte: autor

Respondente #05

Quadro D.5: *Perfil Respondente #05*

Resposta	2022/01/19 9:55:32 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Vendas
Posição	Head Customer Success
Tempo na Posição	1 ano
País	Brasil

Fonte: autor

Respondente #06

Quadro D.6: *Perfil Respondente #06*

Resposta	2022/01/19 10:31:26 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Outras
Posição	CEO
Tempo na Posição	12 anos
País	Brasil

Fonte: autor

Respondente #07

Quadro D.7: *Perfil Respondente #07*

Resposta	2022/01/19 10:34:07 AM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Serviços de TI
Posição	Líder de Soluções para Seguros
Tempo na Posição	2 anos
País	Brasil

Fonte: autor

Respondente #08

Quadro D.8: *Perfil Respondente #08*

Resposta	2022/01/19 10:34:07 AM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Desenvolvimento de Produtos
Posição	Consultor
Tempo na Posição	4 anos
País	Brasil

Fonte: autor

Respondente #09

Quadro D.9: *Perfil Respondente #09*

Resposta	2022/01/19 8:23:21 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Serviços de TI
Posição	Delivery
Tempo na Posição	10 anos
País	Brasil

Fonte: autor

Respondente #10

Quadro D.10: *Perfil Respondente #10*

Resposta	2022/01/19 9:00:29 PM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Outras
Posição	Engenheiro de Homologação de Veículos
Tempo na Posição	17 anos
País	Brasil

Fonte: autor

Respondente #11

Quadro D.11: *Perfil Respondente #11*

Resposta	2022/01/19 9:08:03 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Serviços de TI
Posição	Engenheiro de Sistemas
Tempo na Posição	17 anos
País	Brasil

Fonte: autor

Respondente #12

Quadro D.12: *Perfil Respondente #12*

Resposta	2022/01/19 9:54:29 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Pesquisa e Desenvolvimento
Posição	Pesquisador
Tempo na Posição	5 meses
País	Brasil

Fonte: autor

Respondente #13

Quadro D.13: *Perfil Respondente #13*

Resposta	2022/01/19 10:50:43 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Suporte
Posição	Engenheiro de Suporte
Tempo na Posição	24 anos
País	Estados Unidos

Fonte: autor

Respondente #14

Quadro D.14: *Perfil Respondente #14*

Resposta	2022/01/20 12:45:07 AM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Outras
Posição	Gerente
Tempo na Posição	6 anos
País	Brasil

Fonte: autor

Respondente #15

Quadro D.15: *Perfil Respondente #15*

Resposta	2022/01/20 7:10:25 AM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Serviços de TI
Posição	Consultor Sênior
Tempo na Posição	3 anos
País	Brasil

Fonte: autor

Respondente #16

Quadro D.16: *Perfil Respondente #16*

Resposta	2022/01/20 8:46:47 AM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Pré-Vendas
Posição	Arquiteto
Tempo na Posição	24 anos
País	Brasil

Fonte: autor

Respondente #17

Quadro D.17: *Perfil Respondente #17*

Resposta	2022/01/20 8:55:06 AM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Pesquisa e Desenvolvimento
Posição	Administrador de Banco de Dados
Tempo na Posição	9 anos
País	Argentina

Fonte: autor

Respondente #18

Quadro D.18: *Perfil Respondente #18*

Resposta	2022/01/20 9:34:00 AM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Pré-Vendas
Posição	Engenheiro Sênior LATAM
Tempo na Posição	2 anos
País	Brasil

Fonte: autor

Respondente #19

Quadro D.19: *Perfil Respondente #19*

Resposta	2022/01/20 10:59:31 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Serviços de TI
Posição	Head of IT, Architecture and Infrastructure
Tempo na Posição	2 anos
País	Brasil

Fonte: autor

Respondente #20

Quadro D.20: *Perfil Respondente #20*

Resposta	2022/01/20 11:02:38 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Serviços de TI
Posição	VP IT SW Engineering
Tempo na Posição	28 anos
País	Brasil

Fonte: autor

Respondente #21

Quadro D.21: *Perfil Respondente #21*

Resposta	2022/01/20 11:53:47 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Serviços de TI
Posição	Gerente de Projetos
Tempo na Posição	5 anos
País	Brasil

Fonte: autor

Respondente #22

Quadro D.22: *Perfil Respondente #22*

Resposta	2022/01/20 12:50:00 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Suporte
Posição	Gerente
Tempo na Posição	19 anos
País	Brasil

Fonte: autor

Respondente #23

Quadro D.23: *Perfil Respondente #23*

Resposta	2022/01/20 2:32:09 PM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Engenharia
Posição	Gerente de Infraestrutura
Tempo na Posição	5 anos
País	Brasil

Fonte: autor

Respondente #24

Quadro D.24: *Perfil Respondente #24*

Resposta	2022/01/20 11:11:10 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Suporte
Posição	Engenheiro de Suporte
Tempo na Posição	13 anos
País	Estados Unidos

Fonte: autor

Respondente #25

Quadro D.25: *Perfil Respondente #25*

Resposta	2022/01/20 11:51:18 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Suporte
Posição	Engenheiro de Suporte
Tempo na Posição	22 anos
País	Estados Unidos

Fonte: autor

Respondente #26

Quadro D.26: *Perfil Respondente #26*

Resposta	2022/01/20 11:57:57 PM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Engenharia
Posição	Gerente de Arquitetura
Tempo na Posição	11 anos
País	Argentina

Fonte: autor

Respondente #27

Quadro D.27: *Perfil Respondente #27*

Resposta	2022/01/21 9:57:23 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Vendas
Posição	Diretor
Tempo na Posição	3 anos
País	Brasil

Fonte: autor

Respondente #28

Quadro D.28: *Perfil Respondente #28*

Resposta	2022/01/21 11:02:09 AM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Suporte
Posição	Engenheiro de Suporte
Tempo na Posição	10 anos
País	Índia

Fonte: autor

Respondente #29

Quadro D.29: *Perfil Respondente #29*

Resposta	2022/01/21 3:27:31 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Serviços de TI
Posição	Superintendente
Tempo na Posição	3 meses
País	Brasil

Fonte: autor

Respondente #30

Quadro D.30: *Perfil Respondente #30*

Resposta	2022/01/21 11:24:02 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Suporte
Posição	Analista de Sistemas
Tempo na Posição	3 anos
País	Brasil

Fonte: autor

Respondente #31

Quadro D.31: *Perfil Respondente #31*

Resposta	2022/01/22 11:42:39 AM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Vendas
Posição	Supervisor
Tempo na Posição	11 anos
País	Brasil

Fonte: autor

Respondente #32

Quadro D.32: *Perfil Respondente #32*

Resposta	2022/01/23 5:10:17 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Serviços de TI
Posição	Engenheiro de Suporte
Tempo na Posição	2 anos
País	República Theca

Fonte: autor

Respondente #33

Quadro D.33: *Perfil Respondente #33*

Resposta	2022/01/23 7:42:20 PM GMT-3
Quantidade Funcionários	Mais de 1000
Área	Serviços de TI
Posição	Gerente de Projetos
Tempo na Posição	1 ano
País	Suiça

Fonte: autor

Respondente #34

Quadro D.34: *Perfil Respondente #34*

Resposta	2022/01/24 7:20:53 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Outras
Posição	CEO
Tempo na Posição	2 anos
País	Brasil

Fonte: autor

Respondente #35

Quadro D.35: *Perfil Respondente #35*

Resposta	2022/01/24 7:20:53 AM GMT-3
Quantidade Funcionários	Menos de 1000
Área	Desenvolvimento de Produtos
Posição	Consultor Sênior
Tempo na Posição	2 anos e meio
País	Portugal

Fonte: autor

D.2 Resposta dos Respondentes

D.2.1 Respondente #01

a. Privacidade

a.1 Concordo

a.2 Concordo

a.3 Concordo totalmente

a.4 Concordo totalmente

Sem comentários.

b. ***Malware***

b.1 Concordo

b.2 Concordo totalmente

b.3 Neutro

b.4 Concordo totalmente

Sem comentários.

c. ***Ransomware***

c.1 Concordo totalmente

c.2 Concordo

c.3 Concordo

c.4 Concordo totalmente

Sem comentários.

d. Vazamento de Informação

d.1 Discordo totalmente

d.2 Concordo

d.3 Neutro

d.4 Concordo totalmente

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo

e.2 Concordo

e.3 Concordo totalmente

e.4 Concordo totalmente

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo

f.3 Não concordo

f.4 Concordo totalmente

Sem comentários.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo

Sem comentários

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo totalmente

h.3 Concordo totalmente

h.4 Neutro

Sem comentários.

D.2.2 RESPONDENTE #02

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo totalmente

a.3 Concordo totalmente

a.4 Discordo totalmente

As leis de proteção não impactam a adoção de novas tecnologias e sim exigem um correto tratamento dos dados pessoais e sua forma de utilização.

b. ***Malware***

b.1 Concordo totalmente

b.2 Concordo

b.3 Concordo totalmente

b.4 Concordo

Dependendo do tipo de malware e os cuidados tomados pelas empresas com a segurança da informação, uma catástrofe pode ocorrer.

c. ***Ransomware***

c.1 Concordo

c.2 Concordo totalmente

c.3 Concordo

c.4 Discordo totalmente

Empresas que não se preocupam com ransomware podem ter sérios problemas.

d. Vazamento de Informação

d.1 Neutro

d.2 Concordo

d.3 Concordo

d.4 Discordo totalmente

As novas leis de proteção de dados criaram uma exigência legal de adequação das empresas em relação a proteção dos dados dos consumidores.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Infelizmente não conseguimos ter 100% de segurança para evitar os ataques criminosos e estamos sujeitos e este tipo de cenário.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Discordo

f.4 Concordo totalmente

Existe a necessidade do mundo dos negócios em processamento distribuido das informações, não temos como fugir deste cenário.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo

g.3 Concordo

g.4 Concordo totalmente

Técnica amplamente utilizada pelos *hackers*.

h. Divulgação de Informação

h.1 Discordo totalmente

h.2 Concordo totalmente

h.3 Discordo totalmente

h.4 Concordo totalmente

Quanto mais propagamos a informação maior o risco de exposição.

D.2.3 RESPONDENTE #03

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo totalmente

a.3 Concordo totalmente

a.4 Concordo totalmente

Beyond the social, anthropological, commercial, legal, security, and moral concerns, data privacy also impacts behavioral and cognitive aspects. We could consider the recent issues related to Cambridge Analytics and Facebook as some kind of "Cognitive War", for example.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Concordo

b.4 Concordo totalmente

Malware per se is a form of armament, by definition.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

I could say that perfect security doesn't exist. What is possible to achieve is at most the feeling of security.

d. Vazamento de Informação

d.1 Concordo

d.2 Concordo totalmente

d.3 Concordo totalmente

d.4 Concordo totalmente

The digital data only will be inviolable if stored on well kept, disconnected, turned-off devices.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Data Theft/Manipulation occur more often if the data has notorious value. I could say worthless data can be lost without harming. The point is what could be very worthless data. Actually any kind of data has some value. Maybe the value is so small that it does not worth the theft.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Neutro

f.4 Concordo totalmente

Unauthorized access and fraud are very old crimes. Actually digital authorization and authentication present more resources than analogical methods. The very issue resides on the human aspect of these crimes.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

Again, the human aspect is the very issue. But phishing can bring, spread and use all the other criminal cyber-tools, harming dramatically our society.

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo totalmente

h.3 Concordo totalmente

h.4 Concordo totalmente

We have to understand that an agreement always relates to people beyond those who signed it. It is not because an agreement is good for some that it will be good for all. Disclosing information to confidential subjects does not assure information is in good hands. Things are not always what they seem.

D.2.4 RESPONDENTE #04

a. Privacidade

a.1 Concordo

a.2 Concordo

a.3 Neutro

a.4 Neutro

I believe that people can always adapt. A few years ago, providing personal data wasn't very important to most people.

b. *Malware*

b.1 Concordo

b.2 Concordo totalmente

b.3 Concordo

b.4 Concordo totalmente

By the last examples we have, such as attacks on websites known stores, or attacks on the government, it indicates that we aren't prepared, in case there is a global attack, knowing that almost everything is connected today, there will be a big breakdown.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

This type of "kidnapping", combined with ways to have power/money with crypto, will increase the malicious people options.

d. Vazamento de Informação

d.1 Discordo

d.2 Concordo totalmente

d.3 Neutro

d.4 Concordo totalmente

Your data reflects your consumption and your profile. If your data is not safe, basically whoever gets that data will try to profit somehow.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

I believe that the data of a citizen in itself, which doesn't have some power, may not have an impact, however, obtaining data from a group, it can affect important decisions or direct some decision that impacts in the future.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Neutro

f.4 Concordo

I believe that digitizing data is a path of no return, and so is sharing. There will be many challenges to this protection.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

As a way of trying to obtain personal data, mass phishing is one of the easiest ways to obtain this data.

h. Divulgação de Informação

h.1 Concordo totalmente

h.2 Neutro

h.3 Concordo

h.4 Concordo totalmente

Your data with unauthorized organizations, indicates misuse and malicious purposes.

D.2.5 RESPONDENTE #05

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo

a.3 Concordo totalmente

a.4 Discordo totalmente

Solutions like One Trust can help with all privacy concerns.

b. *Malware*

b.1 Concordo totalmente

b.2 Neutro

b.3 Discordo totalmente

b.4 Concordo

Malware always existed and always will all exist at technology world.

c. *Ransomware*

c.1 Neutro

c.2 Concordo

c.3 Concordo totalmente

c.4 Concordo totalmente

Sem comentários.

d. Vazamento de Informação

d.1 Discordo totalmente

d.2 Concordo

d.3 Neutro

d.4 Concordo totalmente

Solutions like Snowflake can help with transfer local data to the cloud, avoid Information Leakage.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo

e.3 Concordo

e.4 Neutro

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Discordo totalmente

f.3 Discordo totalmente

f.4 Concordo

Sem comentários.

g. *Phishing*

g.1 Concordo

g.2 Neutro

g.3 Concordo

g.4 Neutro

Sem comentários

h. Divulgação de Informação

h.1 Neutro

h.2 Concordo totalmente

h.3 Concordo totalmente

h.4 Concordo totalmente

Sem comentários.

D.2.6 RESPONDENTE #06

a. Privacidade

a.1 Neutro

a.2 Concordo

a.3 Discordo

a.4 Discordo

A maior parte das pessoas nem sabe para o que seus dados servem. São alheias à isso. Quem está preocupado tem um megafone potente e acaba chamando uma atenção desproporcionalmente maior dando a entender que está "todo mundo preocupado", quando na verdade existem apenas alguns preocupados. Da minha parte, enquanto meus dados forem usamos apenas para fins de marketing e oferecer produtos alinhados com meus desejos, me sinto ótimo com isso, inclusive me poupa tempo de pesquisa na internet.

b. *Malware*

b.1 Discordo totalmente

b.2 Concordo

b.3 Neutro

b.4 Concordo

Sem comentários.

c. *Ransomware*

c.1 Concordo

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo

Sem comentários.

d. Vazamento de Informação

d.1 Neutro

d.2 Concordo

d.3 Neutro

d.4 Concordo totalmente

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo

e.4 Concordo

Sem comentários.

f. Acesso não Autorizado

f.1 Neutro

f.2 Concordo totalmente

f.3 Neutro

f.4 Concordo totalmente

Sem comentários.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo

g.3 Neutro

g.4 Concordo totalmente

Sem comentários

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo

h.3 Neutro

h.4 Concordo

Sem comentários.

D.2.7 RESPONDENTE #07

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo totalmente

a.3 Concordo totalmente

a.4 Concordo

A Privacidade de dados é um tema cada vez mais presente nas discussões corporativas e relevante do ponto de vista de definição de Políticas e Normas de condução.

b. *Malware*

b.1 Concordo totalmente

b.2 Discordo

b.3 Concordo

b.4 Concordo

Não vejo que a existência de *malware* esteja impactando a (r)evolução tecnológica, mas sim concordo que é atualmente visto como uma ameaça crítica para as empresas. Acho, contudo, que já há, de maneira geral, uma percepção de riscos muito bem apurada por parte das empresas.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Exemplo prático foram os recentes ataques ao Ministério da Saúde e ao Laboratório Fleury, que impactaram serviços diretos à população.

d. Vazamento de Informação

d.1 Discordo

d.2 Concordo totalmente

d.3 Concordo

d.4 Concordo

Acho que o uso pontual e indevido da personalização, não impacta fortemente a confiança na evolução tecnológica, mas arranha.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo totalmente

f.2 Concordo

f.3 Neutro

f.4 Concordo totalmente

Sem comentários.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Neutro

Sem comentários

h. Divulgação de Informação

h.1 Concordo totalmente

h.2 Concordo

h.3 Discordo

h.4 Discordo totalmente

A abertura de informação não é algo ruim, desde que respeite as regras da LGPD.

D.2.8 Respondente #08

a. Privacidade

a.1 Concordo

a.2 Concordo totalmente

a.3 Concordo totalmente

a.4 Concordo totalmente

Data privacy is undoubtedly an extremely important issue. Despite not being in the internal context of an organization, I see how people are afraid to embark on new technologies like PIX and join fintechs. This thought is in line with the fear of having your data leaked or misused. This is no different within organizations.

b. *Malware*

b.1 Concordo

b.2 Concordo totalmente

b.3 Concordo

b.4 Concordo totalmente

It is not in vain that one of the most important sectors for an organization today is the information security sector. There is a very high risk of attack and a successful attack can cause immeasurable damage to the company.

c. *Ransomware*

c.1 Concordo

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

I agree one hundred percent. This type of attack can not only cause financial loss, but also discredit the company in the market among others.

d. Vazamento de Informação

d.1 Neutro

d.2 Concordo totalmente

d.3 Concordo totalmente

d.4 Concordo totalmente

I myself am very afraid of how my data is being used. For example, I feel completely uncomfortable when I say something and then when I go into a software and have an advertisement about what I said.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

I believe that both businesses as well as citizens are far from being with their data safely.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Concordo

f.4 Concordo totalmente

That's a very delicate issue. Further progress is needed on data security to ensure that no serious problems happen.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo

g.3 Concordo

g.4 Neutro

Sem comentários

h. Divulgação de Informação

h.1 Discordo totalmente

h.2 Discordo totalmente

h.3 Neutro

h.4 Concordo totalmente

As I wrote earlier, I feel completely violated when I get offers of something I searched for in a search engine or that I simply talked about in a conversation outside of a device. I never authorized this to be done.

D.2.9 RESPONDENTE #09

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo totalmente

a.3 Concordo totalmente

a.4 Concordo

Sem comentários.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo

b.3 Concordo

b.4 Concordo

Sem comentários.

c. *Ransomware*

c.1 Concordo

c.2 Neutro

c.3 Concordo totalmente

c.4 Concordo totalmente

Sem comentários.

d. Vazamento de Informação

d.1 Discordo

d.2 Concordo

d.3 Concordo totalmente

d.4 Concordo

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo

e.2 Concordo

e.3 Concordo

e.4 Concordo

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Neutro

f.3 Concordo totalmente

f.4 Neutro

Sem comentários.

g. *Phishing*

g.1 Concordo

g.2 Concordo

g.3 Concordo totalmente

g.4 Concordo totalmente

Sem comentários

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo totalmente

h.3 Concordo

h.4 Concordo

Sem comentários.

D.2.10 RESPONDENTE #10

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo

a.3 Concordo totalmente

a.4 Concordo

Ainda temos muitos pontos em aberto em termos de regulamentação, contudo as grandes empresas ou as multinacionais tem uma política bem rigorosa e usam a tecnologia para bloquear a transferência de dados da empresa para uma pasta pessoal na internet, drive externo etc.

b. *Malware*

b.1 Discordo totalmente

b.2 Discordo

b.3 Discordo totalmente

b.4 Discordo totalmente

Cada vez mais os hackers tem tentado sequestrar as empresas, invadindo o sistema e pedindo um resgate para não danificar o sistema.

c. *Ransomware*

c.1 Concordo

c.2 Concordo

c.3 Concordo totalmente

c.4 Concordo totalmente

Sem comentários.

d. Vazamento de Informação

d.1 Discordo

d.2 Concordo

d.3 Concordo

d.4 Concordo

No começo eu não confiava em ter dados na nuvem, contudo hoje a tecnologia está tão avançado que é mais barato e seguro ter os dados na nuvem do que em um drive físico em casa.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo

e.3 Concordo

e.4 Concordo

Não necessariamente precisa de roubar os dados, hoje temos muitos dados pessoais na internet que possibilita os pessoas sofrerem golpes.

f. Acesso não Autorizado

f.1 Concordo

f.2 Discordo

f.3 Discordo

f.4 Concordo

Os aplicativos de bancos para smartphones melhoram muito, contudo em São Paulo teve uma onde de assaltados, no qual robavam o Smartphone desbloqueado e em poucos minutos eram roubados grande quantidade de dinheiro da conta.

g. *Phishing*

g.1 Concordo

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

Phishing é feito através de emails, SMS, ou mesmo por outros aplicativos de mensagens. Ou mesmo criando perfil falso para aplicar golpes.

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo

h.3 Concordo

h.4 Discordo

Sem comentários.

D.2.11 RESPONDENTE #11

a. Privacidade

a.1 Concordo

a.2 Neutro

a.3 Concordo totalmente

a.4 DIscordo totalmente

Nem sempre novas tecnologias impactam a segurança dos dados. Muitas vezes ela pode agregar mais segurança na proteção dos mesmos.

b. *Malware*

b.1 Neutro

b.2 Neutro

b.3 Concordo

b.4 Neutro

A existência de riscos também faz com que as empresas busquem melhores soluções de segurança. Sem riscos existentes menor investimento nesse impetrante tópico.

c. *Ransomware*

c.1 Concordo

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Esse é mais um tipo de ataque que qualquer empresa pode sofrer. E se concretizando sim causa perdas financeiras e pior ainda de imagem.

d. Vazamento de Informação

d.1 Neutro

d.2 Concordo

d.3 Concordo

d.4 Concordo totalmente

Toda empresa visa o lucro. Perdeu a confiabilidade do cliente dificilmente a empresa conseguiria refazer a imagem de que é segura.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo

e.3 Concordo totalmente

e.4 Concordo totalmente

Todos estamos vulneráveis e cabe a todos principalmente empresas e governos aplicarem boas políticas de segurança afim de proteger sempre as pessoas físicas, além delas mesmas também tomarem medidas de proteção.

f. Acesso não Autorizado

f.1 Concordo totalmente

f.2 Concordo totalmente

f.3 Neutro

f.4 Discordo totalmente

Digitalização financeira se refere em deixar a vida do cliente mais fácil e mais barata. Não deveria implicar em deixá-la menos segura.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo

g.3 Concordo totalmente

g.4 Neutro

Phising também causa grandes prejuízos dado que o elo fraco é o usuário que muitas vezes se deixa conduzir à conclusão desse golpe.

h. Divulgação de Informação

h.1 Discordo

h.2 Neutro

h.3 Discordo totalmente

h.4 Concordo

Menos é mais. Quanto menos expor melhor será a garantia de segurança.

D.2.12 RESPONDENTE #12

a. Privacidade

a.1 Concordo

a.2 Neutro

a.3 Concordo totalmente

a.4 Concordo

Sem comentários.

b. *Malware*

b.1 Concordo

b.2 Concordo

b.3 Concordo

b.4 Neutro

Sem comentários.

c. *Ransomware*

c.1 Concordo

c.2 Concordo

c.3 Neutro

c.4 Concordo

Sem comentários.

d. Vazamento de Informação

d.1 Discordo

d.2 Neutro

d.3 Neutro

d.4 Concordo

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo

e.2 Concordo

e.3 Concordo

e.4 Concordo

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo

f.3 Neutro

f.4 Concordo

Sem comentários.

g. *Phishing*

g.1 Concordo

g.2 Neutro

g.3 Neutro

g.4 Neutro

Sem comentários

h. Divulgação de Informação

h.1 Discordo

h.2 Concordo

h.3 Neutro

h.4 Neutro

Sem comentários.

D.2.13 RESPONDENTE #13

a. Privacidade

a.1 Concordo

a.2 Concordo

a.3 Concordo

a.4 Concordo

Sem comentários.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Concordo totalmente

b.4 Concordo totalmente

It happens every day.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

This thing is getting worse.

d. Vazamento de Informação

d.1 Concordo

d.2 Concordo

d.3 Concordo

d.4 Concordo totalmente

Data is everything.

e. Roubo e Manipulação de Dados

e.1 Concordo

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo

Data security must be taken seriously.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo

f.3 Concordo totalmente

f.4 Concordo

This issue is important.

g. *Phishing*

g.1 Discordo totalmente

g.2 Discordo

g.3 DIscordo totalmente

g.4 Concordo totalmente

Sem comentários

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo

h.3 Concordo

h.4 Concordo

Somehow your data is always out there.

D.2.14 RESPONDENTE #14

a. Privacidade

a.1 Concordo

a.2 Concordo

a.3 Concordo

a.4 Concordo totalmente

Apesar da regulamentação ter avançado bastante com relação a privacidade e utilização de dados, a transformação digital e a implementação de ferramentas está evoluindo em um ritmo superior, criando gaps e riscos não considerados, expondo todos seus usuários.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Concordo totalmente

b.4 Concordo totalmente

Independente da evolução das medidas de defesa, os ataques digitais (rasonware, malware, etc) estão evoluindo de forma significativa, sendo a principal porta de entrada, o próprio usuário que é ludibriado pela engenharia por trás do golpe.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

O maior perigo é a engenharia criada por trás do golpe, onde a principal porta de entrada acaba sendo o operador/usuário, que acaba sendo ludibriado pela engenharia/arquitetura desenhada por trás do objetivo.

d. Vazamento de Informação

d.1 Discordo

d.2 Concordo

d.3 Concordo totalmente

d.4 Concordo totalmente

Muitas empresas privadas se preocupam, entretanto o setor estatal está muito defasado e aquém do esperado.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo

e.3 Concordo totalmente

e.4 Concordo

No geral, sempre existe a expectativa de ganho econômico ou de status por trás dos ataques, sendo que o sequestro de dados eh mais comum que a destruição ou incapacitação em si.

f. Acesso não Autorizado

f.1 Discordo

f.2 Concordo totalmente

f.3 Concordo totalmente

f.4 Concordo

Existem ferramentas para não permitir o acesso não autorizado, entretanto, ele eh muito deficitário em todas os segmentos e linhas de negocios.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

Utilizando o interesse/curiosidade do usuário, acabam sendo extremamente eficazes. As vias, no geral, não estão preparadas para enfrentar esse tipo de problema.

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo totalmente

h.3 Discordo

h.4 Discordo

Tudo depende do nicho de mercado que a indústria está inserida.

D.2.15 RESPONDENTE #15

a. Privacidade

a.1 Concordo

a.2 Concordo totalmente

a.3 Concordo

a.4 Concordo totalmente

Sem comentários.

b. *Malware*

b.1 Concordo

b.2 Discordo

b.3 Neutro

b.4 Discordo

In general, systems are getting more and more decentralised, with less risks of a "global" threat.

c. *Ransomware*

c.1 Concordo

c.2 Neutro

c.3 Concordo totalmente

c.4 Concordo

Sem comentários.

d. Vazamento de Informação

d.1 Neutro

d.2 Concordo

d.3 Discordo

d.4 Concordo totalmente

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo

e.2 Concordo totalmente

e.3 Concordo

e.4 Concordo totalmente

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo

f.3 Concordo

f.4 Concordo totalmente

Sem comentários.

g. *Phishing*

g.1 Discordo

g.2 Discordo

g.3 Discordo

g.4 Neutro

Sem comentários

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo totalmente

h.3 Discordo totalmente

h.4 Discordo

Sem comentários.

D.2.16 RESPONDENTE #16

a. Privacidade

a.1 Concordo

a.2 Discordo totalmente

a.3 Concordo totalmente

a.4 Discordo

Não há como desassociar o tema da privacidade no processo de transformação digital. Não acredito que os cuidados com a privacidade seja um impeditivo para utilização de algumas tecnologias, mas sem dúvida demandará maiores esforços de desenvolvimentos e implementação.

b. *Malware*

b.1 Concordo

b.2 Neutro

b.3 Discordo

b.4 Discordo

Cyber Security é imprescindível nos dias atuais. Assim como os tipos de ataques evoluem a cada dia, as ferramentas de segurança também. Na minha opinião o elo mais fraco da segurança continua sendo as pessoas, por esse motivo o foco em treinamentos e processos nas empresas é fundamental.

c. *Ransomware*

c.1 Concordo

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Tem sido muito comum esse tipo de ataque em vários setores. A iniciativa privada já adota várias ferramentas e processos para se proteger, mas me preocupa muito a defasagem de investimentos e cuidados no setor público.

d. Vazamento de Informação

d.1 Discordo

d.2 Concordo

d.3 Concordo

d.4 Concordo totalmente

O fato de usar cloud não aumenta na minha opinião o risco de vazamento de dados. Os cuidados com os dados devem ser os mesmos quando hospedados on premises.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo

e.3 Concordo

e.4 Concordo

Os dados das empresas e dos usuários em geral já é um dos recursos mais valiosos e cobiçados na sociedade.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Discordo

f.4 Concordo

O setor bancário e financeiro já foi digitalizado a muito tempo. O que tem indicado agora no setor é o uso de infraestrutura em cloud, mas o controle nessas empresas e setores já é muito desenvolvido e eficientes.

g. *Phishing*

g.1 Concordo

g.2 Concordo

g.3 Concordo totalmente

g.4 Concordo

Phishing é um dos melhores exemplos da vulnerabilidade de caráter social, explorando usuários de todos os níveis de instrução.

h. Divulgação de Informação

h.1 Discordo

h.2 Concordo

h.3 Discordo

h.4 Concordo

As informações de preferências e comportamento de consumo na minha opinião é o que é mais explorado pelas empresas e setores, e sem o devido consentimento e ciência dos consumidores.

D.2.17 RESPONDENTE #17

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo totalmente

a.3 Concordo totalmente

a.4 Concordo totalmente

The disable of cookies is now a practice more and more usual.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo

b.3 Concordo

b.4 Concordo totalmente

In my work we run GNU/Linux, the malaware is null, perhaps I dont have a clear idea about this issue.

c. *Ransomware*

c.1 Neutro

c.2 Neutro

c.3 Concordo

c.4 Concordo

In my work we using GNU/Linux and perhaps the major problems are the rootkits.

d. Vazamento de Informação

d.1 Concordo totalmente

d.2 Concordo totalmente

d.3 Concordo totalmente

d.4 Concordo totalmente

The cloud is only one computer in another place with my data.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Nowdays is one the biggest problems in cybersecurity.

f. Acesso não Autorizado

f.1 Concordo totalmente

f.2 Concordo totalmente

f.3 Concordo totalmente

f.4 Concordo totalmente

If our data is in a server out of our control, they are in risk.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

In my experience is the most used attack.

h. Divulgação de Informação

h.1 Concordo totalmente

h.2 Concordo

h.3 Concordo

h.4 Concordo

The AWS services and similar are used more and more.

D.2.18 RESPONDENTE #18

a. Privacidade

a.1 Concordo totalmente

a.2 Discordo totalmente

a.3 Discordo totalmente

a.4 Discordo totalmente

In the field of Pre Sales I'm noticing larger companies taking GPDR more seriously.

b. *Malware*

b.1 Concordo

b.2 Neutro

b.3 Discordo

b.4 Discordo

Sem comentários.

c. *Ransomware*

c.1 Discordo

c.2 Discordo

c.3 Concordo

c.4 Concordo

Sem comentários.

d. Vazamento de Informação

d.1 Discordo

d.2 Concordo

d.3 Discordo

d.4 Concordo totalmente

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo

e.3 Concordo totalmente

e.4 Concordo totalmente

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Discordo totalmente

f.4 Concordo

Sem comentários.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Neutro

g.4 Neutro

Sem comentários

h. Divulgação de Informação

h.1 Concordo totalmente

h.2 Concordo totalmente

h.3 Neutro

h.4 Discordo

Sem comentários.

D.2.19 RESPONDENTE #19

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo

a.3 Concordo totalmente

a.4 Concordo

Em certa medida, a adoção é inevitável em diversos casos onde o movimento é massivo na sociedade.

b. ***Malware***

b.1 Concordo totalmente

b.2 Concordo

b.3 Concordo totalmente

b.4 Neutro

O entendo que catástrofe é algo exagerado, pois o investimento de atores atacantes e defensores tem sido mantido em relativo equilíbrio, mas o crescimento do risco é evidente.

c. ***Ransomware***

c.1 Concordo

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Sem comentários.

d. Vazamento de Informação

d.1 Concordo

d.2 Concordo

d.3 Concordo

d.4 Concordo totalmente

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo

f.3 Concordo totalmente

f.4 Concordo

Sem comentários.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo

g.4 Concordo totalmente

Sem comentários

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo totalmente

h.3 Concordo totalmente

h.4 Concordo

Sem comentários.

D.2.20 RESPONDENTE #20

a. Privacidade

a.1 Concordo totalmente

a.2 Neutro

a.3 Concordo

a.4 Concordo

Sem comentários.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Concordo

b.4 Concordo

Sem comentários.

c. *Ransomware*

c.1 Concordo

c.2 Concordo

c.3 Concordo

c.4 Concordo

Sem comentários.

d. Vazamento de Informação

d.1 Concordo

d.2 Concordo totalmente

d.3 Concordo

d.4 Concordo

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo

e.2 Concordo

e.3 Concordo

e.4 Concordo

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Concordo totalmente

f.4 Concordo

Sem comentários.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

Sem comentários

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo

h.3 Concordo

h.4 Concordo

Sem comentários.

D.2.21 RESPONDENTE #21

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo totalmente

a.3 Concordo totalmente

a.4 Concordo

Processos também devem ser definidos e implementados para suportar a segurança de informações internas e dados de clientes.

b. ***Malware***

b.1 Concordo totalmente

b.2 Concordo

b.3 Concordo

b.4 Concordo totalmente

O risco de afetar um CPD pode comprometer a estrutura de toda empresa.

c. ***Ransomware***

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Podem afetar diretamente a situação e a posição da empresa no mercado.

d. Vazamento de Informação

d.1 Concordo

d.2 Concordo totalmente

d.3 Concordo totalmente

d.4 Concordo totalmente

Processos bem definidos, tecnologia e equipe dedicada de segurança podem conduzir e minimizar os riscos de segurança da empresa.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

O problema de roubo de informações pode inclusive estar dentro da empresa.

f. Acesso não Autorizado

f.1 Concordo totalmente

f.2 Concordo totalmente

f.3 Concordo

f.4 Concordo totalmente

A exposição de dados para pessoas indevidas pode levar a prejuízos financeiros graves.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

Prática muito comum nos dias atuais.

h. Divulgação de Informação

h.1 Concordo totalmente

h.2 Concordo

h.3 Concordo totalmente

h.4 Concordo

O risco já existe apenas por trabalharmos com informações.

D.2.22 Respondente #22

a. Privacidade

a.1 Discordo

a.2 Concordo

a.3 Concordo totalmente

a.4 Concordo

Sem comentários.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Concordo totalmente

b.4 Concordo

Sem comentários.

c. *Ransomware*

c.1 Concordo

c.2 Concordo

c.3 Concordo

c.4 Concordo totalmente

Sem comentários.

d. Vazamento de Informação

d.1 Concordo

d.2 Concordo totalmente

d.3 Concordo totalmente

d.4 Concordo totalmente

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Concordo totalmente

f.4 Concordo totalmente

Sem comentários.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo

g.3 Concordo totalmente

g.4 Concordo totalmente

Sem comentários

h. Divulgação de Informação

h.1 Discordo

h.2 Concordo

h.3 Concordo

h.4 Concordo

Sem comentários.

D.2.23 RESPONDENTE #23

a. Privacidade

a.1 Concordo totalmente

a.2 Discordo totalmente

a.3 Concordo totalmente

a.4 Discordo totalmente

Data privacy is part of every technology process.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Discordo totalmente

b.4 Neutro

The problem is not just malware, but all malicious traffic on the Internet.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Neutro

Ransomware attacks, in addition to financial damage, can have other consequences, including on society.

d. Vazamento de Informação

d.1 Concordo

d.2 Neutro

d.3 Concordo totalmente

d.4 Concordo totalmente

Data protection and investment in information security are the main concerns of technology.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Security issues, especially the use of equipment connected to the internet, are unfortunately not treated as priorities.

f. Acesso não Autorizado

f.1 Concordo totalmente

f.2 Concordo totalmente

f.3 Discordo totalmente

f.4 Discordo totalmente

Data can be shared by multiple servers and not by multiple users.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Neutro

g.4 Concordo totalmente

Prishing helps in electronic fraud, criminals use seemingly real messages.

h. Divulgação de Informação

h.1 Discordo

h.2 Concordo totalmente

h.3 Concordo

h.4 Concordo totalmente

The disclosure of user information are practices adopted in digital marketing.

D.2.24 RESPONDENTE #24

a. Privacidade

a.1 Concordo totalmente

a.2 Neutro

a.3 Concordo

a.4 Concordo

Sem comentários.

b. *Malware*

b.1 Concordo totalmente

b.2 Neutro

b.3 Discordo

b.4 Concordo totalmente

Sem comentários.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Sem comentários.

d. Vazamento de Informação

d.1 Discordo

d.2 Concordo totalmente

d.3 Neutro

d.4 Discordo

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo totalmente

f.2 Concordo totalmente

f.3 Concordo

f.4 Concordo totalmente

Sem comentários.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

Sem comentários

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo

h.3 Concordo

h.4 Concordo

Sem comentários.

D.2.25 RESPONDENTE #25

a. Privacidade

a.1 Concordo

a.2 Concordo totalmente

a.3 Concordo totalmente

a.4 Discordo

I wish I could agree that privacy concerns impact adoption. In practice I believe we see blind immediate adoption of new technologies with little thought of privacy concerns. It isn't until full adoption do we see privacy concerns. Facebook for example.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo

b.3 Discordo

b.4 Discordo

So far security products have kept pace to defeat potential Malware attacks.

c. *Ransomware*

c.1 Discordo

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Ransomware is certainly a threat. In practice we have seen these types of attacks that highlight weak environmental security.

d. Vazamento de Informação

d.1 Discordo

d.2 Concordo totalmente

d.3 Concordo

d.4 Discordo

Personal data is held by numerous governments and companies. Even though organizations should protect consumer data, confidence loss is no longer focused. Many have lost confidence but who have we lost confidence in? We no longer know who lost or sold our personal data.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Yes. Malicious attacks happen daily.

f. Acesso não Autorizado

f.1 Concordo

f.2 Discordo

f.3 Discordo

f.4 Concordo totalmente

Security concerns and issues are mitigated by having proper access management software and administration in place.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo

g.3 Discordo

g.4 Concordo totalmente

Phishing is a concern but people have become more aware of phishing tactics. Proper training and internal random testing of employees help.

h. Divulgação de Informação

h.1 Discordo totalmente

h.2 Concordo

h.3 Discordo

h.4 Neutro

I do like online retailers suggesting products. It is rarely help and shows how easily personal data and cookies are used to suggest products.

D.2.26 RESPONDENTE #26

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo

a.3 Concordo totalmente

a.4 Concordo totalmente

I do believe that as anything of used correctly it will be something amazing for human kind, but I do fear for the incorrect use. I do feel that good intentions are not enough, a moral an ethical path must be followed with extreme caution.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Neutro

b.4 Neutro

In the name of making life easier for users we are getting them more ignorant on how everything works hence more vulnerable to being attacked.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo

Ransom ware is a known threat that is being exploited more commonly thanks to new means of money exchange anonymously as crypto currency. It poses a big threat but if correct measures are taken by governments then public services should not be compromised to the point of not being able to provide it.

d. Vazamento de Informação

d.1 Neutro

d.2 Neutro

d.3 Concordo

d.4 Concordo

I think the amount of data we are gathering from people is disgusting. The abuse of AI to predict and influence thoughts is beyond anything I would desire for the future. Personalized advertising may have been created with good intentions but it's now trying to control and influence ourselves.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Sem comentários.

f. Acesso não Autorizado

f.1 Neutro

f.2 Neutro

f.3 Discordo

f.4 Concordo totalmente

Social engineering can easily detect the "normal" non anomalous behavior so as to steal information and not be detected. So even it will detect anomalous behavior it does not mean it is protected. Most of the attacks and leak of information usually comes from inside, so moving to the cloud does not actually mean it will be less protected.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

Once again, in the name of making life easier for users we make them more vulnerable. Even though the most trained professional can sometime have doubts about a phishing.

h. Divulgação de Informação

h.1 Discordo totalmente

h.2 Discordo totalmente

h.3 Neutro

h.4 Concordo totalmente

This a specific topic that should be really taken into account. Data can become a powerful tool for good or bad.

D.2.27 RESPONDENTE #27

a. Privacidade

a.1 Concordo

a.2 Neutro

a.3 Concordo

a.4 Concordo totalmente

It's necessary better control and transparency about personal information. People should be more informed the risks and benefits.

b. *Malware*

b.1 Discordo

b.2 Concordo

b.3 Concordo

b.4 Discordo

Mainly small and medium business are more exposed to malware because usually they don't have a experienced IT security team.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo

c.3 Concordo totalmente

c.4 Concordo totalmente

I know two big companies that suffered ransomware attack. It's necessary take a serious this subject.

d. Vazamento de Informação

d.1 Discordo totalmente

d.2 Concordo

d.3 Concordo

d.4 Concordo totalmente

A lot of companies, specially small and medium, doesn't have a security specialist to guarantee the policy over informations.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo

I have seen a lot of data/info manipulated on the internet and in some small business.

f. Acesso não Autorizado

f.1 Discordo totalmente

f.2 Concordo totalmente

f.3 Concordo

f.4 DIscordo

I consider banks the best for access control but even banks should be concerned about it all time with raising up new technologies.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo

g.4 Concordo totalmente

Phishing can download malware and damage computers.

h. Divulgação de Informação

h.1 Discordo

h.2 Concordo

h.3 Discordo

h.4 Concordo

Information disclosure, that is not public, without permission of affected person/org is a privacy violation and because of this situation GDPR was implemented.

D.2.28 RESPONDENTE #28

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo

a.3 Concordo totalmente

a.4 Discordo

Sem comentários.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Concordo

b.4 Concordo totalmente

Sem comentários.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo

Sem comentários.

d. Vazamento de Informação

d.1 Neutro

d.2 Concordo totalmente

d.3 Concordo totalmente

d.4 Concordo totalmente

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo

f.3 Discordo totalmente

f.4 Concordo totalmente

Sem comentários.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

Sem comentários

h. Divulgação de Informação

h.1 Concordo

h.2 Discordo

h.3 Concordo totalmente

h.4 Concordo totalmente

Sem comentários.

D.2.29 RESPONDENTE #29

a. Privacidade

a.1 Concordo totalmente

a.2 Discordo

a.3 Concordo totalmente

a.4 Concordo totalmente

Sem comentários.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Concordo totalmente

b.4 Concordo

Sem comentários.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Sem comentários.

d. Vazamento de Informação

d.1 Concordo

d.2 Concordo totalmente

d.3 Concordo totalmente

d.4 Concordo totalmente

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Concordo totalmente

f.4 Concordo totalmente

Sem comentários.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

Sem comentários

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo totalmente

h.3 Concordo

h.4 Concordo

Sem comentários.

D.2.30 RESPONDENTE #30

a. Privacidade

a.1 Concordo totalmente

a.2 Neutro

a.3 Concordo totalmente

a.4 Discordo

A tecnologia já é considerada essencial no dia a dia, e as novas tecnologias serão adaptadas para as políticas de privacidade.

b. *Malware*

b.1 Concordo

b.2 Discordo

b.3 Concordo

b.4 Neutro

Os ataques de *malware* tem desafiados as grandes empresas para garantir a segurança e privacidade de seus clientes e colaboradores, mas obrigou as empresas a investirem em processos e tecnologias para se defenderem desse risco.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Os ataques *ransomware* são atualmente as maiores ameaças para as instituições, comprometendo a imagem e a saúde financeira.

d. Vazamento de Informação

d.1 Discordo totalmente

d.2 Concordo

d.3 Concordo

d.4 Concordo totalmente

O uso de *cloud* é a melhor forma de garantir a escalabilidade e resiliência da infraestrutura de forma rápida e segura, mas é dever das empresas fiscalizar os fornecedores para manter o sigilo das informações.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo

e.3 Concordo totalmente

e.4 Concordo

O roubo ou manipulação de dados, afeta tanto instituições e cidadãos, com o objetivo de obter vantagens econômicas ou proporcionar perdas financeiras.

f. Acesso não Autorizado

f.1 Concordo totalmente

f.2 Concordo totalmente

f.3 Neutro

f.4 Concordo

Acessos não autorizados podem ocorrer de varias formas as empresas devem investir em monitoração e em treinamentos para os acessos de seus clientes não serem compartilhados em ataques de engenharia social.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo

g.3 Concordo totalmente

g.4 Concordo

Phishing é um risco de segurança, pois pode causar danos financeiros e na reputação de empresas e cidadãos.

h. Divulgação de Informação

h.1 Neutro

h.2 Neutro

h.3 Discordo

h.4 Neutro

A decisão de quais informações devem ser compartilhadas precisa ser acordada entre as empresas e os clientes e devem ser utilizadas com cautela.

D.2.31 RESPONDENTE #31

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo

a.3 Concordo totalmente

a.4 Concordo totalmente

Digital Transformation requires high involvement of Legal departments and strong security policies from IT related departments.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Concordo totalmente

b.4 Concordo

Cyber criminals have been creating more complex ways of phasing, what has been imposing big challenges for the companies nowadays.

c. *Ransomware*

c.1 Concordo totalmente

c.2 Concordo totalmente

c.3 Concordo totalmente

c.4 Concordo totalmente

Ransomware is a big threat to commercial related companies.

d. Vazamento de Informação

d.1 Discordo

d.2 Concordo totalmente

d.3 Concordo

d.4 Neutro

Info leakage happens not only through systems, but also through people. It's important to give proper legal assessment to protect sensitive info from being stolen internally.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo

e.4 Concordo totalmente

Also a big threat to organizations, that requires special security reinforcement.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Discordo

f.4 Concordo

Digital transformation can even improve the way a customer data is accessed. Just remember in the past simply there was no way to make a complete control of customer data access.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo totalmente

g.3 Concordo totalmente

g.4 Concordo totalmente

This is one of main doors to cyber attacks, as non-IT related people simply can open it by mistake, just clicking in a link.

h. Divulgação de Informação

h.1 Neutro

h.2 Concordo totalmente

h.3 Discordo

h.4 Discordo

Security levels of each kind of information, like consumption behavior or tax ID, should be clearly disclosed to customers and also should be protected according to its level.

D.2.32 RESPONDENTE #32

a. Privacidade

a.1 Concordo

a.2 Concordo totalmente

a.3 Discordo

a.4 Concordo totalmente

Digital implementation is expensive and also efficient there is always a risk of data security.

b. *Malware*

b.1 Concordo totalmente

b.2 Concordo totalmente

b.3 Concordo

b.4 Concordo

Implementation involves risk factors.

c. *Ransomware*

c.1 Concordo

c.2 Concordo

c.3 Concordo

c.4 Concordo

Data loss is serious attack.

d. Vazamento de Informação

d.1 Concordo

d.2 Concordo totalmente

d.3 Neutro

d.4 Concordo totalmente

Securing data gives consumer confidence to believe in upgrading.

e. Roubo e Manipulação de Dados

e.1 Neutro

e.2 Concordo

e.3 Concordo totalmente

e.4 Concordo

Risk involved when there is a data theft.

f. Acesso não Autorizado

f.1 Concordo

f.2 Neutro

f.3 Discordo totalmente

f.4 Neutro

There are pros and cons going digital.

g. *Phishing*

g.1 Concordo

g.2 Concordo

g.3 Concordo

g.4 Concordo

Phishing is a drawback going digital.

h. Divulgação de Informação

h.1 Concordo

h.2 Concordo

h.3 Concordo

h.4 Concordo totalmente

Consumer information should be secured.

D.2.33 RESPONDENTE #33

a. Privacidade

a.1 Concordo totalmente

a.2 Concordo

a.3 Concordo totalmente

a.4 Concordo totalmente

I work for a Swiss company with global communication distribution, which means that data is on the top of discussion at the moment.

b. *Malware*

b.1 Concordo

b.2 Concordo

b.3 Concordo

b.4 Concordo totalmente

Sem comentários.

c. *Ransomware*

c.1 Concordo

c.2 Concordo

c.3 Concordo totalmente

c.4 Concordo totalmente

Sem comentários.

d. Vazamento de Informação

d.1 Discordo

d.2 Concordo totalmente

d.3 Concordo totalmente

d.4 Concordo totalmente

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo

e.4 Concordo totalmente

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Discordo

f.4 Concordo totalmente

Sem comentários.

g. *Phishing*

g.1 Concordo totalmente

g.2 Concordo

g.3 Concordo

g.4 Neutro

Sem comentários

h. Divulgação de Informação

h.1 Concordo totalmente

h.2 Concordo totalmente

h.3 Neutro

h.4 Discordo

Sem comentários.

D.2.34 RESPONDENTE #34

a. Privacidade

a.1 Concordo

a.2 Discordo

a.3 Concordo totalmente

a.4 Concordo totalmente

Sem comentários.

b. *Malware*

b.1 Concordo

b.2 Neutro

b.3 Neutro

b.4 Neutro

Sem comentários.

c. *Ransomware*

c.1 Neutro

c.2 Neutro

c.3 Concordo totalmente

c.4 Concordo

Sem comentários.

d. Vazamento de Informação

d.1 Concordo

d.2 Neutro

d.3 Concordo

d.4 Discordo totalmente

Sem comentários.

e. Roubo e Manipulação de Dados

e.1 Concordo totalmente

e.2 Concordo totalmente

e.3 Concordo totalmente

e.4 Concordo totalmente

Sem comentários.

f. Acesso não Autorizado

f.1 Concordo

f.2 Concordo totalmente

f.3 Concordo

f.4 Neutro

Sem comentários.

g. *Phishing*

g.1 Concordo

g.2 Neutro

g.3 Discordo

g.4 Neutro

Sem comentários

h. Divulgação de Informação

h.1 Concordo totalmente

h.2 Concordo totalmente

h.3 Concordo

h.4 Neutro

Sem comentários.

D.2.35 RESPONDENTE #35

a. Privacidade

a.1 Concordo totalmente

a.2 Discordo totalmente

a.3 Discordo totalmente

a.4 Discordo totalmente

Na Europa há uma grande preocupação em relação a LGPD independente da área de atuação da companhia. Eu mesmo já passei por situações onde precisei assinar documentos para utilização dos meus dados pessoais ao realizar uma consulta em um consultório particular, ao solicitar um cartão de crédito. Situações em que quando morava no Brasil não houve. Na empresa em que estou alocado sempre recebemos emails relacionados a LGPD nos projetos de tecnologia.

b. *Malware*

b.1 Discordo totalmente

b.2 Discordo totalmente

b.3 Discordo totalmente

b.4 Discordo totalmente

Sem comentários.

c. *Ransomware*

c.1 Discordo totalmente

c.2 Discordo totalmente

c.3 Discordo totalmente

c.4 Discordo totalmente

Sem comentários.

d. Vazamento de Informação

d.1 Discordo

d.2 Discordo totalmente

d.3 Neutro

d.4 Discordo

Estamos sempre atentos as atualizações tecnológicas relacionadas a segurança da informação para nos clientes e projetos. A alguns anos a companhia que estou alocado sofreu ataques cibernéticos e sempre tem investido em tecnologias e políticas de segurança dentro da companhia para conseguir identificar com rapidez e prevenir possíveis ataques.

e. Roubo e Manipulação de Dados

e.1 Discordo totalmente

e.2 Discordo totalmente

e.3 Discordo totalmente

e.4 Discordo totalmente

Muitas companhias sofrem ataques mas não permitem que a informação seja divulgada, acredito que em toda grande companhia ocorra semelhante ao que ocorre por aqui na europa.

f. Acesso não Autorizado

f.1 Discordo totalmente

f.2 Discordo totalmente

f.3 Discordo totalmente

f.4 Discordo totalmente

Vivendo na Europa eu tenho assinado muitos mais autorizações de tratamentos de dados.

g. *Phishing*

g.1 Discordo totalmente

g.2 Discordo

g.3 Discordo totalmente

g.4 Discordo totalmente

Sem comentários

h. Divulgação de Informação

h.1 Neutro

h.2 Neutro

h.3 Neutro

h.4 Discordo totalmente

Sem comentários.

D.3 CARTA-CONVITE

Risks Evaluation on Implementing Digital Transformation

Dear Invitee:

I am an MSc student at Universidade Nove de Julho's Information Technology and Knowledge Management program, with Prof. Dr. Ivanir Costa as my advisor. I am kindly requesting your participation in the research study that I am conducting regarding risks evaluation on implementing Digital Transformation.

Based on your strong information technology background and skills, I would like to invite you to answer this survey. If you could, please take 10 minutes reviewing 8 (eight) questions with 4 (four) statements each.

As soon as I have accurate results, I will send you the results.

Sincerely,

Eduardo Stefani
Prof. Dr. Ivanir Costa (Advisor)
Information Technology and Knowledge Management
Universidade Nove de Julho
Sao Paulo
Brazil