UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA APLICADA

SAULO MARQUES DE MORAIS SILVA

UMA METODOLOGIA PARA AVALIAÇÃO DE CUSTOS FINANCEIROS NA IMPLEMENTAÇÃO DE CONTROLES DE SEGURANÇA CIBERNÉTICA PARA PEQUENAS E MÉDIAS EMPRESAS

RECIFE - JUNHO/2024.

SAULO MARQUES DE MORAIS SILVA

UMA METODOLOGIA PARA AVALIAÇÃO DE CUSTOS FINANCEIROS NA IMPLEMENTAÇÃO DE CONTROLES DE SEGURANÇA CIBERNÉTICA PARA PEQUENAS E MÉDIAS EMPRESAS

Dissertação apresentada ao Programa de Pós-Graduação em Informática Aplicada da Universidade Federal Rural de Pernambuco como exigência parcial à obtenção do título de Mestre em Informática Aplicada.

Área de Concentração: Computação Inteligente e Modelagem

Orientador: Prof. Dr. Fernando Antônio Aires Lins
Coorientador: Prof. Dr. Robson Wagner Medeiros de Albuquerque

RECIFE - JUNHO/2024.

Dados Internacionais de Catalogação na Publicação
Sistema Integrado de Bibliotecas da UFRPE
Bibliotecário(a): Suely Manzi – CRB-4 809

S586m Silva, Saulo Marques de Morais.
Uma metodologia para avaliação de custos financeiros na implementação de controles de segurança cibernética para pequenas e médias empresas / Saulo Marques de Morais Silva. – Recife, 2024.
137 f.; il.

Orientador(a): Fernando Antônio Aires Lins.
Co-orientador(a): Robson Wagner Medeiros de Albuquerque.

Dissertação (Mestrado) – Universidade Federal Rural de Pernambuco, Programa de Pós-Graduação em Informática Aplicada, Recife, BR-PE, 2024.

Inclui referências e apêndice(s).

1. Cibernética - Medidas de segurança . 2. Tecnologia da informação - Medidas de segurança. 3. Controle de custo. 4. Empresas - Redes de computadores - Medidas de segurança I. Lins, Fernando Antônio Aires, orient. II. Albuquerque, Robson Wagner Medeiros de, coorient. III. Título

CDD 004

SAULO MARQUES DE MORAIS SILVA

UMA METODOLOGIA PARA AVALIAÇÃO DE CUSTOS FINANCEIROS NA IMPLEMENTAÇÃO DE CONTROLES DE SEGURANÇA CIBERNÉTICA PARA PEQUENAS E MÉDIAS EMPRESAS

Dissertação julgada adequada como requisito parcial para obtenção do título de Mestre em Informática Aplicada (área de concentração: Computação Inteligente e Modelagem) pelo Programa de Pós-Graduação em Informática Aplicada da Universidade Federal Rural de Pernambuco.

Aprovado em: 27/05/2024.

BANCA EXAMINADORA

Profº Dr. Fernando Antônio Aires Lins (Orientador)
Universidade Federal Rural de Pernambuco

Profº Dr. Robson Wagner Medeiros de Albuquerque (Coorientador)
Universidade Federal Rural de Pernambuco

Profº Dr. George Augusto Valença dos Santos (Examinador Interno)
Universidade Federal Rural de Pernambuco

Profº Dr. Rodrigo Nonamor Pereira Mariano de Souza (Examinador Externo)
Universidade Federal Rural de Pernambuco

AGRADECIMENTOS

Agradeço à Universidade Federal Rural de Pernambuco pela oportunidade que me proporcionou ao realizar este curso. Agradeço também a todas as professoras e professores do PPGIA, em especial àqueles que contribuíram diretamente com o meu desenvolvimento durante esta jornada de conhecimento.

Agradeço imensamente ao meu orientador, o Profº Dr. Fernando Aires e ao meu co-orientador, o Profº Dr. Robson Medeiros, aos quais tenho grande carinho, respeito e admiração. Sem eles, este trabalho não teria sido realizado. Obrigado por todo o conhecimento repassado, por toda a paciência utilizada, além da credibilidade depositada em meus esforços ao longo destes anos de trabalho e pesquisa.

Agradeço ao Profº Dr. Rodrigo Nonamor, que além de me incentivar e respaldar este trabalho, ajudou-me bastante em todos os processos necessários junto à universidade. Agradeço também ao professor George Valença, por todo o conhecimento repassado ao longo deste curso.

Agradeço aos meus amados pais, José e Cléia, e também a minha amada esposa, Fernanda Ferro, por compartilharem o dia-a-dia comigo e por me darem o apoio necessário para a finalização deste curso. Amo vocês.

Agradeço a todos os meus colegas de curso, mas em especial a Guilherme Henrique, Paulo Ramos e João Albano, este último agradeço também pela grande parceria e amizade construída ao longo do curso. Não poderia deixar de fora todos os colegas de profissão, que de alguma forma repassaram seus conhecimentos sempre que possível em atividades diversas, mas em especial, agradeço ao meu amigo Daniel Moura, que muito me ensinou desde os tempos de estagiário.

Agradeço ao meu tio Alberto, por sempre me incentivar a estudar. Agradeço também ao meu primo Marsiron, por me incentivar e acreditar em meu sucesso.

Agradeço a todos os meus amigos e amigas de trabalho, que de maneira relevante compartilharam comigo os seus conhecimentos e ouviram-me falar por várias horas, de muito bom grado sobre os assuntos deste trabalho. Por fim, agradeço aos meus amigos pessoais, que em vários momentos motivaram-me para que eu tivesse sucesso ao final deste curso. Em especial, agradeço ao meu amigo Ivson Alberto, por toda a ajuda em alguns momentos deste trabalho, além de sempre me incentivar e torcer para o meu sucesso.

Resumo

Atualmente, as organizações contam com a Tecnologia da Informação para realizar suas atividades. As informações não são mais apenas físicas, mas também digitais, e uma quantidade considerável de dados flui através das redes de computadores. Estes dados são armazenados localmente e em recursos de Computação em Nuvem. Infelizmente, incidentes cibernéticos como acesso não autorizado, violação de dados, exposição de dados e indisponibilidade de serviços tornaram-se comuns nos últimos anos. Para evitar tais problemas, as organizações precisam melhorar o seu nível de segurança cibernética e da informação. Porém, essa melhoria exige diversos investimentos, inclusive financeiros. Diante deste contexto, este trabalho propõe uma metodologia, baseada em processo aderente com a notação *Business Process Management Notation* (BPMN), para avaliar o investimento financeiro necessário para melhorar a segurança cibernética e da informação do ciberespaço de pequenas e médias empresas. A metodologia proposta é composta por vários subprocessos, atividades e eventos que resultam em um conjunto de ações que visa implementar controles de segurança cibernética, alcançando um nível de maturidade robusto e confiável, buscando sempre a conformidade com normas técnicas e *frameworks* de segurança padrões mundialmente reconhecidos. A descrição dos subprocessos, atividades e eventos propostos nesta metodologia auxilia a reprodutibilidade do estudo em ambientes cibernéticos genéricos. A metodologia proposta foi analisada através de um experimento em um ambiente cibernético real, onde se mediu o investimento necessário para que uma determinada organização atinja o nível de segurança desejado dentro de suas expectativas ou restrições financeiras, considerando a conformidade da organização com um *framework* de segurança amplamente adotado. A execução deste experimento possibilitou verificar não apenas a adequabilidade da metodologia proposta, mas permitiu gerar resultados que podem ser usados pela gestão da organização para o planejamento da melhoria de segurança desejada.

Palavras-chave: Cibersegurança; Segurança cibernética; Segurança da informação; Modelo e Notação de Processo (BPMN); Custos; Controles de segurança cibernética.

Abstract

Nowadays, organizations rely on Information Technology to carry out their activities. Information is no longer physical but digital, and a considerable amount of data flows through computer networks, stored locally and in Cloud Computing resources. Unfortunately, cyber incidents such as unauthorized access, data breaches, data exposure, and service unavailability have become common in recent years. To avoid such problems, organizations need to improve their cybersecurity level. However, this improvement requires various investments, including financial. Given this context, this work proposes a methodology based on processes established in Business Process Management Notation (BPMN) to evaluate the financial investment necessary to improve cyber and information security in the cyberspace of small and medium-sized companies. The proposed methodology is composed of several sub-processes, activities, and events that result in a set of actions that aim to implement cybersecurity controls, reaching a robust and reliable level of maturity, always seeking compliance with technical standards and security frameworks globally recognized standards. The description of the sub-processes, activities, and events proposed in this methodology helps the reproducibility of the study in generic cyber environments. The proposed methodology was analyzed through an experiment in a real cyber environment, where it measured the investment necessary for a given organization to achieve the desired level of security within its expectations or financial restrictions, considering the organization's compliance with a widely adopted security framework. The execution of this experiment made it possible to verify not only the suitability of the proposed methodology, but also generate results that can be used by the organization's management to plan the desired security improvement.

Keywords: Cybersecurity; Information security; Process Model and Notation; Costs; Cybersecurity controls.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

Abreviação	**Significado**
ABNT	Associação Brasileira de Normas Técnicas
AVA	Ambiente Virtual de Aprendizagem
BP	*Business Process*
BPMN	*Business Process Model and Notation*
C2M2	*Cybersecurity Capability Maturity Model*
CC	Custo do Controle
CEO	*Chief Executive Officer*
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CHW	Custo com *Hardware*
CIS	*Center for Internet Security*
CISO	*Chief Information Security Officer*
CPD	Centro de Processamento de Dados
CPS	*Cyber-physical system*
CRH	Custo com Recurso Humano
CSC	*Cyber Security Control*
CSG	Custo da Salvaguarda
CSW	Custo com *Software*
ECISC	Estimativa de Custo para Implementação de Segurança Cibernética
FDC	Fator de Distribuição de Contexto
FINRA	*Financial Industry Regulatory Authority*
FQ	Fator de Qualidade

HIPAA	*Health Insurance Portability and Accountability Act*
IEC	*International Electrotechnical Commission*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
IoT	*Internet of Things*
ISO	*International Organization for Standardization*
LGPD	Lei Geral de Proteção de Dados
MFA	*Multi-Factor Authentication*
NBR	Normas Brasileiras Regulamentadoras
NIST	*National Institute of Standards and Technology*
OWASP	*Open Worldwide Application Security Project*
OWASP	*Open Worldwide Application Security Project*
PCI-DSS	*Payment Card Industry Data Security Standard*
PDCA	*Plan-Do-Check-Act*
PME	Pequenas e Médias Empresas
ROI	Retorno sobre o Investimento
SGSI	Sistema de Gestão de Segurança da Informação
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
USB	*Universal Serial Bus*

SUMÁRIO

Capítulo 1

"Se a educação sozinha não transforma a sociedade, sem ela tampouco a sociedade muda."
(Paulo Freire).

1 INTRODUÇÃO

Este capítulo tem o objetivo de apresentar o contexto deste trabalho, a motivação, o problema de pesquisa e os objetivos. Por fim, é descrita a estruturação do trabalho considerando os próximos capítulos.

1.1 Contexto

Nos últimos anos, as organizações vêm acompanhando com interesse o crescimento do número e complexidade dos ataques cibernéticos. O Cert.br acompanha e disponibiliza a quantidade de incidentes no Brasil desde 1999. Desde 2014, só o Cert.br recebeu mais de 500.000 notificações de incidentes todos os anos, com destaque para o ano de 2019, com mais de 700 mil registros (CERT.BR, 2023).

De forma geral, é sabido que estes riscos aumentaram nos últimos anos (SIMON e OMAR, 2020; SABILLON *et al.*, 2017). Ataques cibernéticos como roubo, indisponibilidade, violação e destruição de dados são alguns exemplos de incidentes cibernéticos (UDROIU DUMITRACHE e SANDU, 2022; ROJAS *et al.*, 2022). Este aumento é explicado parcialmente pelo crescimento do uso de recursos computacionais para a realização de atividades pessoais e profissionais (BAR-HAIM *et al*., 2023; MOREIRA *et al.*, 2021; BASHOFI e SALMAN, 2022), principalmente atividades realizadas a partir da modalidade de trabalho home office (BORKOVICH e SKOVIRA, 2020).

Um ato muito comum entre usuários domésticos, e até mesmo administradores de sistemas inexperientes, são contas padrão habilitadas, que facilitam a intrusão de atacantes, tornando todo o ecossistema vulnerável (TALL, ZOU e WANG, 2021). Os números referentes aos incidentes de segurança são tão alarmantes e crescentes que os especialistas na área de segurança dão como certo que em algum momento os seus sistemas serão atacados (VALENZUELA, 2018a; VALENZUELA, 2018b).

Dito isto, surge o desejo de se proteger ciberneticamente em relação aos incidentes cibernéticos cada vez mais comuns, juntamente com o desejo de se saber financeiramente qual o recurso necessário para se obter segurança cibernética. Para responder a este questionamento, a seguinte questão de pesquisa foi gerada: “Como estimar os custos financeiros iniciais para implementar controles de segurança cibernética em ambientes cibernéticos genéricos?”

Apesar da maioria das empresas manterem um ambiente controlado e possuírem controles de segurança em seus espaços corporativos, as organizações de modo geral não estavam preparadas para a mudança abrupta que ocorreu durante a pandemia da COVID-19, com relação ao trabalho a partir de casa (GANAPATI, FRANCO e LE, 2023).

Durante e depois da pandemia da COVID-19, foi possível verificar um aumento significativo de trabalho na modalidade home office (CANEDO *et al*., 2022; KAMTHAN, *et al*., 2023), e atrelado a isto o aumento significativo de documentos sigilosos sendo

transferidos por redes de computadores e armazenados por servidores virtuais (através da Computação em Nuvem), pendrives e computadores pessoais (BORKOVICH e SKOVIRA, 2020).

É possível afirmar que parte expressiva deste contexto veio para ficar. Organizações irão usar recursos computacionais de forma cada vez mais expressiva, e a segurança da informação deverá atuar para que medidas preventivas e mitigatórias estejam em execução para minimizar ou mesmo evitar possíveis perdas. As normas técnicas e padrões de segurança estabelecidos no mercado fornecem maneiras de gerenciar e aplicar medidas preventivas e corretivas para que as organizações possam melhorar o nível de segurança cibernética (DJEBBAR e NORDSTRÖM, 2023).

Na pesquisa desenvolvida nesta dissertação, foi constatado que há vários estudos sobre custos e segurança, porém, grande parte dos estudos estão focados nos custos energéticos, como os estudos de Kansal *et al.* (2010), Tauber e Bhatti (2012a) e Tauber, Bhatti e Yi Yu (2012b). Também foi possível verificar vários estudos com foco apenas na segurança, onde se busca um resultado de quão seguro um sistema é (BARRÈRE *et al.*, 2020; BODEI *et al.*, 2020; CHANG, SON e CHOI, 2020; IMRAN, 2012; LUNA *et al.*, 2011; SCALA e GOETHALS, 2011).

Não é uma tarefa trivial associar os custos sobre as demandas dos controles de segurança cibernética, e ainda mais difícil justificar os investimentos necessários para melhorar a segurança dos ativos de uma organização de modo geral (DUTTA e AL-SHAER 2019b; FRANCO, GRANVILLE e STILLER, 2023; IVKIC *et al.*, 2022; LEE 2021; KALDEREMIDIS *et al.*, 2022).

Restrições orçamentárias dificultam os investimentos em controles de cibersegurança para proteger os ativos das organizações, especialmente nas Pequenas e Médias Empresas (PMEs), que usualmente acreditam que têm poucas chances de serem alvo de ataques cibernéticos. Isto faz com que as PMEs não tenham um plano de segurança cibernética estabelecido, e, com isso, sejam um dos principais alvos de ataques cibernéticos no mundo, onde os ataques bem-sucedidos têm maior incidência do que em empresas que contenham uma estratégia de segurança cibernética bem definida (FRANCO GRANVILLE e STILLER, 2023).

Neste contexto, um desejo comum das organizações é entender e quantificar o investimento necessário para a melhoria do nível de cibersegurança. É sabido que existem empresas de diversos portes, e que algumas terão mais disponibilidade do que outras para investir recursos significativos, inclusive financeiros, nesta melhoria. Contudo, existe uma

lacuna no estado atual da área referente a avaliação do custo financeiro deste tipo de melhoria em organizações de pequeno e médio porte.

Desta forma, o objetivo principal deste trabalho é a proposição de uma metodologia, baseada em processo de negócio, para o levantamento e definição do custo financeiro associado à implementação de ações relacionadas à cibersegurança para pequenas e médias empresas. Mesmo tendo como foco principal as PMEs, de modo geral a metodologia proposta poderá ser utilizada em ambientes cibernéticos genéricos, incluindo os ambientes cibernéticos de grandes empresas, instituições públicas e órgãos governamentais.

Durante a proposição de adequação do espaço cibernético quanto ao nível de maturidade buscado em segurança, algum *framework* de cibersegurança estabelecido ou alguma norma técnica padrão de segurança deverá ser escolhida e determinada para a futura implantação dos controles de segurança, tais como as as ISOs 27002, 27017 e 27032 ou o *NIST*, *CIS v.8* e *C2M2*. Esta metodologia baseada em processos descreverá as atividades necessárias, através de *BPMN* (BOCCIARELLI, *et al.*, 2019; CHINOSI e TROMBETTA, 2011), para o cálculo do investimento necessário, adotando o uso do *framework* de cibersegurança *CIS v*8 como exemplo prático.

1.2 Motivação

Um dos principais desafios de uma organização ao implementar controles de segurança cibernética para adequação de seu estado de maturidade atual de segurança para um estado de maturidade em conformidade com algum padrão de segurança já estabelecido é o fato de não poder estimar os custos financeiros necessários para obter este nível de proteção e seguridade dos dados antes mesmo de iniciar de fato a implementação destes controles (DUTTA e AL-SHAER, 2019a).

Infelizmente, muitas organizações iniciam os seus processos de adequação do estado de maturidade em segurança antes de elaborar um projeto robusto quanto aos recursos necessários exigidos por cada norma técnica, ou *frameworks* de segurança cibernética estabelecidos no mercado. Este problema, em geral, acaba gerando desperdício de recursos financeiros, recursos computacionais e recursos humanos durante todas as fases do processo.

É importante que as empresas, especialmente as pequenas e médias, não desistam no meio do processo de uma implementação de controles de segurança cibernética devido a escassez de recursos advindos de gastos demasiados em apenas um controle ou uma

salvaguarda específica, não tendo o cuidado necessário com todos os dispositivos exigidos por uma norma técnica ou um *framework* de cibersegurança.

As pequenas e médias empresas, considerando todos os tipos de segmento de mercado, representam 7 dos 10 postos de trabalho em mercados emergentes. No Brasil, mais de 80% dos postos de trabalho criados em 2023 foram das micro, pequenas e médias empresas (ONU News, 2024), sendo notória a importância deste tipo de empresa para a economia do país.

O grande problema deste dado, é que se tratando de espaço cibernético, as pequenas e médias empresas estão em um nível de maturidade geralmente abaixo do considerado minimamente seguro. Grande parte destas empresas não possuem um número mínimo de controles de segurança para proteger os seus ativos de cibercriminosos. Além disso, muitas vezes estes controles são implementados de maneira individual e isolada (PAWAR e PALIVELA, 2022), sem perceber o conjunto de soluções que as normas técnicas exigem. Os controles de segurança em sua maioria se complementam, e o conjunto de ações é que torna um ambiente cibernético mais seguro contra vários tipos de ataques cibernéticos.

Para decisões relacionadas à quantidade de recursos financeiros necessários para a implementação de controles de segurança cibernética, é importante compreender as possíveis perdas e impactos negativos que uma organização pode sofrer após receber um ataque cibernético.

Alguns trabalhos buscam estimar os custos necessários para a implantação de controles de segurança em um ambiente cibernético de segmento específico (indústria, hospital, cenários de *Cloud Computing*), além de determinarem a norma técnica ou o *framework* utilizado para adequação a um padrão estabelecido, deixando o estudo direcionado e com uma aplicação restrita (KHAJOUEI, KAZEMI e MOOSAVIRAD, 2016; KOBEZAK *et al.*, 2018 e LEE, JEON e LEE B., 2019).

No entanto, este trabalho é motivado por uma busca em atender ao maior número possível de ambientes cibernéticos, tornando-se uma metodologia genérica, acessível e de fácil compreensão, inclusive para os tomadores de decisão, que ainda hoje apresentam dificuldades para entender as justificativas sobre o investimento em recursos de segurança cibernética e da informação.

1.3 Problema de Pesquisa

Diante do exposto (Seções 1.1 e 1.2) e na revisão tradicional realizada neste trabalho (detalhado no Capítulo 3), foi observado que, durante a implementação de controles de

segurança cibernética em pequenas e médias empresas, falta uma referência que sistematize uma abordagem para calcular os recursos financeiros necessários em um processo de implementação ou adequação do estado de maturidade atual em segurança cibernética para um estado de maturidade em conformidade com padrões estabelecidos.

Para responder esta lacuna nos trabalhos encontrados, objetiva-se responder a seguinte pergunta: como calcular os recursos financeiros necessários para implementar controles de segurança cibernética nas PMEs, considerando a variedade de normas técnicas e *frameworks* de segurança cibernética existentes no mercado?

1.4 Objetivos

1.4.1 Objetivo Geral

O objetivo geral desta metodologia é a proposição de um processo, baseado em *BPMN*, para análise e cálculo dos custos financeiros relacionados à implementação de controles de cibersegurança em pequenas e médias empresas, sistematizado e repetível, que auxilie as organizações na obtenção da conformidade com as normas técnicas e/ou os *frameworks* de segurança cibernética reconhecidos mundialmente.

1.4.2 Objetivos Específicos

Para atingir o objetivo geral foram definidos os seguintes objetivos específicos:

- Guiar equipes e profissionais de segurança da informação no levantamento dos requisitos necessários durante a análise para implementar controles e suas respectivas salvaguardas de segurança cibernética.
- Auxiliar equipes e profissionais de segurança da informação no cálculo dos recursos financeiros necessários para atender os requisitos levantados no objetivo anterior.
- Elevar o nível de maturidade da segurança cibernética das PMEs, através do cumprimento das medidas de segurança constantes nas normas técnicas e nos *frameworks* de cibersegurança.

1.5 Contribuições

A principal contribuição deste trabalho é a proposição de uma metodologia baseada em processos para estimar os custos financeiros na implementação de controles de segurança cibernética em ambientes cibernéticos distintos de pequenas e médias empresas. Adicionalmente, algumas contribuições relacionadas incluem:

- Permitir ajustes e diminuição de recursos financeiros de um mesmo ambiente cibernético, mantendo a implementação dos mesmos controles e salvaguardas exigidas pelas normas técnicas ou *frameworks* de segurança utilizados;
- Possibilitar que tomadores de decisão possam acompanhar e entender melhor os processos que justificam os investimentos necessários para garantir a segurança cibernética;
- Incentivar pequenas e médias empresas a construírem um ambiente cibernético mais seguro, demonstrando que é possível obter a seguridade cibernética com um custo customizado e muitas vezes abaixo do esperado.

1.6 Estruturação do Trabalho

Além deste capítulo, esta dissertação está estruturada da maneira que se segue.

O Capítulo 2 descreve a fundamentação teórica, importante para o entendimento do trabalho proposto, pois detalha os conceitos das normas técnicas, dos *frameworks* de segurança cibernética, da notação de modelagem de processo de negócio (*BPMN*) e apresenta ainda conceitos sobre custos.

O Capítulo 3 descreve a revisão tradicional realizada sobre os trabalhos relacionados à temática desta dissertação. Esta revisão é importante para melhor entender a importância da contribuição desta dissertação frente ao atual estado da arte da área.

O Capítulo 4 apresenta a principal contribuição deste trabalho, que é uma metodologia baseada em processos para levantamento e análise de custos financeiros na implementação de controles de segurança cibernética e da informação para pequenas e médias empresas.

O Capítulo 5 busca avaliar a metodologia baseada em processos proposta através da execução de um experimento prático, em um ambiente cibernético real, tendo como resultado dois possíveis cenários, com custos distintos, onde o segundo cenário gerou uma economia de 45,21% em relação ao primeiro. Isto ilustra a possibilidade de tomada de decisão que a empresa pode ter a partir da aplicação da metodologia proposta nesta dissertação.

Por fim, o Capítulo 6 apresenta as conclusões e trabalhos futuros desta dissertação.

Capítulo 2

"Uma mente que se abre a uma nova ideia jamais voltará ao seu tamanho original."
(Albert Einstein).

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta os conceitos básicos necessários para o entendimento deste trabalho. São apresentados aqui os conceitos e definições sobre segurança da informação, segurança cibernética, das normas técnicas, dos *frameworks* de segurança cibernética e da informação, da notação de modelagem de processo de negócio (*BPMN*), além de conceitos sobre gerenciamento de custos.

2.1 Segurança da Informação

A segurança da informação é baseada em três pilares, que buscam preservar a confidencialidade, integridade e disponibilidade dos dados (ABNT NBR ISO/IEC 27001, 2022).

Segundo a IBM (s.d, Online), “a segurança da informação é a proteção de informações importantes de uma organização, arquivos e dados digitais, documentos em papel, mídia física, até mesmo a fala humana contra acessos, divulgações, alterações ou usos não autorizados”.

2.2 Segurança Cibernética

A segurança cibernética é baseada em cinco funções simultâneas e contínuas, que buscam identificar, proteger, detectar, responder e recuperar os dados digitais (NIST, 2018). A utilização dessas cinco funções em conjunto, traz a robustez necessária para se obter um ambiente cibernético minimamente seguro.

Segundo a IBM (s.d, Online), “a segurança cibernética refere-se a qualquer tecnologia, medida ou prática para prevenir ataques cibernéticos ou mitigar seu impacto”. De acordo com a Cisco Systems (s.d, Online), “a segurança cibernética é a prática de proteger sistemas, redes e programas de ataques virtuais”.

2.3 Normas Técnicas e *Frameworks* de Segurança Cibernética

A **Organização Internacional de Padronização** (*International Organization for Standardization*) e a **Comissão Eletrotécnica Internacional** (*International Electrotechnical Commission*), ***ISO/IEC***, tem como objetivo criar normas que facilitem o comércio e promovam boas práticas de gestão e avanço tecnológico, além de disseminar conhecimentos (INMETRO, 2024, Online).

As **normas *ISO/IEC*** que tratam de **segurança cibernética e da informação** são as da família **27000**, e cada norma desta família traz um segmento diferente das diversas áreas existentes em segurança, tais como: gestão, implementação de controles, gestão de riscos, computação em nuvem, segurança cibernética e afins.

Esta série de normas **estabelece padrões** que garantem que seus sistemas de TI, infraestrutura técnica e processos sejam **seguros, eficientes e alinhados** com as melhores

práticas (*ISO*, 2024, Online). As normas técnicas e os *frameworks* de segurança cibernética utilizam **controles e salvaguardas** para determinarem ações que implementam a segurança de fato.

Os **controles** podem ser entendidos como os menus que separam as ações de segurança por área (exemplo: tratamento de dados, infraestrutura de rede, segurança do *hardware*, segurança do *software*, treinamento de pessoal, etc.).

Já as **salvaguardas** são as ações que estão contidas nos controles, ou seja, nos menus que concentram várias ações de segurança. As salvaguardas trazem a descrição das atividades e dos dispositivos necessários para que a implementação de segurança cibernética ou da informação de fato aconteça.

A norma brasileira regulamentadora **NBR *ISO/IEC* 27001, foi desenvolvida com o intuito de prover um modelo de Sistema de Gestão de Segurança da Informação (SGSI) que visa estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um sistema de gestão** (ABNT *ISO/IEC* 27001, 2022). Esta norma é baseada no modelo "*Plan-Do-Check-Act*" (*PDCA*) que visa a melhoria contínua de todos os processos; dessa forma, o SGSI de uma empresa será atualizado e aprimorado conforme o passar do tempo.

Ainda segundo a ABNT NBR *ISO/IEC* 27001 (2022), **um SGSI é projetado para assegurar a seleção de controles de segurança adequados para proteger os ativos de informação e propiciar confiança às partes interessadas**. Esta norma é voltada para a gestão da organização, estando mais relacionada às estratégias a serem seguidas em um modelo de gestão de segurança da informação de alto nível, mais generalista.

A **ABNT NBR *ISO/IEC* 27002** é uma norma técnica que fornece um conjunto de referência de controles genéricos de segurança da informação, incluindo orientação para implementação (ABNT NBR *ISO/IEC* 27002, 2022). Esta norma é amplamente utilizada para a implementação de controles de segurança da informação, sendo estes controles divididos por temas, especificando a área do controle, tornando o gerenciamento dos controles mais específico e direcionado a setores específicos da organização.

Basicamente, a norma é composta por objetivos, controles e diretrizes. **Esta abordagem tem um objetivo mais técnico, contendo informações relevantes para o SGSI de uma organização, descrevendo os tipos de controle (controles organizacionais, controle de pessoas, controles físicos e controles tecnológicos), o objetivo destes controles (por que convém que o controle seja implementado) e as diretrizes (como o controle deve ser implementado).**

A norma **ABNT NBR *ISO/IEC* 27017** traz uma documentação que aborda mecanismos de segurança voltados para a **computação em nuvem**. Esta norma tem como base a *ISO* 27002:2016, utilizando 37 controles desta norma e adicionando mais 7 controles novos específicos para computação em nuvem.

Estes novos controles trazem informações quanto às responsabilidades compartilhadas em um ambiente de nuvem, contrato entre as partes, proteção e separação do ambiente virtual entre clientes diferentes, requisitos para melhoria das máquinas virtuais, operações administrativas em um ambiente de nuvem, capacitação dos clientes de ambiente em nuvem e sobre o alinhamento do gerenciamento de segurança para redes virtuais e físicas (BRIASMITATMS, 2023, Online).

A norma **NBR *ISO/IEC* 27032** fornece orientação técnica para lidar com riscos comuns de **segurança cibernética** (ABNT NBR *ISO/IEC* 27032, 2015). Esta norma aborda aspectos relevantes sobre as diferenças e as especificidades dos ambientes cibernéticos que compõem a Internet.

Essa diferença entre os espaços cibernéticos cria um cenário de grande desafio aos profissionais de segurança cibernética e os usuários de modo geral da Internet para manterem seus sistemas e ambientes seguros. **A norma fornece orientação técnica para lidar com os riscos de segurança cibernética referentes a ataques de engenharia social, hackerismo, proliferação de *software* malicioso, spywares e *softwares* potencialmente indesejados.**

Em alinhamento com as normas técnicas, os ***frameworks*** são bastante utilizados por profissionais de segurança cibernética e da informação para determinar um **nível de segurança adequado e atualizado quanto às ameaças existentes no ciberespaço**.

O ***NIST*** é um dos mais conhecidos *frameworks* de cibersegurança no mundo. Este *framework* foi desenvolvido nos Estados Unidos da América em uma ação conjunta e colaborativa entre governo, indústria e academia (*NIST*, 2018). **Este *framework* traz consigo uma estrutura das áreas que compõem a segurança cibernética, que são Identificar, Proteger, Detectar, Responder e Recuperar.**

Estas cinco funções, quando analisadas em conjunto, fornecem uma visão estratégica de alto nível do ciclo de vida do gerenciamento de riscos de segurança cibernética. Esta divisão simplifica o processo de analisar e adequar um ambiente cibernético com ações de segurança que elevam o nível de maturidade de cibersegurança.

O ***C2M2*** também é um *framework* desenvolvido nos Estados Unidos da América por empresas dos setores públicos e privados, patrocinado pelo Departamento de Energia dos Estados Unidos (*C2M2*, 2021). Este *framework* é um modelo de maturidade em segurança

cibernética baseado no ***NIST***, que **se concentra na implementação e gestão de práticas de segurança cibernética associadas aos ativos de informação, tecnologia da informação e tecnologia de operações e os ambientes em que operam.**

A ***OWASP*** é uma fundação sem fins lucrativos que trabalha para melhorar a segurança do *software* (*OWASP*, s.d., Online). **A *OWASP* disponibiliza várias ferramentas e documentações referentes à segurança para aplicativos, com o intuito de que qualquer indivíduo ou empresa possa conceber, desenvolver, adquirir, operar e manter aplicativos e *softwares* confiáveis**. A documentação mais utilizada e conhecida da comunidade é o *OWASP Top 10*, reconhecido mundialmente por desenvolvedores como uma documentação que contribui para uma codificação mais segura de aplicativos (*OWASP*, 2021).

O ***CIS* v8** é um reconhecido *framework* de cibersegurança no mundo.

> Os controles CIS refletem o conhecimento combinado de especialistas de todas as partes do ecossistema (empresas, governos, indivíduos), com todas as funções (times de respostas e analistas de ameaças, tecnólogos, operadores e defensores de tecnologia da informação (TI), pesquisadores de vulnerabilidades, fabricantes de ferramentas, provedores de soluções, usuários, formuladores de políticas, auditores, etc.) e em muitos setores (governo, poder, defesa, finanças, transporte, academia, consultoria, segurança, TI, etc.), que se uniram para criar, adotar e apoiar estes controles. (CIS Controls, 2021, p. 1).

Este *framework* disponibiliza um *check-list* com ações que efetivam os procedimentos a serem implementados em um ambiente cibernético. **O conjunto de ações descritos no *CIS* torna o ambiente adequado e em conformidade com os dispositivos de segurança cibernética atuais.**

O *CIS v8* define as ações de salvaguardar os ativos através de módulos, que vão do módulo 1 ao módulo 3. O módulo IG1 é definido como módulo de higiene cibernética básica, voltado para pequenas e médias empresas, que contempla 15 controles, dos 18 totais, e 56 salvaguardas, das 153 salvaguardas totais. O módulo IG2 contempla todos os requisitos do módulo IG1, além de controles e salvaguardas a mais, tornando-se um módulo intermediário, contemplando os 18 controles e 130 salvaguardas da documentação. Por fim, o módulo IG3 contempla todos os 18 controles e todas as 153 salvaguardas, utilizando todas as ações de segurança da documentação.

Desta forma, foram apresentadas as documentações que cerceiam a base deste trabalho, segurança cibernética e segurança da informação, normas técnicas e *frameworks* de segurança estabelecidos mundialmente.

A segurança da informação e a segurança cibernética se distinguem em pontos específicos, e cada documentação é voltada para uma área determinada. A Figura 2.1 ilustra a classificação de cada documentação e as relaciona às suas respectivas áreas.

Figura 2.1 - Mapa mental: Normas técnicas e *frameworks.*

Fonte: Autor, 2024.

Este trabalho foi desenvolvido para atender aos requisitos do módulo IGI do *CIS v.*8, voltado para as pequenas empresas, sem deixar de observar todo o contexto de normas e *frameworks* mencionados acima.

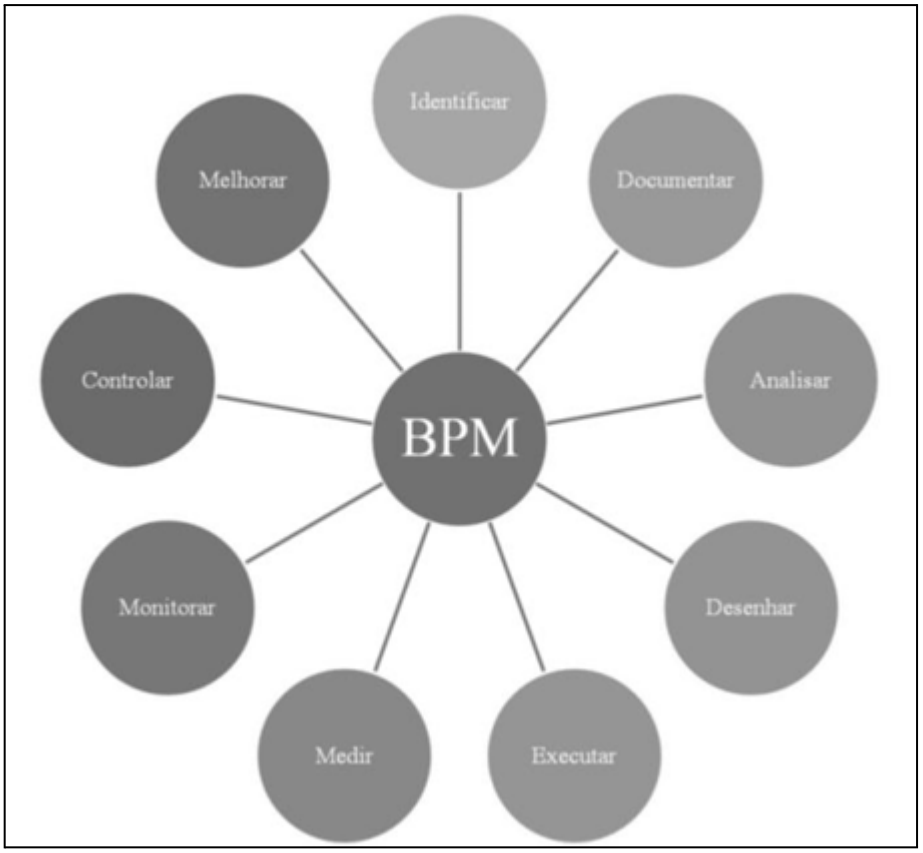
2.4 *Business Process Management* (BPM)

Business Process Management (em português, Gerenciamento de Processos de Negócio) busca aplicar um conjunto de práticas que foca na melhoria contínua dos processos em uma empresa. Uma definição formal para *BPM*, constante no livro BPM CBOK é a seguinte:

> *BPM* é uma abordagem disciplinar para identificar, desenhar, executar, documentar, medir, monitorar, controlar e melhorar processos de negócio, automatizados ou não, para alcançar resultados consistentes e alinhados com os objetivos estratégicos da organização (BPM CBOK, apud BRITTO, 2012, p. 121).

Segundo o livro Guia para Formação de Analistas de Processos, 2011, apud Britto, 2012, p. 123, *BPM* possui um ciclo de vida, dividido em 9 etapas, **Identificar, Documentar, Analisar, Desenhar, Executar, Medir, Monitorar, Controlar e Melhorar,** conforme ilustra a Figura 2.2.

Figura 2.2 - Ciclo de Vida *BPM* Estendido com Fase de Análise.



Fonte: (Capote, 2012 p. 123.)

2.5 *Business Process Modeling Notation* (*BPMN*)

A notação de modelagem de processo de negócio (*BPMN*) é uma notação gráfica, representada por símbolos, utilizada para modelar fluxos de trabalho. Segundo Bocciarelli *et al.* (2019, p. 1440), "*Business Process Management Notation* é uma notação gráfica padrão para a representação de *BPs* (*Business Process*, em português, Processo de Negócio) que é facilmente legível por todos os atores envolvidos em *BPM*".

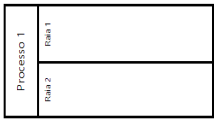
A *BPMN* na versão 2.0, a mais atual no momento, amplia o escopo de sua versão anterior, sendo capaz de formalizar a execução semântica para todos os elementos *BPMN*, além de definir um mecanismo de extensibilidade para extensões de modelo de *BPs* (CHINOSI e TROMBETTA, 2011).

A *BPMN* é um padrão gráfico, extraoficial de mercado, presente em diversas suítes de *BPM*, que auxiliam empresas de modo geral a representarem os processos de negócio da empresa, através de símbolos, que geram diagramas, mapas e modelos de processo (VALENÇA, 2012).

Diversas ferramentas e *softwares* são utilizados para desenvolver modelagem em *BPMN*. Existem *softwares*, tais como o CAMUNDA e o BIZAGI, que podem ser instalados em um computador para a realização de modelagem localmente e *off-line*, e existem também soluções online, tais como o *BPMN Editor* e o *BPMN.IO*, que trazem os símbolos e principais funções da notação na versão 2.0.

Todos os símbolos de *BPMN* utilizados neste trabalho serão ilustrados a seguir na Tabela 2.1.

Tabela 2.1 - Símbolos e objetos do BPMN v2.0.

Símbolo	Nome	Significado
	Piscina	Representa um participante do processo.
	Raia	Representa uma função ou um departamento.

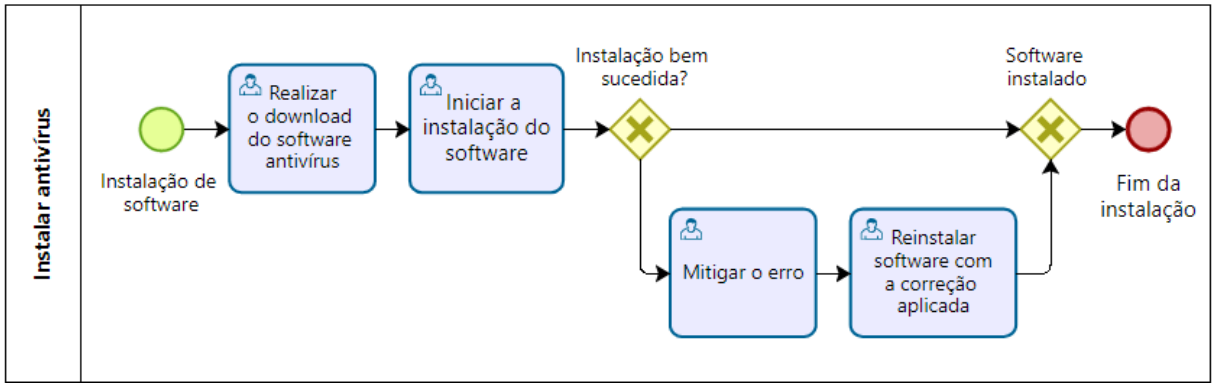
	Evento de início	Representa o início de um processo.
	Evento de final	Representa a finalização de um processo.
	Fluxo de sequência	Relaciona os elementos indicando a direção do fluxo.
	Associação	Associa informações e artefatos com objetos de fluxo.
	Evento intermediário de Regra ou condicional	Representa um evento no meio de um processo, que exige a execução de uma tarefa ou condição previamente estabelecida, para que haja o andamento do processo. Enquanto não cumprida, o processo permanece parado.
	Evento intermediário de sinal	Representa o envio de um sinal com uma ou várias informações que o interessado ainda não possui.
	Evento intermediário de sinal	Representa o recebimento de um sinal com uma ou várias informações que o interessado ainda não possui.
	Gateway exclusivo	Representa uma decisão exclusiva. Quando este gateway aparece no fluxo, apenas um caminho poderá ser seguido.
	Gateway paralelo	Representa uma interação paralela. Quando este gateway aparece no fluxo, todos os caminhos devem ser seguidos simultaneamente.
	Objeto de dados	Representa um artefato que contém informações.

	Atividade/tarefa	Representa uma atividade comum. Geralmente é utilizada por todo o fluxo.
	Atividade Subprocesso	Representa uma atividade que contém outras atividades dentro dela.
	Atividade *loop*	Representa uma atividade que se repete até determinada condição preestabelecida ser cumprida.

Fonte: Autor (2024).

A Figura 2.3 demonstra um processo, representado através de *BPMN*, como um exemplo prático da utilização da notação. O exemplo demonstra um processo para a instalação de um *software* antivírus em um computador.

Figura 2.3 - Exemplo prático do uso de *BPMN*



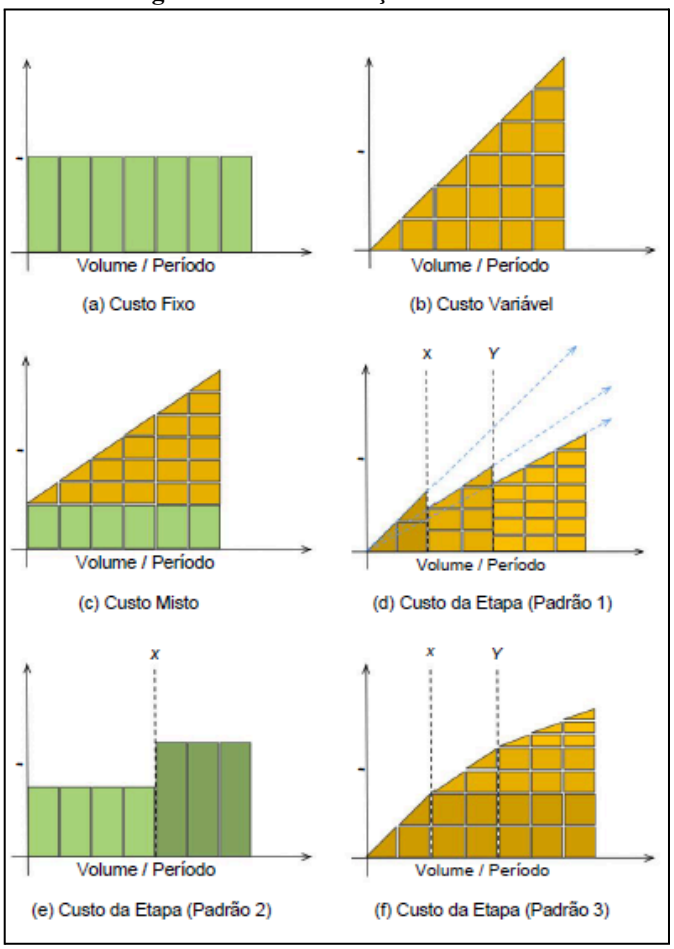
Fonte: Autor, 2024.

2.6 Custos

Segundo Medeiros (2017, p. 29), “custo é todo o gasto necessário para criar e vender produtos e serviços”. De maneira mais abrangente, o custo pode ser entendido também como todo o recurso financeiro necessário para se obter, desenvolver, implementar ou usufruir de algo. Segundo Bragg, 2014; Horngren, Datar e Rajan, 2011; Hansen e Mowen, 2012, apud. Medeiros, 2018, p. 29, “os custos podem ser classificados de acordo com o seu comportamento, que é normalmente referido como custo fixo, variável, misto e escalonado.

Basicamente, o custo classificado como **fixo** permanece inalterado, independente da quantidade adquirida do produto, ou do consumo do serviço. Já o custo **variável**, tem a característica de ser considerado de acordo com o uso do produto ou serviço. O custo classificado como **misto** tem a característica de unir os custos do tipo **fixo** e **variável**. O custo do produto ou serviço tem um preço inicial fixo, porém conforme o aumento do consumo/ utilização o custo final torna-se variável. Por fim, o custo classificado como **escalonado**, possui três padrões diferentes, que são: **Padrão a**: o custo começa com um valor definido e muda ao atingir um nível pré-estabelecido, e conforme o volume/ consumo aumenta, o valor vai alterando conforme atinge os níveis pré-definidos. **Padrão b:** o custo é fixo até um determinado limite, e após este limite ser extrapolado, o custo é alterado para um novo valor. **Padrão c:** Um custo específico é definido como uma unidade de volume, onde este custo é alterado conforme a mudança de período (MEDEIROS, 2017). A Figura 2.4 ilustra todos estes tipos de custos.

Figura 2.4 - Classificação dos Custos



Fonte: (Medeiros, 2017, p. 30).

O gerenciamento dos custos do projeto inclui os processos envolvidos em estimativas, orçamentos e controle dos custos, de modo que o projeto possa ser terminado dentro do orçamento aprovado (PMBOK, 2008, p. 131).

O gerenciamento de custo, além de estar relacionado ao planejamento, estimativa e controle de custo, também está intimamente ligado à tomada de decisão sobre qualquer operação que envolve valores financeiros (HANSEN e MOWEN, 2015).

Segundo Medeiros (2017, p. 29), "a estimativa de custos permite a previsão do custo e definição do orçamento para realizar a composição de um serviço." É justamente com esta visão que este trabalho foi desenvolvido, com o objetivo de gerar uma estimativa de custo para implementar controles de segurança cibernética em um ambiente cibernético empresarial de qualquer segmento de mercado (educação, saúde, varejo, etc.), com o intuito de promover uma previsão de custo e definição de orçamento mais próximo da realidade.

Existem várias definições e classificações de tipos de custos, que são definidos através de suas características ou usabilidade. Dentre várias possibilidades, os custos podem ser definidos como diretos ou indiretos. Segundo Santos (2018), o custo direto está ligado a um item específico, que pode ser identificado facilmente e individualmente, como um produto ou uma matéria-prima, por exemplo. Já o custo indireto é gerado por múltiplas atividades que não podem ser identificadas facilmente e nem quantificadas nos produtos finais, como materiais de consumo diversos, depreciação de equipamentos, etc.

2.7 Considerações Finais

Este capítulo apresentou conceitos básicos para o entendimento deste trabalho. Foram apresentados conceitos sobre segurança da informação, segurança cibernética, normas técnicas, *frameworks* de segurança, *Business Process Model Notation* (*BPMN*) e conceitos sobre gerenciamento de custos.

Inclusive, as normas técnicas e os *frameworks* utilizados como base para o desenvolvimento da modelagem da abordagem proposta nesta dissertação foram descritas.

Uma breve descrição sobre os símbolos presentes na modelagem desenvolvida por este trabalho foram apresentadas na Tabela 2.1, com o objetivo de facilitar o entendimento dos processos, mesmo que o leitor não tenha o amplo domínio da notação *BPMN*.

Finalmente, uma breve descrição sobre gerenciamento de custos foi apresentada com intuito de destacar ideias que serão importantes para a estimativa de custos efetivada pelo processo proposto nesta dissertação.

Capítulo 3

"Não podemos prever o futuro, mas podemos criá-lo."
(Peter Drucker).

3 METODOLOGIA DE PESQUISA

Este capítulo apresenta as características do método de pesquisa utilizado para obter e ranquear os trabalhos relacionados ao tema de análise de custos na implementação de controles de segurança cibernética e ao tema de melhoria da segurança cibernética com o uso de controles de segurança. Os trabalhos relacionados foram levantados através de uma revisão tradicional, utilizando alguns recursos de uma revisão sistemática.

3.1 Visão Geral

O objetivo deste capítulo é apresentar a revisão tradicional realizada para buscar trabalhos relacionados à análise de custos na implementação de controles de segurança cibernética.

3.2 Procedimentos da Revisão Tradicional

A pesquisa deu-se início com a necessidade de se conhecer o estado atual da arte quanto aos estudos relacionados à análise de custos financeiros em relação à implementação de controles de segurança cibernética.

O método da pesquisa foi dividido em 3 fases: planejamento, condução e resultados, seguindo o modelo de uma revisão sistemática. Dessa forma, os artigos selecionados foram em menores quantidades, porém têm mais relação com o objetivo principal deste trabalho.

Como o assunto deste trabalho tem uma especificidade considerável, custos financeiros associados ao uso de controles de segurança cibernética, afunilar o conteúdo da busca foi necessário como o que é realizado em uma revisão sistemática. Desta maneira, os resultados das pesquisas realizadas nas bases de busca foram mais assertivos, minimizando a quantidade de trabalhos com conteúdos não relacionados.

3.2.1 Fase 1 - Planejamento

O planejamento é desenvolvido através de um conjunto de ações para determinar o percurso da revisão sistemática.

A primeira ação define o tema e a questão da pesquisa. Esta revisão busca responder a seguinte pergunta: “Como estimar os custos financeiros para implementar controles de segurança cibernética em ambientes cibernéticos?”

Foram considerados também trabalhos que envolvessem apenas a utilização de controles de segurança e elevasse o nível de maturidade da segurança cibernética e da informação, mesmo sem a análise de custos financeiros. O uso de controles de segurança é um pilar deste trabalho, sendo importante verificarmos como eles têm sido aplicados em ambientes cibernéticos atualmente.

Perguntas secundárias surgiram durante o processo de identificação do tema, complementando-o. A segunda ação consiste em definir o método de pesquisa. Nesta etapa,

são definidas as palavras-chaves e a(s) string(s) de busca nos motores científicos previamente selecionados.

Neste trabalho, duas *strings* de busca genérica foram desenvolvidas para consultar as três bases de dados utilizadas, a saber, *ACM*, *IEEE Xplore* e *Science Direct*. Outras duas bases de dados adicionais não foram consultadas por motivos distintos, conforme é definido e ilustrado na Tabela 3.1. A cadeia de pesquisa foi definida como: (“cybersecurity”) AND (“cost”) para a *string* 1; e (“cybersecurity”) AND (“control”) para a *string* 2. As strings utilizadas foram definidas após alguns ajustes, mediante a realização de testes e o uso de outras strings.

A terceira ação consiste em definir os critérios de inclusão e exclusão. Nesta etapa se define quais os critérios a serem avaliados nos trabalhos científicos encontrados nas bases de dados de divulgação científica. Todas estas informações e maiores detalhes seguem ilustradas na Tabela 3.1.

Tabela 3.1 - Planejamento da Pesquisa Mediante o Uso de Alguns Recursos da Revisão Sistemática.

Protocolo de Revisão Sistemática		
Objetivo:	Buscar as principais referências bibliográficas e técnicas relacionadas à implementação de controles de segurança cibernética e da informação, além de estimar e considerar os custos relacionados ao uso destes mesmos controles.	
Questões de Pesquisa		**Justificativa**
RQ1	Como estimar os custos para elevar o nível de maturidade em segurança cibernética já existente?	Há uma necessidade de mercado em se obter previamente os valores necessários para promover uma melhora no nível de maturidade em segurança cibernética já existente.
RQ2	Existe algum modelo de custos para implementação de controles de segurança que atenda a diferentes tipos de negócio?	Modelos de custos genéricos para a implementação de controles de segurança que atendam a vários tipos de negócios não foram encontrados.
RQ3	Existe algum modelo de custos para implementação de controles de segurança que atenda a várias normas técnicas ou frameworks de segurança?	Modelos de custos genéricos que atendam a várias normas técnicas e vários frameworks não foram encontrados.

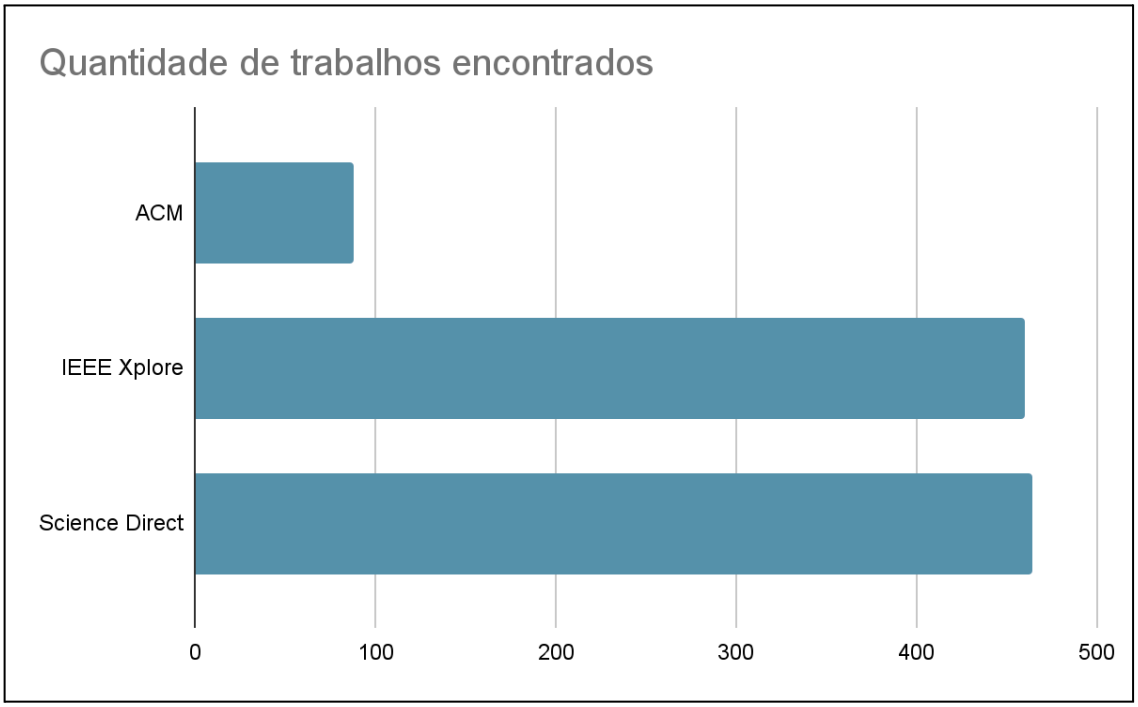
RQ4	Como elevar o nível da segurança cibernética em ambientes controlados através da implementação de controles de segurança cibernética?	Fomentar um espaço cibernético mais seguro para todas as organizações, sugerindo a adoção de normas técnicas ou frameworks de segurança cibernética para a implementação de controles de segurança, realizando uma implementação guiada em observância com o conjunto de soluções de segurança exigidos por essas documentações.	
String de busca	**Utilizadas**: cybersecurity AND cost; cybersecurity AND control; **Não utilizadas**: information security AND cost; information security control; cybersecurity AND money.		
Limite de tempo	6 anos		
Área	Ciências da Computação, Engenharia.		
Tipo de publicação	Artigos científicos, dissertações, teses.		
Fonte	Nome / URL	Utilizado?	Por que não?
	ACM Digital Library	Sim	
	IEEE Xplore	Sim	
	SpringerLink	Não	Não foi possível acessar com as credenciais da universidade, mediante a plataforma CAFE.
	Google Scholar	Não	Foi decidido não utilizar pelo fato desta base trazer também resultados de bases menos importantes.
	Science Direct	Sim	
Critério de inclusão		**Critério de exclusão**	
CI1	Incluir cibersegurança no título.	CE1	Não fornece resumo ou título.
CI2	Incluir custos em qualquer parte do texto.	CE2	Não pode ser um estudo primário (editoriais, sumários ou bloco de notas, tutoriais, posts, etc.)
CI3	Incluir o uso de controles de segurança em qualquer parte do texto.	CE3	Se não houver possibilidade de obter acesso a versão completa da publicação/ documento.
CI4	Incluir normas técnicas ou framework de cibersegurança em qualquer parte do texto.	CE4	Se não tiver relação com segurança cibernética ou da informação.
CI5	Precisa ser: Artigo, dissertação ou tese.		

Fonte: Autor (2023).

3.2.2 Fase 2 - Condução

Nesta etapa da revisão tradicional, os artigos foram obtidos por meio da *string* de busca definida na etapa 3.2.1. Posteriormente, foram analisados por meio de critérios qualitativos e contextuais. O retorno das *strings* de busca apresentou 1.012 artigos ao todo. Foram realizadas duas buscas em cada base de dados com as *strings* já mencionadas, e a Figura 3.1 apresenta a soma dos resultados da pesquisa por base científica.

Figura 3.1 - Resultado da Pesquisa



Fonte: Autor, 2023.

Em seguida, foi realizada a triagem de artigos, sendo este o primeiro nível de seleção seguindo os critérios de inclusão e exclusão definidos. Critérios de inclusão e exclusão são utilizados para excluir estudos que não sejam relevantes para responder às questões de pesquisa (PETERSEN *et al.*, 2008).

Após esta primeira seleção, que resultou na seleção de 51 trabalhos, foi realizada a leitura destes trabalhos, para analisar possíveis rejeições de um ou mais artigos.

A execução deste processo resultou na seleção de 24 artigos que passaram nos critérios de inclusão e exclusão.

Em seguida, foi definido o Fator de Distribuição de Contexto (FDC) para sintetizar e caracterizar os artigos em áreas específicas e filtrar a qualidade dos artigos. Nesta fase, utilizamos como base o trabalho de Silva (2019, p. 34).

O Fator de Distribuição de Contexto (FDC) define as propostas de trabalhos em duas categorias: a primeira delas (FDC1) é definada pelo trabalho propor algum cálculo ou análise de custos. A segunda categoria do Fator de Distribuição (FDC2) é definida pelo trabalho propor o uso de controles de cibersegurança ou de segurança da informação.

Foram avaliados 24 artigos de acordo com os fatores desenvolvidos e descritos nesta seção. Serão demonstrados os 15 trabalhos mais bem avaliados utilizados neste estudo, conforme ilustra a Tabela 3.2.

Tabela 3.2 - Lista dos 15 Trabalhos Mais Bem Avaliados

ID	Título de Trabalho	FDC1	FDC2	Fonte
1	*On the Cost of Cyber Security in Smart Business*	Sim	Sim	*IEEE Xplore - 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*
2	*CyberTEA a Technical and Economic Approach for Cybersecurity Planning and Investment*	Sim	Sim	*IEEE Xplore - NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*
3	*GTM Game Theoretic Methodology for Optimal Cybersecurity Defending Strategies and Investments*	Sim	Sim	*ACM - ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security*
4	*A Novel Model for Cybersecurity Economics and Analysis*	Sim	Sim	*IEEE Xplore - 2017 IEEE International Conference on Computer and Information Technology (CIT)*
5	*Socially Optimal IT Investment for Cybersecurity*	Sim	Sim	*ScienceDirect - Decision Support Systems*
6	*Cybersecurity: Risk Management Framework and Investment Cost Analysis*	Sim	Sim	*ScienceDirect - Business Horizons*
7	*Cyber Defense Matrix: A New Model for Optimal Composition of Cybersecurity Controls to Construct Resilient Risk Mitigation*	Sim	Sim	*ACM - HotSoS '19: Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*
8	*A Security Cost Modelling Framework for Cyber-Physical Systems*	Sim	Não	*ACM - ACM Transactions on Internet Technology*
9	*LCCI: A Framework for Least Cybersecurity Controls to be Implemented for Small and Medium Enterprises*	Não	Sim	*ScienceDirect - International Journal of Information Management Data Insights*

10	*Practitioners' Views on Cybersecurity Control Adoption and Effectiveness*	Não	Sim	*ACM - ARES '21: Proceedings of the 16th International Conference on Availability, Reliability and Security*
11	*Analysis of Appropriate Standards to Solve Cybersecurity Problems in Public Organizations*	Não	Sim	*ACM - ICISDM '20: Proceedings of the 2020 the 4th International Conference on Information System and Data Mining*
12	*Industrial Control Systems Cybersecurity: Back to Basic Cyber Hygiene Practices*	Não	Sim	*IEEE Xplore - 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)*
13	*Reference Framework "HOGO" for Cybersecurity in PMEs Based on ISO 27002 and 27032*	Não	Sim	*IEEE Xplore - 2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*
14	*Cybersecurity Framework for SMEs in Peru Based on ISO/IEC 27001 and CSF NIST Controls*	Não	Sim	*IEEE Xplore - 2023 18th Iberian Conference on Information Systems and Technologies (CISTI)*
15	*A Multi-Perspective Methodology for Evaluating the Security Maturity of Data Centers*	Não	Sim	*IEEE Xplore - 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*

Fonte: Autor (2023).

3.2.3 - Resultados e Discussões

Esta seção tem o objetivo de apresentar a discussão dos principais trabalhos selecionados após a análise mais criteriosa, seguindo conceitos de revisão sistemática, buscando analisar a proposta do trabalho e os resultados apresentados por ele, com base nos quatro fatores de qualificação.

Custos para Cibersegurança

Ivkic *et al.* (2017) propõem, em seu trabalho, um modelo de análise (*SCMF - Security Cost Modeling Framework*) para separar os custos de segurança dos custos totais de um *CPS* (Cyber-physical system, em português, Sistema Ciber-Físico). O modelo é capaz de medir, normalizar e agregar custos funcionais e custos de segurança de um *CPS*.

O modelo foi testado através de um estudo experimental considerando dois casos distintos, e os autores apontaram os seguintes resultados: 1) o modelo descreve formalmente um *CPS* baseado em suas interações, componentes participantes e tarefas funcionais relacionadas à segurança; 2) as métricas do modelo podem ser utilizadas para medir as tarefas relacionadas à segurança e calcular os custos resultantes; 3) por fim, os autores descrevem duas formas de implementar um *CPS* e afirmam ter reduzido em 33% os custos de implementação de segurança no caso 2. Esta proposta é próxima ao proposto neste trabalho, pois trouxe resultados de custos referentes a tarefas relacionadas à segurança, além de demonstrar economia de recursos financeiros no caso 2.

Franco, Granville e Stiller (2023), propõem uma abordagem técnica e econômica para planejamento e investimento em cibersegurança. Os autores dividiram a abordagem em 5 fases, um quadro e um conjunto de soluções para o planejamento e investimento adequado em cibersegurança.

Os autores buscam indicar o melhor investimento possível em cibersegurança, considerando os requisitos cibernéticos e as suas dimensões econômicas, ponderando os potenciais impactos econômicos de ataques cibernéticos e o custo-benefício das contra medidas de proteção a esses ataques, tendo como resultado a sugestão de um valor financeiro para investimento em controles de segurança cibernética.

Assim como a proposta desta dissertação, esta abordagem é voltada especialmente às pequenas e médias empresas, com o objetivo de tornar o ambiente cibernético que estas empresas estão inseridas mais seguro, uma vez que elas geralmente dispõem de poucos recursos para investir em cibersegurança, tornando-se o tipo de empresa mais vulnerável do ecossistema e um alvo corriqueiro dos ciberatacantes.

Em Kalderemidis *et al.* (2022), os autores propõem uma ferramenta de *software*, baseada em teoria dos jogos, para auxiliar os gestores em segurança da informação na tomada de decisão quanto aos controles de cibersegurança a serem implementados, onde calculam os investimentos necessários desta implementação, mediante a análise de dados de uma simulação de ataques cibernéticos recebidos pela organização.

Ao utilizar a metodologia proposta, chamada de *GTM* (*Game Theoretic Methodology*), os autores concluíram que é possível criar estratégias defensivas de maneira automática, eficazes em diversos cenários, mesmo o ambiente cibernético exposto a variados tipos de ataques (ataques baseados em teoria dos jogos ou ataques desordenados), sendo também possível visualizar estratégias de investimentos ideais mediante as estratégias utilizadas na metodologia proposta.

Apesar de indicarem os controles a serem implementados e também calcularem os custos necessários na implementação de controles de segurança, o trabalho dos autores define estas recomendações de investimento após incidentes cibernéticos simulados, na tentativa de obter um cenário de investimento ótimo como uma maneira de responder a ataques cibernéticos recebidos, fortalecendo o cenário de segurança após os ataques.

Já a metodologia proposta neste trabalho de dissertação tem o mesmo objetivo de calcular os investimentos necessários na implementação de controles de segurança, porém, com o objetivo de criar um cenário cibernético seguro, mediante a adoção de uma norma técnica ou *framework* de cibersegurança padrão, antes mesmo que qualquer ataque cibernético aconteça, seguindo as recomendações básicas de segurança cibernética, resultando em conformidade com normas técnicas e *frameworks* consolidados no mercado, minimizando ou até mesmo impedindo que perdas diversas possam acontecer às organizações advindas de ataques cibernéticos.

Em Rathod e Hamalainen (2017), é proposto um modelo para analisar a economia da segurança cibernética. O modelo proposto é baseado em um pensamento estratégico e de longo prazo, buscando o melhor cenário para o custo-benefício dos investimentos com cibersegurança. O modelo realiza uma abordagem holística à cibersegurança, analisando não apenas as tecnologias, mas também as dimensões institucionais, econômicas, de governança e humanas.

O modelo divide a análise em cinco grupos, definidos como operações de cibersegurança; conformidade da cibersegurança com padrões estabelecidos; pessoas e cultura organizacional; pessoas, processos e tecnologias; e por fim, investimento em cibersegurança.

Dessa forma, segundo os autores, é possível analisar e quantificar os valores financeiros necessários para implementar as melhores práticas de segurança cibernética garantindo o entendimento dos tomadores de decisão, trazendo valores financeiros quantificáveis.

Apesar de trazer valores financeiros quantificáveis, assim como esta dissertação, o trabalho dos autores tem foco no custo-benefício sobre os investimentos em cibersegurança. Já este trabalho tem o foco em estimar os investimentos necessários para se obter cibersegurança desde a concepção do ambiente cibernético, implementando um conjunto de ações de segurança mediante a utilização de alguma norma técnica de segurança ou de algum *framework* de cibersegurança estabelecido e reconhecido mundialmente.

Paul e Wang (2019), propõem uma análise para determinar o melhor investimento em cibersegurança levando em consideração o conceito de custo social, composto por custos

privados e de externalidade, para capturar o valor econômico decorrido no tempo das perdas infligidas aos utilizadores de um serviço sob ataque cibernético.

Os autores defendem que o primeiro investimento deve ser realizado em mecanismos de defesa e prevenção, através de controles e salvaguardas estabelecidos em normas técnicas e *frameworks* de segurança. Adicionalmente, os autores defendem que após o primeiro investimento em contramedidas de segurança, os recursos disponíveis devem ser investidos em medidas de detecção e contenção.

Chegou-se a conclusão que investimentos adicionais em medidas de prevenção, após controles de segurança estarem em funcionamento e estabelecidos no ambiente cibernético, trazem pouco ou nenhum impacto na redução dos impactos sociais, porém, investimentos em detecção e contenção tem maior impacto no custo social e resulta em uma configuração mais adequada das salvaguardas de segurança cibernética.

Este trabalho teve uma importância significativa para a elaboração desta dissertação, pois ele estabelece uma relação quanto ao uso de controles de segurança da informação e cibernética com os seus respectivos custos associados, e reflete sobre o nível de segurança adquirido pelo ambiente cibernético após os novos investimentos.

Lee (2021), propõe justificar os investimentos em segurança cibernética através de uma estrutura desenvolvida em 4 camadas. Cada camada analisa um determinado segmento da estrutura de gestão de riscos proposta.

A camada 1, Ecossistema Cibernético, trata de assuntos sobre clientes, parceiros da cadeia de suprimento, intrusos/hackers, agências reguladoras, consultores cibernéticos e desenvolvedores de tecnologia cibernética. A camada 2, Infraestrutura de Cibersegurança, trata da organização, funcionários e tecnologias cibernéticas. A camada 3, Avaliação de Risco Cibernético, trata da identificação dos riscos, quantidade dos riscos e da análise de investimento cibernético. A camada 4, Desempenho Cibernético, trata da implementação de controles de segurança, monitoramento e controle de ataque, além da melhoria contínua do processo.

O autor também define um valor específico para cada tipo de ataque cibernético, e toma esses valores como base de dados para estimar o montante de perda financeira em ataques cibernéticos bem sucedidos em ambientes cibernéticos sem contramedidas, e posteriormente, compara as perdas financeiras estimadas do ambiente após a aplicação da estrutura proposta, com controles de segurança implementados.

Dessa maneira, é possível perceber o impacto positivo na diminuição do valor financeiro perdido a cada ataque cibernético sofrido pela organização. O trabalho deste autor,

contribui para esta pesquisa pelo fato de trazer informações diretamente relacionadas sobre os possíveis impactos financeiros que uma organização pode sofrer após ataques cibernéticos, e o quanto o uso de controles de segurança cibernética e da informação podem proteger os ativos minimizando a perda de recursos financeiros.

Dutta e Al-shaer (2019a), propõem demonstrar uma abordagem inovadora e automatizada para auxiliar a tomada de decisão entre a implantação de controles de segurança, a mitigação de riscos e o ROI (Retorno sobre Investimento), através da utilização de uma matriz denominada *CDM* (*Cyber Defense Matrix*, em português, Matriz de Defesa Cibernética).

Esta matriz determina quais controles de segurança são necessários, onde serão implementados (Rede, Dispositivos, Pessoas, Aplicativos e Dados) e o porquê deles serem eficazes (é especificado os ataques que os controles protegem). A abordagem foi testada em experimentos preliminares, e os autores apontaram que os resultados trouxeram duas descobertas.

A primeira foi que a abordagem de redução de modelo baseada na relação custo-benefício de produtos pode melhorar o ROI e, ao mesmo tempo, reduzir significativamente a complexidade na tomada de decisão. A segunda foi que a complexidade de um problema depende em grande parte do número de ativos, tolerância ao risco e o orçamento disponível para a implantação de controles de segurança.

Assim como este trabalho de dissertação, o trabalho dos autores busca auxiliar os tomadores de decisão sobre os investimentos em dispositivos de segurança cibernética, utilizando controles de segurança para aumentar o nível de segurança cibernética do ambiente testado.

Ivkic *et al.* (2022), propõem uma metodologia para medir custos de controles de segurança cibernética para serviços em nuvem, considerando os riscos que a implementação dos serviços em nuvem podem gerar.

A metodologia é baseada em um modelo de negócio que avalia se um dispositivo inteligente pode ser inserido em uma empresa e se comunicar através de serviço em nuvem, aplicando controles de segurança específicos de um norma técnica estabelecida (ABNT NBR ISO/IEC 2017) para eliminar os riscos de segurança e medir as despesas adicionais resultantes do uso desses controles.

Os autores apontaram que os resultados podem ajudar na investigação inicial sobre como medir os custos da segurança em automatização de sistemas IoT. Esta medição dos custos necessários para implementar controles de segurança cibernética é também a principal

motivação deste trabalho, porém, o trabalho dos autores especifica a norma técnica utilizada (ABNT NBR ISO/IEC 2017), e este trabalho, amplia o escopo da pesquisa e propõem uma metodologia genérica, que pode ser utilizada com várias normas técnicas e vários *frameworks* de cibersegurança.

Controles para Cibersegurança

Pawar e Palivela (2022), propõem uma estrutura mínima de controles de segurança cibernética para ser implementada em pequenas e médias empresas. Este trabalho tem o mesmo objeto de estudo desta dissertação, a implementação de controles de segurança cibernética para PMEs, porém os objetivos são diferentes.

Os autores buscam propor uma metodologia de implementação de controles de segurança priorizando os controles mais necessários para cada tipo de PME considerando a tríade da segurança da informação, que são integridade, disponibilidade e confidencialidade, ao invés de implementar controles de segurança de maneira aleatória e generalista.

Já a proposta deste trabalho de dissertação reside em estimar os custos necessários para implementar controles de segurança cibernética para PMEs, haja vista a importância comprovada da implementação de controles de segurança nos ambientes cibernéticos citada por vários autores nos trabalhos relacionados.

Os autores revelam que, em sua pesquisa, 115 empresas de vários países participaram voluntariamente enviando os dados sobre controles de segurança utilizados em seus ambientes cibernéticos.

Em quase 50% das empresas entrevistadas, os controles de segurança implementados não tinham conformidade ou faziam referência a algum padrão estabelecido. Quase 30% das empresas afirmaram não ter controles de segurança implementados, e 15% informaram que talvez tivessem controles de segurança vigentes em seus ambientes cibernéticos.

Outro dado relevante da pesquisa é que, nas empresas onde há controles de segurança vigentes, mais de 70% são físicos e menos de 5% possuem controles para serviços virtuais.

Os autores defendem que as PMEs devem identificar qual o ativo de missão crítica da empresa, e priorizar a implementação do controle de segurança que irá melhor salvaguardar este ativo crítico, além de observar e implementar os controles básicos para todo espaço cibernético.

Por fim, os autores concluíram que as PMEs têm grandes dificuldades em encontrar soluções simples e fáceis para proteger os seus ativos da melhor maneira possível. Afirmam

ainda que há realmente a necessidade de recomendações mínimas e graduais às PMEs para implementar controles de segurança cibernética.

A falta de financiamento, a dificuldade em encontrar quais os controles de cibersegurança são mais adequados e a falta de recursos qualificados são os principais problemas identificados durante a investigação.

Dito isto, este trabalho de dissertação busca atuar na lacuna existente dos estudos realizados no passado, com o objetivo de auxiliar as PMEs a obterem dados quanto aos custos financeiros necessários para a implementação de controles de segurança cibernética para alcançar um estado de maturidade elevado em segurança.

A estimativa de custos para implementar os controles de segurança, poderá ser refeita várias vezes, permitindo que os tomadores de decisão cheguem a valores adequados às suas expectativas ou até mesmo aos seus limites orçamentários, porém, mantendo-se o elevado nível de segurança e a conformidade desejada com as normas técnicas ou os *frameworks* de segurança estabelecidos no mercado.

Axon *et al.* (2021), propõem colher a opinião de profissionais de segurança cibernética a respeito da adoção e eficácia de controles de segurança cibernética para as organizações de modo geral.

Os autores utilizaram o *framework* de segurança cibernética do *CIS*, o mesmo *framework* de segurança utilizado nesta dissertação, porém em uma versão anterior. Na época da publicação do trabalho citado, o *CIS CSCs* continha 20 controles.

Foram utilizados questionários online e entrevistas qualitativas com 30 profissionais, todos com mais de 10 anos de experiências em cibersegurança e em vários níveis de atuação, de CISOs a analistas de testes de penetração.

O estudo utilizou a escala de Likert de cinco pontos, com categorias de resposta definidas como muito ineficaz, ineficaz, neutro, eficaz, muito eficaz. Apesar da dificuldade em chegar a um consenso quanto ao uso dos controles que compõem o *framework* de segurança, os autores chegaram a algumas conclusões.

Embora todos os controles foram considerados como eficazes e muito eficazes, os controles mais citados pelos profissionais como mais eficazes foram o CSC3 “Avaliação de vulnerabilidade”, CSC4 “Privilégios de administrador” e o CSC19 “Resposta a Incidentes”.

Em contrapartida, os controles mais implantados nos ambientes cibernéticos segundo os entrevistados foram o CSC8 “Defesas contra *malware*”, CSC12 “Defesas de limite”, CSC7 “Defesa de *webmail*” e o CSC11 “Dispositivos de rede seguros”. O que chama a atenção neste

levantamento é o fato de que nenhum dos controles listados como mais eficazes estavam entre os mais utilizados nos ambientes cibernéticos.

Por fim, os autores concluíram que a eficácia quanto a implementação de controles de segurança variam em diferentes contextos organizacionais, sendo afetados por vários fatores, como as características da organização, os seus objetivos, como configuram os controles em seus ambientes, com quais tipos de ataques elas lidam, a prioridade de salvaguardar determinados ativos, o setor de atuação da empresa, além da experiência e maturidade da organização em segurança cibernética, determinam a implementação e adoção de controles de segurança cibernética.

Este estudo mostrou-se importante para esta pesquisa de mestrado, pelo fato de enfatizar a importância da utilização de *frameworks* de segurança e a implementação de controles e salvaguardas de segurança para proteger ambientes cibernéticos.

Em Toapanta *et al.* (2020), os autores propõem um estudo para analisar a situação de segurança cibernética em instituições públicas do Equador. É realizada uma análise sobre padrões de segurança cibernética e da informação, como as ISO/IEC 15408 e ISO/IEC 17799, que tratam dos requisitos necessários para um desenvolvimento de *software* seguro, e diretrizes que orientam boas práticas para um sistema de gestão de segurança da informação, respectivamente.

O objetivo dos autores é demonstrar que os controles de segurança destes padrões são eficazes e ajudam as organizações a salvaguardar os dados das organizações públicas de cibercriminosos. Para chegar a conclusão do nível de maturidade e conformidade das organizações públicas do Equador, os autores utilizaram como método uma investigação documental.

Foram analisados os controles estabelecidos pelas normas padrões, projetos e estudos de caso na América Latina, América do Norte e União Européia, leis e regulamentos nacionais e internacionais, além dos dados fornecidos pelo *Government Information Security Scheme Ranking* (EGSI) sobre as organizações do Equador.

Os autores chegaram à conclusão que as organizações não são confiáveis, pois várias organizações sofreram algum tipo de incidente cibernético, principalmente o vazamento de dados. Relatam que isso se deveu pelo menos em parte à falta de conformidade com normas que estabelecem controles de segurança cibernética.

Os autores também afirmam que para diminuir e combater os incidentes, é necessário investir em segurança cibernética, com o desafio de considerar o valor do investimento para

proteger os ativos das organizações, uma vez que as organizações não dispõem da mesma quantidade de recursos financeiros para isso.

Dado este fato e em observância à lacuna existente nos trabalhos acadêmicos pesquisados, este trabalho de dissertação propõe justamente uma metodologia para auxiliar pequenas e médias empresas e organizações de modo geral a estimarem os custos financeiros necessários para implementar controles de segurança, alcançando o status de conformidade desejado com normas padrões estabelecidas no mundo inteiro.

Malatji (2022), propõe rechaçar a importância dos controles cibernéticos básicos, comumente chamados de higiene cibernética, em sistemas de controle industrial (ICS).

O autor realizou uma pesquisa baseada em artigos publicados de 2012 a 2022, com títulos que contivessem “higiene cibernética” e “ICS”. O objetivo principal deste estudo foi apresentar ataques cibernéticos reais bem sucedidos a várias grandes empresas do mundo, inclusive empresas de serviço crítico, como a *Water CI*, em Oldsmar, Flórida, nos Estados Unidos.

Ao relatar vários ataques cibernéticos, o estudo correlaciona o método de ataque e entrada dos invasores aos sistemas atacados, com os controles e técnicas para salvaguardar os ambientes cibernéticos.

Malatji afirma que as principais vulnerabilidades exploradas em ataques a sistemas ICS são a exploração de dia zero, sistemas não atualizados com *patches* de segurança, política de senhas fracas, má gestão de controle de acesso e ataques através de mídia removíveis, como as de tipo USB, por exemplo.

Por fim, o autor conclui que a implementação de controles cibernéticos de higiene básica dificultam o sucesso do invasor com oito práticas de segurança, sendo elas, revisar e alterar senhas com frequência, manusear adequadamente dispositivos e mídias removíveis, gerenciar ativamente atividades de autenticação e autorização de usuários, treinamento de conscientização sobre segurança para a força de trabalho, o não compartilhamento de informações confidenciais e privadas, avaliar o risco de segurança cibernética, restringir, segregar e separar o acesso físico à rede de computadores e dispositivos ICS e realizar atualizações frequentes de *patches* de segurança para solucionar problemas de vulnerabilidades e ataques do tipo dia zero.

Este trabalho serviu de base para determinarmos a escolha da implementação dos controles classificados como higiene cibernética no *framework* de segurança *CIS v8* no experimento prático durante a aplicação da metodologia proposta. É possível afirmar que os controles aplicados nesta dissertação são mais numerosos do que no artigo de Malajti, que

aborda 8 controles; este trabalho de dissertação, em seu experimento, considerou 15 controles, com 56 ações de salvaguarda.

Cruzado *et al.* (2022), os autores desenvolveram um *framework* denominado "HOGO", que é uma representação de um quadro de referência baseado nas boas práticas e nos controles de segurança das ISOs 27002 e 27032.

O quadro de referência proposto pelos autores tem o objetivo de reduzir os possíveis riscos de segurança cibernética para as PMEs, aumentando a segurança nas operações online, nas informações financeiras, protegendo a imagem e a relação com os clientes e fornecedores, além de proteger a informação.

Para desenvolver o quadro de referência "HOGO" os autores fizeram o cruzamento de dados das duas normas adotadas, identificando os controles repetíveis, as divergências e os complementos entre os documentos, gerando um referencial de 58 controles de segurança cibernética.

Os autores afirmam ter aplicado o *framework* proposto em um estudo de caso real, em uma PME do setor logístico, onde observou-se a melhoria na segurança e o aumento na conformidade do ambiente cibernético testado em relação às ISOs adotadas. Por fim, os autores afirmam que com a adoção do modelo de referência proposto "HOGO", é possível elevar o nível de maturidade das PMEs quanto à segurança da Internet, infraestrutura crítica da informação, segurança de redes e segurança da informação.

Em Angelo, Alexis e Lenis (2023), os autores propõem implementar uma estrutura de segurança cibernética para PMEs no Peru com base na ISO 27001 e no *framework* de segurança *CSF NIST*.

Os autores utilizam o ciclo de Deming (*PDCA*) para estruturar a sua implementação e garantir o processo de melhoria contínua do quadro de segurança cibernética das pequenas e médias empresas. O trabalho ressalta que em 7 fases é possível organizar os controles utilizados na melhoria da segurança cibernética, e ao todo 40 controles de segurança serão analisados e implementados nos ambientes cibernéticos.

As 7 fases estão distribuídas da seguinte maneira: definir a política de segurança, identificar os controles de segurança, justificar a aplicação dos controles, determinar o perfil da empresa, aplicar os controles de segurança, auditar internamente para identificar o nível de maturidade atual, e por fim, revisar a melhoria contínua do processo.

Ao aplicar os 40 controles de segurança cibernética seguindo o modelo proposto do artigo, os autores afirmam aumentar o nível de segurança em 40% do estado inicial, saindo de

um estado de segurança classificado como “insuficiente” e alcançando o estado de classificação como “maduro”.

Lima, Lima R. e Lins (2017), os autores propõem uma metodologia para avaliação da maturidade de segurança de data centers. Esta metodologia é composta por uma análise ponderada sobre um conjunto abrangente de normas técnicas de segurança da informação para data centers.

O objetivo é avaliar e melhorar o nível de maturidade de segurança utilizando as ações mais indicadas, que são controles citados simultaneamente em várias normas, para data centers. A metodologia foi aplicada em um estudo de caso real, e os autores apontaram que os resultados serviram principalmente para dois aspectos: 1) entender o contexto real de segurança do ambiente do data center; 2) definir políticas para melhorar a segurança.

3.3 - Considerações Finais

Como visto, os trabalhos relacionados mencionam os custos com cibersegurança e citam a eficácia e a importância dos controles de segurança cibernética em um ambiente computacional pertencentes às organizações de modo geral. No entanto, estes trabalhos buscam justificar em sua maioria o custo-benefício dos investimentos em segurança cibernética necessários para manter o ambiente cibernético minimamente seguro, seguindo as normas e *frameworks* de segurança.

Outra constatação é que alguns trabalhos até trazem valores financeiros para a implementação de controles de cibersegurança, porém são desenvolvidos para normas e *frameworks* específicos e para um ambiente cibernético também específico, como em Ivkic *et al*. no trabalho intitulado como “*On the Cost of Cyber Security in Smart Business*”.

Percebendo esta lacuna na literatura, foi decidido expandir o escopo utilizado em estudos anteriores, desenvolvendo uma metodologia mais genérica possível, que pudesse ser utilizada com qualquer norma técnica ou *framework* de segurança respaldado mundialmente, e em qualquer ambiente cibernético, numa organização de qualquer setor, com foco principal nas pequenas e médias empresas, que são atualmente a maioria em nosso ecossistema empresarial.

O diferencial da metodologia proposta nesta dissertação aos estudos relacionados também dá-se pelo fato de demonstrar uma maneira para que as empresas possam iniciar um processo de implementação de controles de segurança, ou até mesmo melhorar um ambiente cibernético com algum nível de segurança já existente, relacionando o nível de segurança

buscado com o custo de investimento financeiro necessário, possibilitando a criação de um ambiente cibernético mais seguro e em conformidade, criando barreiras de proteção aos ataques cibernéticos mais comuns e praticados na atualidade.

Também será possível visualizar os custos individuais de cada controle de segurança e assim refazer escolhas mediante várias opções de estratégia e de mercado, diminuindo os custos quando necessário, resultando em valores menores, mantendo um nível similar de maturidade e conformidade com as normas e *frameworks* de segurança, além de auxiliar no entendimento dos tomadores de decisão sobre os investimentos necessários para desenvolver ou manter o ambiente cibernético seguro.

Por fim, a análise dos trabalhos relacionados deixa claro a importância da contribuição desta dissertação, fundamentando o desenvolvimento da metodologia proposta que será detalhada no próximo capítulo.

Capítulo 4

"Nós só podemos ver um pouco do futuro, mas o suficiente para perceber que há muito a fazer." (Alan Turing).

4 UMA METODOLOGIA PARA AVALIAÇÃO DE CUSTOS FINANCEIROS NA IMPLEMENTAÇÃO DE CONTROLES DE SEGURANÇA CIBERNÉTICA PARA PEQUENAS E MÉDIAS EMPRESAS

Este capítulo apresenta a principal contribuição desta dissertação, que é uma metodologia baseada em processo para definição e análise de custos financeiros na implementação de controles de segurança cibernética para pequenas e médias empresas.

Os processos estão representados na notação *BPMN*, formalismo amplamente difundido e aceito, para facilitar a sua adoção e aplicação por organizações interessadas. Esta metodologia aborda aspectos práticos para se obter uma estimativa de custo de uma implementação de controles de segurança cibernética de uma maneira sistemática e padronizada.

4.1 Visão Geral da Metodologia para Avaliação de Custos Financeiros na Implementação de Controles de Segurança Cibernética para PMEs

A metodologia proposta para estimar o custo financeiro inicial na implementação de controles de cibersegurança em ambientes cibernéticos genéricos de pequenas e médias empresas oferece um plano de ação para se obter os valores financeiros necessários para implementar segurança cibernética ou da informação no ambiente cibernético de qualquer organização, especialmente as pequenas e médias empresas.

A metodologia baseada em processo é ilustrada através de diversos diagramas realizados em *BPMN* e oferece informações sobre custos que entregam como resultado valores financeiros de cada etapa do projeto. Apesar da metodologia ser genérica e ter sido desenvolvida para atender ao maior número de organizações possível, são necessários alguns conhecimentos para que haja o entendimento do que é proposto.

Para entender todo o processo, é importante ter conhecimento da notação *BPMN*, pois a modelagem guia o aplicador da metodologia por um processo detalhado, com vários caminhos a serem escolhidos conforme a necessidade de cada ambiente, o que pode gerar resultados de custos distintos. Por este motivo, no capítulo 2, há uma explicação detalhada de todos os recursos utilizados neste trabalho de *BPMN*, conforme demonstra a Tabela 2.1.

O aplicador desta metodologia deve conter conhecimentos sólidos em segurança da informação e segurança cibernética. A metodologia proposta irá demonstrar, através da modelagem, atividades importantes e necessárias para atender aos requisitos das normas técnicas e dos *frameworks* de segurança adotados por um projeto, fazendo verificações quanto às aquisições de *hardware, software* e a utilização de recursos humanos em cada ação necessária de segurança utilizada.

O conhecimento em segurança da informação e em cibersegurança são necessários para entender o que as normas e os *frameworks* determinam para implementar segurança. O conhecimento nesta área também é necessário para criar um plano de ação e soluções de acordo com as necessidades do ambiente cibernético específico.

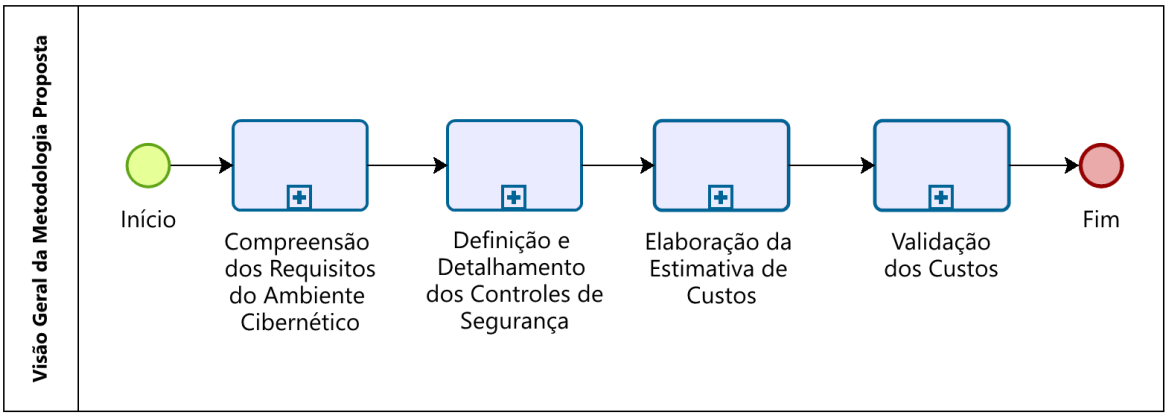
A proposta desta metodologia é abordar todo o recurso necessário para implementar a segurança cibernética e relacionar os custos financeiros necessários desta implementação, gerando como resultado vários custos, que serão explicados nas próximas subseções.

A metodologia proposta é dividida em 4 subprocessos principais. Estes subprocessos principais foram definidos após a realização de várias análises das normas técnicas e dos

frameworks de segurança cibernética, onde se buscou dividir as etapas principais de uma implementação de controles de segurança cibernética em um ambiente cibernético.

Através da metodologia proposta é possível estimar os custos financeiros para a implementação de controles de segurança cibernética em um ambiente cibernético genérico, seguindo a modelagem desenvolvida para ações de implementação de segurança cibernética na norma técnica ou *framework* adotado. A Figura 4.1 apresenta uma visão geral da metodologia proposta, que está dividida em 4 subprocessos principais.

Figura 4.1 - Visão Geral da Metodologia Proposta



Fonte: Autor, 2023.

O primeiro subprocesso é chamado de **Compreensão dos Requisitos do Ambiente Cibernético**. Este subprocesso tem o objetivo de obter informações sobre o tipo de negócio e entender o possível tratamento de dados no ambiente cibernético da empresa. Informações importantes como detalhar os recursos humanos de tecnologia da informação e fornecer informações sobre os espaços físicos da empresa expostos à metodologia são fornecidas neste subprocesso.

Durante a execução do segundo subprocesso, **Definição e Detalhamento dos Controles de Segurança**, serão analisadas informações sobre a contratação ou a utilização de recursos humanos existentes na organização, aquisições e/ou utilização de *hardware* existentes na organização, aquisições e/ou utilização de *software* existentes na organização.

Após definir as seleções descritas acima, os custos são calculados no subprocesso chamado de **Elaboração da Estimativa de Custos**, executando somas desenvolvidas para cada atividade geradora de custos, além de verificar a possibilidade de custos extras com a aquisição e/ou utilização de *hardware* e *software* em cada salvaguarda.

Por fim, no subprocesso definido como **Validação de Custos**, os custos devem ser avaliados junto ao cliente. Caso o cliente não esteja satisfeito com o custo obtido, o processo

poderá ser refeito e novas estimativas de custos poderão ser geradas por meio de novas escolhas em uma ou mais salvaguardas.

Depois de aprovado, o processo é finalizado e os valores de custos e a descrição das atividades são entregues ao cliente.

4.2 Subprocesso: Compreensão dos Requisitos do Ambiente Cibernético

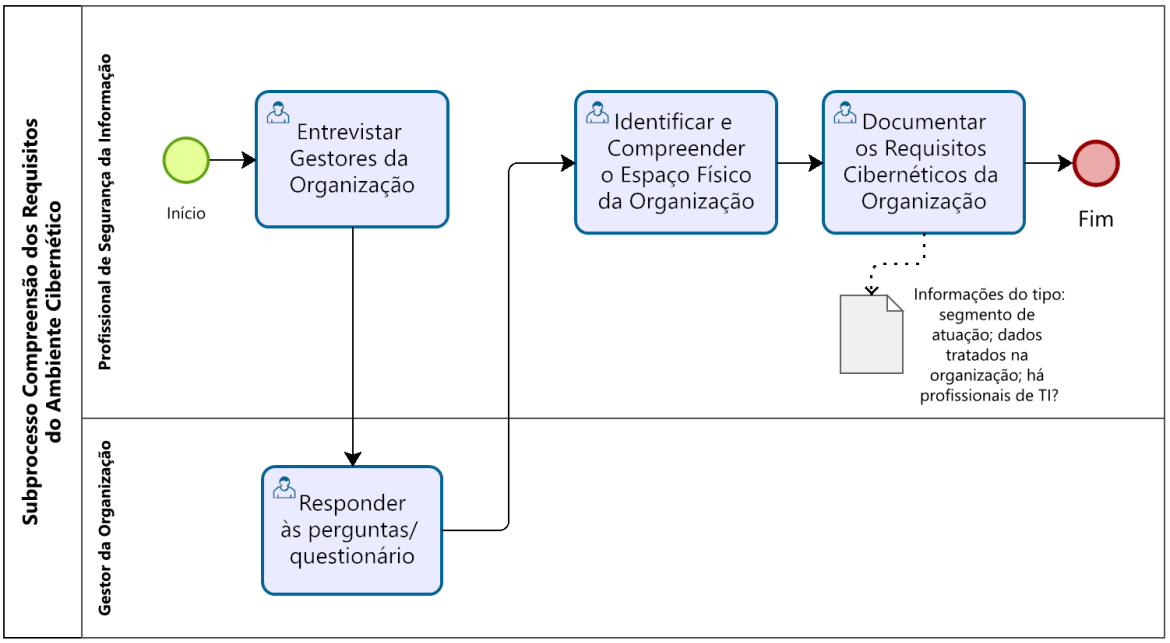
Neste subprocesso, o objetivo principal é compreender o ambiente cibernético da organização avaliada. Para tanto, propõe-se a realização de entrevista com o(s) gestor(es), diretores e/ou stakeholders envolvidos nos processos da empresa, através da atividade **Entrevistar Gestores da Organização**. Esta entrevista pode, por exemplo, ser realizada através de um formulário eletrônico com questões-chave predefinidas.

Os dados desta entrevista permitem compreender o tipo de negócio da empresa e até mesmo relacioná-la a um *framework* específico de segurança cibernética, ou ajustes exigidos em leis específicas do país em que a organização estiver inserida sempre que necessário. Existem leis e *frameworks* de segurança específicos para o setor da saúde (HIPAA, 2013) e o setor financeiro (FINRA, PCI-DSS, 2022), por exemplo.

Nessa entrevista inicial, é necessário documentar a existência de profissionais de tecnologia da informação na empresa. Além disso, é necessário verificar a existência de profissionais de TI com conhecimentos sólidos em segurança da informação e cibersegurança para realizar as ações descritas na metodologia proposta. Caso não exista profissional com esse perfil na organização, ele deverá ser contratado, e esse custo deverá ser considerado.

Em seguida, chega-se até a atividade **Identificar e Compreender o Espaço Físico da Organização**. Desta forma, ao analisar os controles de segurança cibernética utilizados no projeto da organização, é possível determinar instalações adequadas quanto ao armazenamento, controle de acesso e infraestrutura das redes de computadores da organização. Por fim, é necessário documentar todas as informações obtidas para executar o próximo subprocesso, por isso, a modelagem traz a atividade **Documentar os Requisitos Cibernéticos da Organização**. O modelo *BPMN* deste subprocesso está disponível na Figura 4.2.

Figura 4.2 - Subprocesso Compreensão dos Requisitos do Ambiente Cibernético.



Fonte: Autor, 2023.

As principais verificações e cada ação fundamental para a execução da metodologia proposta também podem ser compreendidas através da Tabela 4.1.

Tabela 4.1 - Ações do Subprocesso Compreensão dos Requisitos do Ambiente Cibernético.

Ação	**Ator**	**Descrição da atividade**
Entrevistar Gestores da Organização	Profissional de SI	Colher informações a respeito da organização; o tipo de dados tratado e manipulado pela empresa; saber se a empresa possui profissional de TI em segurança da informação.
Responder às perguntas/questionário	Gestor da Organização	Fornecer as informações solicitadas com clareza e assertividade.
Identificar e Compreender o Espaço Físico da Organização	Profissional de SI	Conhecer a infraestrutura física da empresa (desta forma pode-se definir melhor os serviços a serem utilizados, físicos ou em nuvem);
Documentar os Requisitos Cibernéticos da Organização	Profissional de SI	Documentar as informações para utilizá-las nos próximos subprocessos.

Fonte: Autor (2024).

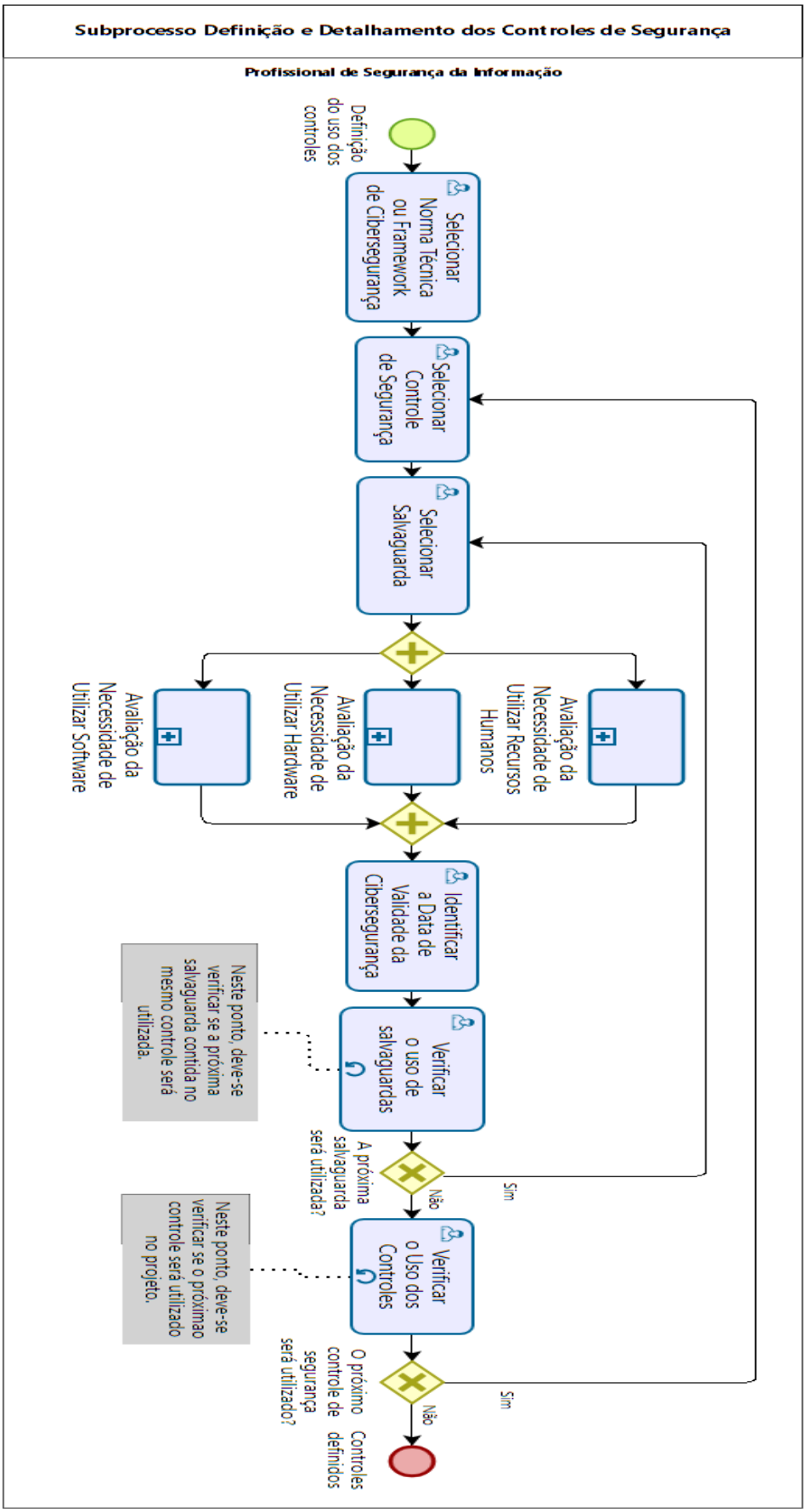
4.3 Subprocesso: Definição e Detalhamento dos Controles de Segurança

No subprocesso **Definição e Detalhamento dos Controles de Segurança**, são definidas e detalhadas as ações que implementam a segurança cibernética através da seleção de controles e de suas respectivas salvaguardas. A seleção de controles e salvaguardas, trazem de fato os mecanismos de segurança e determinam o nível de maturidade em segurança cibernética alcançado.

A atividade de destaque deste subprocesso principal é a que **define a norma técnica ou o *framework* a ser utilizado.** Também destacam-se os subprocessos **Avaliação da Necessidade de Utilizar Recursos Humanos, Avaliação da Necessidade de Utilizar *Hardware*** e o subprocesso **Avaliação da Necessidade de Utilizar *Software*,** uma vez que estas seleções geram vários custos no projeto. Outra atividade com grande importância para a metodologia proposta, é a atividade chamada de **Identificar a Data de Validade da Segurança Cibernética,** atividade esta que define a data limite da seguridade do ambiente cibernético.

A Figura 4.3 apresenta uma visão geral da modelagem do subprocesso **Definição e Detalhamento dos Controles de Segurança**. Este subprocesso possui outros três subprocessos internos, que também serão detalhados nesta seção.

Figura 4.3 - Subprocesso: Definição e Detalhamento dos Controles de Segurança



Fonte: Autor, 2023.

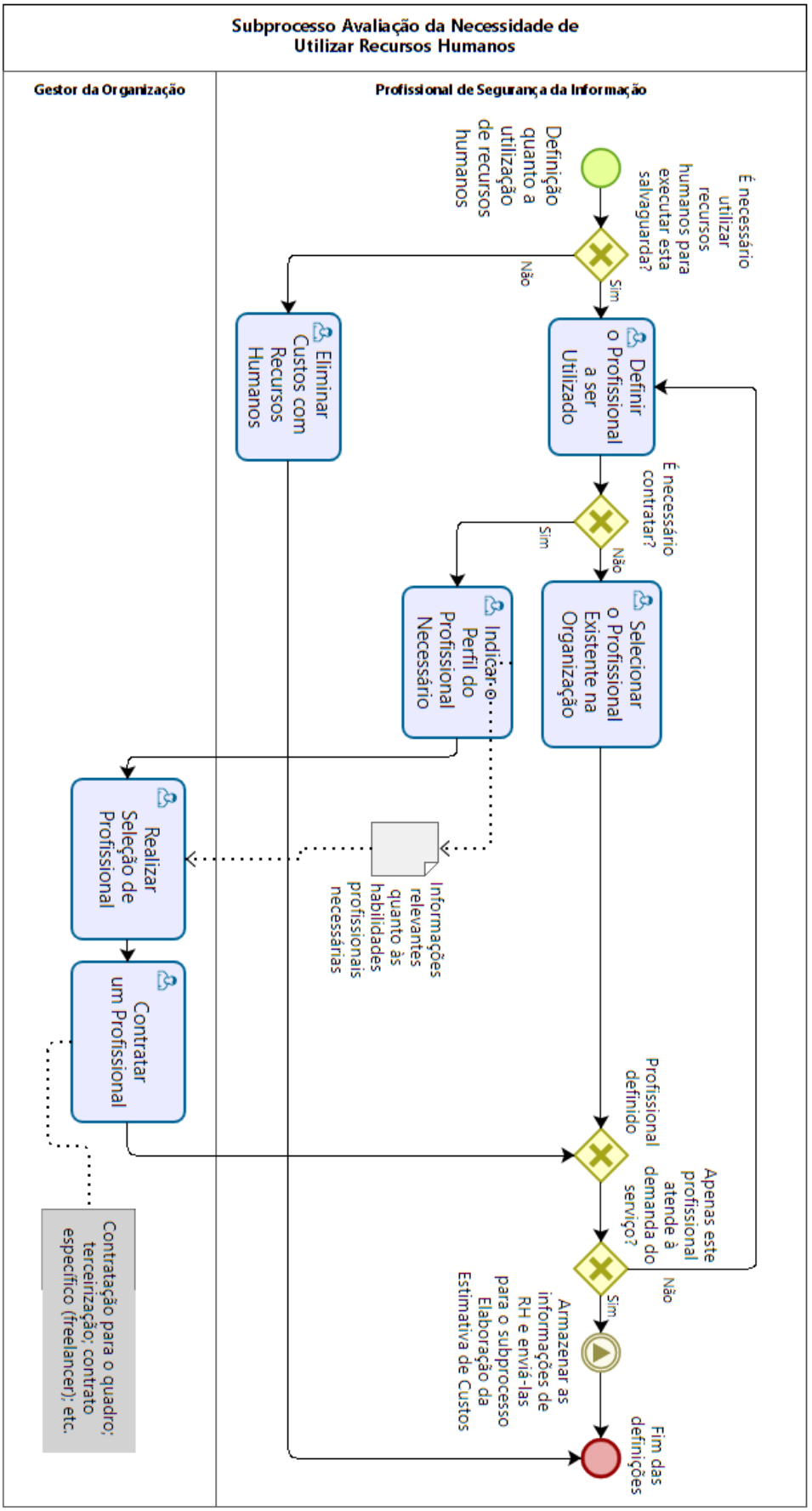
O processo inicia-se com a **seleção de uma norma técnica ou *framework* de segurança cibernética**. Em seguida, **seleciona-se um controle de segurança**, e posteriormente uma **salvaguarda** contida nesse mesmo controle. As principais verificações e cada ação fundamental para a execução do subprocesso **Definição e Detalhamento dos Controles de Segurança** também podem ser compreendidas através da Tabela 4.2.

Tabela 4.2 - Ações do Subprocesso Definição e Detalhamento dos Controles de Segurança.

Ação	**Ator**	**Descrição da atividade**
Selecionar norma técnica ou *framework* de cibersegurança	Profissional de SI	Definir qual a documentação será seguida para nortear a implementação de cibersegurança. Neste ponto, o aplicador da metodologia já tem informações suficientes para definir a norma técnica mais adequada ou o *framework* de cibersegurança mais adequado ao ambiente cibernético.
Selecionar controle de segurança	Profissional de SI	Deve-se selecionar o primeiro controle de segurança da documentação definida no passo anterior.
Selecionar salvaguarda	Profissional de SI	Deve-se selecionar a primeira salvaguarda (ação que implementa algum dispositivo de segurança cibernética) contida no controle selecionado no passo anterior.

Ao iniciar o subprocesso **Avaliação da Necessidade de Utilizar Recursos Humanos**, modelado na Figura 4.4, é verificada a utilização de recursos humanos para a implementação da salvaguarda.

Figura 4.4 - Subprocesso: Avaliação da Necessidade de Utilizar Recursos Humanos.



Fonte: Autor, 2023.

A principal tomada de decisão neste subprocesso é aquela que **pondera a demanda de serviço *versus* a mão de obra necessária** para executar a tarefa determinada pela salvaguarda. A quantidade de profissionais envolvidos em um projeto impacta significativamente nos custos. Essa relação negligenciada leva a contratações inesperadas que muitas vezes são mais custosas devido à falta de um planejamento adequado.

Após o levantamento dos requisitos relativos à utilização de recursos humanos, a informação é **armazenada** para ser posteriormente utilizada no subprocesso **Elaboração da Estimativa de Custos**. As principais verificações e cada ação fundamental para a execução do subprocesso **Avaliação da Necessidade de Utilizar Recursos Humanos** também podem ser compreendidas através da Tabela 4.3.

Tabela 4.3 - Ações do Subprocesso Avaliação da Necessidade de Utilizar Recursos Humanos.

Ação	Ator	Descrição da atividade
Decisão sobre utilizar recurso humano para executar a salvaguarda	Profissional de SI	Definir se há a necessidade de utilizar recurso humano para executar a atividade descrita na salvaguarda.
Eliminar o custo com recurso humano OU definir a utilização do recurso humano	Profissional de SI	A depender da decisão tomada no passo anterior, deve-se informar se não haverá custo com recurso humano, ou se o recurso humano se faz necessário.
Se necessário utilizar recurso humano, definir se haverá a contratação do profissional OU se haverá o aproveitamento de um profissional de segurança da informação disponível na empresa	Profissional de SI	Verificar se há profissional de segurança da informação disponível na empresa para executar a atividade da salvaguarda, ou se este profissional deve ser contratado.
Se necessário contratar, indicar o perfil do profissional necessário para atender a demanda da salvaguarda.	Profissional de SI	Fornecer ao gestor da empresa o perfil do profissional necessário, ou seja, descrever as habilidades profissionais fundamentais para a execução das atividades relacionadas à segurança cibernética.
Realizar a seleção do profissional de TI	Gestor da empresa	Solicitar ao setor de RH da empresa a contratação de um funcionário de TI
Contratar o profissional em	Gestor da empresa	Realizar a contratação do

segurança da informação		profissional de TI
Ponderar a quantidade de profissional de TI *versus* a demanda de serviço exigido pela salvaguarda.	Profissional de SI	Verificar se o profissional de TI é suficiente para a demanda de serviço associada à salvaguarda, ou se deve haver mais profissionais para execução da tarefa.
Armazenar as informações para que possam ser utilizadas no subprocesso Elaboração da Estimativa de Custos	Profissional de SI	Detalhar as informações sobre o recurso humano utilizado e definir os seus respectivos custos.

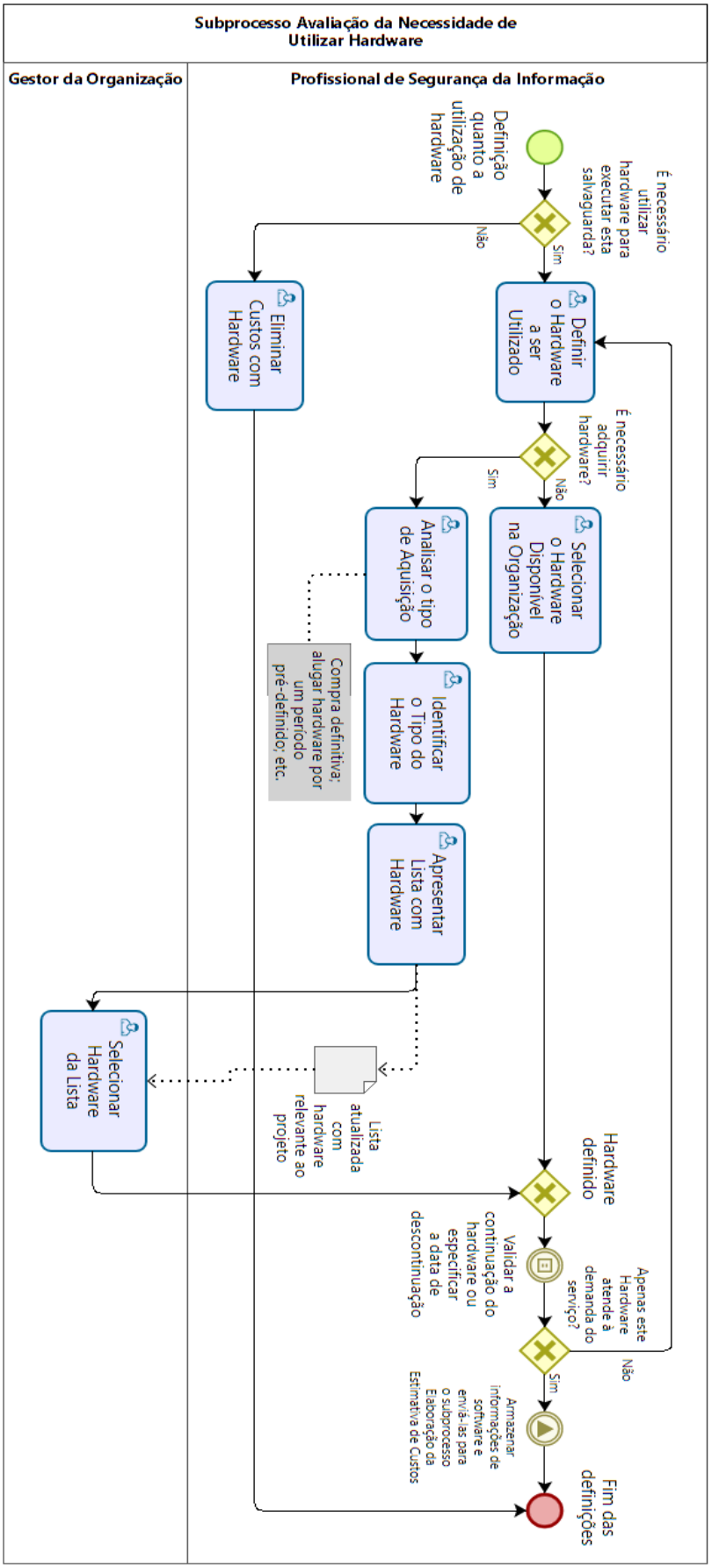
Fonte: Autor (2024).

O próximo subprocesso, **Avaliação da Necessidade de Utilizar *Hardware***, verifica a necessidade de utilização de *hardware* para implementação da salvaguarda. Muitas salvaguardas incluem o uso de *hardware* para fornecer algum nível ou camada de segurança no ambiente cibernético.

Por exemplo, no *CIS v8*, na salvaguarda 4.4, a implementação de *firewall* para servidores é especificada. Esse *firewall* geralmente é executado em computadores físicos da organização ou através de *hardware* próprio. Outro exemplo prático do uso de *hardware* para atender aos requisitos de segurança cibernética ou da informação, segundo exigências da norma técnica ou do *framework* de cibersegurança, é a utilização de servidores físicos, para suportar servidores lógicos, geralmente sistemas de *backups* ou sistemas operacionais controladores de domínio, que gerenciam as atividades lógicas dentro de um ambiente cibernético, como o controle de acesso a dados, *logins* em horários específicos, registro de *logs* para realização de auditorias, além de várias outras práticas de gerenciamento que os servidores de rede e infraestrutura dispõem a uma organização.

A Figura 4.5 ilustra todo o modelo do subprocesso **Avaliação da Necessidade de Utilizar Hardware**.

Figura 4.5 - Subprocesso: Avaliação da Necessidade de Utilizar *Hardware*



Fonte: Autor. 2023.

Quando há necessidade de aquisição de novo *hardware* para o projeto, este subprocesso possui uma atividade importante, que fornece uma lista de recomendações de aquisição de *hardware*. A lista é apresentada ao cliente para uma tomada de decisão mais assertiva, evitando aquisições inadequadas ou insuficientes para atender aos requisitos de salvaguarda e do ambiente cibernético. Um erro deste tipo pode ter grande impacto nos custos finais de um projeto, pois pode ocorrer diversas vezes, em cada ação de segurança implementada.

Além disso, há também o evento que **valida o uso do *hardware*** no projeto. Esta validação acontece através de um estudo junto ao fabricante do *hardware* utilizado, sobre a condição do mesmo suportar aplicações atuais que recebam atualizações e *patches* de segurança. A data de validação do *hardware* pode ser definida como indeterminada, ou ter uma data específica de descontinuação, uma vez que o *hardware* torne-se obsoleto.

Outra importante tomada de decisão, é a que **pondera a demanda do serviço *versus* a disponibilidade de *hardware***. A quantidade de *hardware* deve sempre atender às necessidades do ambiente cibernético e aos requisitos de salvaguarda.

Por fim, as informações são **armazenadas em um evento** para serem posteriormente utilizadas no subprocesso **Elaboração da Estimativa de Custos**. As principais verificações e cada ação fundamental para a execução do subprocesso **Avaliação da Necessidade de Utilizar *Hardware*** também podem ser compreendidas através da Tabela 4.4.

Tabela 4.4 - Ações do Subprocesso Avaliação da Necessidade de Utilizar *Hardware*.

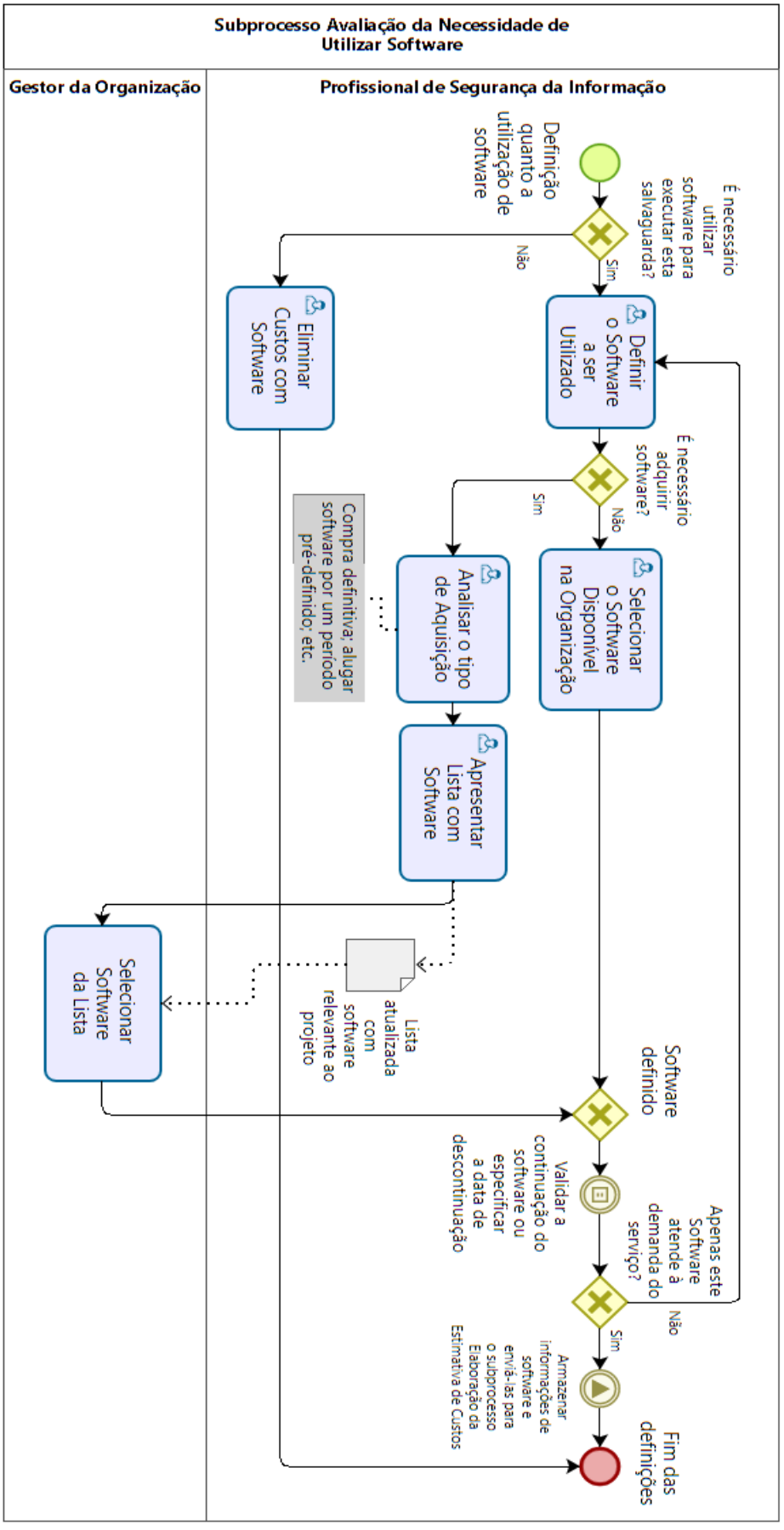
Ação	Ator	Descrição da atividade
Decisão sobre utilizar *hardware* para executar a salvaguarda	Profissional de SI	Definir se há a necessidade de utilizar *hardware* para executar a atividade descrita na salvaguarda
Eliminar o custo com *hardware* OU definir a utilização do mesmo	Profissional de SI	A depender da decisão tomada no passo anterior, deve-se informar se não haverá custo com *hardware*, ou se o *hardware* se faz necessário.
Decisão sobre adquirir ou não um *hardware*	Profissional de SI	Deve-se indicar a utilização de um *hardware* disponível na organização, ou indicar o tipo de aquisição de *hardware*.
Selecionar o *hardware* disponível na organização	Profissional de SI	Caso tenha sido tomada no passo anterior a decisão de não adquirir um *hardware*, deve-se selecionar um *hardware* já disponível na empresa que atenda aos requisitos da salvaguarda.

Analisar o tipo de aquisição	Profissional de SI	Caso tenha sido tomada no passo anterior a decisão de adquirir um *hardware*, deve-se analisar o tipo de aquisição, ou seja, geralmente uma compra definitiva do *hardware* ou é realizado o aluguel do *hardware* mediante contrato.
Identificar o tipo do *hardware*	Profissional de SI	Definir se o *hardware* será físico ou virtual.
Apresentar lista com *hardware*	Profissional de SI	Disponibilizar ao Gestor da empresa uma lista com opções de *hardware* relevantes ao projeto, que atendam às necessidades da salvaguarda e também do ambiente cibernético. Desta maneira, evita-se a aquisição de *hardware* insuficiente, ou até mesmo um super *hardware*, elevando o custo do projeto sem necessidade.
Selecionar *hardware* da lista	Gestor da empresa	Definir qual o *hardware* da lista será adquirido.
Validar a continuação do *hardware* ou especificar a data de descontinuação	Profissional de SI	Verificar se o *hardware* existente na organização e aproveitado para o projeto está obsoleto. Caso positivo, o *hardware* deve ser descartado e uma aquisição de *hardware* deve ser realizada. Caso o caminho escolhido tenha sido o de adquirir um *hardware*, verificar se o *hardware* adquirido suporta os sistemas mais atuais, evitando assim a aquisição de um *hardware* não atual.
Decisão sobre o *hardware* ser suficiente para suprir a demanda do serviço	Profissional de SI	Verificar se o *hardware* em questão supre a necessidade da salvaguarda, ou se será necessário a utilização de mais *hardware.*
Armazenar as informações de *hardware* e enviá-las ao subprocesso Elaboração da Estimativa de Custo.	Profissional de SI	Armazenar detalhadamente todas as informações referente ao *hardware* para que possam ser utilizadas no próximo subprocesso.

Fonte: Autor (2024).

Depois de analisar os requisitos de *hardware* e dos recursos humanos, é hora de avaliar os requisitos de *software*. O subprocesso **Avaliação da Necessidade de Utilizar *Software***, mostrado na Figura 4.6, é semelhante ao de *hardware*, mas traz consigo informações específicas sobre o *software*.

Figura 4.6 - Subprocesso: Avaliação da Necessidade de Utilizar *Software*.



Fonte: Autor, 2023.

Assim como no subprocesso anterior, quando é necessária a aquisição de novos *softwares*, este subprocesso traz uma **lista com recomendações de *software*** adequados aos requisitos da salvaguarda e aos requisitos do ambiente cibernético.

Após as definições de qual *software* utilizar, deve-se **validar** o uso do *software* através do evento que **verifica a continuação ou descontinuação do *software***. De acordo com os documentos analisados, *frameworks* e padrões técnicos de segurança cibernética e da informação já mencionados, um ambiente cibernético seguro não pode haver *software* descontinuado (*CIS v8*, 2021), pois *software* nesta condição não recebe mais atualizações de segurança que corrigem vulnerablidades descobertas ao longo de sua vida útil.

Em seguida, há a importante tomada de decisão que **pondera a demanda do serviço *versus* a disponibilidade do *software***. A quantidade de *software* deve sempre atender às necessidades do ambiente cibernético e aos requisitos de salvaguarda. Por fim, as informações são **armazenadas no evento** para serem posteriormente utilizadas no subprocesso **Elaboração da Estimativa de Custos**.

Em sequência, é necessário executar a atividade **Identificar a Data de Validade da Cibersegurança** (ver Figura 4.3). Dada a importância do fato de não se permitir *software* descontinuado ou *hardware* obsoleto em um ambiente cibernético, esta atividade analisa as informações constantes no evento de cada *hardware* e cada *software* existente no projeto, para definir uma possível data de descontinuação de algum recurso utilizado.

Caso haja algum *hardware* ou *software* com data definida de descontinuação por seus mantenedores ou desenvolvedores no ambiente cibernético, esta data será definida por esta metodologia como a data de vencimento da segurança cibernética do ambiente. Uma vez que um recurso seja descontinuado e não receba mais atualizações de segurança, este ambiente torna-se inseguro, devendo a organização substituí-lo, antes mesmo da expiração desta data informada.

Em seguida, é necessário **verificar se todas as salvaguardas do controle foram analisadas**, e posteriormente **verificar o uso de todos os controles** envolvidos no projeto. Assim que todos os controles e salvaguardas tiverem suas definições realizadas, é possível partir para o próximo subprocesso, **Elaboração da Estimativas de Custos**. As principais verificações e cada ação fundamental para a execução do subprocesso **Avaliação da Necessidade de Utilizar *Software*** também podem ser compreendidas através da Tabela 4.5.

Tabela 4.5 - Ações do Subprocesso Avaliação da Necessidade de Utilizar *Software*.

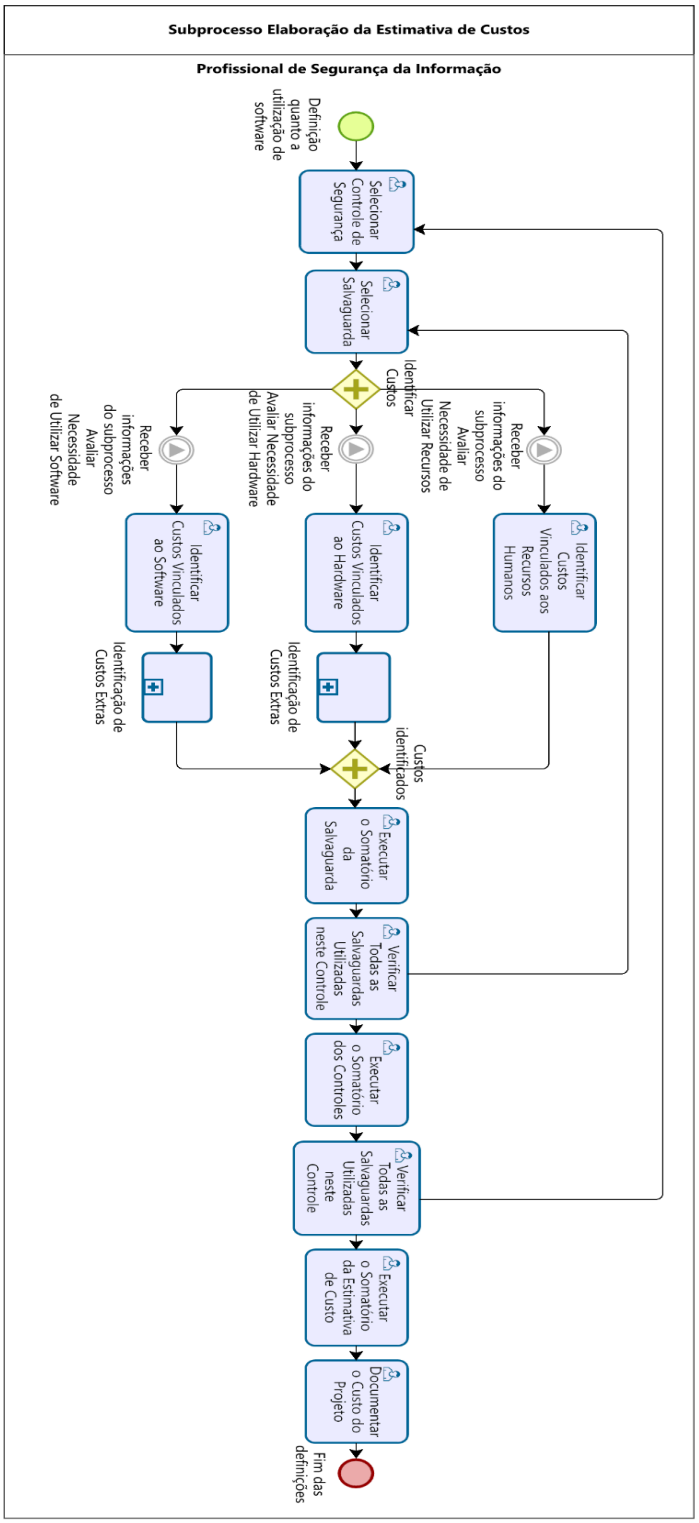
Ação	Ator	Descrição da atividade
Decisão sobre utilizar *software* para executar a salvaguarda	Profissional de SI	Definir se há a necessidade de utilizar *software* para executar a atividade descrita na salvaguarda.
Eliminar o custo com *software* OU definir a utilização do mesmo	Profissional de SI	A depender da decisão tomada no passo anterior, deve-se informar se não haverá custo com *software*, ou se o *software* se faz necessário.
Decisão sobre adquirir ou não um *software*	Profissional de SI	Deve-se indicar a utilização de um *software* disponível na organização, ou indicar o tipo de aquisição de *software*.
Selecionar o *software* disponível na organização	Profissional de SI	Caso tenha sido tomada no passo anterior a decisão de não adquirir um *software*, deve-se selecionar um *software* já disponível na empresa que atenda aos requisitos da salvaguarda.
Analisar o tipo de aquisição	Profissional de SI	Caso tenha sido tomada a decisão de adquirir um *software* no passo anterior, deve-se analisar o tipo de aquisição, ou seja, geralmente uma compra definitiva do *software* ou é realizado o aluguel do *software* mediante contrato.
Apresentar lista com *software*	Profissional de SI	Disponibilizar ao Gestor da empresa uma lista com opções de *software* relevantes ao projeto, que atendam às necessidades da salvaguarda e também do ambiente cibernético. Desta maneira, evita-se a aquisição de *software* insuficiente, ou até mesmo um super *software*, elevando o custo do projeto sem necessidade.
Selecionar *software* da lista	Gestor da empresa	Definir qual o *software* da lista será adquirido.
Validar a continuação do *software* ou especificar a data de descontinuação	Profissional de SI	Verificar se o *software* está descontinuado ou tem data de descontinuação divulgada pela empresa. Se descontinuado, um *software* atualizado deve ser adquirido. Se houver data de descontinuação divulgada, esta data precisa ser explícita ao pessoal envolvido no projeto de segurança, pois uma vez que esta data seja atingida, o ambiente cibernético estará vulnerável a incidentes cibernéticos.
Decisão sobre o *software* ser suficiente para suprir a demanda do serviço	Profissional de SI	Verificar se o *software* em questão supre a necessidade da salvaguarda, ou se será necessário a utilização de mais *software.*
Armazenar as informações de software e enviá-las ao subprocesso Elaboração da Estimativa de Custo.	Profissional de SI	Armazenar detalhadamente todas as informações referente ao *software* para que possam ser utilizadas no próximo subprocesso.

Fonte: Autor (2024).

4.4 Subprocesso: Elaboração da Estimativa de Custos

A estimativa de custos será gerada durante a execução do subprocesso **Elaboração da Estimativa de Custos**, conforme mostrado na Figura 4.7.

Figura 4.7 - Subprocesso Elaboração da Estimativa de Custos



Fonte: Autor, 2023.

Como resultado, este subprocesso irá detalhar o custo de cada salvaguarda, cada controle e, finalmente, o custo total de implementação dos controles de segurança cibernética da organização.

Este subprocesso começa com a **seleção de um controle de segurança** e posteriormente também especifica a **seleção de uma salvaguarda**. Os custos contidos numa salvaguarda são os seguintes: Custo de Recursos Humanos (CRH), Custo de *Hardware* (CHW) e seus possíveis custos extras, Custo de *Software* (CSW) e seus possíveis custos extras.

Seguindo a modelagem, é necessário identificar o custo de cada atividade geradora de custo de uma salvaguarda. Nesta etapa, são **recebidas as informações dos subprocessos anteriores**, com as suas respectivas seleções e custos atrelados. A execução do subprocesso, até este ponto pode ser também apreciada através da Tabela 4.6

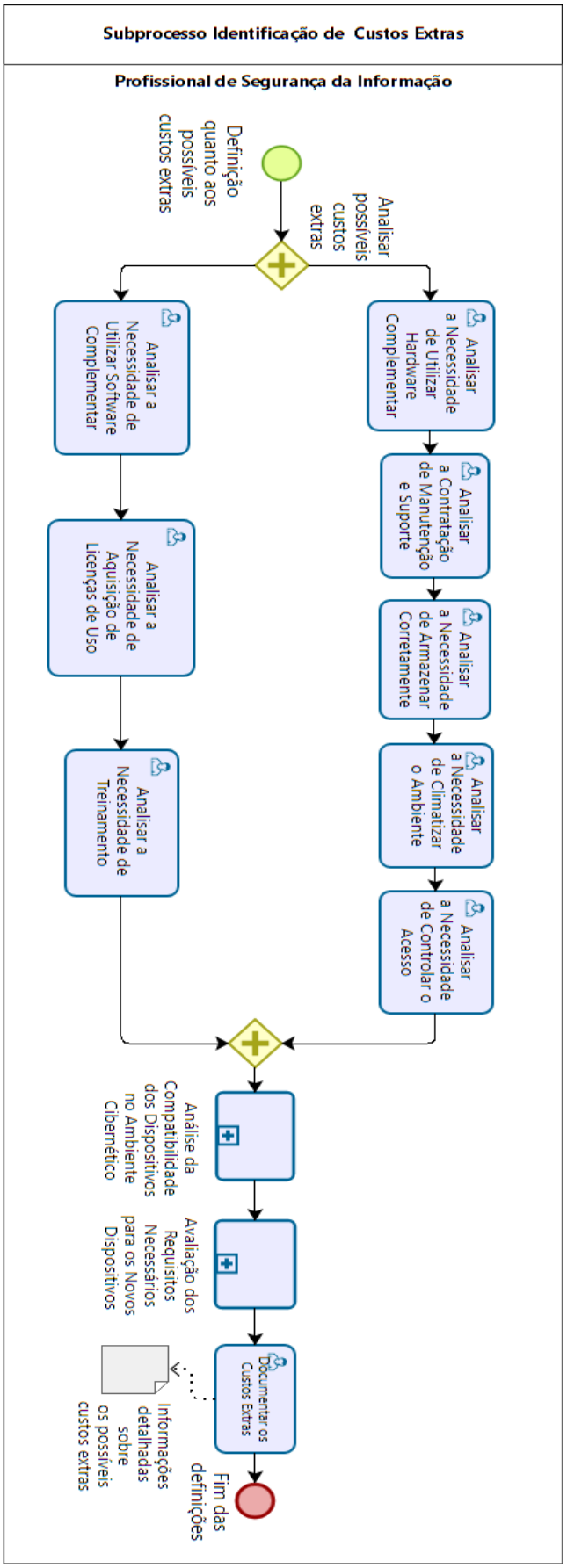
Tabela 4.6 - Ações do Subprocesso Elaboração da Estimativa de Custos.

Ação	**Ator**	**Descrição da atividade**
Selecionar controle de segurança	Profissional de SI	Determinar qual o controle de segurança será utilizado.
Selecionar salvaguarda	Profissional de SI	Determinar qual a salvaguarda será utilizada.
Receber informações sobre avaliar a necessidade de utilizar recursos humanos	Profissional de SI	Receber as informações geradas no subprocesso anterior, detalhando as características de cada recurso humano utilizado e seus respectivos custos associados.
Identificar os custos vinculados aos recursos humanos	Profissional de SI	Obter os custos vinculados aos recursos humanos para poder gerar a estimativa de custo.
Receber informações sobre avaliar a necessidade de utilizar *hardware*	Profissional de SI	Receber as informações geradas no subprocesso anterior, detalhando as características de cada *hardware* utilizado e seus respectivos custos associados
Identificar os custos vinculados ao *hardware*	Profissional de SI	Obter os custos vinculados ao *hardware* para poder gerar a estimativa de custo.
Receber informações sobre avaliar a necessidade de utilizar *software*	Profissional de SI	Receber as informações geradas no subprocesso anterior, detalhando as características de cada *software* utilizado e seus respectivos custos associados
Identificar os custos vinculados ao *software*	Profissional de SI	Obter os custos vinculados ao *software* para poder gerar a estimativa de custo.

Fonte: Autor (2024).

Após as atividades **Identificar os Custos Vinculados ao *Hardware*** e **Identificar os Custos Vinculados ao *Software,*** é necessário **verificar a possibilidade de seus respectivos custos extras**, através da execução do subprocesso **Identificação de Custos Extras** conforme demonstra a Figura 4.8.

Figura 4.8 - Subprocesso Identificação de Custos Extras



Fonte: Autor, 2023.

Os custos extras podem ser formados por atividades geradoras de custos, como a possibilidade de **aquisição de um *hardware* ou *software* complementar**, **contratação de manutenção e suporte**, **proporcionar um armazenamento adequado**, **controlar a temperatura do ambiente**, **controlar o acesso físico**, **adquirir licença de uso**, **treinamento e suporte a sistemas**. As principais verificações e cada ação fundamental para a execução do subprocesso **Identificação de Custos Extras** também podem ser compreendidas através da Tabela 4.7.

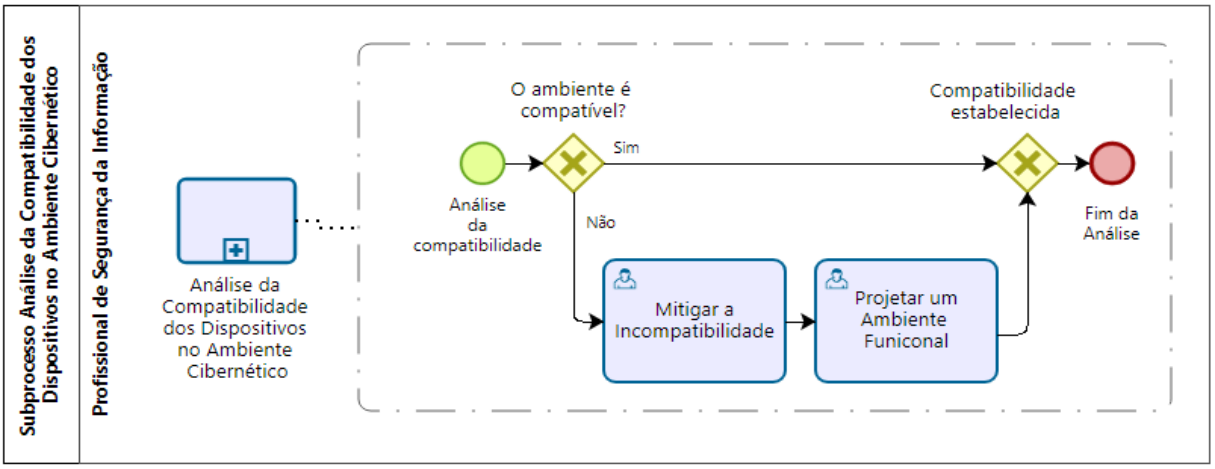
Tabela 4.7 - Ações do Subprocesso Identificação de Custos Extras.

Ação	**Ator**	**Descrição da atividade**
Analisar a necessidade de utilizar *hardware* complementar	Profissional de SI	Há *hardware* e *software* que exigem a utilização de *hardware* específico ou *hardware* complementar para que se obtenha o funcionamento adequado. Logo, em toda utilização de *hardware* ou *software* deve-se ter este cuidado para que não haja erros na execução do projeto.
Analisar a contratação de manutenção e suporte	Profissional de SI	Há *hardware* e *software* que dependem de manutenção e suporte especializado. Desta forma, este custo precisa ser considerado.
Analisar a necessidade de armazenar corretamente	Profissional de SI	Há *hardware* que necessita de um armazenamento específico. Logo, faz-se necessário sempre verificar a questão de armazenamento do *hardware* utilizado no projeto.
Analisar a necessidade de climatizar o ambiente	Profissional de SI	É necessário que o *hardware* esteja sempre em um ambiente climatizado, com temperaturas baixas e controladas. Caso o espaço físico da empresa não tenha um ambiente nestas condições, isto precisa ser providenciado e seu custo deve ser considerado.
Analisar a necessidade de controlar o acesso	Profissional de SI	Acesso ao CPD deve sempre ser controlado. Caso a empresa não tenha um controle de acesso já estabelecido, este custo deve ser considerado.
Analisar a necessidade de utilizar *software* complementar	Profissional de SI	Há *hardware* e *software* que exigem a utilização de *software* específico ou *software* complementar para que se obtenha o funcionamento adequado. Logo, em toda utilização de *hardware* ou *software* deve-se ter este cuidado para que não haja erros na execução do projeto.
Analisar a necessidade de aquisição de licenças de uso	Profissional de SI	Verificar se o *software* a ser utilizado no projeto requer uma licença de uso. Os custos neste quesito podem variar bastante.
Analisar a necessidade de treinamento	Profissional de SI	Vários *hardware* e *software* demandam mão de obra especializada para ser utilizado. É comum que o treinamento a estes dispositivos tenha um custo associado.

Fonte: Autor (2024).

Após estas verificações, faz-se necessário **analisar a compatibilidade e a interoperabilidade** dos dispositivos que compõem o ambiente cibernético, conforme ilustra a Figura 4.9.

Figura 4.9 - Subprocesso Análise da Compatibilidade dos Dispositivos no Ambiente Cibernético.



Fonte: Autor, 2023.

O subprocesso inicia com a **verificação do ambiente ser compatível**. Se positivo, o processo é encerrado. Caso contrário, é necessário **mitigar a incompatibilidade** dos dispositivos que compõem o projeto e posteriormente deve-se **projetar um ambiente funcional**, levando em consideração as particularidades de cada dispositivo utilizado. Uma vez ajustada a questão de incompatibilidades, o processo pode ser encerrado. As principais verificações e cada ação fundamental para a execução do subprocesso **Análise da Compatibilidade dos Dispositivos no Ambiente Cibernético** também podem ser compreendidas através da Tabela 4.8.

Tabela 4.8 - Ações do Subprocesso Análise da Compatibilidade dos Dispositivos no Ambiente Cibernético.

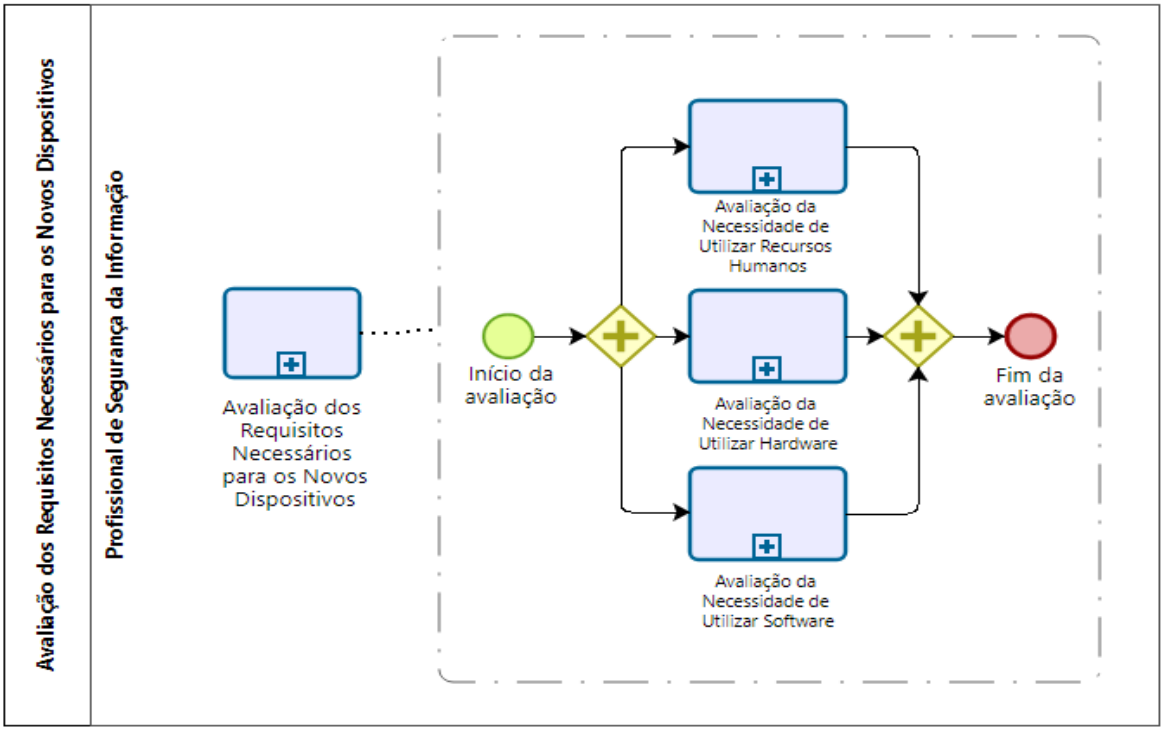
Ação	**Ator**	**Descrição da atividade**
Verificar se a compatibilidade do ambiente cibernético	Profissional de SI	Verificar se os dispositivos utilizados no projeto de segurança do ambiente cibernético são compatíveis. Se positivo, o processo é encerrado.
Mitigar a incompatibilidade	Profissional de SI	Analisar e pontuar todo o problema de incompatibilidade entre os dispositivos que compõem o espaço cibernético da empresa.
Projetar um ambiente funcional	Profissional de SI	Resolver todos os problemas de incompatibilidade

		do ambiente cibernético da empresa.

Fonte: Autor (2024).

Em seguida é **avaliado os requisitos necessários para os novos dispositivos**, onde novamente é verificado a **utilização de recursos humanos**, ***hardware*** e ***software*** necessários para compor a perfeita execução dos possíveis novos recursos adicionados ao ambiente cibernético, conforme ilustra a imagem 4.10.

Figura 4.10 - Subprocesso Avaliação dos Requisitos Necessários para os Novos Dispositivos.



Fonte: Autor, 2023.

Neste ponto, são executados os mesmos subprocessos descritos anteriormente (ver Figura 4.4, Figura 4.5 e Figura 4.6). Para verificar as ações fundamentais para a execução do subprocesso **Avaliação dos Requisitos Necessários para os Novos Dispositivos** através de tabela, ver Tabela 4.3, Tabela 4.4 e Tabela 4.5.

Por fim, tudo deve ser **documentado** para posteriormente ser usado nas atividades seguintes. Após as definições dos possíveis custos extras, é possível prosseguir na modelagem até a atividade **Executar o Somatório da Salvaguarda** (ver Figura 4.7).

Mais uma vez, vale ressaltar que o custo de uma salvaguarda será formado pelo custo atrelado à utilização de recursos humanos, aquisição e/ou utilização de *hardware* e seus possíveis custos extras, aquisição e/ou utilização de *software* e seus possíveis custos extras.

O custo com os recursos humanos (CRH) será definido através das seguintes equações:

- Ctp = Custo de cada tipo de profissional
- tP = Tipo do profissional
- vP = Valor do profissional
- qP = Quantidade de profissionais

$$Ctp = (tP \times vP) \times qP$$

$$CRH = \sum_{i=1}^{n} Ctp_i$$

Para cada tipo de profissional diferente, é necessário aplicar a equação **Ctp** para definir o valor monetário de cada tipo de profissional. É natural que uma organização tenha mais de um profissional, e estes profissionais tenham cargos diferentes, o que ocasiona custos também distintos. Só após a definição de todos os valores dos tipos de profissionais diferentes, é executado o cálculo do somatório **CRH**.

O custo com o *Hardware* (CHW) será definido através das seguintes equações:

- Cth = Custo com o tipo de *hardware*
- tH = Tipo do *hardware*
- vH = Valor do *hardware*
- qH = Quantidade de *hardware*
- Ce = Custo extra

$$Cth = [(tH \times vH) \times qH] + Ce$$

$$CHW = \sum_{i=1}^{n} Cth_i$$

Em uma única salvaguarda, pode ser utilizado mais de um *hardware* para atender aos requisitos da mesma. Desta forma, é necessário aplicar a equação **Cth** em todo *hardware* diferente, para só depois calcular o somatório **CHW**.

O custo com o *Software* (CSW) será definido através das seguintes equações:

- Cts = Custo com o tipo de *software*
- tS = Tipo do *software*
- vS = Valor do *software*
- qS = Quantidade de *software*
- Ce = Custo extra

$$Cts = [(tS \times vS) \times qS] + Ce$$

$$CSW = \sum_{i=1}^{n} Cts_i$$

Assim como no *hardware*, em uma única salvaguarda, pode ser utilizado mais de um *software* para atender aos requisitos da mesma. Desta forma, é necessário aplicar a equação **Cts** em todo *software* diferente, para só depois calcular o somatório **CSW**.

A soma dos custos contidos nestes subprocessos determinam o valor do Custo da Salvaguarda (CSG), que se dará pela seguinte equação:

$$CSG = \Sigma CRH + \Sigma CHW + \Sigma CSW$$

Após realizar os cálculos de projeção de custos para todas as salvaguardas do mesmo controle, é necessário calcular o custo do controle como um todo. Uma atividade específica soma os valores de todas as salvaguardas utilizadas para um mesmo controle, para obter o valor do Custo do Controle (CC) selecionado.

Essa soma é realizada através da seguinte equação:

$$CC = \sum_{i=1}^{n} CSG_i$$

Após realizar os cálculos de projeção de custos para todos os controles individualmente, é necessário somar os custos de todos esses controles para obter o custo total estimado da implementação da segurança cibernética na organização. O custo total de um projeto é definido pela equação chamada de ECISC.

Esta soma final será calculada usando a seguinte equação:

$$ECISC = \sum_{i=1}^{n} CC_i$$

Por fim, é gerado um documento com todos os custos envolvidos no projeto.

4.5 Subprocesso: Validação dos Custos

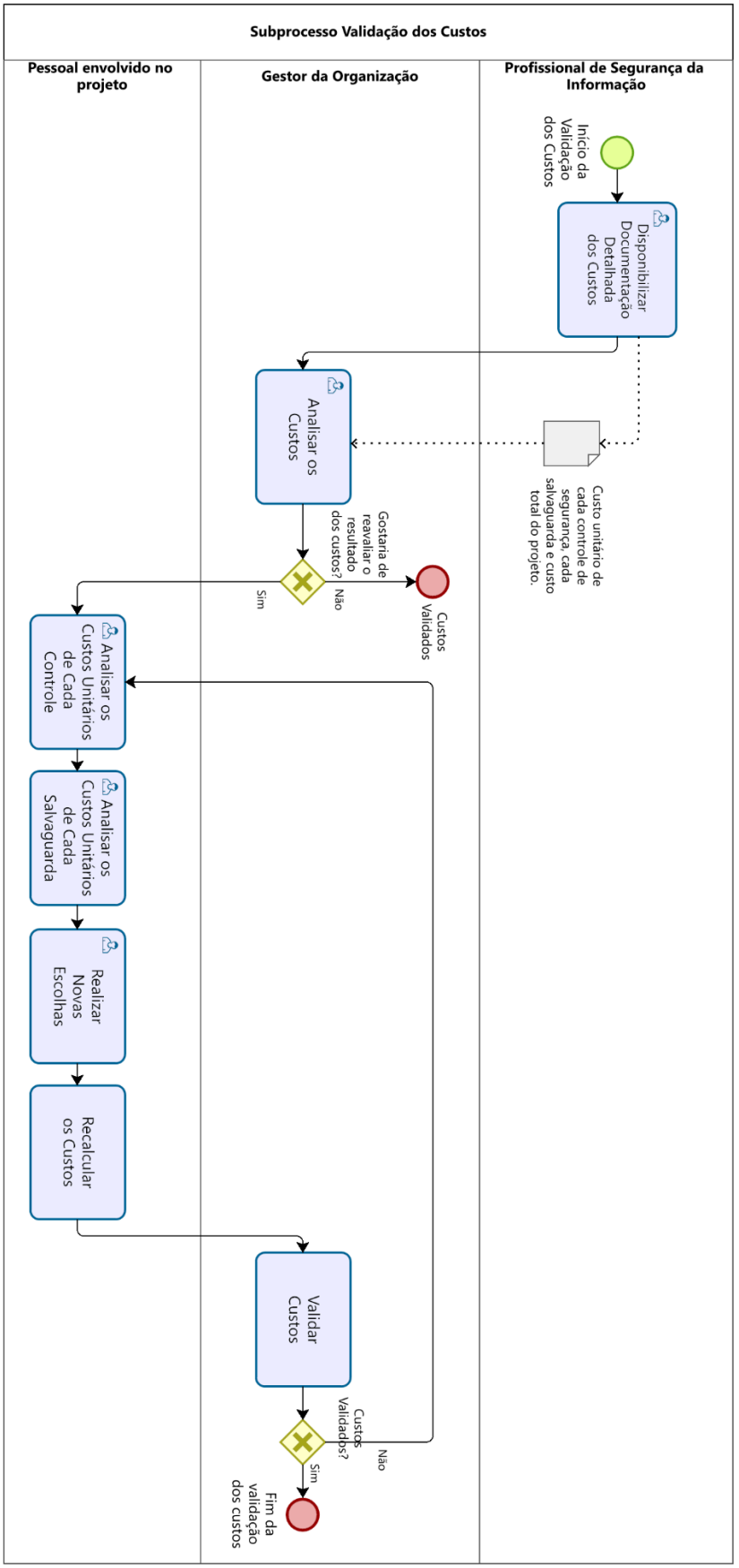
O subprocesso **Validação dos Custos** é usado para avaliar os custos projetados associados à melhoria da segurança cibernética com o cliente. Para iniciar a validação dos custos gerados, é entregue ao cliente o resultado da somatória (ECISC) através da atividade **Disponibilizar Documentação Detalhada dos Custos,** realizada no subprocesso **Elaboração da Estimativa de Custos**. Os custos são demonstrados ao cliente com o valor unitário de cada salvaguarda, cada controle, além do custo total do projeto.

Caso o cliente pretenda **reavaliar os valores de custos**, de maneira que estes possam ser mais atrativos e adequados à sua realidade financeira, novas escolhas deverão ser feitas relativamente à implementação de salvaguardas e controles de cibersegurança, e essas escolhas poderão impactar questões de custos relacionadas com o uso de recursos humanos, *hardware* e *software* no projeto.

A partir de novas escolhas, é possível gerar novas estimativas de custos. Este novo orçamento é novamente apresentado ao cliente para uma nova avaliação e pode ser refeito diversas vezes até um determinado valor de custo aceitável.

Ao longo deste subprocesso são avaliados o benefício da implementação da salvaguarda, do controle e do investimento financeiro necessário. Deseja-se um equilíbrio adequado entre a qualidade da melhoria da segurança e o possível custo a ser investido pelo cliente. O modelo *BPMN* do subprocesso é mostrado na Figura 4.11.

Figura 4.11 - Subprocesso Validação dos Custos



Fonte: Autor, 2023.

As principais verificações e cada ação fundamental para a execução do subprocesso **Validação dos Custos** também podem ser compreendidas através da Tabela 4.9.

Tabela 4.9 - Ações do Subprocesso Validação dos Custos.

Ação	Ator	Descrição da atividade
Disponibilizar documentação detalhada dos custos	Profissional de SI	O custo de cada controle, cada salvaguarda e de todo o projeto deve ser entregue ao gestor da empresa.
Analisar os custos	Gestor da empresa	Tomar ciência de todos os custos do projeto.
Decisão sobre reavaliar o custos	Gestor da empresa	Decidir se o projeto continua com os custos e os dispositivos associados a ele, ou se reavalia os custos com o objetivo de diminuir o valor financeiro com a substituição dos dispositivos de segurança.
Analisar o custo unitário de cada controle	Pessoal envolvido no projeto	Tomar ciência dos custos de cada controle utilizado no projeto.
Analisar o custo unitário de cada salvaguarda	Pessoal envolvido no projeto	Tomar ciência dos custos de cada salvaguarda utilizada no projeto.
Realizar novas escolhas	Pessoal envolvido no projeto	Definir qual(is) controle(s) e salvaguardas serão modificados para que a diminuição de custos aconteça.
Recalcular os custos	Pessoal envolvido no projeto	Reutilizar os somatórios da metodologia para recalcular os custos dos controles e salvaguardas modificadas.
Validar custos	Gestor da empresa	Os novos custos devem ser entregues ao gestor da empresa para nova análise. Caso positivo, o processo pode ser encerrado. Se negativo, o diagrama retorna até a atividade de selecionar o controle e segue o fluxo das atividades até que a validação dos custos aconteça.

Fonte: Autor (2024).

4.6 Considerações Finais

Este capítulo apresentou a principal contribuição desta dissertação. O processo necessário para se obter uma estimativa de custo financeiro para a realização de uma implementação de controles de segurança em um ambiente cibernético foi modelado.

Subprocessos, tarefas, eventos e *gateways* de decisão foram ilustrados através de imagens que representam e guiam as ações necessárias para buscar a conformidade com a norma técnica ou um *framework* de segurança adotado em um projeto.

Através da modelagem apresentada, empresas, especialmente as pequenas e médias poderão estimar os valores financeiros necessários para usufruir de um ambiente cibernético seguro e em conformidade com documentações respaldadas e estabelecidas mundialmente.

Capítulo 5

5 APLICAÇÃO DA METODOLOGIA PROPOSTA

Este capítulo apresenta uma aplicação da metodologia proposta por este trabalho, que teve por objetivo avaliar e validar a metodologia proposta. Além disso, o experimento mostra de forma prática como utilizar o processo modelado da metodologia proposta para gerar o resultado do custo total de uma implementação de controles de segurança cibernética em uma organização.

Um único experimento foi realizado e duas estimativas de custos distintos foram geradas para o mesmo ambiente cibernético. A diferença entre as estimativas de custo foi de R$ 287.820,00, onde a segunda conseguiu uma economia de 45,21% em relação à primeira, contemplando os mesmos requisitos exigidos pelo *framework* de segurança utilizado, e o mais importante, mantendo a conformidade.

O experimento foi realizado em um departamento acadêmico de computação de uma universidade federal do Brasil. O departamento acadêmico foi escolhido pelo fato de possuir requisitos cibernéticos suficientes para proporcionar um uso completo da metodologia proposta. São vários laboratórios de informática, salas de ensino com computadores e outros dispositivos conectados à rede de computador, setores administrativos com computadores, além de profissionais de TI, que compõem parte de alguns subprocessos desta metodologia.

Outro importante fato é que, de acordo com as definições do SEBRAE, o departamento acadêmico se compara a uma empresa de médio porte, contendo mais de 50 e menos de 100 funcionários, quando esta é do segmento de comércio e serviços (SEBRAE, 2013, p. 17).

Neste experimento, foi adotado o *framework* de segurança cibernética *CIS v*8 para estabelecer as ações de segurança cibernética no ambiente testado. Ao final deste experimento, foi gerado uma documentação detalhada das ações a serem tomadas e os seus respectivos custos financeiros.

5.1 Introdução

O cenário avaliado neste capítulo se baseia no desejo de uma organização em obter uma estimativa de custos financeiros para implementar controles de segurança cibernética, ou para melhorar o nível de maturidade em segurança cibernética atual para um nível de maturidade cibernética mais elevado e em conformidade com alguma norma técnica ou *framework* de segurança cibernética e da informação estabelecido.

5.2 Aplicação da Metodologia: Estimativa de Custo 1

O departamento acadêmico exposto a esta metodologia possui um parque computacional considerável, com mais de 300 computadores funcionando diariamente, sendo ele o maior parque entre todos os departamentos acadêmicos da universidade avaliada.

No momento em que foi realizado este experimento, o departamento acadêmico não tinha autonomia sobre o funcionamento da segurança cibernética de seu parque. Outro departamento da universidade desempenha esse papel. O objetivo do departamento é de implementar o seu próprio cenário de segurança cibernética, tornando-se o gestor de seu parque computacional.

Desta forma, de todos os padrões técnicos e *frameworks* analisados, o *CIS v.*8 foi adotado para determinar as ações de implementação de segurança cibernética do departamento. A escolha deste *framework* deu-se principalmente pelo fato dele conter módulos específicos de acordo com o tamanho da empresa. Desta forma, podemos selecionar o módulo voltado para pequenas empresas, que é um dos focos deste trabalho.

Os controles e as salvaguardas estabelecidos neste projeto são considerados no módulo IG1, voltado para as pequenas empresas, que inclui 15 controles (de um total de 18 controles), compostos por 56 salvaguardas (de um total de 153 salvaguardas), definidas como higiene cibernética básica (*CIS*, 2021).

Os controles e as suas respectivas salvaguardas utilizados no módulo IG1 são apresentados na Tabela 5.1.

Tabela 5.1 - Controles e Salvaguardas do módulo IG1 do *CIS v.*8.

Controle 1 - Inventário e controle de ativos da empresa	
Salvaguarda	**Título**

1.1	Estabelecer e manter um inventário detalhado de ativos da empresa
1.2	Adereçar ativos não autorizados
Controle 2 - Inventário e controle de ativos de *software*	
Salvaguarda	**Título**
2.1	Estabelecer e manter um inventário de *software*
2.2	Certificar-se de que o *software* autorizado seja atualmente suportado
2.3	Adereçar a *software* não autorizado
Controle 3 - Proteção de dados	
Salvaguarda	**Título**
3.1	Estabelecer e manter um processo de gerenciamento de dados
3.2	Estabelecer e manter um inventário de dados
3.3	Configurar listas de controle de acesso a dados
3.4	Aplicar retenção de dados
3.5	Descartar de dados com segurança
3.6	Criptografar dados em dispositivos de usuário final
Controle 4 - Configuração segura de ativos corporativos e software	
Salvaguarda	**Título**
4.1	Estabelecer e manter um processo de configuração seguro
4.2	Estabelecer e manter um processo de configuração seguro para infraestrutura de rede
4.3	Configurar o bloqueio automático de sessão em ativos corporativos
4.4	Implementar e gerenciar um *firewall* em servidores
4.5	Implementar e gerenciar um *firewall* em dispositivos de usuário final
4.6	Gerenciar com segurança ativos corporativos e *software*
4.7	Gerenciar contas padrão em ativos corporativos e *software*
Controle 5 - Gestão de contas	
Salvaguarda	**Título**

5.1	Estabelecer e manter um inventário de contas
5.2	Usar senhas exclusivas
5.3	Desativar contas inativas
5.4	Restringir privilégios de administrador a contas de administrador dedicadas
Controle 6 - Gerenciamento de controle de acesso	
Salvaguarda	**Título**
6.1	Estabelecer um Processo de Concessão de Acesso
6.2	Estabelecer um Processo de Revogação de Acesso
6.3	Exigir *MFA* para aplicativos expostos externamente
6.4	Exigir *MFA* para acesso remoto à rede
6.5	Exigir *MFA* para acesso administrativo
Controle 7 - Gerenciamento Contínuo de Vulnerabilidade	
Salvaguarda	**Título**
7.1	Estabelecer e manter um processo de gerenciamento de vulnerabilidade
7.2	Estabelecer e manter um processo de remediação
7.3	Executar gerenciamento automatizado de *patches* do sistema operacional
7.4	Executar gerenciamento automatizado de *patches* de aplicativos
Controle 8 - Gerenciamento de registro de auditoria	
Salvaguarda	**Título**
8.1	Estabelecer e manter um processo de gerenciamento de registro de auditoria
8.2	Coletar registros de auditoria
8.3	Garantir armazenamento adequado de registros de auditoria
Controle 9 - Proteções de e-mail e navegador da web	
Salvaguarda	**Título**
9.1	Garantir o uso apenas de navegadores e clientes de e-mail com suporte total
9.2	Usar serviços de filtragem de DNS

Controle 10 - Defesas contra malware	
Salvaguarda	**Título**
10.1	Implantar e manter software antimalware
10.2	Configurar atualizações automáticas de assinatura antimalware
10.3	Desativar execução automática e reprodução automática para mídia removível
Controle 11 - Recuperação de dados	
Salvaguarda	**Título**
11.1	Estabelecer e manter um processo de recuperação de dados
11.2	Executar backups automatizados
11.3	Proteger os dados de recuperação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação
Controle 12 - Gerenciamento de infraestrutura de rede	
Salvaguarda	**Título**
12.1	Certificar-se de que a infraestrutura de rede esteja atualizada
Controle 13 - Não é contemplado no módulo IG1	
Controle 14 - Conscientização de segurança e treinamento de habilidades	
Salvaguarda	**Título**
14.1	Estabelecer e manter um programa de conscientização de segurança
14.2	Treinar membros da força de trabalho para reconhecer ataques de engenharia social
14.3	Treinar membros da força de trabalho em boas práticas para autenticação
14.4	Treinar a força de trabalho nas boas práticas para manuseio de dados
14.5	Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados
14.6	Treinar membros da força de trabalho sobre como reconhecer e relatar incidentes de segurança
14.7	Treinar a força de trabalho sobre como identificar e relatar se seus ativos corporativos estão falhando ao realizar atualizações de segurança
14.8	Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos

	em redes inseguras
Controle 15 - Gestão de Provedores de Serviços	
Salvaguarda	**Título**
15.1	Estabelecer e manter um inventário de provedores de serviços
Controle 16 - Não é contemplado no módulo IG1	
Controle 17 - Gerenciamento de resposta a incidentes	
Salvaguarda	**Título**
17.1	Designar pessoal para gerenciar tratamento de incidentes
17.2	Estabelecer e manter informações de contato para relatar incidentes de segurança
17.3	Estabelecer e manter um processo empresarial para relatar incidentes
Controle 18 - Não é contemplado no módulo IG1	

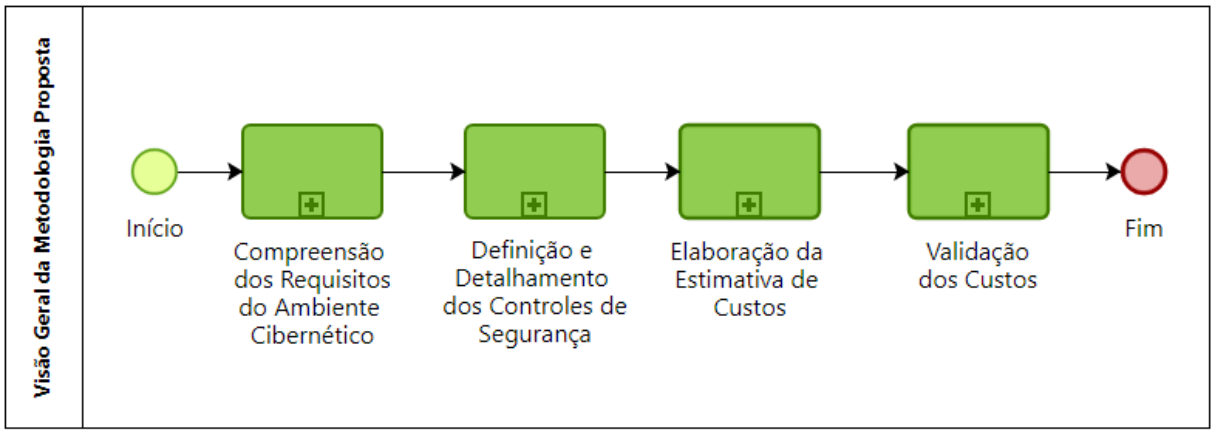
Fonte: Autor (adaptado do *CIS v.*8, 2024).

Adiante, será demonstrado a utilização da metodologia proposta em uma salvaguarda, mais especificamente a salvaguarda 3.3, contida no controle 3 (ver Tabela 5.1). O mesmo processo foi utilizado em todas as outras salvaguardas do projeto. O resultado dos dispositivos escolhidos e os custos associados a eles estão presentes ao longo do texto neste capítulo e nas Tabelas 5.3 e 5.4.

As ações que foram executadas durante o experimento serão representadas através da cor verde, que ilustram o caminho percorrido em todo o processo. As atividades, subprocessos, eventos e *gateways* que estiverem de cor branca não foram utilizados no cenário específico. Contudo, eles continuam sendo relevantes, pois podem eventualmente serem utilizados em outros estudos de caso e cenários.

A metodologia proposta apresenta em seu diagrama 4 subprocessos principais, representados na Figura 5.1.

Figura 5.1 - Execução dos Subprocessos Principais da Metodologia Proposta

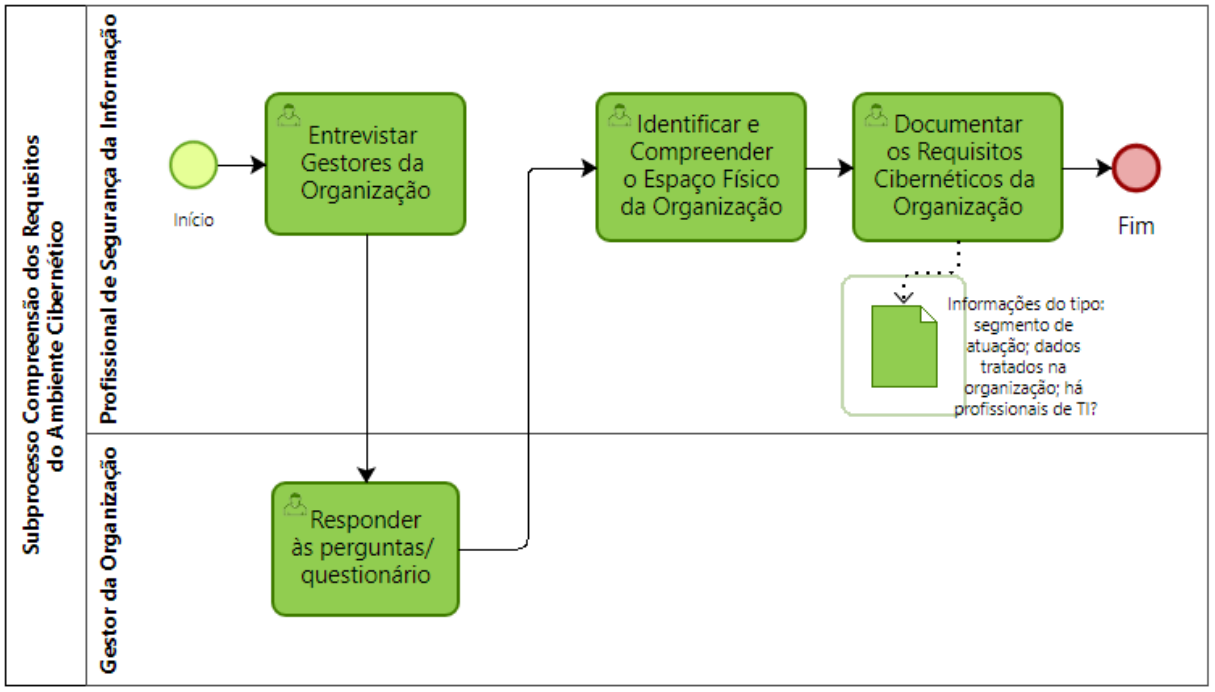


Fonte: Autor, 2023.

5.2.1 Subprocesso: Compreensão dos Requisitos do Ambiente Cibernético

A aplicação do subprocesso **Compreensão dos Requisitos do Ambiente Cibernético** começa com uma entrevista para entender os requisitos cibernéticos da empresa que está sendo testada. Esta entrevista foi realizada com o diretor do departamento acadêmico da universidade. A Figura 5.2 ilustra que todas as atividades deste subprocesso foram executadas.

Figura 5.2 - Execução do Subprocesso Compreensão dos Requisitos do Ambiente Cibernéticos



Fonte: Autor, 2023.

Durante a entrevista, foi utilizado um questionário eletrônico com algumas perguntas-chave para conhecer o segmento de atuação da empresa, além de seus dados processados e armazenados. O questionário utilizado pode ser verificado no APÊNDICE A. Os atores desta entrevista foram um profissional de segurança da informação e o diretor do departamento acadêmico. Para melhor ilustrar o contexto da empresa avaliada, as perguntas e respostas se encontram reproduzidas abaixo, conforme demonstra a Tabela 5.2.

Tabela 5.2 - Atividade Entrevistar Gestor da Organização.

Perguntas (Profissional de SI)	**Respostas** (Gestor da empresa)
Qual é o segmento de negócio da empresa/ organização? (Ex: Educação, Saúde, Agro, Farmacêutica...)	Educação.
A sua empresa trata e/ou armazena dados de seus clientes?	Sim.
Caso a resposta da pergunta anterior tenha sido "Sim", descreva abaixo os tipos de dados tratados. Caso tenha sido não, rechace a negativa escrevendo "Não".	Os dados tratados por nosso departamento estão ligados às pessoas, como o nome completo, CPF e nº de matrícula. A maior questão, é o fato destes dados serem públicos, do governo federal, além de serem dados confidenciais das pessoas, que no nosso caso são alunos e servidores.
A empresa/organização possui profissionais de TI para ficar à frente do projeto de segurança cibernética?	Sim.
Caso a resposta da pergunta anterior tenha sido "Sim", escreva abaixo todos eles. Cite o tipo, sua especialidade e a quantidade de cada profissional. Não precisa especificar as atividades destes profissionais. (Ex: Analista de TI - Programador - 5; Analista de TI - Gerente de projeto - 1; Analista de TI - Segurança da Informação - 3; Técnico de informática - Suporte ao usuário - 4; Técnico de informática - Manutenção de hardware - 5). Caso tenha respondido "Não", rechace a negativa escrevendo: Não.	Técnico em Tecnologia da Informação; Infraestrutura de redes de computadores e gerenciamento de projeto; 1. Técnico de Laboratório em Informática; Suporte ao usuário, manutenção de micro e segurança; 1.
Marque as caixas de seleção de acordo com o espaço físico da organização que servirá como infraestrutura de TI. ☐ É necessário construir, ampliar ou separar algum espaço físico? ☐ É necessário climatizar? ☐ É necessário controlar o acesso físico?	Todas selecionadas. ☑ É necessário construir, ampliar ou separar algum espaço físico? ☑ É necessário climatizar? ☑ É necessário controlar o acesso físico?
Especifique as informações de cada caixa selecionada na questão anterior.	Iremos separar um espaço físico já existente em nossa organização para acomodar os ativos de TI,

	pois criaremos um CPD. Será necessário climatizar a sala, hoje não temos essa infraestrutura no local escolhido para ser o CPD. Queremos controlar o acesso físico através de fechaduras eletrônicas.
Informe sobre as aplicações, ferramentas, softwares e sistemas indispensáveis utilizados em seu ambiente cibernético.	Utilizamos AVA, Moodle e SIGAA que são ferramentas disponibilizadas pela universidade. Além destas, temos vários laboratórios de informática e estações de trabalho administrativas com a necessidade de utilizar o sistema operacional Windows.

Fonte: Autor, (2023).

Através do formulário utilizado, foi possível constatar as necessidades do ambiente cibernético do departamento quanto à infraestrutura existente e a infraestrutura desejada. Conforme as respostas registradas, é possível perceber que o setor de atuação da organização é o de Educação, o que deu liberdade para determinar a norma técnica ou *framework* de segurança estabelecido no mercado, uma vez que não há documentação de segurança específica para o setor de Educação.

Em contrapartida, foi constatado que a instituição trata dados sensíveis do usuário, fazendo-se necessário a utilização da LGPD, criada no Brasil em 2018 e sancionada em 2020, através da lei de nº 13.709 (GOV.BR, 2018). Sendo assim, mecanismos de proteção aos dados também foram levados em consideração para determinar a escolha do *framework* utilizado no projeto do departamento, que foi o *CIS Critical Security Controls Version 8* (*CIS v8*), da organização *Center for Internet Security* .

Também, de acordo com as respostas, foi possível detectar que a empresa possui profissionais de TI para desenvolver e executar o projeto de segurança cibernética do departamento. A última questão se refere à infraestrutura física da organização. Neste experimento, foi realizada uma visita presencial para conhecer os locais indicados pelo departamento acadêmico que farão parte do projeto.

Estas informações serão utilizadas no próximo subprocesso, relacionadas principalmente aos custos extras, que por muitas vezes são esquecidos durante a elaboração de um projeto de cibersegurança, mas que impactam consideravelmente nos custos finais de todo projeto. Por fim, as informações foram documentadas, sendo suficientes para a realização das atividades previstas neste subprocesso.

5.2.2 Subprocesso Definição e Detalhamento de Controles de Segurança

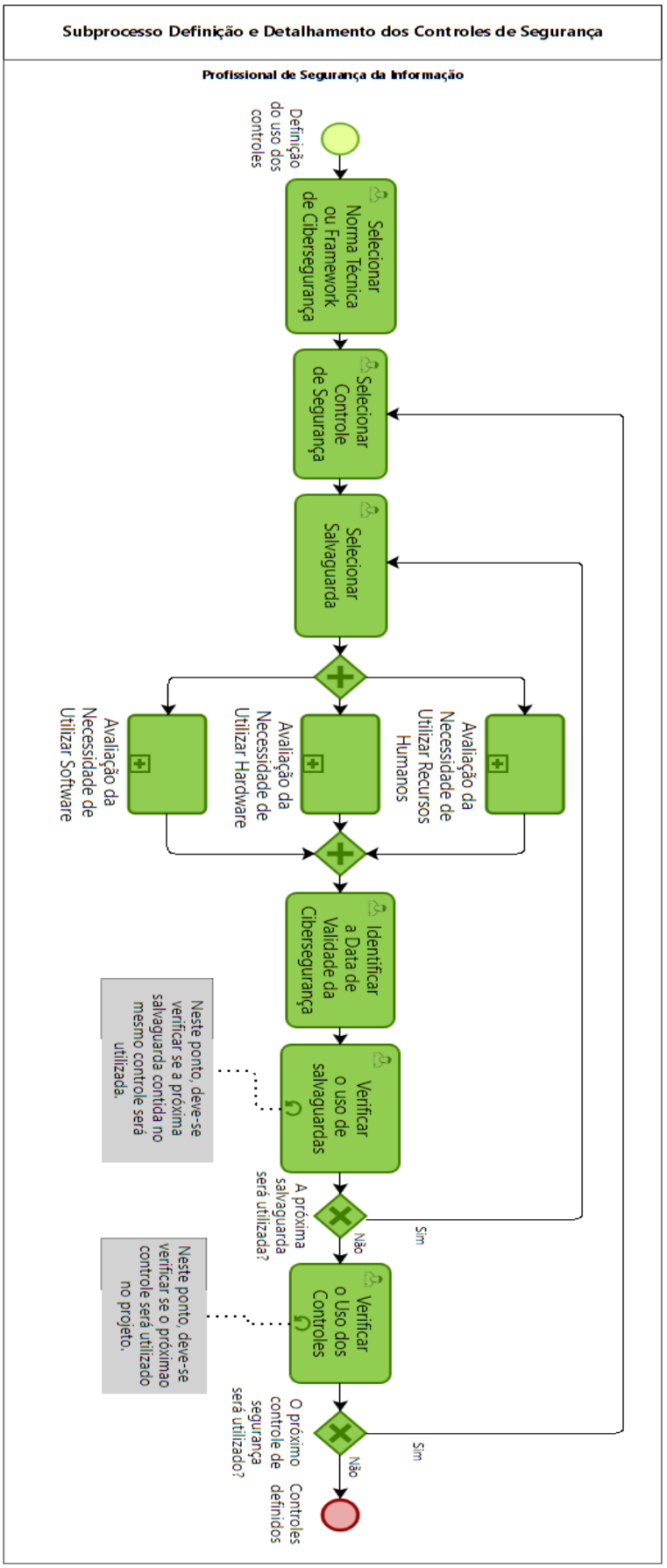
Este subprocesso é aplicado a todos os controles e todas as salvaguardas utilizadas no projeto. As definições feitas neste ponto servem como requisitos para atender às demandas de controles e suas respectivas salvaguardas, além das necessidades da empresa.

Para ilustrar a execução deste subprocesso, será utilizado como exemplo o controle 3 do *CIS* v8, definido como Proteção de Dados, que visa desenvolver processos e controles técnicos para identificar, classificar, tratar, reter e descartar dados com segurança. Já a salvaguarda será a 3.3, definida como Configurar lista de controle de acesso a dados, que visa controlar o acesso aos dados com base na necessidade de conhecimento do usuário.

A estratégia para atender a esta salvaguarda exige a implementação de um controlador de domínio no ambiente cibernético, que gerencia a criação de usuários e controla o acesso a pastas e documentos por meio de políticas de grupo.

Com o **controle e salvaguarda definidos**, se **analisa as necessidades de utilizar recursos humanos, *hardware* e *software*** para implementá-los, seguindo as atividades descritas no processo modelado. Após estas verificações, são executadas as atividades de **Identificar a Data de Validade da Cibersegurança**, que está associada ao uso de *hardware* e *software* nas salvaguardas, além da atividade que verifica o uso das **salvaguardas** e posteriormente a atividade que verifica o uso dos **controles** que farão parte do projeto. A Figura 5.3 demonstra a execução do processo modelado no capítulo anterior.

Figura 5.3 - Execução do Subprocesso Definição e Detalhamento de Controles de Segurança.

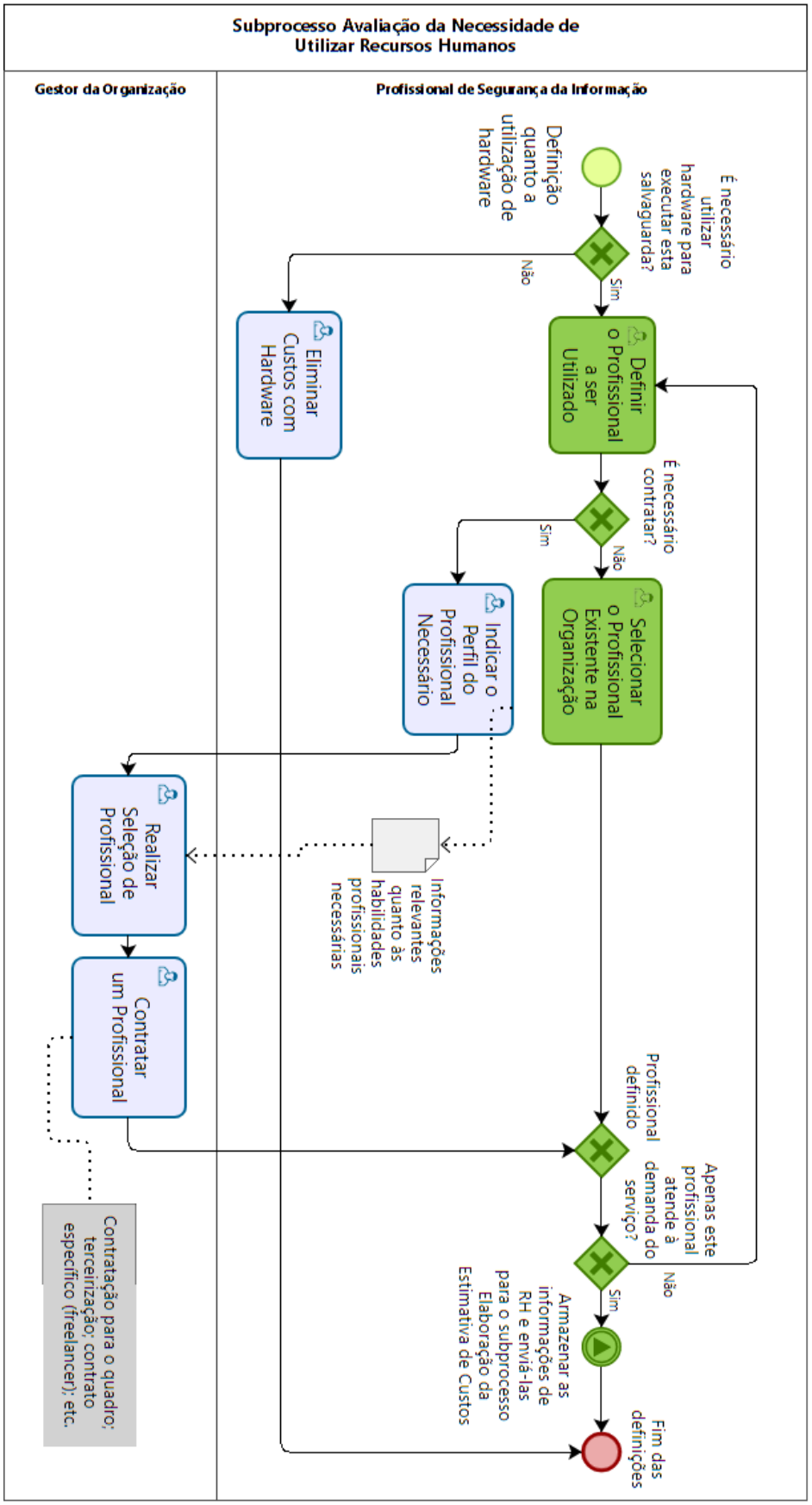


Fonte: Autor, 2023.

Dentro do subprocesso Definição e Detalhamento de Controles de Segurança, há três subprocessos, que serão detalhados adiante. Primeiramente, verificou-se a **necessidade de utilizar recursos humanos** para a implementação da salvaguarda. Neste caso, verificou-se que esta necessidade existe. Foi apontado então, pelo diretor do departamento, um **profissional existente** do departamento acadêmico da universidade. Este profissional tem conhecimentos sólidos em segurança cibernética e da informação, atendendo aos requisitos da metodologia proposta.

Em seguida, é **verificada a demanda do serviço *versus* a disponibilidade de recursos humanos**, onde apenas este profissional foi suficiente para realizar as tarefas da salvaguarda em questão. Por fim, **as informações foram armazenadas no evento** para serem utilizadas posteriormente. A Figura 5.4 ilustra o caminho percorrido na execução deste subprocesso.

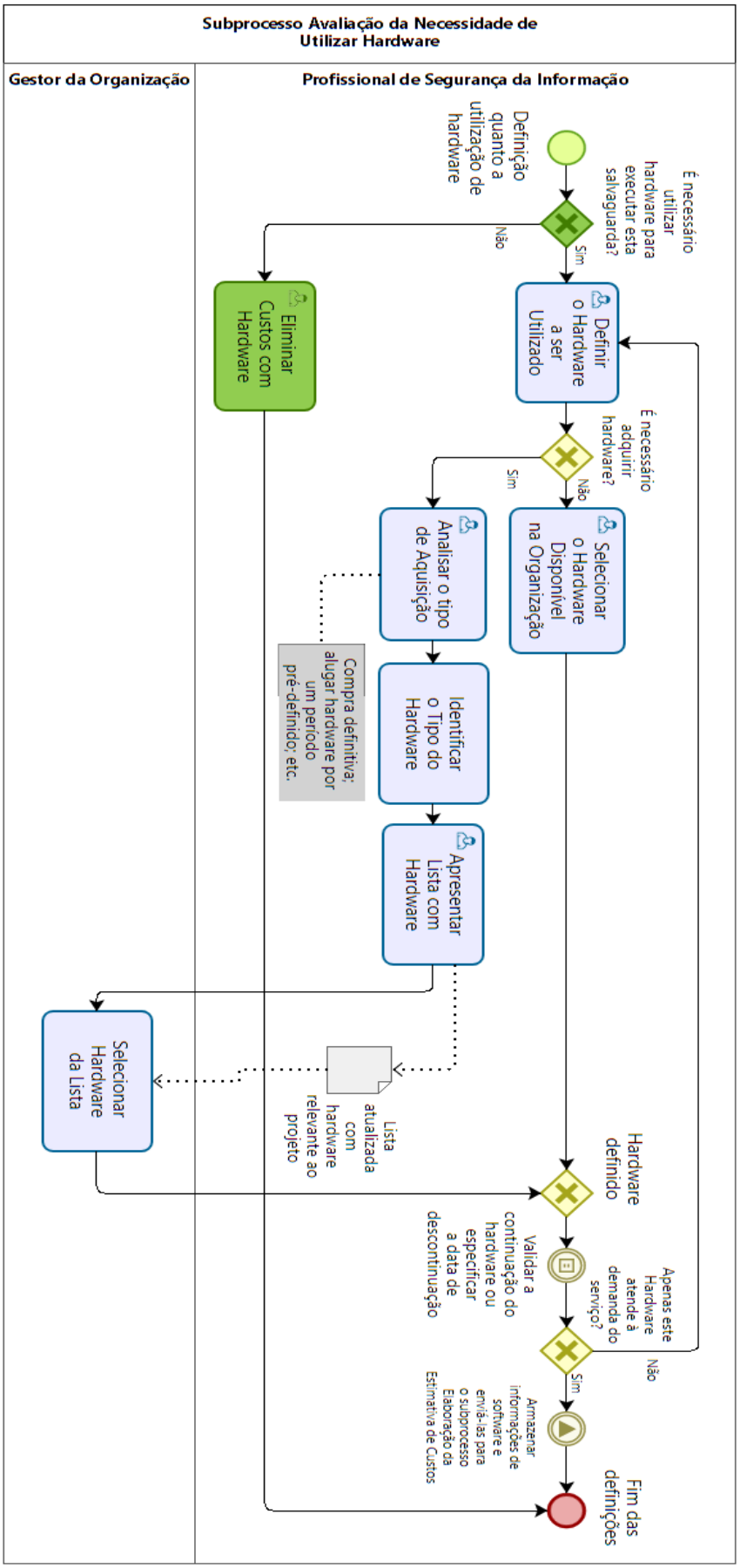
Figura 5.4 - Execução do Subprocesso Avaliação da Necessidade de Utilizar Recursos Humanos.



Fonte: Autor, 2023.

Após as definições relativas aos recursos humanos, **verificou-se a necessidade de utilização de *hardware*** para a mesma salvaguarda. A Figura 5.5 evidencia a execução do subprocesso correspondente. A primeira verificação **avalia a necessidade de utilização de *hardware***. Neste caso, foi visto que não existe esta necessidade. Seguindo a modelagem do subprocesso, **os custos com *hardware* foram eliminados**, e o processo encerrado conforme mostrado na figura em questão.

Figura 5.5 - Execução do Subprocesso Avaliação da Necessidade de Utilizar *Hardware.*



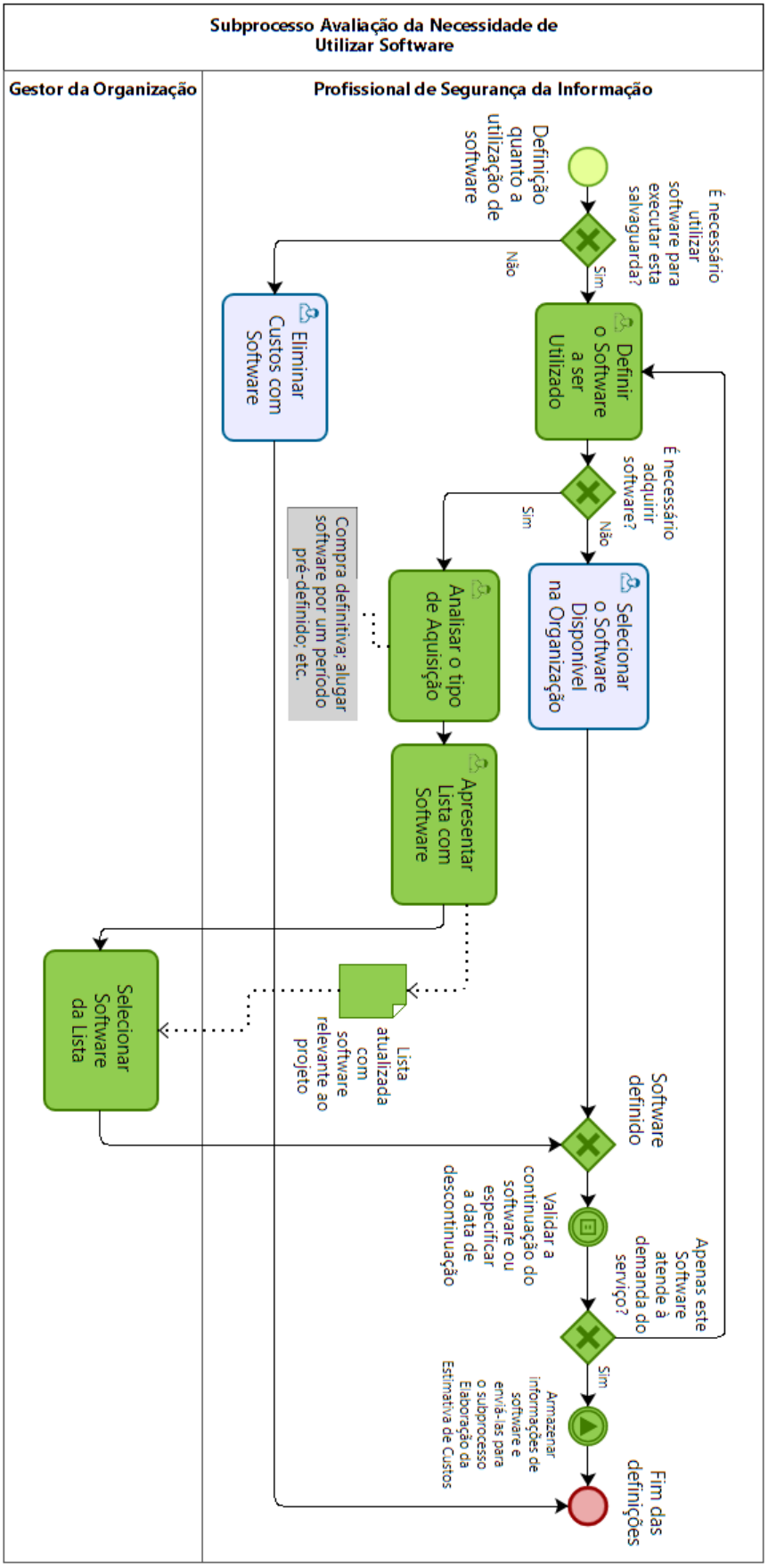
Fonte: Autor, 2023.

Em seguida, o subprocesso **Avaliação da Necessidade de Utilizar *Software*** começa com uma verificação que **avalia a necessidade de usar *software*** para a salvaguarda. Para esta salvaguarda, a resposta foi positiva. Adiante, **verificou-se a necessidade de aquisição de *software***, o que também se revelou positivo. Portanto, foi apresentada uma **lista contendo *softwares*** *Windows Server* em diferentes versões, sendo que todas essas versões são adequadas aos requisitos da salvaguarda e às necessidades do ambiente cibernético.

Conforme mencionado anteriormente, um controlador de domínio *Windows Server* foi definido para atender aos requisitos desta salvaguarda. O *Windows Server* foi definido para este ambiente visando à interoperabilidade entre os hosts servidor e clientes, pois existe a necessidade de que parte deste ambiente seja em *Windows* devido à utilização de outros aplicativos e sistemas que funcionam apenas em estações de trabalho com *Windows*. Essas informações foram extraídas durante a entrevista no subprocesso **Compreensão dos Requisitos do Ambiente Cibernético**.

O cliente refletiu sobre o seu atual parque tecnológico e projeções de crescimento e escolheu uma das versões sugeridas. Adiante, o uso do *software* foi **validado** por não haver data de descontinuação divulgada pela empresa mantenedora do mesmo. Em seguida, foi **verificada a quantidade de *software versus* a demanda do serviço**. Neste caso, uma única aquisição de *software* foi suficiente para satisfazer o requisito da salvaguarda. Por fim, as informações foram **documentadas** para serem enviadas para o próximo subprocesso. A Figura 5.6 ilustra a execução do processo pelo aplicador da metodologia.

Figura 5.6 - Execução do Subprocesso Avaliação da Necessidade de Utilizar *Software*.



Fonte: Autor, 2023.

Em seguida, a próxima atividade (ver Figura 5.3) **Identificar a Validade da Cibersegurança**, tem o objetivo de colher informação sobre a validade cibernética do *hardware* e/ou do *software* utilizado no projeto. O período de validade desta salvaguarda foi classificado como indeterminado, uma vez que o *software* definido se encontra na versão mais atual e não há data de descontinuação anunciada pela empresa que o mantém.

A atividade posterior, **Verificar Todas as Salvaguardas Utilizadas neste Projeto**, verifica se todas as salvaguardas contidas em um mesmo controle foram analisadas. Seguindo a modelagem, passamos para a análise da próxima salvaguarda deste mesmo controle de segurança, e assim sucessivamente até a análise da última salvaguarda utilizada neste controle.

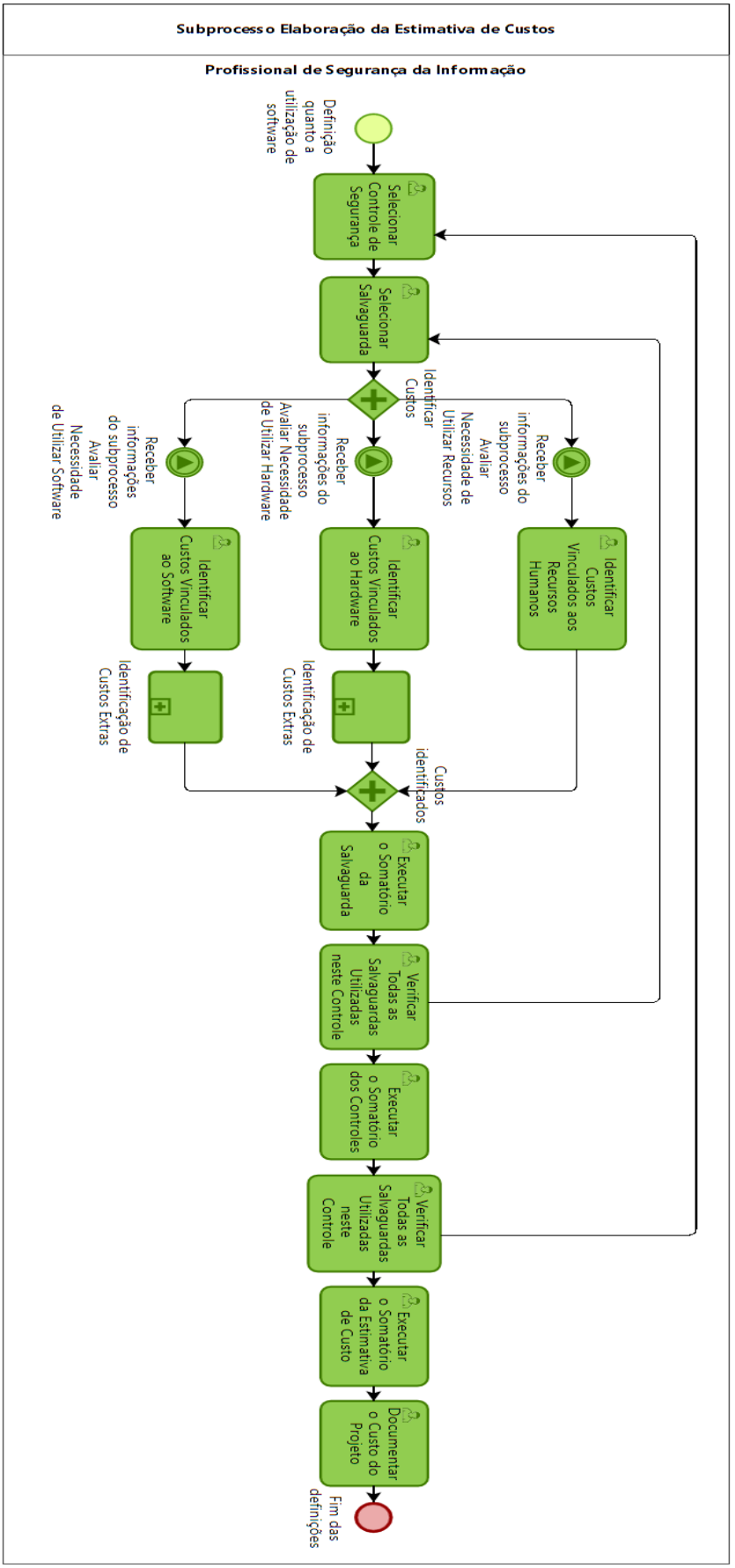
Uma vez positiva a verificação desta atividade e analisadas todas as salvaguardas do mesmo controle, é possível chegar na próxima atividade também do tipo *loop*, que verifica a utilização dos controles, **Verificar Todos os Controles Utilizadas neste Projeto**. Uma vez positivo e verificado todos os controles utilizados no experimento, este subprocesso foi encerrado, verificando todos os requisitos necessários.

Após estas verificações, foi possível passar para o próximo subprocesso.

5.2.3 Subprocesso: Elaboração da Estimativa de Custos

O subprocesso **Elaboração da Estimativa de Custos** inicia com a seleção do controle de segurança cibernética utilizado no projeto. Assim como o subprocesso anterior, este subprocesso é aplicado a todos os controles e todas as salvaguardas utilizadas no projeto. Para ilustrar a aplicação da modelagem neste subprocesso, mais uma vez, como exemplo, será utilizado o controle 3 e sua respectiva salvaguarda 3.3. A Figura 5.7 ilustra a execução deste subprocesso.

Figura 5.7 - Execução do Subprocesso Elaboração da Estimativa de Custos



Fonte: Autor, 2023.

Após a **seleção do controle e da salvaguarda**, são **recebidas as informações do subprocesso anterior** com todas as definições dos requisitos necessários para executar as ações definidas na salvaguarda.

Neste experimento, não houve custo com recursos humanos, pois o profissional utilizado já fazia parte da empresa e seus salários eram pagos pela organização, não envolvendo recursos adicionais do departamento.

Quando foi **verificada a necessidade de utilizar *hardware*** para esta salvaguarda, inicialmente constatou-se que não haveria necessidade de aquisição de *hardware*. Porém, ao receber informações sobre a utilização do *software*, constatou-se que além da aquisição do *software*, o *software* exigia indiretamente a aquisição do *hardware* (servidor físico) adequado para a sua utilização, que por sua vez exigiu um *rack* para que fosse armazenado de maneira adequada, uma fechadura eletrônica para realizar o controle de acesso, além de exigir que o espaço onde o *hardware* estará fisicamente localizado seja climatizado, e estes custos foram considerados durante a execução do subprocesso **Identificação de Custos Extras**. Todos estes custos foram levantados com o cliente e definidos para serem calculados no somatório da salvaguarda.

Foram utilizadas as fórmulas anteriormente citadas para definição do custo desta salvaguarda, resultando no valor de R$ 80.929,21. Em seguida, foi identificado o custo de todas as salvaguardas utilizadas no controle 3 para determinar o custo total do controle.

O custo desse controle foi o mesmo da salvaguarda 3.3 (R$ 80.929,21), pois a salvaguarda 3.3 foi a única que trouxe custos para esse controle específico. Após a realização dos cálculos para todos os demais controles, todo o custo do projeto foi calculado pela fórmula ECISC.

O custo de todo o projeto foi estimado em R$ 636.574,92. Se verificou que 5 controles, dos 15 selecionados, geram custos para o projeto, e 6 salvaguardas, das 56 selecionadas, geram custos para o projeto. Em seguida, um documento detalhado com todos os custos acima descritos foi gerado.

Custos dos Controles de Segurança e das Salvaguardas

Os controles e as salvaguardas com custos acima de zero serão apresentados na Tabela 5.3. O experimento considera 15 controles (de 18) e 56 salvaguardas (de um total de 153)

estabelecido no *CIS* v8. Destes 15 controles, 5 contêm custos financeiros, e das 56 salvaguardas, 6 contêm custos financeiros.

As definições dos controles e das salvaguardas definidas como sem custos, serão apresentadas na próxima subseção, concluindo assim, todo o ambiente cibernético exposto à metodologia proposta. Os custos apresentados na Tabela 5.3 referem-se aos requisitos levantados pelo aplicador da metodologia proposta no ambiente cibernético avaliado.

Tabela 5.3 - Custos financeiros de Controles e Salvaguardas.

Controle 2 - Inventário e controle de ativos de *software*	**Salvaguarda 2.2 - Assegurar que o *software* autorizado seja atualmente suportado**
Custos	
Recursos Humanos	R$ 0,00
Hardware	R$ 0,00
Software	R$ 454.116,00
Custos Extras	R$ 0,00
Custo da Salvaguarda	R$ 454.116,00
Custo do Controle	R$ 454.116,00
Justificativa: Substituir o sistema operacional de 284 estações de trabalho. Estas máquinas estão operando com um sistema operacional descontinuado, o que torna o ambiente cibernético inseguro, principalmente por não receberem mais atualizações de segurança. Um dos objetivos desta metodologia proposta é propor um ambiente cibernético seguro e em conformidade com padrões estabelecidos por profissionais e entidades de segurança cibernética e da informação mundialmente reconhecidos. Manter qualquer computador com sistema operacional descontinuado em um ambiente torna este ambiente não conforme e inseguro.	
Controle 3 - Proteção de dados	**Salvaguarda 3.3 - Configurar listas de controle de acesso a dados**
Custos	
Recursos Humanos	R$ 0,00
Hardware	R$ 0,00
Software	R$ 30.651,90
Custos Extras	R$ 50.277,31
Custo da Salvaguarda	R$ 80.929,21
Custo do Controle	R$ 80.929,21
Justificativa: É necessário estabelecer um controlador de domínio na rede de computadores. Um controlador de domínio é capaz de gerenciar o controle de acesso lógico a pastas e documentos digitais, baseado no privilégio do usuário, conforme a necessidade do perfil de cada usuário. O acesso às informações estão	

diretamente ligados ao nível de privilégio de cada cargo na organização, por exemplo: um diretor de recursos humanos terá mais privilégio de acesso do que um técnico em logística. Cada usuário deve ter os seus devidos acessos, conforme a necessidade do cargo que possuem para exercer as suas atividades competentes. Essa configuração impede que documentos sejam acessados por pessoas indevidas. Os custos extras são referentes a aquisições que o *software* exigiu indiretamente, tais como um servidor físico, *rack*, climatização e fechadura eletrônica.

Controle 4 - Configuração segura de ativos corporativos e *software*	**Salvaguarda 4.4 - Implementar e gerenciar um firewall nos servidores**
Custos	
Recursos Humanos	R$ 0,00
Hardware	R$ 85.298,40
Software	R$ 0,00
Custos Extras	R$ 0,00
Custo da Salvaguarda	R$ 85.298,40
Custo do Controle	R$ 88.057,71
Justificativa: Toda rede de computadores deve possuir um firewall, permitindo acesso legítimo ou bloqueando acesso indevido a rede interna da organização. Todo o tráfego de dados em uma rede de computadores controlada deve passar por um firewall, antes de se comunicar com a internet. O firewall, dentre outras funcionalidades, tem como grande vantagem impedir que vários tipos de ataques cibernéticos sejam bem-sucedidos ao ambiente cibernético de uma organização.	

Controle 4 - Configuração segura de ativos corporativos e *software*	**Salvaguarda 4.5 - Implementar e gerenciar um firewall nos dispositivos de usuário final**
Custos	
Recursos Humanos	R$ 0,00
Hardware	R$ 0,00
Software	R$ 2.759,31
Custos Extras	R$ 0,00
Custo da Salvaguarda	R$ 2.759,31
Custo do Controle	R$ 88.057,71
Justificativa: Um *firewall* em dispositivo de usuário final, faz o controle de segurança local do dispositivo, de maneira individual. Geralmente esta solução está incluída em um *software* que disponibiliza um conjunto com várias soluções de segurança, tais como um antivírus ou um antimalware. Além de verificar em tempo real possíveis ameaça e tráfego de rede anômalo no computador local, através de um firewall de dispositivo final é possível criar regras de acesso do computador, fazendo com o que a estação de trabalho não seja utilizada para outros fins, que não os necessários para desempenhar as atividades competentes da organização.	

Controle 6 - Gestão do controle de acesso	**Salvaguarda 6.4 - Exigir MFA para acesso remoto à rede**
Custos	
Recursos Humanos	R$ 0,00
Hardware	R$ 0,00
Software	R$ 2.673,00
Custos Extras	R$ 0,00
Custo da Salvaguarda	R$ 2.673,00
Custo do Controle	R$ 2.673,00
Justificativa: Uma rede de computadores controlada, é baseada em privilégio de usuário. Neste cenário, usuários administradores podem definir várias regras de acesso num ambiente cibernético do qual faz parte. Para evitar que problemas catastróficos aconteçam por acesso indevido a rede, é necessário utilizar Múltiplo Fator de Autenticação (MFA), garantindo uma camada a mais de proteção em acessos com maiores privilégios de acesso.	
Controle 11 - Recuperação de dados	**Salvaguarda 11.2 - Executar backups automatizados**
Custos	
Recursos Humanos	R$ 0,00
Hardware	R$ 10.799,00
Software	R$ 0,00
Custos Extras	R$ 0,00
Custo da Salvaguarda	R$ 10.799,00
Custo do Controle	R$ 10.799,00
Justificativa: Para esta salvaguarda foi definido a utilização de um Servidor de Backup NAS. Por motivos diversos um dado lógico poderá ser perdido, corrompido ou até mesmo estar inacessível sob circunstâncias de um ataque cibernético. O backup traz a possibilidade de recuperar e acessar estes dados, impedindo maiores problemas à organização decorrente da perda destes dados.	
Custo total da Estimativa de Custo do projeto: R$ 636.574,92	

Fonte: Autor (2024).

Como já mencionado anteriormente, verificou-se que o maior custo neste ambiente cibernético estava relacionado com *software*, com a aquisição de sistema operacional. Através da execução do processo modelado foi possível visualizar essa particularidade neste ambiente cibernético.

A Tabela 5.4 mostra os custos com mais detalhes para cada aquisição analisada na metodologia proposta. Mais uma vez, a concentração de recursos gastos com sistemas operacionais da fabricante *Microsoft Windows* é clara. Outro custo que chama a atenção e destoa dos demais neste ambiente cibernético, é o custo de investimento com o *firewall*, conforme ilustra a Tabela 5.4.

Tabela 5.4 - Detalhamento dos Custos

Controle	Salvaguarda	Custo	Descrição
2	2.2	R$ 454.116,00	Sistema operacional *Windows 11 Pro* (284 licenças).[1]
3	3.3	R$ 30.651,90	Sistema operacional *Windows Server 2022 Data Center* - 16 Core.[2]
		R$ 33.749,00	Servidor *Rack PowerEdge* R760.[3]
		R$ 12.073,00	*Dell APC Rack NetShelter SX* 42U 19" 600mm x 1070mm[4]
		R$ 2.555,41	Climatização da sala destinada para o CPD. A sala tem 12m² e para este espaço foi orçado um ar condicionado split de 12.000 BTUs.[5]
		R$ 1.899,90	Fechadura eletrônica Intelbras MFR 7000.[6]
4	4.4	R$ 85.298,40	*Fortinet Fortigate 200F + Unified Threat Protection (UTP)*.[7]
4	4.5	R$ 2.759,31	*Firewall* para dispositivo do usuário final – Antivírus *Avast Premium Security* - Licença para o período de um ano aos 310 computadores do ambiente cibernético testado.[8]
6	6.4	R$ 2.673,00	MFA - Autenticação Multifator Cisco DUO Premier - Foram orçadas 5 licenças do MFA, destinadas para os seguintes usuários pelo período de um ano: Diretor e vice-diretor do departamento; o coordenador de TI do departamento; os 2 técnicos de TI que gerenciam o parque computacional do departamento.[9]
11	11.4	R$ 10.799,00	Servidor de *backup* NAS Synology - DS723+ - 16 TB - AMD Ryzen R1600 Dual-Core 2.6GHz - 2GB DDR4 - 2x 1GbE - Inclui 2 HDs NAS de 8TB.[10]

Fonte: Autor (2024).

[1] https://www.microsoft.com/pt-br/d/windows-11-pro/dg7gmgf0d8h4

[2] https://www.microsoft.com/pt-br/windows-server/pricing

[3] https://www.dell.com/pt-br/shop/servidores-armazenamento-rede/servidor-rack-poweredge-r760/spd/poweredge-r760/pe_r760_15724_bcc_1

[4] https://www.dell.com/pt-br/shop/dell-apc-rack-netshelter-sx-42u-19-600mm-x-1070mm/apd/ab210052/energia-refrigera%C3%A7%C3%A3o-e-infraestrutura-de-data-cen

[5] https://www.ferreiracosta.com/produto/469120/ar-condicionado-split-springer-midea-inverter-12000btus-220v-42agvci12m5

[6] https://loja.intelbras.com.br/fechadura-embutir-mfr-7000/p

[7] https://www.firewall1.com.br/firewall/fortinet-fortigate-200f-unified-threat-protection-utp--p

[8] https://www.avast.com/pt-br/premium-security#pc

[9] https://duo.com/editions-and-pricing

[10] https://www.fourserv.com.br/produto/nas-synology-ds723-16-tb-amd-ryzen-r1600-dual-core-26ghz-2gb-ddr4-2x-1gbe-inclu/537782

Controles de Segurança e Salvaguardas sem custo

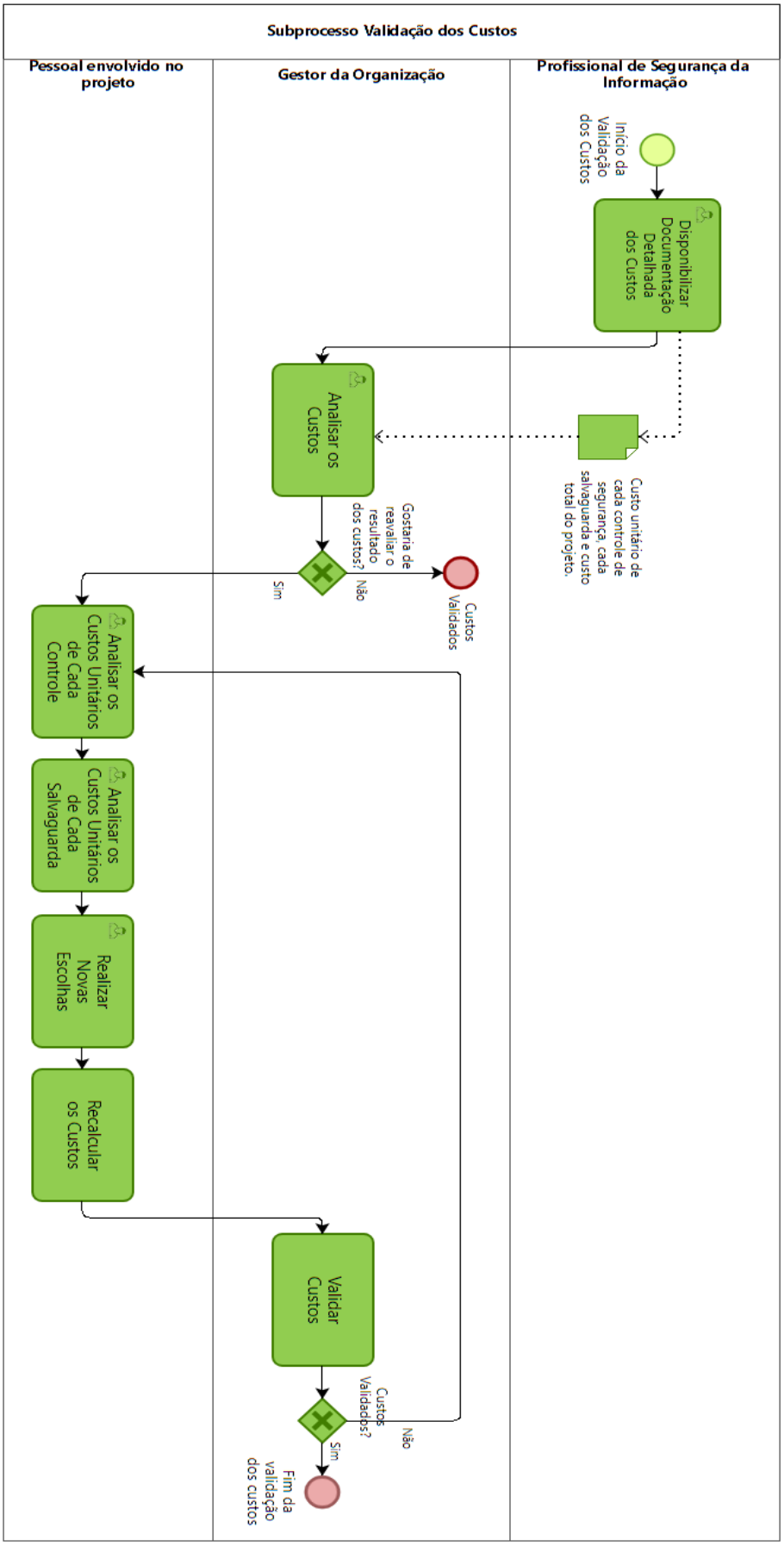
No APÊNDICE B serão apresentados todos os controles e todas as salvaguardas tidas como sem custos que fizeram parte do projeto de implementação de controles de cibersegurança do departamento acadêmico.

Várias salvaguardas são apenas documentação sobre boas práticas e outras utilizam algum recurso que o respectivo custo já foi considerado em um salvaguarda anterior. Todos estes controles e salvaguardas que compõem o projeto do ambiente cibernético exposto a esta metodologia, podem ser verificados no APÊNDICE B.

5.2.4 Subprocesso: Validação dos Custos

No subprocesso **Validação dos Custos**, os resultados da estimativa de custos foram disponibilizados ao cliente por meio de um documento que detalha o valor unitário de cada controle, de cada salvaguarda e o custo total de todo o projeto de implementação de controles de segurança cibernética para a organização. Este subprocesso foi executado conforme exposto na Figura 5.8.

Figura 5.8 - Execução do Subprocesso Validação dos Custos.



Fonte: Autor, 2023.

O cliente analisou os resultados de sua estimativa de custo para implementação de controles de segurança, e pôde tirar algumas conclusões de suas escolhas, escolhas estas que definiram o melhor cenário possível de seu ambiente cibernético, com as melhores ferramentas de administração de redes de computador e segurança cibernética adequadas às suas atividades e em conformidade com o *framework* de segurança adotado.

Foi possível verificar que havia grande concentração de recursos na salvaguarda 2.2, do controle 2, com a aquisição de um novo sistema operacional para 284 computadores, uma vez que o ambiente continha essa quantidade de máquinas com sistema operacional descontinuado, trazendo vulnerabilidades ao ambiente cibernético, em desconformidade com o *framework* utilizado.

Também foi possível verificar que havia um valor considerável na salvaguarda 4.4, do controle 4, com a aquisição de um *firewall* (a aquisição já contempla *hardware* e *software* em um único custo). Após o cliente visualizar os custos envolvidos de suas definições, foi decidido gerar um novo custo através de novas escolhas, no intuito de obter um custo final de menor valor monetário. Estas novas definições serão demonstradas em outra seção, denominada como **Aplicação da Metodologia: Estimativa de Custo 2**.

5.3 Aplicação da Metodologia: Estimativa de Custo 2

Após a análise do resultado da estimativa de custo inicial, o cliente decidiu realizar mais uma estimativa de custo para o seu ambiente, tendo em vista um valor de investimento mais baixo que o primeiro.

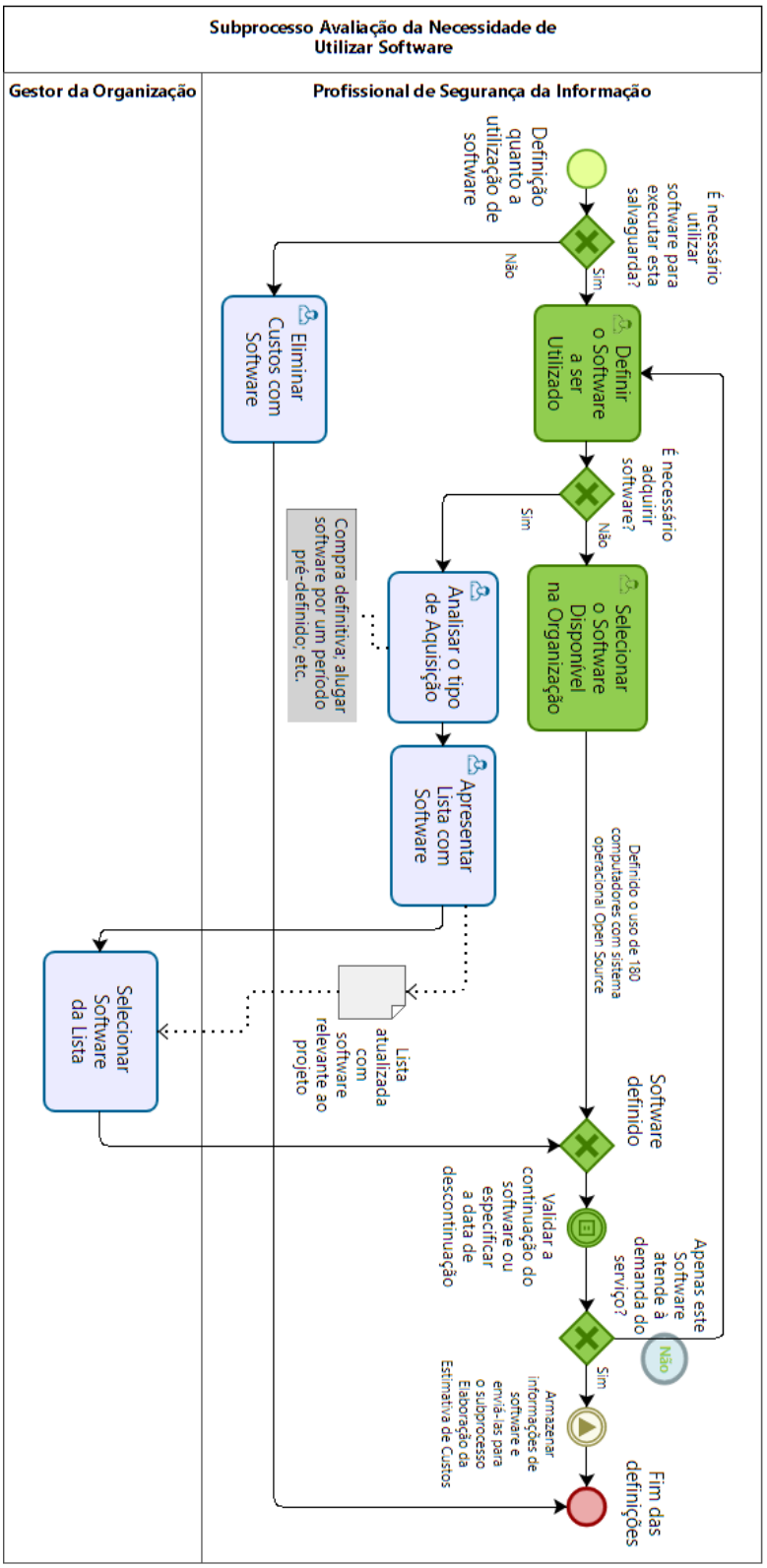
Mediante a documentação detalhada de custos entregue ao cliente, foi possível verificar a grande concentração de recursos em 3 controles, e posteriormente em 3 salvaguardas. O controle 2 e sua respectiva salvaguarda 2.2, o controle 3 e sua respectiva salvaguarda 3.3, e, por fim, o controle 4 e sua respectiva salvaguarda 4.4.

O cliente decidiu manter os custos das salvaguardas 3.3 e 4.4 devido às suas importâncias no projeto. A salvaguarda escolhida para ter novas seleções realizadas foi a 2.2, mais onerosa do projeto, referente a R$ 454.116,00, que faz jus a atualização do sistema operacional de 284 estações de trabalho. Verificou-se a possibilidade de utilizar parte do parque computacional com um sistema operacional *Open Source*.

Desta maneira, o cliente definiu que o seu parque poderia ser dividido entre distribuições com sistema operacional do tipo *Windows* e sistema operacional do tipo Linux.

Foi definido que 180 computadores ficariam com Linux Ubuntu 22.04.4 LTS. A Figura 5.9 ilustra o processo.

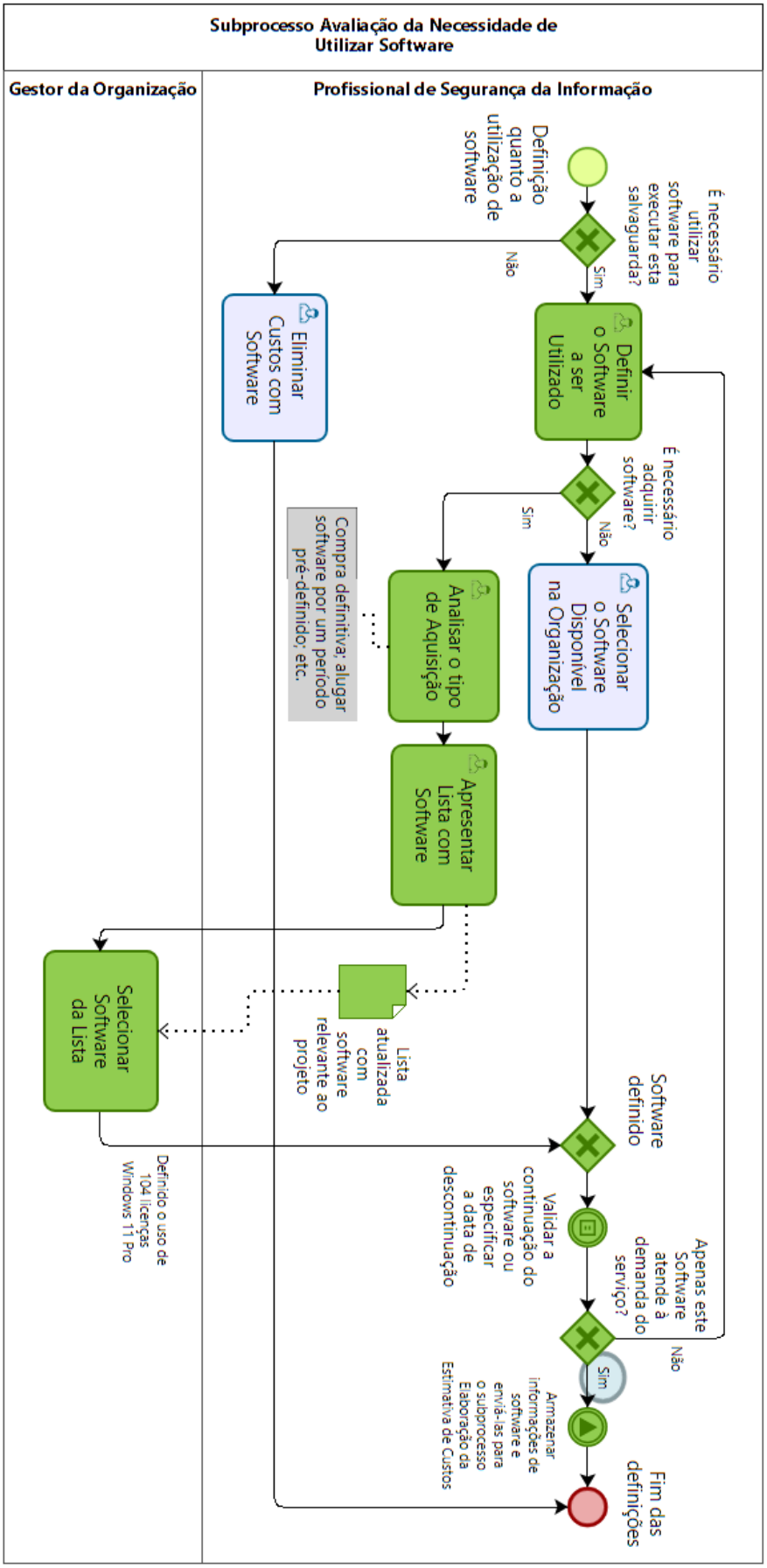
Figura 5.9 - Execução do Subprocesso Avaliação da Necessidade de Utilizar *Software*.



Fonte: Autor, 2023.

Seguindo a modelagem, após a **verificação da demanda quanto ao número de computadores do parque computacional e o número de distribuições *open source* determinadas**, percebeu-se que ainda haviam computadores que necessitavam de sistema operacional para funcionar, desta maneira, houve o retorno até a atividade **Definir o *Software* a ser Utilizado**, onde, nas atividades seguintes foi definido a aquisição de 104 licenças de *Windows 11 Pro*. A Figura 5.10 ilustra o processo, até a finalização do subprocesso.

Figura 5.10 - Execução do Subprocesso Avaliação da Necessidade de Utilizar *Software*.

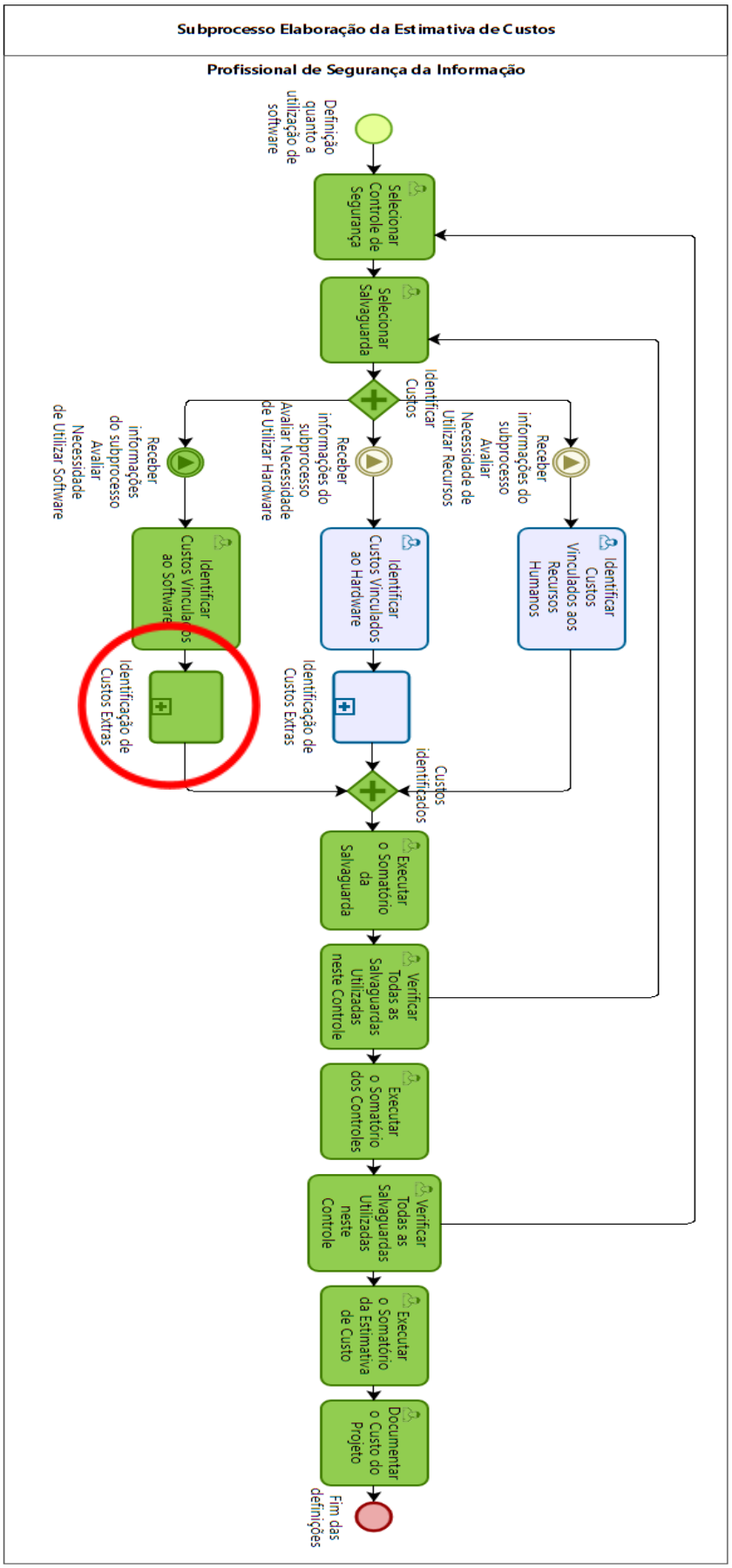


Fonte: Autor, 2023.

Após finalizar este subprocesso, retornamos à execução das atividades restantes do subprocesso **Definição e Detalhamento dos Controles de Segurança** até a sua finalização (ver Figura 5.3).

Em seguida, iniciou-se o subprocesso **Elaboração da Estimativa de custos**, onde, seguindo a modelagem, expandiu-se o subprocesso **Identificação de Custos Extras**, conforme ilustra a Figura 5.11.

Figura 5.11 - Execução do Subprocesso Elaboração da Estimativa de Custos



Fonte: Autor, 2023.

Ao expandir o subprocesso **Identificação de Custos Extras**, todas as atividades do subprocesso foram executadas (ver Figura 4.8) e desta forma a execução da modelagem prosseguiu.

Através da execução do subprocesso **Análise da Compatibilidade dos Dispositivos no Ambiente Cibernético**, foi possível identificar que a mudança do sistema operacional em parte do parque computacional do departamento exigiria, de maneira indireta, um outro controlador de domínio, pela não compatibilidade entre o servidor e as estações clientes com um outro tipo de sistema operacional. Esta inclusão deu-se para promover o controle de acesso a dados e outras exigências do *framework* de segurança adotado.

Desta maneira, foi decidido utilizar um servidor também *Open Source, Ubuntu Server 22.04.4 LTS*, não precisando investir valores monetários em *software*. Após as definições realizadas para **mitigar a incompatibilidade**, a princípio foi definido que um novo *hardware* (servidor físico) deveria ser adquirido para comportar o novo controlador de domínio.

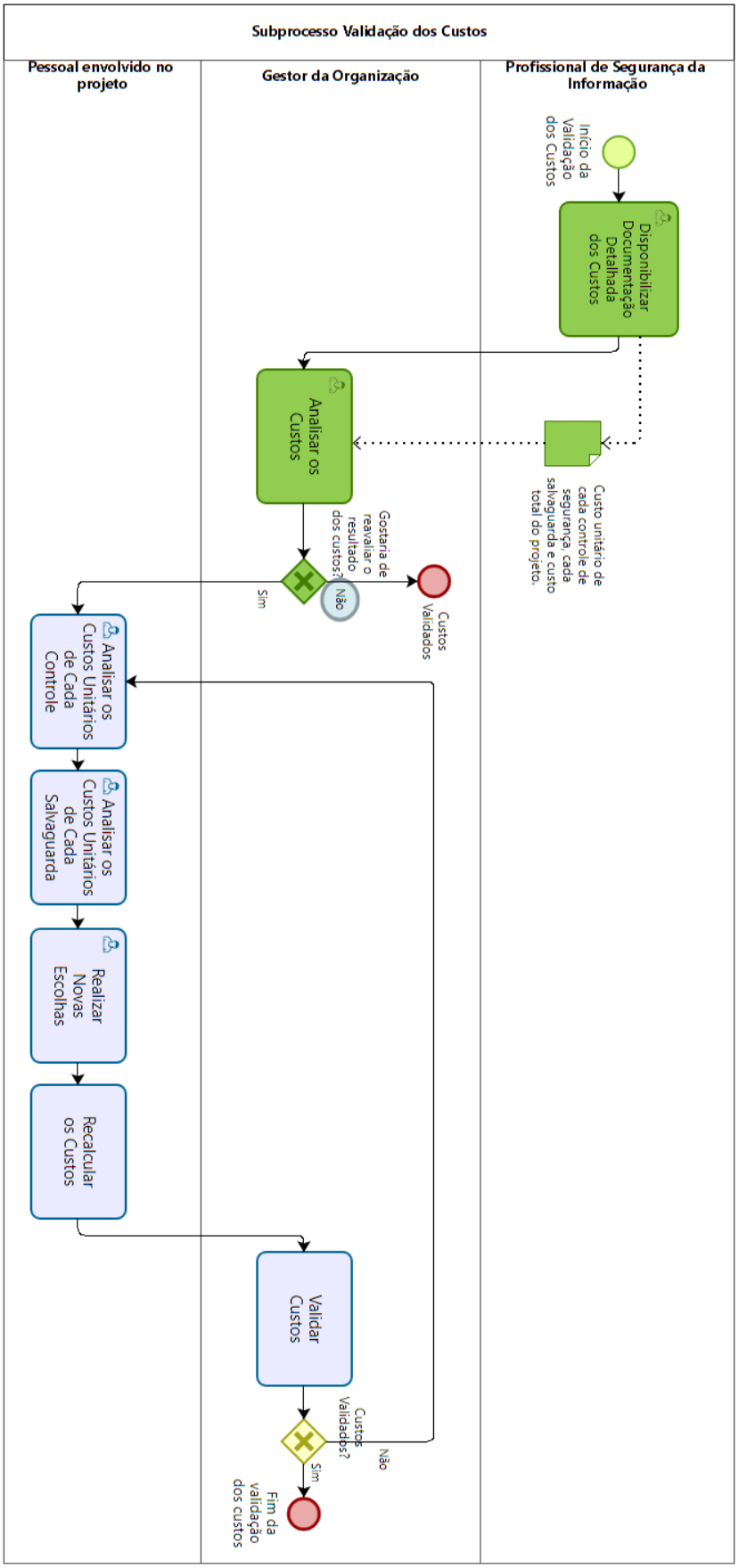
Porém, ao seguir a modelagem e executar o subprocesso **Avaliação da Necessidade de Utilizar *Hardware***, contido no subprocesso **Avaliação dos Requisitos Necessários para os Novos Dispositivos,** foi possível verificar que o servidor físico anteriormente adquirido para suportar o *Windows Server* também suportaria o novo servidor lógico *Open Source Ubuntu Server 22.04.4 LTS*, através da tecnologia de virtualização (*Hyper-V*) da empresa *Microsoft*.

Ao Executar o subprocesso **Avaliação da Necessidade de Utilizar Recurso Humano**, foi possível verificar o quadro de funcionários do departamento, onde um dos técnicos disponíveis no departamento é especialista em distribuições *open source*, suprindo a necessidade de mão-de-obra qualificada para utilização do novo sistema operacional implementado, resultando em custo zero.

Após as verificações de todos os subprocessos, atividades, eventos e *gateways* desta salvaguarda, foi concluído o processo das novas escolhas, e um documento com os novos custos detalhados deste subprocesso foi gerado como resultado.

Em seguida, o subprocesso **Validação dos Custos** foi iniciado, onde os novos custos foram entregues ao cliente de maneira detalhada, conforme a metodologia proposta determina. O cliente validou o processo do cenário 2, não querendo mais realizar uma nova estimativa. A Figura 5.13 ilustra o processo.

Figura 5.13 - Execução do Subprocesso Validação dos Custos.



Fonte: Autor, 2023.

Através destas novas seleções, o parque computacional do departamento acadêmico continuou em conformidade com o *framework* de segurança *CIS v8*, e foi possível evitar a aquisição de 180 licenças do *Windows 11 Pro* que faziam parte da primeira estimativa.

Essa mudança resultou em uma economia de R$ 287.820,00, que representa uma economia de aproximadamente 45,21% do valor total em comparação a primeira estimativa de custo realizada.

A segunda estimativa de custo entregue ao cliente ficou com o valor total de R$ 348.754,92. Já o custo da salvaguarda 2.2, refeita através da metodologia saiu do custo inicial de R$ 454.116,00 para R$ 166.296,00.

5.4 Considerações Finais

Este capítulo apresentou um experimento com o objetivo de aplicar a metodologia proposta nesta dissertação em um cenário de uso real e significativo.

Durante o experimento, ficou constatado que a modelagem desta metodologia guiou o aplicador para projetar os possíveis e variados custos associados a cada ação de implementação dos controles de cibersegurança julgados necessários no ambiente cibernético do departamento acadêmico.

Finalmente, a execução do experimento mostrou não apenas que a metodologia proposta nesta dissertação, descrita no capítulo anterior, é viável, mas também evidenciou que custos podem ser gerados e avaliados de variadas formas, inclusive com diferentes cenários dentro do mesmo ambiente cibernético.

Desta forma, pode-se arguir que a metodologia se mostrou importante não apenas para a mensuração dos custos de implementação, mas para a própria segurança em si, pois possibilitou que a mesma qualidade de segurança desejada fosse atingida com um custo menor e mais acessível à organização avaliada.

Capítulo 6

"Você nunca sabe que resultados virão da sua ação. Mas se você não fizer nada, não existirão."

(Mahatma Gandhi)

6 CONCLUSÕES E TRABALHOS FUTUROS

Este capítulo apresenta as conclusões desta dissertação e também descreve os trabalhos futuros esperados a partir deste trabalho. Após a realização de uma revisão tradicional e um estudo aprofundado do estado da arte sobre o assunto, encontram-se neste capítulo as constatações obtidas após a aplicação da metodologia proposta no experimento.

6.1 Visão Geral

Este trabalho de dissertação mostrou que calcular e avaliar o custo financeiro da implementação de controles e salvaguardas de segurança cibernética não é trivial. Contudo, ao se utilizar a metodologia proposta, foi possível estimar, de forma sistemática e repetível, os custos de implementação de controles de segurança cibernética, possibilitando que a organização pudesse sair do estado atual de maturidade de segurança para um nível mais elevado, que cumpra os requisitos de padrões amplamente difundidos de segurança cibernética e as necessidades particulares de uma organização.

Neste contexto, é possível afirmar que a metodologia proposta é capaz de gerar informações relevantes relacionadas aos custos financeiros necessários para a implementação de controles de segurança cibernética. Além disto, a metodologia foi descrita através de uma abordagem baseada em processos, e modelada através de *BPMN*, um formalismo que vem sendo amplamente utilizado. Isto é uma vantagem, que melhora a possibilidade de reprodução desta metodologia por possíveis usuários e pesquisadores interessados.

Durante a aplicação da metodologia constatou-se também que a modelagem atende às necessidades do *framework* adotado no experimento, o *CIS* v8, além de estimar diversos outros custos extras que puderam ser identificados através das considerações da modelagem.

Observou-se também que, após a execução do processo proposto, foi possível visualizar a concentração de recursos financeiros em controles e salvaguardas específicas. A modelagem, por sua vez, traz a possibilidade de refazer escolhas de maneiras específicas, atuando diretamente onde estão envolvidos os grandes valores, permitindo ao cliente recalcular os custos e adequar o seu projeto de implementação de segurança cibernética à sua realidade financeira.

Não menos importante, a metodologia proposta mostrou-se eficaz em relação à economia de recursos financeiros ao projetar uma implementação de controles de segurança cibernética em um ambiente genérico, fazendo-a de maneira responsável, possibilitando a redução dos custos, porém, mantendo o nível de segurança adequado e permanecendo em conformidade com o *framework* de cibersegurança utilizado.

6.2 Contribuições

A principal contribuição deste trabalho consistiu na proposição de uma metodologia baseada em processo para analisar e definir custos financeiros na implementação de controles de segurança cibernética em ambientes genéricos, com a flexibilidade de utilização com várias normas técnicas e/ou vários *frameworks* de segurança estabelecidos no mercado.

A metodologia proposta foi desenvolvida através de um padrão amplamente conhecido (*BPMN*), o que facilita a sua adoção por várias empresas e organizações de diversos setores de atuação, além dos cálculos matemáticos serem bem acessíveis e de simples execução, expandindo assim a sua utilização para grande parte da população.

O estado da arte atual traz soluções de cibersegurança caras e onerosas para as empresas de modo geral, o que reflete na existência de ambientes cibernéticos inseguros em sua grande maioria, sem o mínimo de controles de segurança aplicados, especialmente nas PMEs.

Este trabalho de dissertação busca trazer uma solução para se obter um ambiente cibernético minimamente seguro, desenvolvendo uma metodologia para guiar o profissional de segurança da informação na implementação de controles e salvaguardas de segurança cibernética em um ambiente cibernético qualquer, utilizando uma norma técnica ou um *framework* de cibersegurança para se estabelecer uma conformidade respaldada quanto ao nível de maturidade em segurança cibernética, especialmente para as PMEs que não dispõem de recursos financeiros abundantes.

6.3 Limitações

Uma limitação deste trabalho está relacionada ao tempo. É necessário bastante tempo para aplicar e avaliar a metodologia em muitos padrões estabelecidos e utilizados pelo mundo inteiro, além de aplicar a mesma metodologia em vários ambientes cibernéticos distintos. Embora os esforços estivessem concentrados para tornar esta metodologia a mais genérica possível, não é possível afirmar, no momento, que a mesma funcione em qualquer norma técnica e em qualquer *framework* de cibersegurança.

Outra limitação possível é o fato de não poder estimar todo o custo possível em uma implementação de controles de segurança, pois cada ambiente cibernético é particular, e por consequência, esta metodologia pode não prever todas as possibilidades de custos, sendo os seus resultados uma estimativa mais próxima da realidade, prevendo os custos comumente existentes em vários ambientes cibernéticos conhecidos.

A questão temporal, também mostra-se um desafio limitador para os resultados da pesquisa, uma vez que nossas estimativas podem ficar rapidamente defasadas, dada a rapidez com que os custos com recursos humanos, *hardware, softwares* e outros equipamentos que compõem os custos extras podem ser modificados com o passar do tempo.

6.4 Trabalhos Futuros

Como trabalho futuro, pretende-se executar o processo proposto em outros estudos de caso, abordando outros *frameworks* de segurança como o NIST e o C2M2, por exemplo, e também em normas técnicas amplamente utilizadas como as ISOs 27002, 27017 e 27032.

Pretende-se também estimar e analisar um custo financeiro ideal para implementar controles de segurança cibernética em ambientes genéricos, impondo um limite de investimento para salvaguardar ativos da empresa. Estudos nesse sentido já foram desenvolvidos, como o modelo de Gordon-Loeb (GORDON e LOEB, 2002) e por Willemson (WILLEMSON, 2010), onde o investimento em segurança é determinado pelo valor da perda estimada ou pelo nível da ameaça cibernética.

Porém, na pesquisa sistemática realizada não foram encontrados estudos que estimassem um investimento financeiro ideal para implementar controles de segurança para proteger os ativos de modo geral, em busca da conformidade com as normas técnicas ou *frameworks* de segurança cibernética quaisquer, sendo este um objetivo para trabalhos futuros.

Por fim, pretendemos também fornecer uma descrição mais formal da modelagem de custos proposta nesta dissertação.

REFERÊNCIAS

ANGELO EDÚ, M. L.; ALEXIS, G. P.; LENIS, W. P. Cybersecurity framework for SMEs in Peru based on ISO/IEC 27001 and CSF NIST controls. 2023. **IEEE 18th Iberian Conference on Information Systems and Technologies (CISTI)**, Aveiro, Portugal, 2023, pp. 1-7, doi: 10.23919/CISTI58278.2023.10211874.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001. Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro, 2022. 23 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002. Segurança da informação - Segurança cibernética e proteção à privacidade - Controles de segurança da informação. Rio de Janeiro, 2022. 191 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27017. Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem. Rio de Janeiro, 2016. 49 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27032. Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética. Rio de Janeiro, 2015. 62 p.

AXON, L.; EROLA, A.; RENSBURG, A. J. V.; NURSE, J. R. C.; GOLDSMITH, M.; CREESE, S. Practitioners' Views on Cybersecurity Control Adoption and Effectiveness. **New York, NY, USA: ACM, 2021**. Disponível em: <http://dx.doi.org/10.1145/3465481.3470038>. Acesso em: 20 feb. 2024.

BAR-HAIM, R.; EDEN, L.; KANTOR, Y.; AGARWAL, V.; DEVEREUX, M.; GUPTA, N.; KUMAR, A.; ORBACH, M.; ZAN, M. Towards Automated Assessment of Organizational Cybersecurity Posture in Cloud. **New York, NY, USA: ACM, 2023**. Disponível em: <http://dx.doi.org/10.1145/3570991.3571008>. Acesso em: 20 feb. 2024.

BARRÈRE, M.; HANKIN, C.; NICOLAOU, N.; ELIADES, D. G.; PARISINI, T. Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies. **Journal of Information Security and Applications**. 2020. [S. l.], v. 52, p. 102471. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2214212619311342?via%3Dihub>. Acesso em: 22 mar. 2024.

BASHOFI, I.; SALMAN, M. Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. 2022. **IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)**, Malang, Indonesia, 2022. Disponível em: <http://dx.doi.org/10.1109/cyberneticscom55287.2022.9865640>. Acesso em: 20 feb. 2024.

BOCCIARELLI, P.; D'AMBROGIO, A.; GIGLIO, A.; PAGLIA, E. Bpmn-Based Business Process Modeling And Simulation. 2019. **Proceedings of the 2019 Winter Simulation Conference, 2019**. Disponível em: <https://ieeexplore.ieee.org/document/9004960>. Acesso

em: 29 nov. 2023.

BODEI, C.; DEGANO, P.; FERRARI, G. L.; GALLETA, L. Security Metrics at Work on the Things in IoT Systems. **From Lambda Calculus to Cybersecurity Through Program Analysis**. Cham: Springer International Publishing, 2020, p. 233–255.

BORKOVICH, D. e SKOVIRA, R. Working From Home: Cybersecurity in the Age of Covid-19. 2020. **Issues in Information Systems**. [S1], v. 21, Issue 4, pp. 234-246, 2020. Disponível em: <https://doi.org/10.48009/4_iis_2020_234-246>. Acesso em: 07 dez. 2023.

BORKOVICH, D.; SKOVIRA, R. WORKING FROM HOME: CYBERSECURITY IN THE AGE OF COVID-19. **Issues in Information Systems**, [S. l.], ano 2020, v. 21, n. 4, p. 234-246, set. 2020. DOI 10.48009/4_iis_2020_234-246. Disponível em: https://doi.org/10.1145/3587062.3587066. Acesso em: 5 jun. 2024.

BRITTO, Gart. **BPM Para Todos:** Uma Visão Geral Abrangente, Objetiva e Esclarecedora sobre Gerenciamento de Processos de Negócio | BPM. 1. ed. Rio de Janeiro: Gart Capote, 2012. 228 p. ISBN 13: 978-1470005412. Disponível em: https://dpo.unb.br/images/phocadownload/dpr/biblioteca/bpm_para_todos-_julho_2013.pdf. Acesso em: 26 jun. 2024.

BRASIL. Lei nº 13709, 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Palácio do Planalto, 2019. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 23 mar. 2024.

BRIASMITATMS. Código de Conduta ISO/IEC 27017:2015 para Controles de Segurança de Informações - Microsoft Compliance. **Microsoft Learn**, [s.d.]. Disponível em: <https://learn.microsoft.com/pt-br/compliance/regulatory/offering-iso-27017>. Acesso em: 2 mar. 2024.

CANEDO, E.; CALAZANS, A.; SILVA, G.; MASSON, E. ICT Practitioners' Perception of Working from Home During the Covid-19 Pandemic: Exploring Gender Differences. **SBES '22: Proceedings of the XXXVI Brazilian Symposium on Software Engineering**, Virtual Event, Brazil, p. 47-57, 5 out. 2022. Disponível em: <https://doi.org/10.1145/3555228.3555248>. Acesso em: 5 jun. 2024.

CENTER FOR INTERNET SECURITY. **Controles CIS Versão 8**. Nova York, 2021, 89 p.

CHANG, B.-M.; SON, J. C.; CHOI, K. A GQM Approach to Evaluation of the Quality of SmartThings Applications Using Static Analysis. **KSII Transactions on Internet and Information Systems**, 2020. [S. l.], v. 14, n. 6. Disponível em: <https://doi.org/10.3837/tiis.2020.06.003>. Acesso em: 22 mar. 2024.

CHINOSI, M.; TROMBETTA, A. BPMN: An introduction to the standard. 2011. **Computer Standards & Interfaces**. [S1], v. 34, Issue 1, jan. 2012, p.124-134. Disponível em: <https://doi.org/10.1016/j.csi.2011.06.002>. Acesso em: 07 dez. 2023.

CISCO SYSTEMS INCORPORATION. CISCO. **O que é segurança digital?** [S. l.], s.d. Disponível em: https://www.cisco.com/c/pt_br/products/security/what-is-cybersecurity.html. Acesso em: 6 jun. 2024.

CRUZADO, C. F.; BACA, R. L. S.; LÓPEZ, H. L. G.; SALINAS, A. E. I. Reference framework “HOGO” for cybersecurity in SMEs based on ISO 27002 and 27032. 2022. **12th International Conference on Cloud Computing, Data Science & Engineering (Confluence)**, Noida, India, 2022. Disponível em: <http://dx.doi.org/10.1109/confluence52989.2022.9734116>. Acesso em: 20 feb. 2024.

DJEBBAR, F.; NORDSTRÖM, K. A Comparative Analysis of Industrial Cybersecurity Standards. **IEEE Access**, 2023. [S. l.], v. 11, p. 85315–85332. Acesso em: 20 feb. 2024.

DUTTA, A.; AL-SHAER, E. Cyber Defense Matrix: A New Model for Optimal Composition of Cybersecurity Controls to Construct Resilient Risk Mitigation. 2019a. **HOTSOS’19**, New York, NY, USA: ACM, 2019. Disponível em: <http://dx.doi.org/10.1145/3314058.3317725>. Acesso em: 20 feb. 2024.

DUTTA, A.; AL-SHAER, E. “What”, “Where”, and “Why” Cybersecurity Controls to Enforce for Optimal Risk Mitigation. 2019b. **IEEE Conference on Communications and Network Security (CNS)**, Washington, DC, USA. Disponível em: <http://dx.doi.org/10.1109/cns.2019.8802745>. Acesso em: 21 feb. 2024.

FINANCIAL INDUSTRY REGULATORY AUTHORITY. FINRA. **Small Firm Cybersecurity Checklist**. Washington, DC, EUA., jun. 2020. Disponível em: https://www.finra.org/compliance-tools/cybersecurity-checklist. Acesso em: 5 jun. 2024.

FRANCO, M. F.; GRANVILLE, L. Z.; STILLER, B. CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment. 2023. **IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA**, 2023. Disponível em: <http://dx.doi.org/10.1109/noms56928.2023.10154307>. Acesso em: 20 feb. 2024.

GANAPATI, S; FRANCO, L. O.; LE, A. N. American State Government Cybersecurity Policies. **DGO '23: Proceedings of the 24th Annual International Conference on Digital Government Research**, Gdańsk, Poland, p. 637-638, 14 jul. 2023. Disponível em: https://doi.org/10.1145/3598469.3598540. Acesso em: 5 jun. 2024.

GORDON, L. A.; LOEB, M. P. The economics of information security investment. **ACM Transactions on Information and System Security**, 2002. [S. l.], v. 5, n. 4, p. 438–457. Disponível em: <https://doi.org/10.1145/581271.581274>. Acesso em: 18 mar. 2024.

HANSEN, D. R.; MOWEN, M. M. **Gestão de Custos**. São Paulo: Cengage Learning, 2009.

INCIDENTES Notificados ao CERT.br: Incidentes notificados voluntariamente ao CERT.br por CSIRTs, administradores de redes e usuários finais. ***In*: Cert.br.** [S. 1.], 8 fev. 2024. Disponível em: https://stats.cert.br/incidentes/. Acesso em: 5 jun. 2024.

IMRAN, T. M. Towards Information Security Metrics Framework for Cloud Computing. **International Journal of Cloud Computing and Services Science (IJ-CLOSER)**, 2012. v. 1, n. 4. Disponível em: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=bc587ee2237f259e49965f21cf77265aad49dafe> . Acesso em: 22 mar. 2024.

INMETRO. **Responsabilidade Social**. [s.d.]. Disponível em:

<http://www.inmetro.gov.br/qualidade/responsabilidade_social/o-que-iso.asp>. Acesso em: 2 mar. 2024.

INTERNATIONAL BUSINESS MACHINES CORPORATION. IBM. **O que é a segurança da informação?** [S. l.], s.d. Disponível em: https://www.ibm.com/br-pt/topics/information-security. Acesso em: 6 jun. 2024.

INTERNATIONAL BUSINESS MACHINES CORPORATION. IBM. **O que é cibersegurança?** [S. l.], s.d. Disponível em: https://www.ibm.com/br-pt/topics/cybersecurity. Acesso em: 6 jun. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. IT sector and related standards. **ISO**, [s.d.]. Disponível em: <https://www.iso.org/sectors/it-technologies>. Acesso em: 2 mar. 2024.

IVKIC, I.; WOLFAUER, S.; OBERHOFER, T.; TAUBER, M. On the cost of cyber security in smart business. 2017. **12th International Conference for Internet Technology and Secured Transactions (ICITST)**, Cambridge, UK, 2017. Disponível em: <http://dx.doi.org/10.23919/icitst.2017.8356395>. Acesso em: 20 feb. 2024.

IVKIĆ, I.; SAILER, P.; GOUGLIDIS, A.; MAUTHE, A.; TAUBER, M. A Security Cost Modelling Framework for Cyber-Physical Systems. **ACM Transactions on Internet Technology**, 2022. [S. l.], v. 22, n. 2, p. 1–31. Disponível em: <https://doi.org/10.1145/3450752>. Acesso em: 20 feb. 2024.

KALDEREMIDIS, I.; FARAO, A.; BOUNTAKAS, P.; PANDA, S.; XENAKIS, C. GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments. 2022. **ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security**, 2022. Disponível em: <http://dx.doi.org/10.1145/3538969.3544431>. Acesso em: 20 feb. 2024.

KAMTHAN, P.; SHAHMIR, N. On the Implications of COVID-19 Pandemic-Induced "Work From Home" in the Software Industry. **ACM SIGSOFT Software Engineering Notes**, New York, NY, United States, v. 48, n. 2, p. 12-13, 11 abr. 2023. Disponível em: https://doi.org/10.1145/3587062.3587066. Acesso em: 5 jun. 2024.

KANSAL, A.; ZHAO, F.; LIU, J.; KOTHARI, N.; BHATTACHARYA, A. A. Virtual machine power metering and provisioning. 2010. **SoCC '10: Proceedings of the 1st ACM symposium on Cloud computing**. New York, USA, ACM, 2010. Disponível em: <http://dx.doi.org/10.1145/1807128.1807136>. Acesso em: 22 mar. 2024.

KHAJOUEI, H.; KAZEMI, M.; MOOSAVIRAD, S. H. Ranking information security controls by using fuzzy analytic hierarchy process. **Information Systems and e-Business Management**, 2016. [S. l.], v. 15, n. 1, p. 1–19. Disponível em: <https://doi.org/10.1007/s10257-016-0306-y>. Acesso em: 20 mar. 2024.

KOBEZAK, P.; MARCHANY, R.; RAYMOND, D.; TRONT, J. Host Inventory Controls and Systems Survey: Evaluating the CIS Critical Security Control One in Higher Education Networks. **Hawaii International Conference on System Sciences**, 2018. Disponível em: <http://dx.doi.org/10.24251/hicss.2018.597>. Acesso em: 22 mar. 2024.

LEE, I. Cybersecurity: Risk management framework and investment cost analysis. **Business Horizons**, 2021. v. 64, n. 5, p. 659–671. Disponível em: <https://doi.org/10.1016/j.bushor.2021.02.022>. Acesso em: 20 feb. 2024.

LEE, S.; JEON, S.; LEE, B. Security Controls for Employees' Satisfaction: Perspective of Controls Framework. **SAGE Open**, Apr. 2019. [S. l.], v. 9, n. 2, p. 215824401985390. Disponível em: <https://doi.org/10.1177/2158244019853908>. Acesso em: 22 mar. 2024.

LIMA, M. V. M.; LIMA, R. M. F.; LINS, F. A. A. A multi-perspective methodology for evaluating the security maturity of data centers. 2017. **IEEE International Conference on Systems, Man, and Cybernetics (SMC)**, Banff, AB, Canada, 2017. Disponível em: <http://dx.doi.org/10.1109/smc.2017.8122775>. Acesso em: 20 feb. 2024.

LUNA, J.; GHANI, H.; GERMANUS, D.; SURI, N. A Security Metrics Framework for the Cloud. 2011. **Proceedings of the International Conference on Security and Cryptography, Seville, Spain**, 2011. Disponível em: <http://dx.doi.org/10.5220/0003446902450250>. Acesso em: 22 mar. 2024.

MALATJI, M. Industrial control systems cybersecurity: Back to basic cyber hygiene practices. 2022. **International Conference on Electrical, Computer and Energy Technologies (ICECET), Prague, Czech Republic**, 2022. Disponível em: <http://dx.doi.org/10.1109/icecet55527.2022.9872810>. Acesso em: 20 feb. 2024.

MEDEIROS, Robson Wagner Albuquerque de. **Cost Management of Service Composition.** 2017. Tese (Doutorado) - University of Twente, 2017.

MOREIRA, F. R.; SILVA FILHO, D. A.; NZE, G. D. A.; SOUZA JÚNIOR, R. T.; NUNES, R. R. Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology. **IEEE Access**, 2021. [S. l.], v. 9, p. 129605–129618. . Acesso em: 20 feb. 2024.

NAÇÕES UNIDAS. ONU. **Pequenas e médias empresas criam 7 em cada 10 postos de trabalho em mercados emergentes**. ONU News, 27 Jun. 2023. Disponível em: <https://news.un.org/pt/story/2023/06/1816647>. Acesso em: 18 mar. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **The NIST Cybersecurity Framework (CSF) 2.0, NIST.CSWP.29**. Gaithersburg, 2024, 32 p.

OPEN WORLDWIDE APPLICATION SECURITY PROJECT. **OWASP Top 10:2021**, [s.d.]. Disponível em: <https://owasp.org/Top10/pt_BR/>. Acesso em: 23 mar. 2024.

PAUL, J. A.; WANG, X. (Jocelyn). Socially optimal IT investment for cybersecurity. **Decision Support Systems**, 2019. [S. l.], v. 122, p. 113069. Acesso em: 20 feb. 2024.

PAWAR, S.; PALIVELA, H. LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). **International Journal of Information Management Data Insights**, 2022. [S. l.], v. 2, n. 1, p. 100080. Disponível em: <https://doi.org/10.1016/j.jjimei.2022.100080>. Acesso em: 20 feb. 2024.

PCI SECURITY STANDARDS COUNCIL. **Payment Card Industry Padrão de Segurança de Dados (PCI-DSS) - Requisitos e Procedimentos de Teste**, Versão 4.0, PT, 2022.

PETERSEN, K.; FELDET, R.; MUJTABA, S.; MATTSSON, M. Systematic mapping studies in software engineering. **EASE‘08: Proceedings of the 12th international conference on Evaluation and Assessment in Software Engineering**, Italy, p. 68-77, 26 jun. 2008. Disponível em: https://dl.acm.org/doi/10.5555/2227115.2227123. Acesso em: 13 dez. 2023.

PMI. **Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK)**. 4. ed. Newtown Square, Pennsylvania, EUA.: Project Management Institute, Inc., 2008. 337 p. ISBN 978-1-933890-70-8. Disponível em: https://www.cin.ufpe.br/~if717/slides/PMBOK.pdf. Acesso em: 5 jun. 2024.

RATHOD, P.; HAMALAINEN, T. A Novel Model for Cybersecurity Economics and Analysis. 2017. **IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland**, 2017. Disponível em: <http://dx.doi.org/10.1109/cit.2017.65>. Acesso em: 20 feb. 2024.

ROJAS, A. J. S.; VALENCIA, E. F. P.; AGUIRRE, A. J.; MOLINA, M. M. J. Cybersecurity maturity model for the protection and privacy of personal health data. 2022. **IEEE 2nd International Conference on Advanced Learning Technologies on Education & Research (ICALTER)**, Lima, Peru, 2022. Disponível em: <http://dx.doi.org/10.1109/icalter57193.2022.9964729>. Acesso em: 20 feb. 2024.

SABILLON, R.; RUIZ, S. J.; CAVALLER, V.; CANO, J. A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM). 2017. **International Conference on Information Systems and Computer Science (INCISCOS), Quito, Ecuador**, 2017. Disponível em: <http://dx.doi.org/10.1109/inciscos.2017.20>. Acesso em: 20 feb. 2024.

SANTOS, M. A. **Contabilidade de Custos.** Salvador: UFBA, 2018.

SCALA, N. M.; GOETHALS, P. L. A Model for and Inventory of Cybersecurity Values: Metrics and Best Practices. **Handbook of Military and Defense Operations Research**. Chapman and Hall/CRC, 2020, p. 305–330.

Serviço Brasileiro De Apoio Às Micro E Pequenas Empresas. SEBRAE. **Anuário do Trabalho na Micro e Pequena Empresa**. Brasília, DF, Brasil, 2013. Disponível em: https://sebrae.com.br/Sebrae/Portal%20Sebrae/Anexos/Anuario%20do%20Trabalho%20Na%20Micro%20e%20Pequena%20Empresa_2013.pdf. Acesso em: 6 jun. 2024.

SILVA, Vladimir Gualberto da. **Planejamento de capacidade em nuvens educacionais privadas considerando aspectos de desempenho e custo**. 2019. Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, 2019.

SIMON, J.; OMAR, A. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. **European Journal of Operational Research**, 2020. [S. l.], v. 282, n. 1, p. 161–171. Disponível em: <https://doi.org/10.1016/j.ejor.2019.09.017>. Acesso em: 20 feb. 2024.

TALL, A. M.; ZOU, C. C.; WANG, J. Integrating Cybersecurity Into a Big Data Ecosystem. 2021. **MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM)**, San Diego, CA, USA. Disponível em:

<http://dx.doi.org/10.1109/milcom52596.2021.9652997>. Acesso em: 20 feb. 2024.

TAUBER, M.; BHATTI, S. N. The Effect of the 802.11 Power Save Mechanism (PSM) on Energy Efficiency and Performance during System Activity. 2012a. **IEEE International Conference on Green Computing and Communications**, Besancon, France, 2012. Disponível em: <http://dx.doi.org/10.1109/greencom.2012.81>. Acesso em: 22 mar. 2024.

TAUBER, M.; BHATTI, S. N.; YI YU. Towards energy-awareness in managing wireless LAN applications. 2012b. **IEEE Network Operations and Management Symposium**, Maui, HI, USA, 2012. Disponível em: <http://dx.doi.org/10.1109/noms.2012.6211930>. Acesso em: 22 mar. 2024.

TOAPANTA, S. M. T.; E., G. S. G.; GALLEGOS, L. E. M. Analysis of appropriate standards to solve cybersecurity problems in public organizations. 2020. **ICISDM '20: Proceedings of the 2020 the 4th International Conference on Information System and Data Mining**, New York, USA: ACM, 2020. Disponível em: <http://dx.doi.org/10.1145/3404663.3404678>. Acesso em: 20 feb. 2024.

U.S. DEPARTMENT OF ENERGY. **Cybersecurity Capability Maturity Model, Version 2.0, C2M2**. Washington, 2021, 90 p.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES. **HIPAA Administrative Simplification Regulation Text**. Washington, 2013, 115 p.

UDROIU, A.-M.; DUMITRACHE, M.; SANDU, I. Improving the cybersecurity of medical systems by applying the NIST framework. 2022. **14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)**, Ploiesti, Romania, 2022. Disponível em: <http://dx.doi.org/10.1109/ecai54874.2022.9847498>. Acesso em: 20 feb. 2024.

VALENÇA, G. **BPMN (Business Process Modeling Notation)**. Recife, Pernambuco, Brasil., 31 out. 2012. Disponível em: https://www.cin.ufpe.br/~processos/TAES3/slides-2012.2/Introducao_BPMN.pdf. Acesso em: 18 jun. 2024.

VALENZUELA, D. Á. Agenda legislativa sobre ciberseguridad en Chile. **Revista Chilena de Derecho y Tecnología**, [S. l.], v. 7, n. 2, p. 1–3, 2018a. DOI: 10.5354/0719-2584.2018.51992. Disponível em: <https://rchdt.uchile.cl/index.php/RCHDT/article/view/51992>. Acesso em: 22 mar. 2024.

VALENZUELA, D. Á. Ciberseguridad en América Latina y ciberdefensa en Chile. **Revista Chilena de Derecho y Tecnología**, [S. l.], v. 7, n. 1, p. 1–2, 2018b. DOI: 10.5354/0719-2584.2018.50416. Disponível em: <https://rchdt.uchile.cl/index.php/RCHDT/article/view/50416>. Acesso em: 22 mar. 2024.

WILLEMSON, J. Extending the Gordon and Loeb Model for Information Security Investment. **Conferência Internacional sobre Disponibilidade, Confiabilidade e Segurança de 2010**, Cracóvia, Polônia, 2010, pp.

APÊNDICE

APÊNDICE A - Questionário Online do subprocesso Compreender os Requisitos do Ambiente Cibernético.

Compreender Requisitos do Ambiente Cibernético

A intenção deste formulário é de documentar as respostas sobre os pontos e ações importantes do espaço cibernético do cliente como parte da metodologia proposta para calcular os custos financeiros de implementação de cibersegurança em ambientes genéricos.

saulomarques.morais@gmail.com Mudar de conta

* Indica uma pergunta obrigatória

E-mail *

Seu e-mail

Qual é o segmento de negócio da empresa/ organização? (Ex: Educação, Saúde, Agro, Farmacêutica...) *

Sua resposta

A sua empresa trata ou armazena dados de seus clientes? *

- ◯ Sim
- ◯ Não

Caso a resposta da pergunta anterior tenha sido "**Sim**", descreva abaixo os tipos de dados tratados. Caso tenha sido não, rechace a negativa escrevendo "**Não**". *

Sua resposta

A empresa/organização possui profissionais de TI para ficar a frente do projeto de segurança cibernética? *

- ◯ Sim
- ◯ Não

Caso a resposta da pergunta anterior tenha sido "**Sim**", escreva abaixo todos eles. Cite o tipo, sua especialidade e a quantidade de cada profissional. Não precisa especificar as suas atividades. (Ex: Analista de TI - Programador - 5; Analista de TI - Gerente de projeto - 1; Analista de TI - Segurança da Informação - 3; Técnico de informática - Suporte ao usuário - 4; Técnico de informática - Manutenção de hardware - 5). Caso tenha respondido "**Não**", rechace a negativa escrevendo: **Não**. *

Sua resposta

Marque as caixas de seleção de acordo com o espaço físico da organização que servirá como infraestrutura de TI. *

- [ ] É necessário construir, ampliar ou separar algum espaço físico?
- [ ] É necessário climatizar?
- [ ] É necessário controlar o acesso físico?

Especifique as informações de cada caixa selecionada na questão anterior. *

Sua resposta

Informe sobre as aplicações, ferramentas , softwares e sistemas indispensáveis utilizados em seu ambiente cibernético.

Sua resposta

Uma cópia das suas respostas será enviada para o endereço de e-mail fornecido

Enviar

Limpar formulário

Nunca envie senhas pelo Formulários Google.

APÊNDICE B - Controles e Salvaguardas que Compõem o Ambiente Cibernético do Departamento Acadêmico considerados como sem custos.

Controle 1 - Inventário e controle de ativos corporativos	**Salvaguarda 1.1 - Estabelecer e manter um inventário detalhado de ativos corporativos**
Custo	R$ 0
Justificativa: Esta atividade é definida como manual, e será realizada pelos técnicos que o departamento possui, por isso é considerada sem custo. Todo o processo de proteção de segurança começa pela realização de um inventário bem detalhado e preciso de todos os ativos corporativos que armazenam ou processam dados. É necessário identificar todo o parque computacional, para só depois projetar as estratégias de defesa. Ficou decidido que o inventário será realizado de maneira manual pelos profissionais que cuidam deste ambiente cibernético.	
Controle 1 - Inventário e controle de ativos de *software*	**Salvaguarda 1.2 - Endereçar ativos não autorizados**
Custo	R$ 0
Justificativa: Esta atividade será realizada pelos técnicos que o departamento possui, por isso é considerada sem custo. Ficou decidido que os ativos não autorizados na rede, após descobertos, serão removidos da rede. Configurações no controlador de domínio, *firewall* ou até mesmo diretamente nos *switches* gerenciáveis podem desativar a conexão do dispositivo não autorizado. A melhor estratégia será definida pelos profissionais responsáveis conforme suas decisões.	
Controle 2 - Inventário e controle de ativos de *software*	**Salvaguarda 2.1 - Estabelecer e manter um inventário de *software***
Custo	R$ 0
Justificativa: Esta atividade é definida como manual, e será realizada pelos técnicos que o departamento possui, por isso é considerada sem custo. Todo o processo de proteção de segurança começa pela realização de um inventário bem detalhado e preciso. Neste caso, todos os *softwares* licenciados e instalados no ambiente cibernético devem ser controlados. O inventário de *software* ficou definido para ser realizado a cada seis meses pelos profissionais responsáveis do departamento acadêmico.	
Controle 2 - Inventário e controle de ativos de *software*	**Salvaguarda 2.3 - Endereçar o *software* não autorizado**
Custo	R$ 0
Justificativa: Esta é uma tarefa definida como manual, e será realizada pelos técnicos que o departamento possui, por isso é considerada sem custo. Os *softwares* não autorizados, serão desinstalados das máquinas imediatamente.	
Controle 3 - Proteção de dados	**Salvaguarda 3.1 - Estabelecer e manter um processo de gestão de dados**

Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma documentação de boas práticas. Ficou definido que a gestão do departamento acadêmico irá desenvolver a documentação, junto à coordenação de TI também do departamento. Dessa forma, a salvaguarda é definida como sem custo, pelos profissionais já fazerem parte do quadro de profissionais, sendo pagos por autoridade superior ao departamento.	
Controle 3 - Proteção de dados	**Salvaguarda 3.2 - Estabelecer e manter um inventário de dados**
Custo	R$ 0
Justificativa: Esta é uma tarefa definida como manual, e será realizada pelos técnicos que o departamento possui, por isso é considerada sem custo. O inventário de dados é necessário principalmente no que diz respeito aos dados sensíveis. Este tipo de dado será monitorado uma vez ao ano.	
Controle 3 - Proteção de dados	**Salvaguarda 3.4 - Aplicar retenção de dados**
Custo	R$ 0
Justificativa: Esta é uma tarefa definida como manual, e será realizada pelos técnicos que o departamento possui, por isso é considerada sem custo. Os dados serão armazenados em locais adequados e criptografados, além de prazos mínimos e máximos determinados e estabelecidos por documentação do departamento acadêmico.	
Controle 3 - Proteção de dados	**Salvaguarda 3.5 - Descartar dados com segurança**
Custo	R$ 0
Justificativa: Esta é uma tarefa definida como manual, e será realizada pelos técnicos que o departamento possui, por isso é considerada sem custo. Os dados serão descartados conforme os seus tipos. Sendo dados sensíveis, será descartado conforme documentação do departamento gerada em observância à LGPD.	
Controle 3 - Proteção de dados	**Salvaguarda 3.6 - Criptografar dados em dispositivos de usuário final.**
Custo	R$ 0
Justificativa: Esta tarefa será realizada pelos técnicos que o departamento possui, por isso é considerada sem custo. As ferramentas são nativas do sistema operacional utilizado, como a *Windows BitLocker* e a *DM-Crypt* para as distribuições *Microsoft* e *Linux* respectivamente. As máquinas estarão com a criptografia ativada para garantir a segurança dos dados.	
Controle 4 - Configuração segura de ativos corporativos e *software*	**Salvaguarda 4.1 - Estabelecer e manter um processo de configuração segura**

Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma documentação de boas práticas. Ficou definido que a gestão do departamento acadêmico irá desenvolver a documentação, junto à coordenação de TI também do departamento. Dessa forma, a salvaguarda é definida como sem custo, pelos profissionais já fazerem parte do quadro de profissionais, sendo pagos por autoridade superior ao departamento.	
Controle 4 - Configuração segura de ativos corporativos e *software*	**Salvaguarda 4.2 - Estabelecer e Manter um Processo de Configuração Segura para a Infraestrutura de Rede**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma documentação de boas práticas. Esta salvaguarda será realizada pelo técnico de TI em infraestrutura de redes do departamento, por isso é definida como sem custo.	
Controle 4 - Configuração segura de ativos corporativos e software	**Salvaguarda 4.3 - Configurar o bloqueio automático de sessão nos ativos corporativos**
Custo	R$ 0
Justificativa: Esta salvaguarda pode ser atendida através de configuração local do dispositivo final do usuário, determinando o bloqueio automático da sessão do usuário, após 15 minutos de inatividade e para dispositivos móveis, com o tempo máximo de 2 minutos de inatividade. Além da configuração direta no sistema operacional dos dispositivos finais do usuário, é possível gerenciar as seções dos usuários através do controlador de domínio. Por serem uma configuração nativa nos sistemas operacionais utilizados, esta salvaguarda é considerada sem custo.	
Controle 4 - Configuração segura de ativos corporativos e *software*	**Salvaguarda 4.6 - Gerenciar com segurança os ativos e *software* corporativos**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo estabelecer meios de acesso seguros aos ativos e *softwares* corporativos. Ficou definido que o acesso aos ativos será permitido apenas por protocolos considerados seguros, como o SSH e HTTP. O técnico de TI em infraestrutura de redes será o responsável por essas configurações, por isso a salvaguarda é considerada sem custo.	
Controle 4 - Configuração segura de ativos corporativos e *software*	**Salvaguarda 4.7 - Gerenciar contas padrão nos ativos e *software* corporativos**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma ação de boas práticas. Esta atividade será realizada pelos técnicos do departamento, por isso é definida como sem custo. As contas padrões e contas de super usuário serão desativadas por padrão em todos os dispositivos do ambiente cibernético do departamento acadêmico.	

Controle 5 - Gestão de Contas	**Salvaguarda 5.1 - Estabelecer e manter um inventário de contas**
Custo	R$ 0
Justificativa: Esta é uma tarefa definida como manual, e será realizada pelos técnicos que o departamento possui, por isso é considerada sem custo. Ficou definido que o inventário de contas de usuário será gerenciado semestralmente ou quando houver mudança significativa em usuários com algum poder administrativo no domínio.	
Controle 5 - Gestão de Contas	**Salvaguarda 5.2 - Usar senhas exclusivas**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Ficou definido, como exigência do *framework* adotado, que todo ativo corporativo terá senha de gerenciamento exclusiva, e as senhas serão definidas com no mínimo 14 caracteres sem o uso de MFA, e com no mínimo 8 caracteres mais o uso de MFA (*CIS,* 2021).	
Controle 5 - Gestão de Contas	**Salvaguarda 5.3 - Desabilitar contas inativas**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Esta atividade será desempenhada pelos técnicos do departamento acadêmico, onde as contas inativas por mais de 45 dias serão desativadas pelo administrador de domínio.	
Controle 5 - Gestão de Contas	**Salvaguarda 5.4 - Restringir privilégios de administrador a contas de Administrador dedicadas**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Esta configuração será realizada no controlador de domínio. Ficou definido que no ambiente cibernético do departamento, cada administrador terá acesso privilegiado apenas nos serviços dos quais for responsável. Não haverá conta de administrador com acesso total ao sistema. Essa prática evita que após um ataque bem sucedido a uma conta de administrador, o atacante tenha acesso total à rede e seus serviços. Dessa forma, a violação ficará restrita apenas aos serviços e locais que o usuário violado possuir, impedindo um desastre maior.	
Controle 6 - Gestão do Controle de Acesso	**Salvaguarda 6.1 - Estabelecer um Processo de Concessão de Acesso**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Esta configuração será realizada no controlador de domínio. Ficou definido que o	

acesso de cada usuário será determinado conforme o cargo exercido pelo colaborador e mediante a necessidade das atividades realizadas por ele para alcançar os objetivos da organização.

Controle 6 - Gestão do Controle de Acesso	**Salvaguarda 6.2 - Estabelecer um Processo de Revogação de Acesso**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Esta configuração será realizada no controlador de domínio. Ficou definido que o acesso de cada usuário será revogado imediatamente após qualquer mudança ou alteração no perfil do colaborador da empresa. Seja um desligamento, onde a revogação é total e permanente, ou uma alteração no cargo ou função, revogando o acesso aos locais do antigo cargo sempre que necessário.	

Controle 6 - Gestão do Controle de Acesso	**Salvaguarda 6.3 - Exigir MFA para aplicações expostas externamente**
Custo	R$ 0
Justificativa: No momento do experimento e aplicação da metodologia, o departamento afirma não utilizar aplicações externas e de terceiros. Por este motivo, a salvaguarda é considerada sem custo, pela não aplicação da mesma no ambiente cibernético do departamento.	

Controle 6 - Gestão do Controle de Acesso	**Salvaguarda 6.5 - Exigir MFA para acesso administrativo**
Custo	R$ 0
Justificativa: O departamento definiu que as contas administrativas de modo geral, não necessitam de MFA por padrão. Por este motivo, a salvaguarda é considerada sem custo. Os casos onde o MFA é considerado importante e consequentemente aplicado no ambiente, foram considerados na salvaguarda 6.4.	

Controle 7 - Gestão contínua de vulnerabilidades	**Salvaguarda 7.1 - Estabelecer e manter um processo de gestão de vulnerabilidade**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma ação de boas práticas, por isso é considerada sem custo. Ficou definido da gestão do departamento, juntamente com a coordenação de TI do próprio departamento criar e estabelecer uma documentação para nortear as ações de gerenciamento sobre vulnerabilidades.	

Controle 7 - Gestão contínua de vulnerabilidades	**Salvaguarda 7.2 - Estabelecer e manter um processo de remediação**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma ação de boas práticas, por isso é considerada sem custo. Ficou definido da gestão do departamento, juntamente com a coordenação de TI do próprio departamento criar e estabelecer uma documentação para nortear as ações de gerenciamento sobre os	

processos de remediação.	
Controle 7 - Gestão contínua de vulnerabilidades	**Salvaguarda 7.3 - Executar a gestão automatizada de *patches* do sistema operacional**
Custo	R$ 0
Justificativa: Esta salvaguarda pode ser atendida através de uma configuração no controlador de domínio, por isso é considerada sem custo, uma vez que o custo foi considerado em uma salvaguarda anterior.	
Controle 7 - Gestão contínua de vulnerabilidades	**Salvaguarda 7.4 - Executar a gestão automatizada de *patches* de aplicações**
Custo	R$ 0
Justificativa: Esta salvaguarda pode ser atendida através de uma configuração no controlador de domínio, por isso é considerada sem custo.	
Controle 8 - Gestão de registros de auditoria	**Salvaguarda 8.1 - Estabelecer e manter um processo de gestão de log de auditoria**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Ficou definido da gestão do departamento, juntamente com a coordenação de TI do próprio departamento criar e estabelecer uma documentação para nortear as ações de gerenciamento sobre os registros de logs da empresa.	
Controle 8 - Gestão de registros de auditoria	**Salvaguarda 8.2 - Coletar logs de auditoria**
Custo	R$ 0
Justificativa: Esta salvaguarda pode ser atendida através de uma configuração nos ativos localmente, por isso é considerada sem custo. Os técnicos do departamento acadêmico farão o controle destes registros de logs.	
Controle 8 - Gestão de registros de auditoria	**Salvaguarda 8.3 - Garantir o armazenamento adequado do registro de auditoria**
Custo	R$ 0
Justificativa: Os registros de logs serão armazenados conforme a documentação desenvolvida pela gestão do departamento. O armazenamento será feito em instâncias disponíveis no ambiente cibernético do departamento, por isso esta salvaguarda é considerada sem custo.	
Controle 9 - Proteções de e-mail e navegador Web	**Salvaguarda 9.1 - Garantir o uso apenas de navegadores e clientes de e-mail suportados plenamente**

Custo	R$ 0
Justificativa: Esta salvaguarda pode ser atendida através de configuração no controlador de domínio, por isso é considerada sem custo. Ficou determinado que apenas *softwares* autorizados previamente serão instalados no ambiente controlado.	
Controle 9 - Proteções de e-mail e navegador Web	**Salvaguarda 9.2 - Usar serviços de filtragem de DNS**
Custo	R$ 0
Justificativa: Esta salvaguarda pode ser atendida através de configuração no *firewall*, por isso é considerada sem custo. Esta prática evita que usuários de modo geral possam acessar sites mal-intencionados.	
Controle 10 - Defesas contra malware	**Salvaguarda 10.1 - Instalar e manter um *software* anti-malware**
Custo	R$ 0
Justificativa: Esta salvaguarda é atendida por uma salvaguarda anterior, por isso é considerada sem custo. Todos os ativos corporativos, sempre que possível, terão um *software* anti-malware instalado localmente.	
Controle 10 - Defesas contra malware	**Salvaguarda 10.2 - Configurar atualizações automáticas de assinatura anti-malware**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Ficou definido que as atualizações contra malware serão instaladas automaticamente, assim que disponibilizadas pelo software de defesa utilizado.	
Controle 10 - Defesas contra malware	**Salvaguarda 10.3 - Desabilitar a execução e reprodução automática para mídias removíveis**
Custo	R$ 0
Justificativa: Esta salvaguarda pode ser atendida através de configuração no controlador de domínio ou localmente, por isso é considerada sem custo. Ficou determinado que as estações de trabalho, por padrão, não executarão mídias removíveis automaticamente. Em alguns locais mais críticos, ou quando o administrador da rede julgar necessário, será desabilitado as entradas de mídias removíveis, como as portas usb, por exemplo.	
Controle 11 - Recuperação de dados	**Salvaguarda 11.1 - Estabelecer e manter um processo de recuperação de dados**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Ficou definido da gestão do departamento, juntamente com a coordenação de TI do próprio departamento criar e estabelecer uma documentação para nortear as ações sobre o processo de	

recuperação de dados.	
Controle 11 - Recuperação de dados	**Salvaguarda 11.3 - Proteger os dados de recuperação**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Ficou definido que o departamento usaria criptografia para garantir a privacidade dos dados de recuperação.	
Controle 11 - Recuperação de dados	**Salvaguarda 11.4 - Estabelecer e manter uma instância isolada de dados de recuperação**
Custo	R$ 0
Justificativa: Esta salvaguarda pode ser atendida através de um recurso que o departamento já possui, o Google Workspace, por isso é considerada sem custo. Os backups serão realizados automaticamente através de configurações pré-definidas no servidor de backup NAS para o Google Drive do departamento.	
Controle 12 - Gestão da infraestrutura de rede	**Salvaguarda 12.1 - Assegurar que a infraestrutura de rede esteja atualizada**
Custo	R$ 0
Justificativa: Esta é uma tarefa definida como manual, e será realizada pelos técnicos que o departamento possui, por isso é considerada sem custo. Ficou definido que a gestão do departamento definiria o tempo de verificação quanto às versões de *softwares* utilizadas dos ativos de rede do ambiente cibernético, para que as versões atualizadas e mais recentes sejam instaladas sempre que possível.	
Controle 14 - Conscientização sobre segurança e treinamento de competências	**Salvaguarda 14.1 - Estabelecer e manter um programa de conscientização de segurança**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Ficou definido que a gestão do departamento, juntamente com a coordenação de TI do próprio departamento, irá criar e estabelecer uma estratégia de treinamento de todo o quadro de pessoal do departamento.	
Controle 14 - Conscientização sobre segurança e treinamento de competências	**Salvaguarda 14.2 - Treinar membros da força de trabalho para reconhecer ataques de engenharia social**
Custo	R$ 0
Justificativa: Ficou definido que o treinamento da força de trabalho será realizado através de vídeo aulas e cartilhas informativas desenvolvidas pelos profissionais do próprio departamento. Mensagens de boas vindas com instruções de segurança também serão utilizadas toda a vez que o usuário fizer login na conta administrativa. Esta configuração pode ser realizada no controlador de domínio, por isso é considerada sem	

custo.	
Controle 14 - Conscientização sobre segurança e treinamento de competências	**Salvaguarda 14.3 - Treinar membros da força de trabalho nas melhores práticas de autenticação**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Durante o treinamento em segurança da força de trabalho, os usuários serão instruídos utilizarem senhas consideradas seguras, contendo letras, números e caracteres especiais, com tamanho mínimo de 14 caracteres, além da exigência da alteração de senha em tempo pré determinado pelo controlador de domínio (*CIS*, 2021).	
Controle 14 - Conscientização sobre segurança e treinamento de competências	**Salvaguarda 14.4 - Treinar a força de trabalho nas Melhores Práticas de Tratamento de Dados**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Durante o treinamento em segurança da força de trabalho, os usuários serão instruídos a tratarem os dados manipulados da maneira adequada, conforme o seu tipo e necessidade.	
Controle 14 - Conscientização sobre segurança e treinamento de competências	**Salvaguarda 14.5 - Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Durante o treinamento em segurança da força de trabalho, os usuários serão instruídos a não disponibilizar dados a pessoas não autorizadas.	
Controle 14 - Conscientização sobre segurança e treinamento de competências	**Salvaguarda 14.6 - Treinar Membros da força de trabalho no Reconhecimento e Comunicação de Incidentes de Segurança**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Durante o treinamento em segurança da força de trabalho, os usuários serão instruídos a identificar um incidente ocorrido e a comunicar ao setor responsável imediatamente. Endereços de e-mail e números de telefone serão amplamente difundidos para este tipo de situação.	
Controle 14 - Conscientização sobre segurança e treinamento de competências	**Salvaguarda 14.7 - Treinar a força de trabalho sobre como identificar e comunicar se o seus ativos corporativos estão faltando atualizações de segurança**
Custo	R$ 0

Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Durante o treinamento em segurança da força de trabalho, os usuários serão instruídos a identificar uma falha nas atualizações automáticas de segurança dos softwares utilizados e a comunicar ao setor responsável imediatamente. Endereços de e-mail e números de telefone serão amplamente difundidos para este tipo de situação.	
Controle 14 - Conscientização sobre segurança e treinamento de competências	**Salvaguarda 14.8 -Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Durante o treinamento em segurança da força de trabalho, os usuários serão instruídos a transmitir dados pela rede de computador local ou pela internet de maneira segura, sempre criptografados. Além disso, estratégias de criar e manter um ambiente cibernético seguro em casa serão amplamente difundidas, uma vez que a força de trabalho pode desempenhar as suas atividades de maneira remota.	
Controle 15 - Gestão de provedor de serviços	**Salvaguarda 15.1 - Estabelecer e manter um inventário de provedores de serviços**
Custo	R$ 0
Justificativa: Esta atividade é definida como manual, e será realizada pelos técnicos que o departamento possui, por isso é considerada sem custo. Ficou definido que este inventário será atualizado e revisado anualmente, ou quando houverem mudanças significativas de provedores de serviço no ambiente cibernético.	
Controle 17 - Gestão de respostas a incidentes	**Salvaguarda 17.1 - Designar Pessoal para Gerenciar Tratamento de Incidentes**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Ficou definido que a coordenação de TI trataria os casos de incidentes cibernéticos.	
Controle 17 - Gestão de respostas a incidentes	**Salvaguarda 17.2 - Estabelecer e manter informações de contato para relatar incidentes de segurança**
Custo	R$ 0
Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Endereços de e-mail, números de telefone e os nomes dos responsáveis serão amplamente difundidos para esse propósito.	
Controle 17 - Gestão de respostas a incidentes	**Salvaguarda 17.3 - Estabelecer e manter um processo corporativo para relatar incidentes**
Custo	R$ 0

Justificativa: Esta salvaguarda tem por objetivo criar e estabelecer uma política de boas práticas, por isso é considerada sem custo. Ficou definido da gestão do departamento, juntamente com a coordenação de TI do próprio departamento criar e estabelecer uma documentação sobre as boas práticas para relatar um incidente cibernético.

Fonte: Autor (2024).