FUNDAÇÃO GETULIO VARGAS
ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO

RAFAEL DE QUEIROZ BATISTA

SEGURANÇA DA INFORMAÇÃO: O DILEMA DA EFETIVIDADE DOS INVESTIMENTOS QUANDO O RESULTADO ESPERADO É QUE NADA ACONTEÇA

SÃO PAULO
2023

RAFAEL DE QUEIROZ BATISTA

SEGURANÇA DA INFORMAÇÃO: O DILEMA DA EFETIVIDADE DOS INVESTIMENTOS QUANDO O RESULTADO ESPERADO É QUE NADA ACONTEÇA

Trabalho Aplicado apresentado à Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas, como requisito para a obtenção do título de Mestre em Gestão para a Competitividade.

Linha de pesquisa: Tecnologia da Informação

Orientador: Eduardo de Rezende Francisco

SÃO PAULO

2023

Batista, Rafael de Queiroz.
Segurança da informação : o dilema da efetividade dos investimentos quando o resultado esperado é que nada aconteça / Rafael de Queiroz Batista. - 2023.
44 f.

Orientador: Eduardo de Rezende Francisco.
Dissertação (mestrado profissional MPGC) – Fundação Getulio Vargas, Escola de Administração de Empresas de São Paulo.

1. Tecnologia da informação - Administração. 2. Redes de computadores - Medidas de segurança. 3. Empresas - Redes de computação. I. Francisco, Eduardo de Rezende. II. Dissertação (mestrado profissional MPGC) – Escola de Administração de Empresas de São Paulo. III. Fundação Getulio Vargas. IV. Título.

CDU 004.056

Ficha Catalográfica elaborada por: Raphael Figueiredo Xavier CRB SP-009987/O
Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

RAFAEL DE QUEIROZ BATISTA

SEGURANÇA DA INFORMAÇÃO: O DILEMA DA EFETIVIDADE DOS INVESTIMENTOS QUANDO O RESULTADO ESPERADO É QUE NADA ACONTEÇA

Trabalho Aplicado apresentado à Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas, como requisito para a obtenção do título de Mestre em Gestão para a Competitividade.

Data de Aprovação:
27/02/2023.

Banca examinadora:

_____
Prof. Dr. Eduardo de Rezende Francisco (Orientador)
FGV EAESP

_____
Prof. Dr. Gabriel Silva Cogo
FGV EAESP

_____
Prof. Dr. Álvaro Luiz Massad Martins
FGV EAESP

_____
Prof. Dr. Gilberto Perez
Universidade Presbiteriana Mackenzie

À minha família, pelo apoio desde o primeiro momento até a conclusão deste trabalho.

AGRADECIMENTOS

Ao Professor Doutor Eduardo Francisco, não apenas por aceitar o desafio de orientar este trabalho, mas também pelos valiosos conselhos dados durante nossas quase cinquenta reuniões semanais e por todo o apoio ao longo de todo o processo de pesquisa. Sem este apoio e parceria, certamente a caminhada teria sido muito mais árdua.

Aos meus pais, que sempre me mostraram que educação e o estudo são os elementos mais importantes da formação de um ser humano, e que nunca mediram esforços para que os filhos pudessem ter a melhor instrução que fosse possível. Foi graças a este apoio inicial que pude seguir adiante e chegar até aqui.

À minha família, de quem tantas vezes tive que me afastar durante os períodos de estudo do mestrado e de desenvolvimento deste trabalho. Em especial, à minha querida esposa Márcia, uma apoiadora incondicional desta jornada desde quando ela era apenas um plano.

Aos meus filhos, Eduardo e Carolina, que, embora obrigados a dividir com aulas, livros, artigos e trabalhos um tempo de convivência que seria deles, sempre souberam entender e apoiar. Espero que fiquem orgulhosos do resultado.

RESUMO

Segurança da informação tornou-se um tema relevante na agenda corporativa. As organizações dependem cada vez mais da tecnologia para executar seus processos de negócios, a legislação sobre os processos de tratamento de dados é cada vez mais rígida e os riscos cibernéticos são crescentes, fazendo com que seja necessário investir cada vez mais na proteção dos ativos de informação das organizações. Ao mesmo tempo, os modelos usados para mensurar a qualidade deste investimento são falhos, pois não são capazes de garantir que os principais riscos estão sendo, de fato, mitigados. Foram realizadas entrevistas semiestruturadas com oito executivos e ex-executivos com experiência no tema e analisadas através de triangulação e mineração de texto. Os achados destacam oportunidades de maior alinhamento entre a visão teórica e as ações de caráter prático na gestão dos processos de segurança da informação pelas organizações. Propõe-se, por fim, uma complementação aos modelos de maturidade ou *frameworks* existentes, que apontam um caminho para verificar os benefícios trazidos pelos investimentos em segurança da informação. Isso mitiga a dificuldade de uma avaliação realista, facilitando medir o sucesso de um programa de segurança da informação, ainda que o resultado deste sucesso seja a garantia de que nada de errado vai acontecer.

Palavras-chave: Segurança da informação; Benefícios dos investimentos; Modelos de maturidade.

ABSTRACT

Information security has become a relevant subject in the corporate agenda. Organizations depend more and more on technology to run their business processes, the legislation on data processing is increasingly strict and cyber risks are growing, making it necessary to invest much more to protect the organization’s information assets. At the same time, the models used to measure the quality of these investments are flawed, as they are not capable of guaranteeing that the main risks are being mitigated. Semi-structured interviews were conducted with eight executives and former executives with experience in the subject and analyzed through triangulation and text mining. The findings highlight opportunities for greater alignment between the theoretical view and practical actions in organizations' management of information security processes. Finally, a complement to existing maturity models or frameworks is proposed, pointing out a way to verify the benefits brought by investments in information security. This mitigates de difficulty of a realistic evaluation, making it easier to measure the success of an information security program, even if the result of such success is the guarantee that nothing goes wrong.

Keywords: Information security; Return on investments; Maturity models.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ALE	*Annual loss expectancy*
ARO	*Annualized rate of occurrence*
CEO	*Chief Executive Officer*
CISO	*Chief Information Security Officer*
CSO	*Chief Security Officer*
GDPR	*General Data Protection Regulation*
ISO	*International Organization for Standardization*
ISMS	Sistema de gestão de segurança da informação (*information security managament system*)
NIST	*National Institute of Standards and Technology*
NPV	Valor presente líquido (*net present value*)
ROSI	*Return on Security Investment*
SLE	*Single loss expectancy*
SMM	Modelo de maturidade em segurança da informação (*security maturity model*)

SUMÁRIO

1. INTRODUÇÃO

Cerca de 42% dos executivos brasileiros entrevistados pela consultoria KPMG entendem que digitalização e conectividade são pilares para atingir seus objetivos de crescimento. Ao mesmo tempo, mais de 70% deles consideram que segurança da informação pode ser uma vantagem competitiva, que devem contar com uma estratégia cibernética forte e que é necessário proteger não apenas os próprios ambientes digitais, mas também os de parceiros e de fornecedores (KPMG, 2021). Estes dados nos mostram que, houve, de fato, um aumento da pressão sobre os principais executivos para que implementem medidas capazes de reduzir o número de falhas de segurança em suas organizações (OWUSU KWATENG; AMANOR; TETTEH, 2022).

Os processos de transformação digital vivenciados por organizações dos mais diversos segmentos levaram a um uso mais intensivo da tecnologia da informação. Em alguns setores, a adoção de novas tecnologias foi acelerada em vários anos como consequência da pandemia mundial causada em 2020 pelo vírus SARS-COV-2, conhecida como COVID-19, mudando diversos hábitos da vida das pessoas (HOFFMAN, 2020). Como consequência, as falhas de segurança nestes sistemas tornam-se uma preocupação cada vez maior (MIRTSCH; POHLISCH; BLIND, 2020). O relatório produzido para a IBM Security em 2022 pelo Ponemon Institute indica que o custo médio global de um incidente de segurança é de USD 4,35 milhões, o que representa um aumento de 12,7% quando comparado ao ano de 2020, o último relatório produzido no período anterior à pandemia – no Brasil, o custo médio de um incidente de segurança é de USD 1,38 milhão (IBM SECURITY, 2022). Estes dados mostram que as organizações estão cada vez mais pressionadas a implantar estruturas de controles internos mais robustas para enfrentar as demandas de segurança da informação (CRAM; PROUDFOOT; D'ARCY, 2021).

Outro ponto relevante a ser considerado é que as inovações em TI estão se tornando um catalisador das preocupações relacionadas à privacidade (CICHY; SALGE; KOHLI, 2021), o que traz, como consequência, um endurecimento das leis relacionadas ao tema ao redor do mundo, com a GDPR (*General Data Protection Regulation*) europeia e suas pesadas sanções tendo se tornado uma espécie padrão *de facto* quando se trata da proteção dos dados pessoais (PERNOT-LEPLAY, 2020). Este endurecimento da legislação também atua como um fator que contribui para a necessidade de maior cuidado com a segurança das informações.

Com tudo isso, aumentam o custo e a complexidade de manter o ambiente de TI protegido; afinal, “cibercriminosos jamais desperdiçarão uma oportunidade” (FORTINET, 2022, p. 17, tradução nossa). Ou seja: a proteção precisa ser o mais completa possível, pelo máximo de tempo possível; para o atacante, entretanto, basta uma única falha que possa ser explorada, em um único momento. Há, aí, um desequilíbrio de oportunidades entre quem defende e quem ataca.

Para fazer frente às ameaças a que estão expostas, as organizações deveriam construir programas de segurança da informação com base no gerenciamento de seus riscos (GRITZALIS et al., 2018). Entretanto, embora seja relativamente fácil identificar um risco, é muito difícil quantificá-lo, ou seja, é muito difícil transformá-lo em um valor mensurável que possa a ser comparado a outros passivos da organização (JAQUITH, 2007). Por conta disso, estudos relacionados a controles de segurança da informação se concentram muito mais nos aspectos técnicos do que em informações gerenciais (MIRTSCH; POHLISCH; BLIND, 2020). Como consequência, a qualidade de um programa de segurança da informação é medida, em grande parte das vezes, através de um conjunto de observações de dados que não poderiam ser considerados, efetivamente, como um sistema de métricas que incorpora algum nível de metodologia em sua construção e nem que possa ser comparado entre diferentes organizações (YASASIN; SCHRYEN, 2015). Deste modo, a simples adequação a padrões e *frameworks* de segurança da informação não pode ser tomada como uma medida exata do nível de maturidade em segurança da informação em uma organização (CULOT et al., 2021), uma vez que a maior parte dos incidentes de segurança deriva de algum tipo de falha humana (STAHL; DOHERTY; SHAW, 2012). Portanto, programas de conscientização dos usuários são uma ferramenta importante na prevenção dos incidentes de segurança da informação (KHANDO et al., 2021) e deveriam, em conjunto com as medidas técnicas, fazer parte da medida do nível de maturidade de uma organização sobre o tema (OREHEK; PETRIČ, 2020). Este descompasso entre as medidas técnicas propostas pelos diferentes *frameworks* e as reais necessidades observadas pelos executivos pode ser observada de maneira clara nas certificações emitidas pela ISO – *International Organization for Standardization*: no ano de 2020, enquanto 17053 empresas no Brasil possuíam o selo de certificação em gestão da qualidade pelo padrão ISO 9001, apenas 148 empresas no país possuíam o selo de certificação em gestão de segurança da informação pelo seu equivalente, o padrão ISO 27001 (ISO, 2020).

1.1. OBJETIVOS

Diante deste contexto, este artigo busca responder à seguinte pergunta:

> (P1) como deveria ser construído um modelo que permitisse aferir se o programa de segurança da informação de uma organização é realmente efetivo?

Para responder a esta questão principal e coletar elementos para a elaboração do modelo proposto, foram utilizadas duas perguntas adicionais:

> (P2) na visão dos executivos, os recursos (humanos e financeiros) investidos em segurança da informação estão, de fato, reduzindo os riscos a que estão expostas as organizações?
>
> (P3) o que falta aos *frameworks* existentes para que possam ser usados como um guia para medir a efetividade dos programas de segurança da informação nas organizações?

Entre os anos de 2007 e 2018, foram escritos pelo menos 21 artigos sugerindo um novo modelo de maturidade em segurança da informação (SMM) (RABII et al., 2020), mas, ainda assim, não há modelos que sejam simples de implementar (REA-GUAMAN et al., 2017). Essa divergência entre a produção da academia e as demandas cotidianas das organizações mostra que há necessidade de indicar o que falta aos *frameworks* atuais para que possam servir como uma medida real da efetividade dos programas de segurança da informação adotados nas organizações. Além disso, há também a necessidade de verificar se esta visão é compartilhada entre aqueles que são diretamente responsáveis pela implementação dos programas de segurança da informação nas organizações, na condição de executivos desta área, e os que são responsáveis pela gestão das áreas de TI como um todo, tendo segurança da informação como uma de suas responsabilidades – mas não a única.

A partir deste *gap* identificado, será possível propor os elementos constituintes de um novo modelo que atenda às necessidades das organizações e que incorpore os elementos faltantes aos *frameworks* hoje existentes.

Um outro aspecto não totalmente coberto por grande parte dos *frameworks* disponíveis é a questão do comportamento dos colaboradores de uma organização. Embora a conscientização em segurança da informação seja citada como um dos controles necessários para a implementação de um ISMS (ISO, 2013), não há indicativos claros de como este nível de conscientização deve ser mensurado. A consciência em segurança da informação, aqui entendida como a capacidade dos colaboradores de uma organização tomarem decisões acertadas em segurança da informação, é um fator chave para mitigar os riscos que se apresentam (KHANDO et al., 2021). Este comportamento "seguro" é influenciado não apenas pela cultura de segurança da informação da organização, mas

também pelo suporte recebido pelo colaborador e até mesmo por sua satisfação no trabalho (MCKNIGHT; WARKENTIN, 2020).

Há, portanto, uma variedade enorme de *frameowrks* que buscam medir os níveis de implementação de segurança da informação em uma organização, mas há uma falta de modelos que sejam "focados em cibersegurança, de fácil implementação e adaptáveis a diferentes tipos de organizações" (REA-GUAMAN et al., 2017, p. 288, tradução nossa). Isso porque o tratamento de riscos sistêmicos e de falhas de segurança se aproxima muito mais de um sistema caótico do que de um sistema linear e, portanto, uma abordagem prescritiva não parece o melhor caminho para abordar este tema (BENBYA et al., 2020). De fato, McBride (2005) nos aponta que a adição de elementos de caos e complexidade pode ajudar a entender a dinâmica da implementação e do uso dos sistemas ao longo do tempo. Neste cenário, deveríamos adicionar aos nossos *frameworks* prescritivos elementos que nos permitissem desenvolver o que Rezazade Mehrizi, Nicolini e Rondon (2022) descreveram como aprendizado prospectivo, isto é, a possibilidade de aprender com incidentes futuros de segurança para aplicar medidas futuras de prevenção.

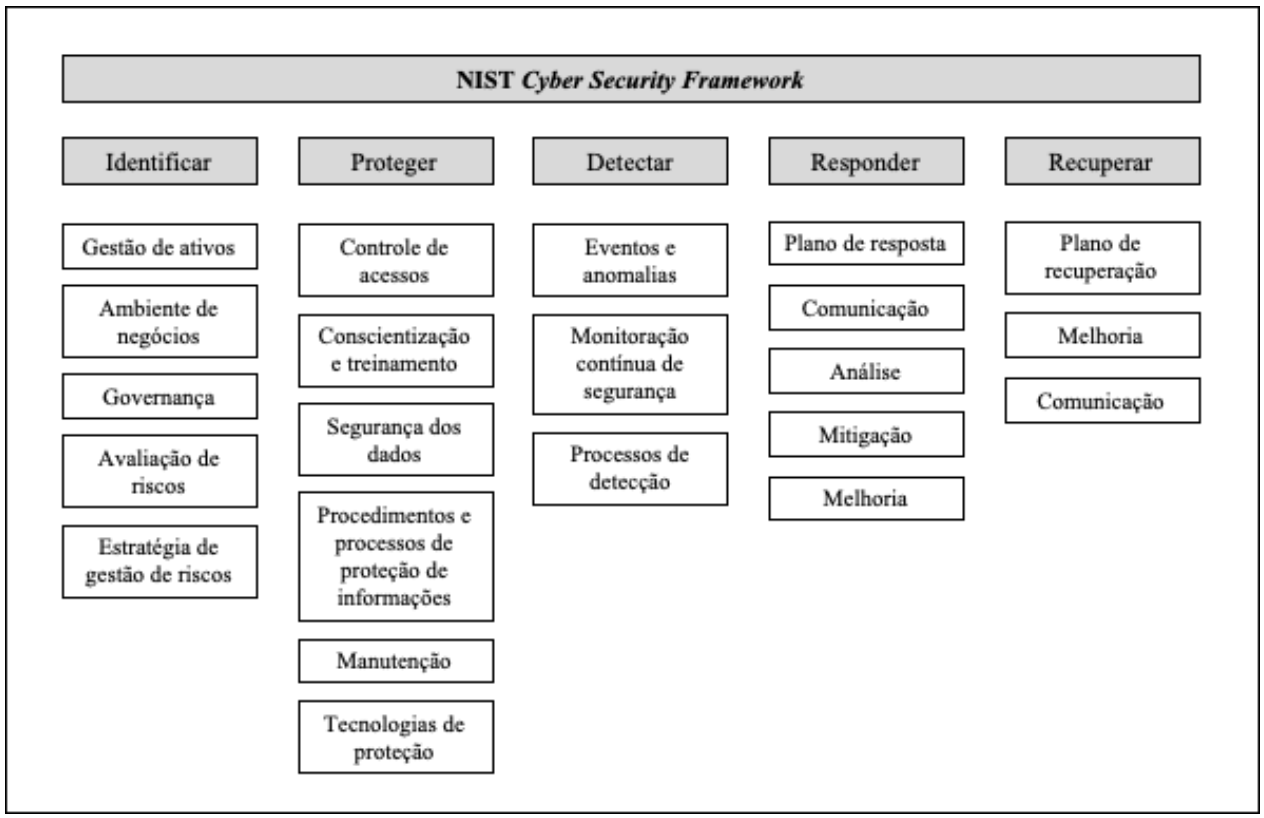
Sendo assim, é possível concluir que há peças faltantes nos *frameworks* usados pelos profissionais de segurança da informação para avaliar a efetividade das medidas que implementam, para comunicar esta efetividade ao corpo diretivo das organizações, para entender se as medidas tomadas estão, efetivamente, associadas a uma redução dos principais riscos a que a organização está exposta e, acima de tudo, para entender como as organizações se comportariam em caso de concretização de alguma das diversas ameaças que enfrentam cotidianamente. A incorporação destes elementos faltantes levaria a um *framework* mais completo, que permitiria a uma organização definir as ações necessárias para enfrentar seus problemas mais relevantes no campo da segurança da informação.

2. FUNDAMENTAÇÃO TEÓRICA

Segurança da informação pode ser definida como conjunto de atividades que tem por objetivo garantir a confidencialidade, a integridade e a disponibilidade dos sistemas. A estes pilares, podemos também agregar os objetivos de autenticidade e não repúdio (GORDON; LOEB, 2006) e, mais recentemente, o objetivo de garantir a privacidade das informações, uma vez que a capacidade de uma organização manter a privacidade dos dados pessoais sob seu controle também está diretamente associada à sua reputação (COMPAGNA et al., 2007). Estes objetivos se traduzem, em última instância, em investimentos que visam mitigar os riscos a que uma organização está exposta, sejam eles internos ou externos (EISENGA; JONES; RODRIGUEZ, 2012).

As falhas de segurança estão cada vez mais comuns, apesar de todos os esforços voltados à sua prevenção (WEIXUN LI; CHUNG MAN LEUNG; YUE, 2023). Grande parte destes esforços, porém, está muito mais voltado a medidas técnicas do que a aspectos econômicos ou financeiros (GORDON; LOEB, 2006). A ISO (*International Organization for Standardization*) propõe um conjunto de requisitos para a implantação de um sistema de gestão de segurança da informação (ISMS), com o objetivo de garantir a segurança das informações das organizações (ISO, 2013). A norma ISO 27001 é o sistema de gestão de SI mais renomado e mais usado em todo o mundo (CULOT et al., 2021). O NIST (*National Institute of Standards and Technology*), por sua vez, recebeu do governo americano a incumbência de criar uma série de controles e medidas de segurança que pudessem ser usadas para identificar e tratar riscos cibernéticos (NIST, 2018). São dois *frameworks* muito utilizados, mas os únicos aspectos financeiros avaliados para justificar sua implementação são as pressões de mercado, em que grandes empresas, muitas vezes, exigem a certificação de seus fornecedores (CULOT et al., 2021). A figura 1 apresenta o modelo desenvolvido pelo NIST.

Figura 1: Representação do framework proposto pelo NIST



Fonte: NIST, traduzido pelo autor (2023)

Lord Kelvin foi um dos mais importantes físicos do século XIX e a ele é atribuída a frase “medir é conhecer; se você não pode medir, você não pode aprimorar” (KELVIN, 1901, tradução nossa). Seu trabalho era sobre termodinâmica, mas a realidade não é diferente em segurança da informação. Portanto, é esperado que se busque estabelecer métricas para definir se as ações de segurança da informação são efetivas na redução dos riscos a que uma organização está exposta (JAQUITH, 2007), sendo um risco, neste contexto, definido como a probabilidade de que um dano possa ocorrer (EISENGA; JONES; RODRIGUEZ, 2012).

Com a popularização do CMM (*Capability Maturity Model*) como método para avaliar o uso das melhores práticas no desenvolvimento de sistemas em uma organização, a partir da década de 1980, abriu-se um caminho para a proposição de modelos de maturidade em diversos outros campos, dentre eles a segurança da informação (RABII et al., 2020). Ao mesmo tempo, as organizações passaram a buscar formas de implementar modelos de gestão de segurança da informação (ISMS) que as permitissem implementar as medidas mais apropriadas para a proteção de seus ativos de informação (MIRTSCH; KINNE; BLIND, 2021). Os *frameworks* usados para a implementação de

um ISMS, porém, não são eficientes na identificação do real nível de maturidade de uma organização com relação à segurança da informação, uma vez que a maturidade está diretamente relacionada com uma cultura de segurança da informação (OREHEK; PETRIČ, 2020). Neste contexto, a cultura de segurança da informação pode ser vista como um conjunto de valores compartilhados dentro de uma organização para proteger seus ativos (UCHENDU et al., 2021, p. 2). Além disso, com frequência, não são considerados os efeitos que um controle proposto pode ter sobre os demais, o que pode gerar a redução no efeito de um controle pela implementação de outro (YOU et al., 2018).

Além da dificuldade em se medir a maturidade de uma organização com relação à segurança da informação no aspecto técnico, há também uma dificuldade em estabelecer o impacto financeiro dos investimentos em segurança da informação para ela. Medidas como o ROSI (*Return on Security Investments*) foram propostas por autores como Yaqoob et al. (2019), mas há um elevado grau de incerteza associado ao impacto das vulnerabilidades que precisaria ser considerado para este tipo de cálculo. O cálculo do ROSI também parte do pressuposto de que é possível estimar, matematicamente, o valor das perdas em caso de um incidente de segurança da informação, o que nem sempre é uma premissa verdadeira (YAQOOB et al., 2019).

3. METODOLOGIA

Devido ao fato de haver poucos trabalhos dedicados a identificar e sistematizar as diferenças entre os modelos existentes para avaliar a maturidade das medidas de segurança da informação implementadas nas organizações (RABII et al., 2020), optou-se pela metodologia qualitativa, pois é um método que permite a livre expressão dos entrevistados (KALLIO et al., 2016). De acordo com Adams (2015, p. 494), um questionário semiestruturado é útil "se você estiver examinando um território desconhecido, com questões desconhecidas, mas potencialmente importantes, e seus entrevistadores precisam de latitude máxima para identificar pistas úteis e persegui-las" (tradução nossa). Estes fatores explicam nossa opção por utilizar uma pesquisa qualitativa, com o uso de um questionário semiestruturado, para identificar os *gaps* existentes nos *frameworks* utilizados para guiar as medidas de segurança da informação nas organizações. O questionário semiestruturado trouxe a vantagem adicional de poder abordar tópicos paralelos relacionados às questões, ampliando a perspectiva das entrevistas (COHEN; CRABTREE, 2006). Ao final da etapa de entrevistas, as transcrições foram codificadas por meio de um software de CAQDAS (*Computer-Assisted Qualitative Analysis Software*), a fim de eliminar qualquer viés de interpretação, além de buscar associações entre conceitos que pudessem ter passado despercebidas na análise inicial. Para esta finalidade, foi utilizado o aplicativo Atlas.ti, na versão 23.0.1 (4141).

Os entrevistados pertenciam a dois grupos distintos, sendo um deles composto por executivos ou ex-executivos que atuam ou atuaram diretamente na gestão de equipes de segurança da informação e o outro composto por executivos ou ex-executivos que atuam ou atuaram na gestão de TI, tendo segurança da informação como uma de suas responsabilidades, mas não a única. A intenção, com esta divisão, foi realizar uma análise do problema sob duas óticas distintas, buscando identificar se haveria diferenças nas visões destes dois grupos sobre o tema em questão, uma vez que há uma tendência de que especialistas em SI tenham uma visão mais aprofundada sobre o tema do que a média dos demais profissionais (WU et al., 2023).

As questões apresentadas no roteiro da entrevista foram extraídas dos artigos *Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management* (HERATH; HERATH; BREMSER, 2010) e *Information and cyber security maturity models: a systematic literature review* (RABII et al., 2020), onde eram algumas das perguntas de pesquisa dos autores. Estes autores propunham questões sobre o modo de aferir a efetividade dos controles

e medidas de segurança da informação implementadas nas organizações e os modos de medir a maturidade de um ISMS a partir destes controles e medidas.

O roteiro da entrevista semiestruturada foi composto por dois grandes blocos, cada um deles contendo sete perguntas. O primeiro bloco tinha como objetivo entender a percepção dos entrevistados sobre a importância dos investimentos em segurança da informação e sua efetividade no trato das principais ameaças enfrentadas pelas organizações. O segundo bloco, por sua vez, tinha como objetivo principal entender, na percepção dos entrevistados, quais eram as falhas nos *frameworks* mais comumente utilizados, quais atributos devem fazer parte de um *framework* que seja realmente efetivo para endereçar as principais questões relativas à segurança da informação e como deveriam ser tomadas as decisões de investimento. Entre o primeiro e o segundo bloco de perguntas, havia um estímulo aos entrevistados para que refletissem sobre os modelos de gestão de segurança da informação existentes. O objetivo deste estímulo foi verificar se haveria diferenças significativas no padrão das respostas após a menção aos modelos de gestão ou se estes apareceriam naturalmente como parte das respostas desde o início da entrevista.

Antes dos dois blocos de perguntas, foi pedido aos entrevistados que fizessem um breve relato de suas carreiras e descrevessem suas experiências com o tema de segurança da informação. Estas informações tinham como objetivo avaliar se haveria diferenças nos padrões de resposta derivadas da experiência dos entrevistados.

O quadro 1 apresenta o roteiro utilizado para as entrevistas semiestruturadas.

Quadro 1: Roteiro para as entrevistas semiestruturadas

Pergunta inicial – experiência e contato com o tema
Breve resumo de sua trajetória: tempo de experiência em TI/Segurança, passagens mais marcantes.
Bloco 1 – Importância dos investimentos em segurança da informação e sua efetividade no trato das principais ameaças enfrentadas pelas organizações
Em sua visão, qual a importância, para uma organização, da alocação de recursos (financeiros e humanos) em segurança da informação?
Em sua opinião, o dinheiro despendido por uma organização em segurança da informação deve ser considerado como um investimento ou como uma despesa?
Em sua opinião, como uma organização deveria avaliar a relação entre os custos e os benefícios de segurança da informação?
Você entende que, de um modo geral, os benefícios gerados por investimentos em segurança da informação superam os custos?
Em sua opinião, as medidas de segurança da informação costumam estar diretamente associadas aos principais riscos enfrentados pelas organizações?
Em sua opinião, as medidas de segurança da informação adotadas pelas organizações são adequadas para reduzir vulnerabilidades e ameaças?
Em sua opinião, há algum modo de aferir a efetividade das diferentes medidas de segurança da informação para uma organização?
Bloco 2 – Falhas nos frameworks atualmente utilizados, atributos de um framework efetivo e método para tomada das decisões de investimento
Em sua visão, esta forma de avaliar o nível de segurança da informação de uma organização está correta?
Em sua opinião, o uso de um modelo de maturidade pode ser útil para aferir a efetividade das medidas de segurança da informação de uma organização? Qual seria o impacto de sua adoção?
Em sua opinião, que atributos um modelo de maturidade de segurança da informação deveria ter para ser efetivo na aferição da efetividade das medidas de segurança da informação em uma organização?
Em sua opinião, quais *stakeholders* deveriam estar envolvidos na definição dos orçamentos de segurança da informação e quais fatores eles deveriam levar em consideração na elaboração deste orçamento?
Qual método você usa ou usaria para se sentir confortável com o volume de investimentos em segurança da informação?
Em sua opinião, os métodos usados hoje pelas organizações para definir despesas e investimentos em segurança da informação são adequados para enfrentar os desafios futuros? Por quê?
Há algo mais que seja importante, na sua visão, para ser trazido para esta discussão?

Fonte: Elaborado pelo autor (2023)

Em ambos os grupos, houve uma concentração intencional em executivos que ocupam ou ocuparam posições em bancos ou em empresas que prestam serviços para bancos, por ser este o segmento que, tradicionalmente, mais gasta e investe em TI no Brasil – em média, os bancos brasileiros investem em mais do que o dobro das empresas do país como proporção de seu faturamento (17,9% do faturamento nos bancos contra 8,7% do faturamento nas médias e grandes empresas brasileiras) (MEIRELLES, 2022).

A tabela 1 apresenta um resumo das experiências dos entrevistados.

Tabela 1: Experiência dos entrevistados

Entrevistado	Sexo	Função na data da entrevista	Experiência com o tema
Entrevistado 1	Masculino	Executivo de operações (incluindo TI)	31 a 35 anos
Entrevistado 2	Masculino	Executivo de TI	21 a 25 anos
Entrevistado 3	Masculino	*General Manager* (ex-executivo de TI)	15 a 20 anos
Entrevistado 4	Masculino	*Venture Capitalist* (ex-executivo de TI)	26 a 30 anos
Entrevistado 5	Masculino	Consultor em SI (ex-executivo de SI)	10 a 15 anos
Entrevistado 6	Masculino	Executivo de SI (setor não financeiro)	16 a 20 anos
Entrevistado 7	Masculino	CEO de empresa de serviços de SI	16 a 20 anos
Entrevistado 8	Feminino	Executivo de SI (setor financeiro)	16 a 20 anos

Fonte: Elaborado pelo autor (2023)

4. RESULTADOS

As entrevistas foram individuais, por meio de vídeo conferência, com os executivos e ex-executivos que aceitaram a carta convite enviada por *e-mail* apresentada no Apêndice A. As sessões foram gravadas para posterior transcrição do conteúdo e uma autorização para esta gravação foi coletada no início da entrevista, sob o compromisso de não divulgação dos dados dos entrevistados ou das empresas em que trabalham e nem das informações obtidas de forma individualizada.

Houve o envio de onze cartas convite, sendo que oito destas foram aceitas. Dos oito executivos e ex-executivos entrevistados, quatro têm ou tiveram atuação direta na gestão de equipes de segurança da informação e outros quatro têm ou tiveram atuação na gestão de TI, tendo segurança da informação como uma de suas responsabilidades, mas não a única. Quatro dos entrevistados, os entrevistados 1, 3, 4 e 8, ocupam ou ocuparam posições executivas em bancos. Dentre os entrevistados, sete eram homens e apenas uma era mulher.

Para os entrevistados com relação direta na gestão de equipes de segurança da informação, convidamos ocupantes de uma diversidade de posições: executivo de SI de organização financeira, executivo de SI de organização não financeira, executivo de empresa de consultoria com especialização em SI e executivo de empresa prestadora de serviços de segurança da informação. Deste modo, buscamos abranger diferentes percepções sobre o tema.

As entrevistas tiveram duração média de 49:59 minutos, com desvio padrão de 12:44 minutos. A entrevista mais curta teve duração de 31:18 minutos e a mais longa teve duração de 1:13:09 hora. A tabela 2 apresenta a duração de cada uma das entrevistas.

Tabela 2: Entrevistas semiestruturadas

Entrevistado	Data da entrevista	Duração da entrevista
Entrevistado 1	30/05/2022	00:58:56
Entrevistado 2	03/06/2022	00:38:29
Entrevistado 3	13/06/2022	00:40:36
Entrevistado 4	14/06/2022	1:13:09
Entrevistado 5	21/06/2022	00:53:57
Entrevistado 6	28/06/2022	00:44:57
Entrevistado 7	05/07/2022	00:58:26
Entrevistado 8	12/08/2022	00:31:18

Fonte: Elaborado pelo autor (2023)

A primeira pergunta do questionário buscava entender a importância atribuída pelos entrevistados à alocação de recursos (humanos e financeiros) em SI pelas organizações. Isso porque, mesmo com

o crescente número de vulnerabilidades e ataques, convencer os gestores sobre investimentos em SI continua sendo o maior desafio dos executivos da área (YAQOOB et al., 2019).

Todos os entrevistados deram respostas que convergiram no sentido de que a alocação de recursos em SI é essencial para o futuro das organizações, pois os incidentes de SI serão cada vez mais frequentes e mais danosos. A causa disso, segundo os entrevistados, são os processos de transformação digital e o fato de que cada vez mais as organizações dependem de suas estruturas de TI. Nas palavras do Entrevistado 1, "*as companhias estão, cada vez mais, virando companhias de tecnologia que têm um propósito de entregar, através da tecnologia, algum serviço*". Esta percepção sobre os processos de transformação digital e sobre uma maior dependência da tecnologia vão ao encontro do observado por Hoffman (2020), que indicou esta transformação não apenas nas organizações, mas também nos hábitos das pessoas.

É interessante notar que, embora todos os entrevistados tenham considerado que deva haver alocação de recursos financeiros em SI, há uma divergência sobre classificar estes valores como despesas ou como investimentos. Tal divergência está alinhada o que se vê já há algum tempo na literatura, que nos mostra que, apesar de muitos gastos em segurança da informação terem mais similaridade com investimentos, muitas organizações tendem a tratá-los como despesas operacionais (GORDON; LOEB, 2006). Esta dificuldade passa pelo fato de que a avaliação dos recursos financeiros alocados em SI deve considerar tanto valores financeiros como valores não-financeiros e, portanto, apenas medir o retorno dos investimentos em segurança da informação (ROSI, na sigla original em inglês) ou o valor presente líquido (NPV, na sigla original em inglês) destes investimentos, como se faz na maioria dos projetos, não é suficiente (EISENGA; JONES; RODRIGUEZ, 2012). Para os entrevistados que têm ou tiveram SI como função principal, a resposta mais comum foi considerar qualquer recurso financeiro despendido em SI como um investimento, sob a explicação de que daria um retorno – ainda que intangível – para a organização. Para os entrevistados que tinham SI apenas como uma de suas responsabilidades, porém, a classificação não deveria ser tão simples, devendo ser considerados como investimentos apenas os recursos destinados ao desenvolvimento de novas capacidades – os recursos destinados à manutenção dos processos cotidianos deveriam ser considerados como despesas.

Um grande risco ao se tratar o dispêndio de recursos em SI – ou parte dele – como despesa é que estas estão sujeitas a variações de acordo com os indicadores da organização. Embora seja natural (e até mesmo requerido) que o orçamento de SI esteja alinhado à capacidade da organização de

arcar com os custos (EISENGA; JONES; RODRIGUEZ, 2012), deveria haver algum nível de proteção para que os gastos de SI não sejam reduzidos em momentos de resultados ruins; afinal, os riscos a que uma organização está exposta não diminuem quando seus indicadores financeiros pioram, e a estratégia de SI deve ter como objetivo mitigar estes riscos (HERATH; HERATH; BREMSER, 2010). Neste sentido, o Entrevistado 4 propôs uma alternativa que pode ser de grande ajuda para tratar desta questão. Sua proposta seria considerar como investimento "*aquilo que foi gasto a mais, como percentual do orçamento de TI, do que no ano anterior*", sendo o restante considerado como despesa. Deste modo, segundo o entrevistado, em momentos de restrição financeira, seria possível diferenciar de modo claro a parcela que se refere à manutenção do nível corrente de segurança daquela que se refere a novas capacidades.

A avaliação dos benefícios dos investimentos em SI apresenta dificuldades similares à avaliação dos benefícios de outros investimentos em TI: a existência de benefícios intangíveis ou que são muito difíceis de quantificar (HERATH; HERATH; BREMSER, 2010). Por exemplo, um dos indicadores financeiros mais utilizados, a expectativa de perda anual (ALE, na sigla original em inglês), é calculado a partir da expectativa de perda em um evento (SLE, na sigla original em inglês) e da taxa de ocorrência anual (ARO, na sigla original em inglês). Embora o cálculo possa ser feito com facilidade, pois é uma simples multiplicação, é extremamente difícil estimar com um bom grau de precisão os valores de SLE e ARO (EISENGA; JONES; RODRIGUEZ, 2012). Os valores exatos só são conhecidos se já tiver havido um incidente de segurança na organização, quando o ideal seria saber se os investimentos estão gerando os benefícios esperados – e o principal benefício é, justamente, evitar incidentes de segurança. Ou, nas palavras dos entrevistados, o principal benefício seria um custo evitado, sendo este custo os valores necessários para recuperar a operação de TI após um incidente de segurança da informação. O Entrevistado 1, o Entrevistado 3 e o Entrevistado 4 definiram esta dificuldade usando exatamente a mesma frase: "*como medir o sucesso de alguma coisa em que o sucesso é não acontecer nada*"? Neste momento, como uma tentativa de capturar os valores intangíveis, os entrevistados ligados à gestão direta de SI começam a mencionar os *frameworks* de SI como uma forma de gerar indicadores que permitiriam saber se a SI estaria boa ou ruim, mesmo que estes não sejam uma forma definitiva de atestar a maturidade da SI de uma organização (YOU et al., 2018).

A partir da constatação de que há uma dificuldade em determinar os benefícios da alocação de recursos em SI, é uma consequência natural que seja igualmente difícil avaliar se estes benefícios

superam os custos, embora os custos possam ser mensurados com maior facilidade e com um grau muito superior de precisão. Ainda assim, os entrevistados expressaram um sentimento de que a resposta para este questionamento seria negativa – ou seja, os benefícios não superariam os custos. Na visão do Entrevistado 5, "*os benefícios não superam os custos porque, muitas vezes, os recursos estão sendo alocados incorretamente*", visão corroborada pelo Entrevistado 7. Os Entrevistados 1, 5 e 6 comentaram que "*há muitos gastos em compra de ferramentas e pouco investimento em pessoas, sem checar a adequação destes gastos ao que a organização realmente precisa*". O Entrevistado 8 fez uma analogia para esta situação, dizendo que "*estamos comprando um monte de Ferraris, mas não temos nem pilotos para dirigi-las e nem pistas para elas andarem*". Estas opiniões estão em linha com a literatura, que mostra que as medidas de SI em uma organização deveriam ser direcionadas para tratar os principais riscos a que esta organização está exposta e com o fato de que grande parte dos incidentes de SI não está relacionada apenas aos sistemas, mas também ao comportamento dos colaboradores (ALAVI; ISLAM; MOURATIDIS, 2016; GRITZALIS et al., 2018; KHANDO et al., 2021).

A efetividade das medidas de SI para a redução de vulnerabilidades e ameaças a que uma organização está exposta também esbarra no fato de que nem sempre as organizações conhecem suas principais vulnerabilidades e as ameaças a que estão expostas. Jaquith (2007) nos mostra que é bastante difícil transformar riscos em valores mensuráveis e os entrevistados corroboram esta percepção, apresentando alternativas para tentar identificar estas vulnerabilidades e ameaças. Para o Entrevistado 6, o caminho para conhecer os principais riscos seria "*realizar estudos de benchmark, comparando a organização a seus pares*". O Entrevistado 4, sugere "*executar testes de penetração para verificar o real nível de proteção*", enquanto os Entrevistados 5 e 7 sugerem "*contratar consultores externos para realizar assessments do ambiente*". Podemos, portanto, concluir que o alinhamento entre as medidas de SI e a redução dos riscos a que uma organização está exposta ainda é um grande problema, ainda que todos conheçam os *frameworks* propostos para guiar as ações de SI, pois todos os entrevistados os mencionaram nas entrevistas mesmo antes de serem estimulados.

Uma questão levantada pelos entrevistados sobre os *frameworks* é o fato de que não medem todo o escopo, pois não são capazes de identificar a importância das medidas para o contexto da organização, ou seja, não há uma diferenciação que permita selecionar os controles mais importantes. Nas palavras dos Entrevistados 1, 2, 3, 5, 7 e 8: "*frameworks são importantes, mas*

medem apenas uma parte do problema". Embora, para o Entrevistado 6, os *frameworks* existentes "*sejam uma linguagem útil para comparar os benchmarks*", o Entrevistado 4 pontuou que "*ter uma boa nota de acordo com um framework não é uma garantia de proteção*", o que foi corroborado pelo Entrevistado 7, que ainda acrescentou que "*ter uma boa nota pode até mesmo atrapalhar, pois passa uma falsa impressão de que está tudo bem*". Este aspecto vai ao encontro do afirmado por Rea-Guaman et al. (2017, p. 288), que diz que há uma falta de modelos que sejam "focados em cibersegurança, de fácil implementação e adaptáveis a diferentes tipos de organizações" (tradução nossa). De acordo com os entrevistados, este é o principal problema enfrentado na avaliação da eficácia das medidas de SI e haveria um impacto extremamente positivo se houvesse um modelo de avaliação que fosse capaz de tratar todos os pontos que não são cobertos nos modelos de uso mais frequente, ou seja, um modelo que fosse capaz de "*medir as pessoas*" (Entrevistados 1, 2 e 5), de "*permitir uma comparação com o mercado*" (Entrevistado 6) e que "*contenha elementos que mostrem como está a segurança na prática*" (Entrevistado 4).

A definição do orçamento de SI mostrou uma diferença entre os entrevistados que, em um primeiro momento, era inesperada. Isto porque não houve uma diferenciação entre aqueles que ocupam ou ocuparam posições diretamente ligadas a SI e aqueles que ocupam ou ocuparam posições em TI com SI sendo uma de suas funções, como esperado antes das entrevistas (WU et al., 2023). A diferença nas respostas se deu de acordo com o nível hierárquico que os entrevistados ocupam ou ocuparam em diferentes organizações. Assim, embora todos tenham afirmado que "as áreas de negócio" devem ser envolvidas nas decisões de investimento em SI, os respondentes que ocupam ou ocuparam cargos de gerência sugerem o envolvimento de diretores; os respondentes que ocupam ou ocuparam cargos de diretoria sugerem o envolvimento do CEO ou presidente da empresa; e os respondentes que já ocuparam cargos de nível mais alto (o chamado *C-Level*) sugerem que o assunto seja tratado pelo Conselho. Mas, ainda que exista esta diferenciação, a mensagem final que os entrevistados deixaram é clara: a organização deve, como um todo, ser envolvida na discussão sobre SI, não deixando as decisões apenas nas mãos dos especialistas. Ou, nas palavras de Russel (2022, p. 2), "embora o CSO ou o CISO definam as agendas de segurança das corporações, outros líderes precisam ter papéis mais ativos".

Os modelos existentes para avaliar se os recursos estão sendo alocados em SI da forma mais eficiente possível, se o nível de SI de uma organização está adequado às suas necessidades e se os benefícios gerados pelos investimentos superam os custos destes investimentos não são suficientes,

de acordo com a opinião unânime dos entrevistados. E, não sendo suficientes para os desafios ora enfrentados, seriam ainda menos suficientes com o surgimento de novas ameaças. Por conta disso, todos os entrevistados apontaram a necessidade de aperfeiçoar os modelos, buscando incorporar elementos que fossem além das medidas técnicas e prescritivas. Afinal, nas palavras deles, "*se você está confortável com SI hoje, provavelmente não está atento a alguma coisa*".

Na tabela 3, estão sintetizadas algumas impressões dos entrevistados sobre os temas propostos no questionário, de acordo com o bloco de perguntas em que foram apresentadas:

Tabela 3: Respostas dos entrevistados

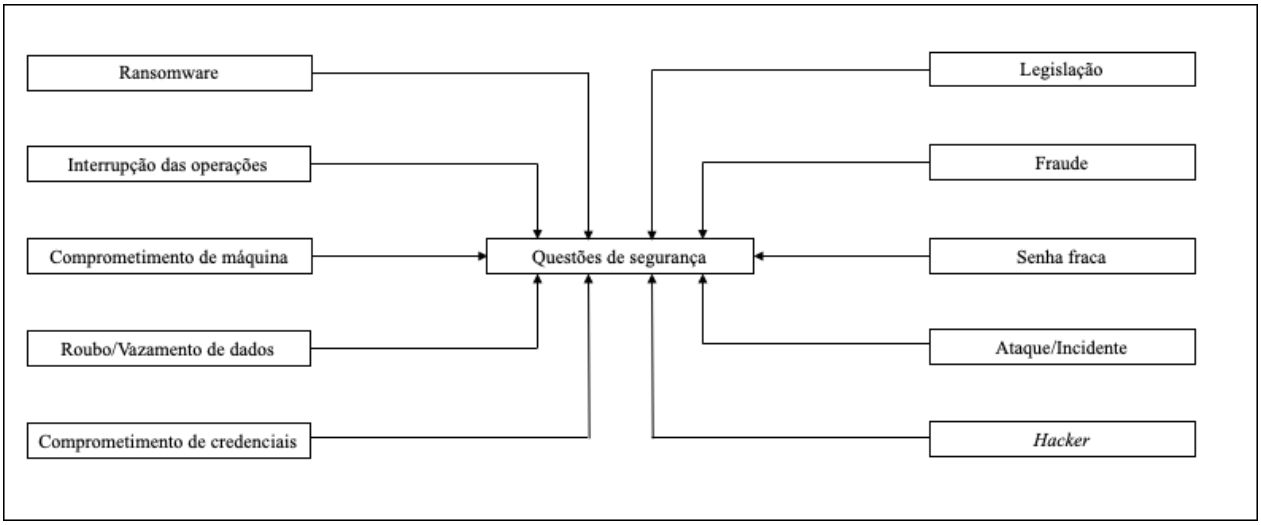
Entrevistado	Principais impressões – bloco 1	Principais impressões – bloco 2
Entrevistado 1	• As companhias estão, cada vez mais, virando companhias de tecnologia que têm um propósito de entregar, através da tecnologia, algum serviço. • Como medir o sucesso de alguma coisa em que o sucesso é não acontecer nada?	• [Com os *frameworks*] todo mundo mede o mapa, o caminho, ninguém mede o resultado.
Entrevistado 2	• Independente de [segurança da informação] ser um investimento ou um gasto, eu tenho que justificar. E, mesmo sendo um gasto, eu tenho que ter retorno para aquilo. • Você pode fazer um monte de investimentos em ferramental, mas, se a gente não trabalhar também o comportamental, é um problema.	• *Frameworks* são importantes, mas medem apenas uma parte do problema. • Se você está confortável com SI hoje, provavelmente não está atento a alguma coisa. • Se eu tivesse que escolher, se só pudesse um ou outro [investir em ferramentas ou em conscientização], eu iria "na veia" na conscientização.
Entrevistado 3	• Como medir o sucesso de alguma coisa em que o sucesso é não acontecer nada?	• *Frameworks* são importantes, mas medem apenas uma parte do problema. • Se [o CISO] está tranquilo é porque não sabe o que está fazendo.
Entrevistado 4	• Deve ser considerado investimento aquilo que foi gasto a mais, como percentual do orçamento de TI, do que no ano anterior. • Como medir o sucesso de alguma coisa em que o sucesso é não acontecer nada? • É essencial executar testes de penetração para verificar o real nível de proteção [de uma organização].	• Ter uma boa nota de acordo com um *framework* não é uma garantia de proteção. • Se eu tivesse um único dólar para investir em segurança, eu investiria em conscientização.

Entrevistado	• Principais impressões – bloco 1	• Principais impressões – bloco 2
Entrevistado 5	• Os benefícios não superam os custos porque, muitas vezes, os recursos estão sendo alocados incorretamente. • Há muitos gastos em compra de ferramentas e pouco investimento em pessoas, sem checar a adequação destes gastos ao que a organização realmente precisa.	• *Frameworks* são importantes, mas medem apenas uma parte do problema. • Medir SI apenas usando um *framework* seria como medir a índole de um adolescente apenas olhando seu boletim escolar.
Entrevistado 6	• O caminho para conhecer os principais riscos seria realizar estudos de *benchmark*, comparando a organização a seus pares.	• Os *frameworks* existentes são uma linguagem útil para comparar os *benchmarks*. • Um CISO nunca pode dormir tranquilo, mesmo fazendo seu trabalho direito.
Entrevistado 7	• Para medir os benefícios, primeiro devemos calcular todos os riscos potenciais, porque o benefício é evitar os riscos. • É importante contratar consultores externos para realizar *assessments* do ambiente.	• *Frameworks* são importantes, mas medem apenas uma parte do problema. • Ter uma boa nota em um *framework* pode até mesmo atrapalhar, pois passa uma falsa impressão de que está tudo bem.
Entrevistado 8	• Estamos comprando um monte de Ferraris [ferramentas modernas de SI], mas não temos nem pilotos para dirigi-las e nem pistas para elas andarem.	• *Frameworks* são importantes, mas medem apenas uma parte do problema. • Fico pensando em como a gente conseguiria alinhar nossos indicadores ao ROI. A gente não tem nenhuma metodologia ainda que a gente consiga mapear.

Fonte: Elaborado pelo autor (2023)

Uma busca nos registros das entrevistas com o uso do *software* Atlas.ti mostrou que há dez questões de segurança que foram abordadas pelos entrevistados e que representam suas principais preocupações sobre o tema. Estas questões são apresentadas na figura 2.

Figura 2: Preocupações em segurança da informação apontadas pelos entrevistados



Fonte: Elaborado pelo autor (2023)

As preocupações foram apresentadas pelos entrevistados nas respostas às perguntas do questionário. A tabela 4 mostra a frequência com que apareceram estas questões.

Tabela 4: Menções às questões de segurança

Questão	Número de ocorrências
Ataque/Incidente	25
Fraude	10
Ransomware	10
Roubo/Vazamento de dados	8
Legislação	7
Senha fraca	6
Hacker	4
Interrupção das operações	4
Comprometimento de credenciais	4
Comprometimento de máquina	1

Fonte: Elaborado pelo autor (2023)

O maior número de menções foi feito a ataques/incidentes. Porém, esta preocupação pode ser agrupada com as menções a *ransomware* e a *hacker*, pois, em todos estes casos, trata-se de uma ação danosa causada por um elemento externo à organização. Em um contraponto, há também a menção a ações danosas que podem ser causadas a partir de elementos internos, como fraude e roubo/vazamento de dados. De todo modo, como também há casos de fraudes e roubos/vazamentos causados por agentes externos, fica claro que a maior preocupação dos entrevistados está nos fatores externos.

As ações propostas pelos entrevistados para melhorar os níveis de maturidade em segurança da informação são apresentadas na tabela 5.

Tabela 5: Ações propostas para melhoria da segurança da informação.

Ação proposta	Número de ocorrências
Conscientização	24
Risk assessment	21
Plano de resposta a incidentes/exercícios de resiliência	16
Gestão de vulnerabilidades	11
Testes de invasão/testes de penetração	10
Consultoria/avaliação externa	5

Fonte: Elaborado pelo autor (2023)

A partir do exposto na tabela 5, é possível concluir que há duas grandes linhas de ação propostas pelos entrevistados para melhorar o nível de segurança da informação em uma organização: a conscientização dos colaboradores e a preparação para eventos reais.

No processo de conscientização, estão incluídas todas as ações de treinamento das equipes, não apenas aquelas ligadas às áreas de tecnologia, mas de todos os colaboradores da organização, incluindo as posições executivas mais altas (*C-Level* e Conselho de Administração). Esta prioridade foi descrita pelo Entrevistado 4: "*se eu tivesse um único dólar para investir em segurança, eu investiria em conscientização*".

A segunda grande linha de ação seriam as atividades que preparam uma organização para eventos reais. Nesta categoria, podemos incluir a execução de testes de invasão por empresas contratadas e a elaboração de planos de resposta a incidentes. Tais simulações estão em linha com o modelo de aprendizado prospectivo apresentado por Rezazade Mehrizi, Nicolini e Rodon (2022), que propõem o aprendizado a partir de incidentes futuros – neste caso, incidentes provocados, de maneira controlada, sob a coordenação da própria equipe responsável por segurança da informação.

5. DISCUSSÃO

Os resultados do processo de entrevista mostram a importância de se aperfeiçoar os métodos existentes para avaliação dos investimentos em SI, uma vez que não é possível afirmar com um razoável grau de assertividade que os recursos investidos estão atingindo o objetivo de reduzir os riscos a que a organização está exposta – e, pior do que isso, há a sensação por parte dos entrevistados de que este objetivo não está sendo atingido. Portanto, torna-se necessário complementar os *frameworks* existentes, que foram entendidos como um bom ponto de partida e como uma linguagem comum para alinhamento dos conceitos envolvidos no tema.

O primeiro aspecto a ser acrescentado seria uma análise detalhada dos riscos a que a organização está exposta. Esta etapa parte do princípio de que qualquer programa de SI deveria ser construído a partir dos riscos enfrentados pela organização (GRITZALIS et al., 2018) e é citada como uma das medidas no processo de implementação de um ISMS de acordo com a norma ISO 27001:2013 (ISO, 2013), mas não como uma etapa anterior à implementação de um ISMS. Por conta disso, este artigo propõe a análise de riscos enfrentados pela organização como o primeiro componente de um novo modelo de avaliação das medidas de SI implementadas, uma vez que os benefícios esperados após a implementação destas medidas estão relacionados à redução destes riscos. Ainda que não seja possível calcular o valor financeiro do risco, já que ainda haverá a dependência dos valores de SLE e ARO anteriormente mencionados, difíceis de estimar com precisão, o simples fato de conhecer os principais riscos já permitirá selecionar as medidas mais importantes dentre os inúmeros controles disponíveis e, ao menos qualitativamente, ter uma indicação sobre os efeitos das ações tomadas.

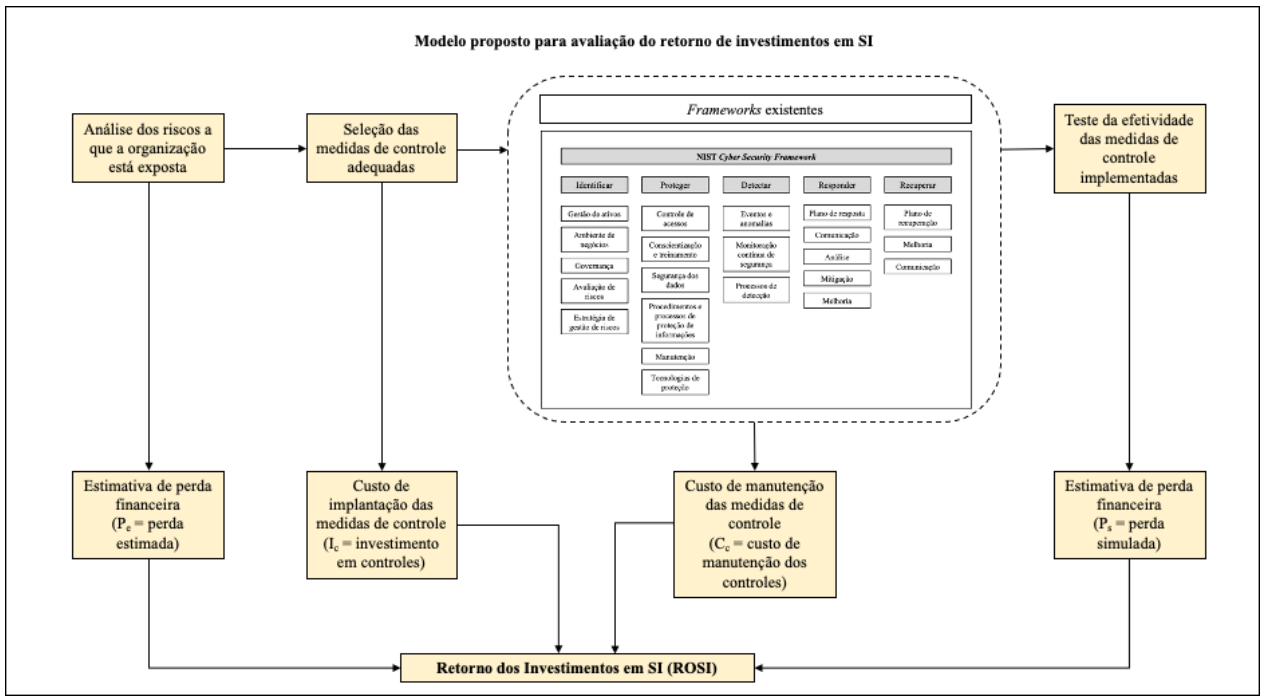
A segunda parte do modelo que proposto é composta pelas medidas técnicas e prescritivas dos *frameworks* existentes. Estas medidas servirão como a base comum para que o novo modelo dialogue com as implementações já existentes. Ao mesmo tempo, a análise prévia dos riscos permitirá que sejam selecionadas, prioritariamente, as medidas de controle mais relevantes para a organização. Assim, ao invés de uma implementação que siga uma receita previamente estabelecida e válida para qualquer contexto, o programa de SI, verdadeiramente, buscará tratar os riscos mais relevantes. Neste ponto, também pode-se fazer uma conexão com os aspectos financeiros, uma vez que é possível calcular, de maneira bastante precisa, o custo de implementação das medidas de SI.

A parte final refere-se ao teste de efetividade dos controles de SI. Esta etapa é essencial no modelo proposto neste artigo, pois permitirá identificar se as ações tomadas estão apresentando o resultado esperado na redução dos riscos. Ao utilizar métodos de engenharia do caos, como os propostos por McBride (2005) e por Benbya et al. (2020), será possível captar, inclusive, a influência do comportamento dos colaboradores da organização no programa de SI, um grande ponto de falha nos *frameworks* mais utilizados. A mesma metodologia usada para o cálculo de SLE e ARO no mapeamento dos riscos pode ser usada, neste ponto, para calcular os impactos causados por ineficiências nos controles de SI. De modo direto, portanto, é possível estimar o benefício financeiro como sendo o custo evitado entre as perdas esperadas na análise de risco e as perdas que efetivamente ocorreriam em incidentes simulados.

A partir do modelo proposto, portanto, há a possibilidade de fazer uma análise dos benefícios financeiros resultantes da implementação das medidas de SI em uma organização. Como já é possível calcular os custos envolvidos na implementação e na manutenção destas medidas, torna-se viável fazer os cálculos que permitem chegar ao ROSI (*Return on Security Investment*), definindo se há, de fato, algum retorno para a organização dos recursos aplicados em SI.

A figura 3 apresenta um esquema do modelo proposto, destacando em amarelo as etapas adicionais que devem ser incorporadas para complementar a avaliação a partir dos *frameworks* tradicionais. Estas etapas adicionais foram provenientes das informações coletadas durante o processo de entrevista, e contemplam as análises prévias que permitem realizar uma estimativa financeira do impacto que pode ser sentido pela organização em caso de materialização dos riscos a que está exposta, a seleção dos controles que gerarão os resultados mais importantes e a etapa posterior de mensuração da efetividade dos controles, garantindo que estão sendo eficientes na mitigação dos riscos.

Figura 3: Modelo proposto para avaliação do retorno de investimentos em SI



Fonte: Elaborado pelo autor (2023)

O fato de haver um modelo em que o retorno sobre o investimento em SI (ROSI) pode ser calculado como uma função da diferença entre o risco financeiro estimado para a organização caso as medidas de SI não sejam implementadas e o risco financeiro estimado a partir de testes realizados no ambiente após a implementação das medidas de SI permitirá que as organizações ajustem, com um grau elevado de precisão, os orçamentos a serem alocados para implementação e manutenção das medidas de controle. Além disso, será mais fácil selecionar, tendo como meta uma melhoria do ROSI, as medidas que devem ser tomadas para, efetivamente, reduzir o impacto das perdas que podem ser causadas por falhas na proteção do ambiente da organização – inclusive aquelas causadas por ações humanas.

6. CONCLUSÕES

6.1. CONTRIBUIÇÕES ACADÊMICAS

Este artigo teve sucesso em responder à pergunta de pesquisa proposta.

> (P1) Como deveria ser construído um modelo que realmente permitisse aferir se o programa de segurança da informação de uma organização é efetivo?

Foi mostrada a necessidade de uma complementação aos modelos de avaliação da SI de uma organização, incorporando aos métodos existentes algumas camadas que foram identificadas como falhas durante o processo de pesquisa, notadamente uma associação das medidas de controle aos riscos a que a organização está exposta e um processo de avaliação posterior que garanta a efetividade dos controles aplicados. O novo modelo proposto, além de completar as partes que faltam aos modelos disponíveis, também tornará possível estabelecer uma conexão com indicadores financeiros, levando a implementação de um ISMS a um ponto em que possa ser comparada com outros projetos da organização e, portanto, permitindo que executivos de outras especialidades possam ser envolvidos nas decisões estratégicas de SI, como se provou necessário na visão dos entrevistados.

As perguntas adicionais foram usadas como meio para alcançar as respostas para a pergunta de pesquisa e indicaram os caminhos que deveriam ser seguidos.

> (P2) Na visão dos executivos, os recursos (humanos e financeiros) investidos em segurança da informação estão, de fato, reduzindo os riscos a que estão expostas as organizações?

Foi identificado que, de fato, na visão dos executivos entrevistados, os investimentos em SI não estão alinhados à redução dos principais riscos enfrentados pelas organizações. Sendo assim, está havendo uma alocação ineficiente dos recursos, que não estão trazendo os benefícios esperados e deixam brechas para a ocorrência de incidentes de SI que podem prejudicar as operações. Essas brechas concentram-se, principalmente, na falta de conscientização dos colaboradores, que abre portas para os mais diversos tipos de fraudes e golpes, além de gerar falhas em processos que, por si só, podem se transformar em incidentes graves. A falha em processos de conscientização e treinamento vai ao encontro do que é apresentado na literatura, que indica que o treinamento dos colaboradores é um pilar importante na prevenção de incidentes de segurança da informação (KHANDO et al., 2021).

(P3) O que falta aos *frameworks* existentes para que possam ser usados como um guia para medir a efetividade dos programas de segurança da informação nas organizações?

Esta pergunta tornou possível identificar aquelas que os executivos entendem ser as principais falhas nos *frameworks* existentes, impedindo que sejam uma forma efetiva de avaliação do estágio das medidas de SI em uma organização. De acordo com este artigo, falta a estes *frameworks* um processo de priorização para assegurar que as medidas de controle a serem implementadas sejam, de fato, as mais relevantes para um dado contexto organizacional, e uma avaliação prática posterior das medidas implementadas, verificando se realmente conduziram a organização ao resultado esperado. Ou, nas palavras de alguns dos entrevistados, "*os frameworks atuais medem o meio, mas não medem o fim*". Deste modo, é possível concluir que as medidas prescritas são importantes e devem ser implementadas em organizações que queiram atingir bons níveis de segurança da informação, mas sua simples adoção, sem um processo mais amplo de verificação de sua eficácia e, sobretudo, sem uma verificação prévia das reais necessidades da organização, não é uma garantia de bons resultados na proteção dos ativos de informação.

6.2. IMPLICAÇÕES GERENCIAIS

O processo de entrevistas realizado para a elaboração deste artigo comprovou a questão apresentada na literatura acadêmica de que há uma grande dificuldade entre os gestores em saber se os gastos em SI estão servindo, efetivamente, para reduzir os riscos a que suas organizações estão expostas. Esta dificuldade traz um paradoxo, pois, ao mesmo tempo em que SI passou a fazer parte das prioridades da alta gestão, é difícil justificar para esta mesma alta gestão as necessidades de investimento e os benefícios gerados; afinal, se os próprios responsáveis pela solicitação e alocação destes recursos estão inseguros sobre seus resultados, como esperar que executivos que não dispõem de conhecimento técnico profundo sobre o tema – como, em geral, acontece nas diretorias e conselhos de administração de grandes empresas – os compreendam e os apoiem?

Diante deste fato, torna-se essencial não apenas poder traduzir os resultados dos investimentos em SI em uma linguagem que seja compreensível aos demais setores de uma organização, para que possam participar ativamente da elaboração dos orçamentos e do planejamento das ações, como também estabelecer parâmetros que permitam aos responsáveis pela gestão de SI saberem se os projetos e ações que estão desenvolvendo trarão os resultados esperados. Os *frameworks* de que

dispomos, infelizmente, não são ferramentas capazes de atender a estas duas demandas, trazendo a necessidade de que sejam complementados por outros processos.

Um dos entrevistados, durante o processo de elaboração deste artigo, trouxe uma excelente analogia para conceituar este problema. Disse ele: "*medir SI apenas usando um framework seria como medir a índole de um adolescente apenas olhando seu boletim escolar*" (Entrevistado 5). Ou seja, assim como o fato de ter boas notas na escola não implica, necessariamente, que um adolescente tenha bom relacionamento com os pais e familiares e nem que não seja um transgressor, a implementação de medidas técnicas listadas em qualquer um dos *frameworks* de SI não implica, necessariamente, que o nível de proteção seja adequado àquela organização. Em ambos os casos – as boas notas no boletim e a implementação correta dos *frameworks* – há indícios de que as ações estão seguindo em um bom curso, mas não é possível afirmar com plena certeza apenas com base nestes dados.

É necessário, portanto, agregar duas novas visões ao que está sendo feito. A primeira delas, anterior a qualquer medida técnica de SI, é conhecer os riscos a que a organização está exposta. Conhecer os riscos é uma medida prescritiva que faz parte de todos os *frameworks* existentes, mas todos eles a abordam sob o ponto de vista técnico, ou seja, indicam que a organização deveria conhecer os riscos técnicos em seu ambiente e os efeitos de sua materialização. O que este artigo propõe é que se vá além disso, vinculando os riscos técnicos aos danos que eles podem causar aos negócios da organização. Deste modo, a análise técnica das ameaças deve estar diretamente vinculada a uma estimativa financeira. Com isso, é possível apresentar ao corpo diretivo da organização uma estimativa das perdas que poderiam ocorrer em caso de materialização dos eventos adversos que se busca evitar, ou seja, apresenta-se de modo mais claro o custo que será evitado a partir das ações de SI.

A segunda visão a ser agregada aos *frameworks* existentes acontece depois da implementação das medidas técnicas. Isso porque, de um modo geral, trabalha-se com o fato de que basta implementar as medidas prescritas e a segurança já será suficiente, o que faz com que o foco de boa parte dos gestores responsáveis por SI seja, simplesmente, seguir a receita, sem se preocupar em saber se a receita está sendo, de fato, efetiva para resolver os problemas. Por isso, não é raro ver casos de organizações que implementam as medidas recomendadas nos *frameworks* e, ainda assim, sofrem incidentes graves de segurança. Isso nos mostra que não basta implementar as medidas de controle, é também preciso testá-las. É preciso simular incidentes no ambiente, forçar tentativas de invasão,

testar o comportamento dos colaboradores, não apenas os envolvidos na operação dos sistemas, mas também daqueles que não têm como função principal as tarefas técnicas de TI ou de SI – e que, na maior parte das vezes, não têm um conhecimento profundo em nenhum destes dois temas. Aqui, há a possibilidade de introduzir os conceitos de engenharia do caos. A geração de incidentes controlados a todo momento ajudará não apenas a melhorar a resiliência do ambiente, mas também a demonstrar onde estão as fragilidades nas medidas de controle, como o comportamento dos colaboradores interfere no cotidiano das ações de SI e, principalmente, qual seria o real impacto financeiro em caso de um incidente de segurança.

É possível perceber, portanto, que o teste da efetividade das medidas de SI traz uma dupla vantagem: além de permitir a correção de rumos e o direcionamento dos gastos para onde há mais necessidade, possibilita, também, a estimativa de perda financeira no caso de concretização dos riscos. Esta estimativa, quando comparada às perdas financeiras estimadas no levantamento inicial dos riscos, permite que se calcule o retorno dos investimentos em SI, se for considerado que o retorno foi o valor de redução de potenciais perdas.

Assim, a introdução de uma avaliação de riscos completa e robusta como ponto inicial do processo de gestão de SI e de processos de teste da resiliência das medidas implementadas permitirão que as ações e projetos atendam de forma bem mais efetiva o objetivo de reduzir os riscos a que as organizações estão expostas.

6.3. LIMITAÇÕES/DELIMITAÇÕES

Este artigo buscou trazer as visões de executivos e ex-executivos com vivência na área de SI, seja ela direta ou indireta. Com isso, buscou-se a experiência cotidiana dos entrevistados para extrair um modelo que atendesse aos principais problemas identificados por eles. Uma continuidade deste trabalho seria a validação do modelo proposto junto a outros executivos de mercado, utilizando o mesmo método de entrevistas semiestruturadas deste artigo. Assim, um novo grupo de executivos seria confrontado com o novo modelo proposto de avaliação de investimentos em SI e, a partir de suas impressões, o modelo pode ser complementado ou ajustado.

Em uma etapa seguinte, pode haver a validação deste novo modelo proposto junto a um público ampliado e que contenha, inclusive, executivos e ex-executivos que não tenham nenhum tipo de relação prévia com a gestão de SI. Para esta etapa, é possível usar métodos quantitativos, com um universo de respondentes bem maior.

Um outro ponto a ser explorado é a parte relativa aos cálculos de risco, tanto os anteriores à implementação de qualquer medida, quanto os posteriores. São estimativas que demandam um volume muito alto de informações e que ainda carecem de metodologias precisas, mas que, ao mesmo tempo, são parte essencial na conexão entre as medidas técnicas tomadas no âmbito de SI e os benefícios financeiros colhidos pela organização. O trabalho para desenvolver e refinar estas metodologias de cálculo e não foi avaliado neste artigo.

REFERÊNCIAS

ADAMS, W. C. Conducting Semi-Structured Interviews. Em: NEWCOMER, K. E.; HATRY, H. P.; WHOLEY, J. S. (Eds.). **Handbook of Practical Program Evaluation**. 4. ed. [s.l.] Jossey-Bass, 2015.

ALAVI, R.; ISLAM, S.; MOURATIDIS, H. An information security risk-driven investment model for analysing human factors. **Information & Computer Security**, v. 24, n. 2, p. 205–227, mar. 2016.

BENBYA, H. et al. Complexity and information systems research in the emerging digital world. **MIS Quarterly: Management Information Systems**, v. 44, n. 1, p. 1–17, 1 mar. 2020.

CICHY, P.; SALGE, T.; KOHLI, R. Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars. **MIS Quarterly**, v. 45, n. 4, 2021.

COHEN, D.; CRABTREE, B. **Qualitative Research Guidelines Project**. Disponível em: <http://www.qualres.org/HomeSemi-3629.html>.

COMPAGNA, L. et al. How to capture, model, and verify the knowledge of legal, security, and privacy experts: A pattern-based approach. **Proceedings of the International Conference on Artificial Intelligence and Law**, p. 149–153, 2007.

CRAM, W. A.; PROUDFOOT, J. G.; D'ARCY, J. When enough is enough: Investigating the antecedents and consequences of information security fatigue. **Information Systems Journal**, v. 31, n. 4, p. 521–549, 2021.

CULOT, G. et al. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. **The TQM Journal**, v. 33, n. 7, p. 76–105, 16 mar. 2021.

EISENGA, A.; JONES, T. L.; RODRIGUEZ, W. Investing in IT security: how to determine the maximum threshold. **International Journal of Information Security and Privacy**, v. 6, p. 75+, 2012.

FORTINET. **Global Threat Landscape Report - A Semiannual Report by FortiGuard Labs**. [s.l: s.n.]. Disponível em: <https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-2022-H1-threat-landscape.pdf>. Acesso em: 20 ago. 2022.

GORDON, L. A.; LOEB, M. P. Budgeting Process for INFORMATION SECURITY EXPENDITURES. **Communications of the ACM**, v. 49, n. 1, p. 121–125, jan. 2006.

GRITZALIS, D. et al. Exiting the Risk Assessment Maze: A Meta-Survey. **ACM Computing Surveys**, v. 51, n. 1, p. 11:1-30, jan. 2018.

HERATH, T.; HERATH, H.; BREMSER, WAYNEG. Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management. **Information Systems Management**, v. 27, n. 1, p. 72–81, 2010.

HOFFMAN, K. E. Digital Transformation, Accelerated: The pandemic has upended almost every aspect of Americans' lives, including how they bank. Which aspects of the COVID-fueled digital acceleration are here to stay? **ABA Banking Journal**, v. 112, n. 5, p. 20–23, set. 2020.

IBM SECURITY. **Cost of a Data Breach Report 2022**. [s.l: s.n.]. Disponível em: <https://www.ibm.com/downloads/cas/3R8N1DZJ>. Acesso em: 16 ago. 2022.

ISO. **Information Security Management Systems, ISO/IEC 27001:2013 (EN)**. , 2013.

ISO. **The ISO Survey of Management System Standard Certifications**. Disponível em: <https://www.iso.org/the-iso-survey.html>. Acesso em: 20 ago. 2022.

JAQUITH, A. **Security Metrics: Replacing Fear, Uncertainty, and Doubt**. 1. ed. [s.l.] Addison-Wesley Professional, 2007.

KALLIO, H. et al. **Systematic methodological review: developing a framework for a qualitative semi-structured interview guide**. **Journal of Advanced Nursing**Blackwell Publishing Ltd, , 1 dez. 2016.

KELVIN, LORD. I. Nineteenth century clouds over the dynamical theory of heat and light. **The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science**, v. 2, n. 7, p. 1–40, 1 jul. 1901.

KHANDO, K. et al. Enhancing employees information security awareness in private and public organisations: A systematic literature review. **Computers & Security**, v. 106, 1 jul. 2021.

KPMG. **KPMG 2021 CEO Outlook: Brasil**. [s.l: s.n.]. Disponível em: <https://assets.kpmg/content/dam/kpmg/br/pdf/2021/10/KPMG-2021-CEO-Outlook-Brasil.pdf>. Acesso em: 20 ago. 2022.

MCBRIDE, N. Chaos theory as a model for interpreting information systems in organizations. **Information Systems Journal**, v. 15, n. 3, p. 233-254–254, 1 jul. 2005.

MCKNIGHT, Z. S.; WARKENTIN, M. Information Security Compliance regarding Security Culture, Job Satisfaction, and Perceived Organizational Support. 2020.

MEIRELLES, F. S. **Uso de TI nas Empresas. Pesquisa Anual FGVCia. 33a Edição, 2022.** [s.l: s.n.]. Disponível em: <https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia_pes_ti_2022_-_relatorio.pdf>.

MIRTSCH, M.; KINNE, J.; BLIND, K. Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. **IEEE**

Transactions on Engineering Management, Engineering Management, IEEE Transactions on, IEEE Trans. Eng. Manage., v. 68, n. 1, p. 87–100, 1 fev. 2021.

MIRTSCH, M.; POHLISCH, J.; BLIND, K. **International Diffusion of the Information Security Management System Standard ISO/IEC 27001: Exploring the Role of Culture**. ECIS 2020 Proceedings. **Anais**...2020. Disponível em: <https://aisel.aisnet.org/ecis2020_rp>

NIST. **Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1**. Gaithersburg, MD: [s.n.]. Disponível em: <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

OREHEK, Š.; PETRIČ, G. A systematic review of scales for measuring information security culture. **Information and Computer Security**, v. 29, n. 1, p. 133–158, 2020.

OWUSU KWATENG, K.; AMANOR, C.; TETTEH, F. K. Enterprise risk management and information technology security in the financial sector. **Information & Computer Security**, v. 30, n. 3, p. 422–451, 1 jan. 2022.

PERNOT-LEPLAY, E. EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model? **Colorado Technology Law Journal**, v. 18, n. 1, p. 25–48, 1 jan. 2020.

RABII, A. et al. Information and cyber security maturity models: a systematic literature review. **Information and Computer Security**, v. 28, n. 4, p. 627–644, 2020.

REA-GUAMAN, A. M. et al. Modelos de Madurez en Ciberseguridad: una revisión sistemática. **Iberian Conference on Information Systems and Technologies, CISTI**, 2017.

REZAZADE MEHRIZI, M. H.; NICOLINI, D.; RODON, J. How Do Organizations Learn from Information System Incidents? A Synthesis of the Past, Present, and Future. **MIS Quarterly**, v. 46, n. 1, p. 531–590, 15 fev. 2022.

RUSSEL, D. **Como tornar a cibersegurança uma prioridade da liderança**. Disponível em: <https://tiinside.com.br/18/08/2022/como-tornar-a-ciberseguranca-uma-prioridade-da-lideranca/>. Acesso em: 18 out. 2022.

STAHL, B. C.; DOHERTY, N. F.; SHAW, M. Information security policies in the UK healthcare sector: a critical evaluation. **Information Systems Journal**, v. 22, n. 1, p. 77–94, jan. 2012.

UCHENDU, B. et al. Developing a cyber security culture: Current practices and future needs. **Computers and Security**, v. 109, 2021.

WEIXUN LI, W.; CHUNG MAN LEUNG, A.; YUE, W. T. WHERE IS IT IN INFORMATION SECURITY? THE INTERRELATIONSHIP AMONG IT INVESTMENT, SECURITY AWARENESS, AND DATA BREACHES. **MIS Quarterly**, v. 47, n. 1, p. 317–342, mar. 2023.

WU, A. Y. (1) et al. Information security ignorance: An exploration of the concept and its antecedents. **Information and Management**, v. 60, n. 2, 1 mar. 2023.

YAQOOB, T. et al. Framework for Calculating Return on Security Investment (ROSI) for Security-Oriented Organizations. **Future Generation Computer Systems**, v. 95, p. 754–763, 1 jun. 2019.

YASASIN, E.; SCHRYEN, G. **Requirements for it security metrics - an argumentation theory based approach**. 23rd European Conference on Information Systems, ECIS 2015. **Anais**...Association for Information Systems, 2015.

YOU, Y. et al. Advanced approach to information security management system utilizing maturity models in critical infrastructure. **KSII Transactions on Internet and Information Systems**, v. 12, n. 10, p. 4995–5014, 2018.

APÊNDICE A – CARTA CONVITE INDIVIDUAL AOS EXECUTIVOS ENTREVISTADOS

Assunto: Pesquisa Acadêmica - Mestrado

Prezado Executivo (a),

Como você está? Espero que esteja tudo bem.

Estou cursando o Mestrado em Gestão da Competitividade em TI na Fundação Getulio Vargas (EAESP/FGV) e, sob a orientação do Prof. Dr. Eduardo de Rezende Francisco, estamos conduzindo uma pesquisa para investigar a percepção de executivos das áreas de TI e de Segurança da Informação sobre como os investimentos em segurança da informação se refletem no nível de maturidade das organizações sobre o tema.

Você está sendo convidado a participar por sua atuação na área de TI/Segurança da Informação.

O processo se dará por meio de uma entrevista individual, conduzida por mim por meio de vídeo conferência, e deve durar cerca de 1 hora. A entrevista será gravada para transcrição e análise. Suas respostas serão confidenciais e usadas somente quando combinadas com outras respostas. As identidades dos respondentes não serão reveladas ou compartilhadas. Os únicos dados pessoais que serão coletados serão suas áreas de conhecimento, experiência profissional e formação acadêmica. Usaremos os resultados da pesquisa em publicação de artigos científicos, apresentação em conferências, webinars, postagens em sites, blogs, mídias tradicionais e mídias sociais.

Esperamos que se sinta à vontade para compartilhar suas próprias percepções sobre o tema, lembrando que sua participação é completamente voluntária.

Caso possa participar, por favor peço que me informe algumas opções de agenda para definirmos um horário que seja adequado para ambos.

Desde já, agradeço por sua ajuda.

Abraços,

Rafael Batista.