CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
UNIDADE DE PÓS-GRADUAÇÃO, EXTENSÃO E PESQUISA
MESTRADO PROFISSIONAL EM GESTÃO E TECNOLOGIA EM SISTEMAS PRODUTIVOS

RODRIGO YOKOYAMA

APLICAÇÃO DE MODELAGEM DE AMEAÇAS EM SEGURANÇA DA INFORMAÇÃO NOS PROCESSOS DE ATUALIZAÇÃO DE PROGRAMAS EM *ENDPOINTS*

São Paulo
Março/2023

RODRIGO YOKOYAMA

APLICAÇÃO DE MODELAGEM DE AMEAÇAS EM SEGURANÇA DA INFORMAÇÃO NOS PROCESSOS DE ATUALIZAÇÃO DE PROGRAMAS EM *ENDPOINTS*

Dissertação apresentada como exigência parcial para a obtenção do título de Mestre em Gestão e Tecnologia em Sistemas Produtivos do Centro Estadual de Educação Tecnológica Paula Souza, no Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos, sob a orientação do Prof. Dr. Carlos Hideo Arima

São Paulo
Março/2023

FICHA ELABORADA PELA BIBLIOTECA NELSON ALVES VIANA
FATEC-SP / CPS CRB8-8390

Yokoyama, Rodrigo

Y54a Aplicação de modelagem de ameaças em segurança da informação nos processos de atualização de programas em endpoints / Rodrigo Yokoyama. – São Paulo: CPS, 2023.

132 f. : il.

Orientador: Prof. Dr. Carlos Hideo Arima

Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivo) – Centro Estadual de Educação Tecnológica Paula Souza, 2023.

1. Modelagem de ameaça. 2. Stride. 3. Dread. 4. Iso 27000. I. Arima, Carlos Hideo. II. Centro Estadual de Educação Tecnológica Paula Souza. III. Título.

RODRIGO YOKOYAMA

Aplicação de modelagem de ameaças em segurança da informação nos processos de atualização de programas em *endpoints*

Prof. Dr. Carlos Hideo Arima
Orientador – CEETEPS

Prof. Dr. Adilson Carlos Yoshikuni
Examinador Externo – Universidade Presbiteriana Mackenzie

Prof. Dr. Napoleão Verardi Galegale
Examinador Interno - CEETEPS

São Paulo, 01 de março de 2023

Dedico este trabalho à minha mãe, que sempre incentivou seus filhos em seus estudos e serem melhores do que ontem.

AGRADECIMENTOS

Nesses anos de mestrado, de muito estudo e esforço gostaria de agradecer algumas pessoas que foram fundamentais para a realização e conclusão deste trabalho.

Primeiramente agradeço aos meus irmãos, André e Soraya: é muito bom saber que posso contar com vocês em todos os momentos. Obrigado por acreditar em mim!

Minha gratidão ao prof. Arima por ter me aceitado como orientando, agradeço por ter acreditado, pela confiança, interesse e disponibilidade que contribuíram para o êxito deste trabalho.

Aos Professores que participaram da minha bancada de defesa, Prof. Napoleão e Prof. Adilson, pelo suporte, análises e elogios que me permitiram apresentar um melhor desempenho no meu processo.

Á minha esposa, Anne, pelo apoio, companheirismo e compreensão, contribuindo para que concluísse com êxito essa jornada.

Aos meus colegas de turma, por compartilharem comigo tantos momentos de aprendizado e por todo o companheirismo ao longo deste percurso.

A todos da empresa pelo suporte, que foram fundamentais para o desenvolvimento da pesquisa que possibilitou a realização deste trabalho.

Aos amigos: Luísa e Victor, pelo auxílio e todo empenho e colaboração possível no desenvolvimento do sistema.

A todos aqueles que contribuíram, de alguma forma, para a realização deste trabalho.

“Um homem não pode entender a arte que está
estudando se apenas procura o resultado final
sem ter tempo para se aprofundar no raciocínio
do estudo”
Miyamoto Musashi

RESUMO

YOKOYAMA, R. Aplicação de modelagem de ameaças em segurança da informação nos processos de atualização de programas em *endpoints*: 132f. Dissertação (Mestrado Profissional em Gestão e Desenvolvimento da Educação Profissional). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2023.

O presente trabalho, pertencente a linha de pesquisa de Sistemas de Informação e Tecnologias Digitais e ao Projeto de Pesquisa Gestão de Tecnologia e Sistemas de Informação, tratando os temas da tecnologia e segurança da informação. Tem por objetivo identificar, descrever e avaliar os impactos da aplicação do método modelagem de ameaça, utilizando normas de gestão de risco, em computadores empresariais com auxílio de um sistema para monitoramento. A metodologia usada para conduzir o estudo foi baseada na *Design Science Research Methodology* que incorpora princípios, práticas e procedimentos necessários para o *design*, desenvolvimento, demonstração e avaliação do processo em questão em conjunto com um elemento da *Canonical Action Research*, viabilizando a melhora no processo. O método proposto para aplicação sugere a adoção de processos e de um sistema para atualização, controle e gestão do Sistema Operacional para redução das ameaças encontradas. A pesquisa foi realizada em uma empresa do ramo jurídico com mais de mil colaboradores que adotaram o modelo *home office* e identificou ameaças utilizando os métodos STRIDE e DREAD e as normas de segurança ISO e NIST. Verificou-se 14 tipos de ameaças que podem ser identificadas e mitigadas com a utilização do método de modelagem de ameaça. Os resultados das avaliações interna e externa foram obtidos por meio de entrevistas semiestruturadas com profissionais da área de tecnologia, que avaliaram o processo como relevante. Como implicação prática, o método e o sistema apresentado podem ser utilizados por áreas de tecnologia e correlatas visando a melhoria da segurança no ambiente. Como implicações teóricas, o trabalho contribui para a extensão da literatura preenchendo parte da lacuna relacionada a modelagem de ameaça e sua aplicação em *endpoints* e a proposta de um sistema para monitoramento.

Palavras-chave: Modelagem de ameaça. STRIDE. DREAD. ISO 27000.

ABSTRACT

YOKOYAMA, R. **A threat modeling methodology applied in a study on existing processes focused on security and program update monitoring in endpoints**: subtítulo [não negritado]. 132f. Dissertação (Mestrado Profissional em Gestão e Desenvolvimento da Educação Profissional). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2023.

This work belongs to the line of research on Information Systems and Digital Technologies and the Research Project on Technology Management and Information Systems, dealing with technology and information security issues. It aims to identify, describe and evaluate the impacts of applying the threat modeling method, using risk management standards, on business computers with the aid of a monitoring system. The methodology used to conduct the study was based on the Design Science Research Methodology, which incorporates principles, practices and procedures necessary for the design, development, demonstration and evaluation of the process in question, together with an element of Canonical Action Research, enabling the improvement in the process. The proposed method for application suggests the adoption of processes and a system for updating, controlling and managing the Operating System to reduce the threats encountered. The research was carried out in a legal company with more than a thousand employees who adopted the home office model and identified threats using the STRIDE and DREAD methods and the ISO and NIST security standards. There were 14 types of threats that can be identified and mitigated using the threat modeling method. The results of the internal and external evaluations were obtained through semi-structured interviews with technology professionals, who considered the process relevant. As a practical implication, the method and system presented can be used by technology and related areas that aim to improve safety in the environment. As theoretical implications, the work contributes to the extension of the literature, filling part of the gap related to threat modeling and its application in endpoints and the proposal of a monitoring system.

Keywords: Threat modeling, STRIDE, DREAD, ISO 27000.

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SIGLAS

BIOS	Sistema Integrado de Entrada e Saída.
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.
CAR	Pesquisa-Ação Canônica.
CVE	Vulnerabilidades e Exposições Comuns.
DREAD	Dano em potencial, Reprodutibilidade, Explorabilidade, Usuários Afetados e Descoberta.
DSRM	Metodologia de pesquisa em *Design Science*.
GMUD	Gestão de mudança.
ISMS	Sistemas de Gerenciamento de Segurança da Informação
ISO	Organização Internacional de Normalização.
NIST	Instituto Nacional de Padrões e Tecnologia.
SGSI	Sistema de Gestão de Segurança da Informação.
STRIDE	Falsificação, Adulteração, Repúdio, Divulgação de informações, Negação de serviço e Elevação de privilégio.
SIMPEP	Simpósio de Engenharia da Produção.
UAC	Controle de Conta de Usuários.

SUMÁRIO

1. INTRODUÇÃO

O Brasil tem 152 milhões de usuários de Internet, o que corresponde a 81% da população do país que possui 10 anos ou mais. Pela primeira vez, o levantamento identificou uma proporção maior de domicílios com acesso à rede (83%) do que indivíduos usuários (81%). Na comparação com 2019, o aumento foi de 12 e de 7 pontos percentuais, respectivamente (CETIC.BR, 2021).

De acordo com o Instituto de Pesquisa Econômica Aplicada (IPEA, 2020), 74 milhões de brasileiros estavam trabalhando no país e, dentre eles, 8,2 milhões atuavam na modalidade conhecida como *home office*. O levantamento mostrou que o número de empresas que pretendem adotar o teletrabalho no pós-pandemia deve crescer cerca de 30%. Os dados utilizados no estudo do Instituto de Pesquisa Econômica Aplicada foram coletados por meio da Pesquisa Nacional por Amostra de Domicílios Contínua (Pnad), realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE) entre maio e novembro de 2019.

Conforme estudo elaborado pela Fundação Instituto de Administração (FIA), em abril de 2020, informações coletadas de 139 pequenas, médias e grandes empresas que atuam em todo o Brasil, no período de 2019 e 2020, 41% dos funcionários das empresas foram colocados em regime de *home office*, quase todos os que teriam a possibilidade de trabalhar a distância, que somavam 46% do total dos quadros. No setor de comércio e serviços, 57,5% dos empregados passaram para o teletrabalho, nas pequenas empresas o percentual ficou em 52% (AGENCIABRASIL, 2020).

Dados são, atualmente, o commodity mais desejado na Era digital; o efeito prático decorrente deste fato é que, quanto maior o volume de dados “controlados” por determinada pessoa ou empresa, maior o poder que ela exercerá em uma economia movida a dados.(VOCESA, 2021).

De acordo com Novaes Neto (2021), a maior parte do volume de dados vazados em 2018 e 2019, está concentrado em menos de sete países, com os EUA, China, Índia e Brasil, tendo a maior representatividade para esses anos. Em 2019, o Brasil, em relação a 2018, subiu para a quinta posição, tendo um aumento de cinco vezes no número de incidentes e um aumento de seis vezes no volume de dados em 2019 (NOVAES NETO et al., 2021).

Esses golpes visam membros do público em geral, bem como milhões de indivíduos que trabalham em casa, trabalhar em casa em massa alcançou um nível de preocupações e desafios de segurança cibernética nunca enfrentados pela indústria e pelos cidadãos (LALLIE et al., 2021).

Tsohou e Holtkamp (2018) citam que, na Era atual, os usuários finais têm um papel importante na proteção da segurança da informação nas organizações. A proteção dos dados requer a implementação de uma combinação de políticas, procedimentos e tecnologia, treinamento dos funcionários da organização para agir de acordo com esses planos e, posteriormente, monitorar a conformidade (MARSHALL; STEINBART, 2018).

A segurança cibernética é um aspecto fundamental de redes, computadores, software e dados. Sem segurança suficiente, esses ativos ficarão vulneráveis a ameaças maliciosas (XIONG; LAGERSTRÖM, 2019).

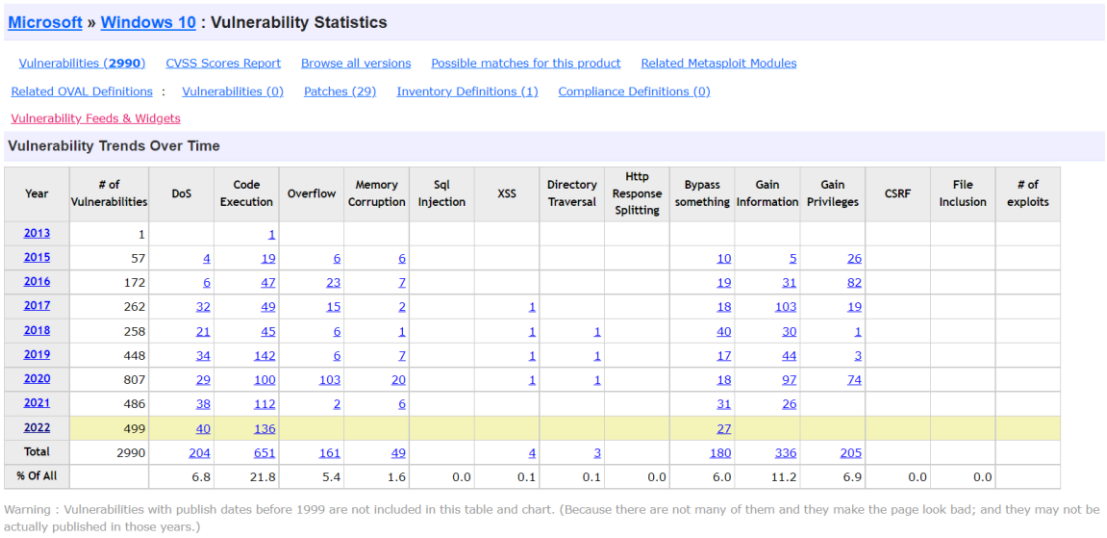
Rabii et al., (2020) sugere que, embora normas como a ISO/IEC 27002 possam fornecer as melhores práticas para ajudar as organizações a proteger seus sistemas de informação, elas não fornecem orientações sobre como as organizações podem melhorar sua segurança da informação para acompanhar esse campo em constante mudança.

Quase todos os sistemas enfrentam uma variedade de ameaças, e mais estão sendo adicionadas constantemente à medida que a tecnologia muda. Essas ameaças podem vir de fora ou de dentro das organizações, e seu impacto pode ser devastador. Os sistemas podem ser impedidos de funcionar completamente ou informações confidenciais podem vazar, o que afetaria a confiança do consumidor no provedor do sistema (SHEVCHENKO, et al., 2018).

As experiências de trabalho em casa revelaram o nível geral de despreparo dos fornecedores de software, principalmente no que diz respeito à segurança de seus produtos (LALLIE et al., 2021).

No ano de 2022, até o mês de novembro, foram constatadas 499 vulnerabilidades relacionadas ao sistema operacional Windows 10, conforme mostra Figura 1:

Figura 1: Vulnerabilidades Windows 10



Microsoft » Windows 10 : Vulnerability Statistics

Vulnerabilities (2990) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (0) Patches (29) Inventory Definitions (1) Compliance Definitions (0)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2013	1		1												
2015	57	4	19	6	6					10	5	26			
2016	172	6	47	23	7					19	31	82			
2017	262	32	49	15	2		1			18	103	19			
2018	258	21	45	6	1		1	1		40	30	1			
2019	448	34	142	6	7		1	1		17	44	3			
2020	807	29	100	103	20		1	1		18	97	74			
2021	486	38	112	2	6					31	26				
2022	499	40	136							27					
Total	2990	204	651	161	49		4	3		180	336	205			
% Of All		6.8	21.8	5.4	1.6	0.0	0.1	0.1	0.0	6.0	11.2	6.9	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Fonte: CVE (2022).

Com base nas informações apresentadas, observa-se um aumento na quantidade de pessoas e profissionais que utilizam computadores no território brasileiro, assim como o aumento na quantidade de profissionais que atuam no modelo *home office* e uma grande quantidade de ameaças existentes em Sistemas Operacionais. Uma análise mais ampla é necessária em relação as ações que podem ser feitas com foco em equipamentos utilizados por este grupo, processos que podem ser criados ou ajustados e medidas que podem ser implementadas para reduzir as ameaças e riscos existentes.

A empresa apresentada neste estudo, composta por mais de mil funcionários, onde 80 profissionais compões a equipe de tecnologia da informação, é uma empresa do ramo jurídico e a utilização e segurança dos *endpoints* é um ponto crucial devido ao conteúdo de terceiros tratados por essa empresa.

Com a tendência de novas tecnologias e utilização de computadores em ambientes externos, que não seja a rede interna da empresa, surgem também novas ameaças que precisam ser mapeadas e controladas, para evitar vazamento de informações empresariais com origem de dispositivos finais.

A empresa enfrentava dificuldade em identificar corretamente quais eram essas ameaças, quais tratativas eram necessárias para remediação e qual versão de cada software deveria ser implantada e mantida no ambiente, acarretando possíveis falhas de segurança e incompatibilidade entre seus softwares devido a possibilidade de existirem softwares

desatualizados, assim como a necessidade de um controle e cronograma para atualização, e se dispôs a participar da pesquisa.

Neste trabalho, apresenta que a utilização do método de modelagem de ameaça com as normas de segurança pode prover um melhor controle e segurança para o ambiente corporativo.

A modelagem de ameaças é proposta como solução para desenvolvimento seguro de aplicativos e avaliações de segurança do sistema. Seu objetivo é ser mais proativo e tornam mais difícil para os invasores realizarem suas intenções maliciosas (XIONG; LAGERSTRÖM, 2019).

Os métodos de modelagem de ameaças são usados para criar uma abstração do sistema; perfis de invasores em potencial, incluindo seus objetivos e métodos; e um catálogo de ameaças potenciais que podem surgir (SHEVCHENKO, et al., 2018).

A junção do método de modelagem de ameaça e normas de segurança pode agregar uma melhor proteção na segurança do ambiente; a modelagem de ameaça contribuirá com a técnica necessária para encontrar vulnerabilidades ainda não mapeadas e o modelo da norma de segurança contribuirá para uma melhor gestão e controle sob os itens encontrados.

Ao identificar, agrupar e analisar as ameaças existentes em um componente destinado ao usuário final, os gestores empresariais poderão contar: com dados que subsidiarão a tomada de decisão assertiva em relação ao risco da ameaça apresentada; mitigar riscos existentes providos de softwares de terceiros; as consequências no ambiente operacional apresentadas na implementação ou atualização de novas tecnologias; reconhecer as limitações e consequências da decisão; identificar, sob a perspectiva de segurança da informação, quais são os riscos de consideração relevante para verificação de concordância ou conflito de interesses nas gestões dos processos de TI.

Mediante pesquisa realizada para a composição do referencial teórico desta dissertação, nota-se a aplicação do método de modelagem de ameaça em outras tecnologias, mostrando redução e mitigação de ameaças após a aplicação do método.

Há a possibilidade de aplicação do método modelagem de ameaça em computadores destinados para usuários finais devido aos riscos apresentados pela adaptação ao modelo de trabalho remoto. Entre os diversos meios encontrados que apresentam a aplicabilidade, não houve demonstração relacionada ao sistema operacional utilizado pela empresa; possibilidade de conciliar o método de modelagem de ameaça com normas de segurança da informação com foco em tratamento de riscos. A utilização do método de modelagem de ameaça com normas

de segurança poderá suprir pontos solicitados em auditorias que para entender se a empresa está em *compliance* com a norma de segurança ISO 27000.

1.1. Questão da pesquisa

Esta pesquisa tem como pergunta orientadora o que segue: Como o método de modelagem de ameaça pode ser aplicado utilizando normas de gestão de risco, com o apoio de um sistema para controle e identificação de riscos de segurança e vulnerabilidades?

A partir das questões de pesquisa foram definidos os objetivos que são apresentados na sequência.

1.2. Objetivos

1.2.1. Geral

O objetivo geral deste estudo consiste em identificar, descrever e avaliar os impactos da aplicação do método modelagem de ameaça, utilizando normas de gestão de risco, em computadores empresariais com auxílio de um sistema para monitoramento.

Para atingir o objetivo principal, os seguintes objetivos específicos foram estabelecidos:

1.2.2. Específicos

- Identificar o problema e motivação por meio do levantamento bibliométrico e revisão da literatura recente e da identificação dos problemas;
- Desenvolver um estudo empírico, visando a melhoria de segurança nos processos utilizando o método de modelagem de ameaça STRIDE e DREAD utilizando as normas ISO/IEC 27000 e NIST 800;
- Elaborar uma abordagem sistemática para controle e identificação das ameaças, riscos e vulnerabilidades encontradas;
- Apresentar um sistema para auxílio no controle e gestão dos resultados;
- Comunicar os resultados da pesquisa.

1.3. Linha de pesquisa

Este trabalho desenvolvido no Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos do pertence à Linha de Pesquisa de Sistemas de Informação e Tecnologias Digitais e ao Projeto de Pesquisa Gestão de Tecnologia e Sistemas de Informação e explorou os temas da tecnologia da informação e segurança da informação.

Os sistemas produtivos e a engenharia de produção tratam de projetos, aperfeiçoamento e implantação de sistemas integrados de pessoas, materiais, informações, equipamentos e energia, para a produção de bens e serviços. Dentro dessa abordagem cabem não apenas os setores produtivos tradicionais, mas também outras atividades como ONGs, redes de empresas, interfaces colaborativas, e as entidades governamentais. (DE JESUS; COSTA, 2014).

Empresas, como os demais órgãos públicos, são orientados ao cumprimento de metas, melhorias de processos, orientação a resultados entre outros. Desse modo, se observa uma interface e associação aos preceitos dos sistemas produtivos aos serviços empresariais.

1.4. Contribuições

Do ponto de vista da gestão e da tecnologia em sistemas produtivos, a pesquisa contribui para a melhoria dos processos existentes relacionados à segurança da informação e operações. Pretende-se com este trabalho, contribuir para que as organizações possam agregar o método de modelagem de ameaça em seus processos cotidianos, e com isso, trazer outros subsídios para o aprofundamento desta temática, assim como a organização na implementação e utilização de a utilização do artefato para atualização de programas.

Sob a perspectiva acadêmica, esta pesquisa colabora com a discussão a respeito da utilização do método de modelagem de ameaça dentro do escopo do usuário final, possibilitando a abertura de novas oportunidades de pesquisa envolvendo contextos específicos descritos neste trabalho. Por meio de um experimento prático, esse estudo contribui com a disseminação do método DSRM em conjunto com o Princípio do Modelo de Processo Cíclico da Pesquisa-ação Canônica e a literatura de modelagem de ameaça, mostrando como a aplicação do método pode melhorar a segurança digital com foco no usuário final. Subsidiar o direcionamento de futuras pesquisas para diminuir as lacunas que porventura possam surgir; oportunizar o desenvolvimento de sistemas e métodos para facilitar o processo de modelagem de ameaça; oportunizar maior utilização do método modelagem de ameaça por outros profissionais e áreas.

1.5. Estrutura da dissertação

Este capítulo apresentou a motivação, a justificativa, a questão de pesquisa, os objetivos, e a estrutura do trabalho de forma resumida. Os próximos capítulos deste trabalho estão organizados da seguinte forma:

O capítulo 2 apresenta a fundamentação teórica que é composta pelos conceitos e definições utilizadas neste trabalho e as principais normas aplicadas à gestão de risco, modelagem de ameaça;

O capítulo 3 apresenta o método utilizado na pesquisa;

O capítulo 4 apresenta a aplicação dos passos do método a análise dos dados obtidos;

E finalmente no capítulo 5 são apresentadas as considerações finais e as oportunidades de continuidade do trabalho e novas pesquisas.

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo encontra-se o referencial teórico nos temas de relevância para este trabalho. O referencial teórico permite verificar o estado do problema a ser pesquisado, sob o aspecto teórico e de outros estudos e pesquisas já realizados (Marconi; Lakatos, 2003).

Neste capítulo são apresentados conceitos sobre gestão de risco e modelagem de ameaça, conceitos necessários para o entendimento deste trabalho.

2.1. Levantamento da literatura sobre modelagem de ameaça

A busca pela fundamentação teórica foi dividida em três, com finalidade de contemplar a identificação do método de modelagem de ameaça, qual o método de modelagem de ameaça mais utilizado na literatura e verificar modelos existentes que utilizem normas e possam sustentar a finalidade deste trabalho. A modo como as buscas foram realizadas podem ser conferidos nos apêndices A, B e C.

Resultado da pesquisa bibliométrica:

Com base nas 3 buscas e 61 artigos encontrados, foi verificado que 3 artigos apareceram mais de uma vez no resultado, quando feito a convergência das três buscas, totalizando 58 artigos relevantes sobre o tema modelagem de ameaças. Os artigos encontram-se listados no Apêndice D.

A meta language for threat modeling and attack simulations (JOHNSON; LAGERSTRÖM; EKSTEDT, 2018) apresenta ataque de Metalinguagem (MAL), que pode ser usada para projetar linguagens de ataque específicas de domínio. O MAL fornece um formalismo que permite a geração semiautomática, bem como o cálculo eficiente de gráficos de ataque grandes. O MAL permite que especialistas em segurança codifiquem o conhecimento específico do domínio para permitir simulações de ataques a sistemas no domínio de interesse. As linguagens de modelagem de ataque específicas de domínio assim geradas podem ser posteriormente usadas e reutilizadas por pessoas com menos experiência em segurança, a fim de avaliar automaticamente a segurança de sistemas específicos dentro do domínio.

No artigo *An agent-based approach to modeling insider threat*, (SOKOLOWSKI; BANKS; DOVER, 2016) apresentam uma nova modelagem de ameaça comportamental levando em consideração o potencial de uma ameaça interna ser desenvolvida em uma organização devido alguns atributos de sua cultura. O modelo considera todos os funcionários da organização e sua probabilidade de se tornarem uma ameaça interna.

Improving information security risk analysis by including threat-occurrence predictive models (FIGUEIRA; BRAVO; LÓPEZ, 2019) propõe um modelo preditivo alternativo para metodologias de análise de risco, particularmente para Magerit, uma adaptação espanhola da ISO/IEC 27005. A proposta é baseada em um cálculo de risco de modificação, substituindo as frequências de ameaças passadas (históricas) por probabilidades de ameaças futuras, levando em consideração as vulnerabilidades atuais do sistema.

No artigo *Machine Learning Models for Secure Data Analytics: A taxonomy and Threat*, Gupta et al. (2020), exploraram modelos e técnicas baseadas em aprendizado de máquina (ML) e aprendizado profundo (DL) que são capazes de identificar e mitigar ataques conhecidos e desconhecidos. Neste artigo, forneceram conhecimentos aos leitores sobre o uso de modelos de ML para proteger dados para análises futuras. Futuramente, os ataques em tempo real aos modelos de ML podem ser explorados com mais detalhes.

Modeling And Analysis Of Identity Threat Behaviors Through Text Mining Of Identity Theft Stories (ZAEEM et al., 2017) Possui o objetivo de analisar os dados de roubo de identidade, esta pesquisa propõe uma abordagem que envolve a coleção inédita de notícias online e reportagens sobre o tema roubo de identidade. Utilizando técnicas de mineração de texto, este artigo apresenta uma análise estatística de padrões de comportamento e recursos usados por ladrões e fraudadores para cometer roubo de identidade, incluindo os atributos de identidade comumente vinculados a crimes de identidade, recursos que os ladrões empregam para conduzir crimes de identidade e padrões temporais de comportamento criminoso. O algoritmo de Avaliação e Predição de Ameaças de Identidade (ITAP) proposto no artigo foi projetado de maneira linear, em que cada etapa pode ser realizada separadamente e integrada para construir todo o mecanismo analítico.

JOHNSON et al., (2016), no artigo pwnpr3d: *an attack-graph-driven probabilistic threat-modeling approach*, apresentam uma abordagem probabilística de modelagem de ameaças para geração automática de gráficos de ataque baseado em modelagem de rede. O objetivo é fornecer às partes interessadas em organizações com uma abordagem holística que fornece visão geral de alto nível e detalhes técnicos. PwnPr3d permite automaticamente identificar e quantificar um amplo conjunto de ameaças, cobrindo a maior parte da classificação STRIDE. Como resultado principal, pwnpr3d identifica e quantifica automaticamente um amplo conjunto de ameaças como: falsificação de identidade, adulteração de dados, divulgação de informações, negação de serviço e escalonamento de privilégios.

Software and attack centric integrated threat modeling for quantitative risk assessment, (POTTEIGER; MARTINS; KOUTSOUKOS, 2016) apresenta uma abordagem quantitativa e

integrada em modelagem de ameaça que combina abordagem centralizadas em software e em técnicas de ataque. Integrando a ameaça centrada no software e a ameaça centrada no ataque, especialistas em segurança são capazes de analisar risco de vulnerabilidade, bem como caminhos específicos que podem ser comprometidos. Atribuindo um valor de risco a cada atributo em um componente de arvore de ataque, torna-se possível uma análise quantitativa padronizada de um componente de sistema.

STRIDE-based threat modeling for cyber-physical systems (KHAN et al., 2017) apresenta uma estrutura de modelagem de ameaças abrangente para CPS usando STRIDE, uma abordagem sistemática para garantir a segurança do sistema no nível do componente, concebe uma metodologia viável e eficaz para aplicar STRIDE e, em seguida, a demonstra em testes de laboratório baseado em ambientes reais. O artigo identificou o STRIDE como uma abordagem eficaz para garantir a segurança do sistema no nível do componente ao identificar vulnerabilidades em nível de componente e suas possíveis consequências físicas, o STRIDE pode lidar com esses desafios de maneira eficaz.

The battle for new york: a case study of applied digital threat modeling at the enterprise level (STEVENS et al., 2018), neste estudo de caso, os autores apresentam uma nova modelagem de ameaças, o Centro de gravidade (CoG) ao New York CityCyber Command: a principal organização de defesa digital da cidade mais populosa dos Estados Unidos. Descobriu-se que a modelagem de ameaças melhorou a autoeficácia; 20 de 25 participantes o incorporaram regularmente em suas tarefas diárias 30 dias após o treinamento, sem aviso prévio. Após 120 dias, as estratégias de mitigação de ameaças projetadas pelo participante forneceram benefícios de segurança tangíveis para NYC, incluindo o bloqueio de 541 tentativas de intrusão exclusivas, evitando o sequestro de cinco contas de usuário com privilégios e abordando três vulnerabilidades de servidor voltadas para o público. No geral, esses resultados sugerem que a introdução da modelagem de ameaças pode fornecer benefícios valiosos em um ambiente corporativo.

Threat modeling – A systematic literature review (XIONG; LAGERSTRÖM, 2019) apresenta uma revisão da modelagem de ameaças com base em consultas sistemáticas em quatro bancos de dados científicos: IEEE Xplore, Scopus, Springer link e Web of Science. Evidenciando os métodos encontrados: STRIDE, árvore de ataque, DREAD entre outros, classificando as modelagens de ameaças encontradas entre automática, manual, formal e gráfica. Como trabalho futuro, os autores propõem um método de modelagem automática de ameaças, baseado na *Meta Attack Language* (MAL), validá-lo em estudo de caso com testes de laboratórios em ambientes baseados em mundo real.

Threat modeling for mobile health systems (CAGNAZZO et al.,2018) enfoca os desafios de segurança e oferece uma solução de mitigação, especialmente com foco na autenticação e criptografia para dispositivos com recursos limitados. Ele identifica ativos em um protótipo de ecossistema *mHealth* e classifica ameaças com a metodologia STRIDE. Além disso, o documento identifica os níveis de risco associados usando DREAD e descreve possíveis estratégias de mitigação para fornecer um ambiente razoável e confiável. Pesquisas futuras validarão a abordagem por meio da implementação em um cenário do mundo real, para obter mais insights. Outro desafio no ecossistema *mHealth* é como os dispositivos de substituição, ou dispositivos que têm uma grande flutuação, são tratados.

Observando que existe adoção pela academia em relação a utilização do método de modelagem de ameaça e uma grande variedade disponível que são considerados métodos para aplicação de modelagem de ameaça. Foi possível confirmar que a adoção do método trará beneficios para a segurança da informação e STRIDE é o método mais utilizado, nos últimos 5 anos, para aplicação de modelagem de ameaça. Foi possível identificar que poucos artigos utilizam normas de segurança para complementar a aplicação de modelagem de ameaça, apesar de ambos tratarem assuntos relacionados aos perigos apresentados em segurança da informação.

Com base nas buscas realizadas e resultados encontrados, verifica-se que a modelagem de ameaça é proposta para aplicação em diversas tecnologias, como exemplo: sistemas de saúde, sistemas ciberfísicos e aprendizado de máquinas, mas nenhum dos artigos analisados apresentou o mesmo proposito deste trabalho, com o foco em *endpoints*, embora os assuntos sejam correlacionados.

2.2. Gestão de risco

Gestão de risco cibernético é o processo de identificação, análise, avaliação e abordagem das ameaças à segurança cibernética de uma organização. Uma abordagem sistemática de gestão de riscos de segurança da informação é necessária para se identificar as necessidades da organização em relação aos requisitos de segurança da informação e para criar um SGSI que seja eficaz (ISO 27005, 2019).

O sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados. (ISO 27001, 2013).

Em uma visão geral, a cibersegurança é constituída por três princípios fundamentais: confidencialidade, integridade e disponibilidade (ISO 27001, 2013) que podem ser definidos como:

- Confidencialidade: visa garantir que a informação não seja acessível a indivíduos, entidades ou processos não autorizados. A confidencialidade deve ser preservada para cada unidade de dados e deve ser mantida enquanto os dados estão armazenados em um sistema, quando são transmitidos e quando chegam ao seu destinatário.
- Integridade: refere-se em consistência do estado da informação. Toda e qualquer modificação não autorizada dos dados, seja ela intencional ou não, é considerada uma violação deste princípio.
- Disponibilidade: visa garantir que a informação esteja disponível para uso legitimo quando necessário, para os usuários com acessos autorizados.

As avaliações de risco são usadas para identificar, estimar e priorizar o risco para as operações organizacionais, ativos organizacionais, indivíduos, outras organizações e a Nação, resultantes da operação e uso de sistemas de informação (NIST, 2012).

De acordo com a ISO/IEC 27005, a análise de riscos pode ser empreendida com diferentes graus de detalhamento, dependendo da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores envolvendo a organização. Convém que a forma da análise seja coerente com o critério de avaliação de riscos desenvolvido como parte da definição do contexto.

2.2.1. ISO/IEC 27000

Os padrões de *International Organizatin for Standardization*, ou Organização Internacional para Padronização, são mais conhecidos como ISO. São regras que servem para normatizar as condutas e processos em organizações e entidades públicas, em diferentes segmentos do mercado. O principal objetivo é criar uma referência qualitativa para que os consumidores tenham o mínimo requerido para que cada grupo ofereça seus produtos ou serviços (CANALTECH, 2022).

As normas da série ISO 27000 fornecem as diretrizes para práticas de gestão da segurança da informação para as organizações conhecidas como SGSI – Sistema de Gestão da Segurança da Informação, são normas definidas internacionalmente, já com bastante maturidade, pois têm sido constantemente renovadas a cada 5 anos e sua origem data de 1995, através da BS7799. (HSBS, 2022).

O conjunto que começa no ISO 27000 trata especificamente da Gestão de Segurança da Informação (CANALTECH, 2022). A norma ISO/IEC 27001 especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação no contexto da organização (ISO 27001, 2013).

A ISO/IEC 27002 é o padrão ISO/IEC 17799 renomeado e é um código de prática para segurança da informação, fornece diretrizes para padrões de segurança da informação organizacional e práticas de gerenciamento de segurança da informação, incluindo a seleção, implementação e gerenciamento de controles levando em consideração o(s) ambiente(s) de risco de segurança da informação da organização. (ISO 27002, 2013). Basicamente, descreve centenas de controles potenciais e mecanismos de controle que podem ser implementados, sujeitos às orientações fornecidas na ISO/IEC 27001.

ISO/IEC 27005 é o nome do padrão da série 27000 que abrange o gerenciamento de riscos de segurança da informação, o padrão oferece diretrizes para riscos de segurança da informação em uma organização, suportando especificamente os requisitos de um ISMS definido pela ISO/IEC 27001 (ISO 27005, 2019).

2.2.1.1. ISO/IEC 27002

A ISO 27002 define uma estrutura de segurança abrangente que consiste em 133 controles específicos organizados em torno de 39 objetivos de controle, esta estrutura equilibrada serve como base tanto para medir a eficácia da organização em lidar com riscos quanto para estruturar um programa de segurança geral da organização. (GOSSEL; MACKEY, 2007).

ISO/IEC 27002 indica alguns controles importantes para este trabalho, que serão utilizados posteriormente, são eles:

1. Controle de acesso

O propósito deste controle é limitar o acesso à informação e aos recursos de processamento da informação. É apropriado que, onde for aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações sejam controlados por um procedimento seguro de entrada no sistema (*log-on*).

2. Restrição sobre o uso e instalação de software

Recomenda-se que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelos usuários.

3. Transferência de informações

Convém que políticas, procedimentos e controles de transferências formais, sejam determinados para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação disponíveis.

4. Dispositivos móveis e trabalho remoto

O objetivo deste controle é garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis. Convém que quando se utilizam dispositivos móveis, cuidados especiais sejam tomados para assegurar que as informações do negócio não sejam comprometidas. Recomenda-se que a política de dispositivos móveis leve em consideração os riscos de se trabalhar com esses dispositivos móveis em ambientes desprotegidos.

5. Backup

É conveniente que cópias de segurança das informações, softwares e das imagens do sistema, sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida pela empresa.

6. Proteção contra códigos maliciosos

A intenção deste controle é garantir que as informações e os recursos de processamento da informação estão protegidos contra códigos maliciosos. É apropriado que sejam implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, em conjunto com um adequado programa de conscientização do usuário

7. Gerenciamento de vulnerabilidades técnicas

Recomenda-se que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso sejam obtidas em tempo hábil, a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas necessárias para lidar com os riscos relacionados.

8. Controles criptográficos

Esse controle visa assegurar o uso adequado e efetivo da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

9. Segurança nas comunicações

É conveniente que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.

2.2.1.2. ISO/IEC 27005

ISO 27005 é uma norma de risco de segurança da informação bem conhecida, as tarefas na ISO27005 incluem a identificação, avaliação e priorização de riscos (AGRAWAL, 2017).

As fases de avaliação de risco consistem em definição de contexto, identificação de risco, análise de risco, avaliação de risco e gerenciamento de risco (REFSDAL et al., 2015).

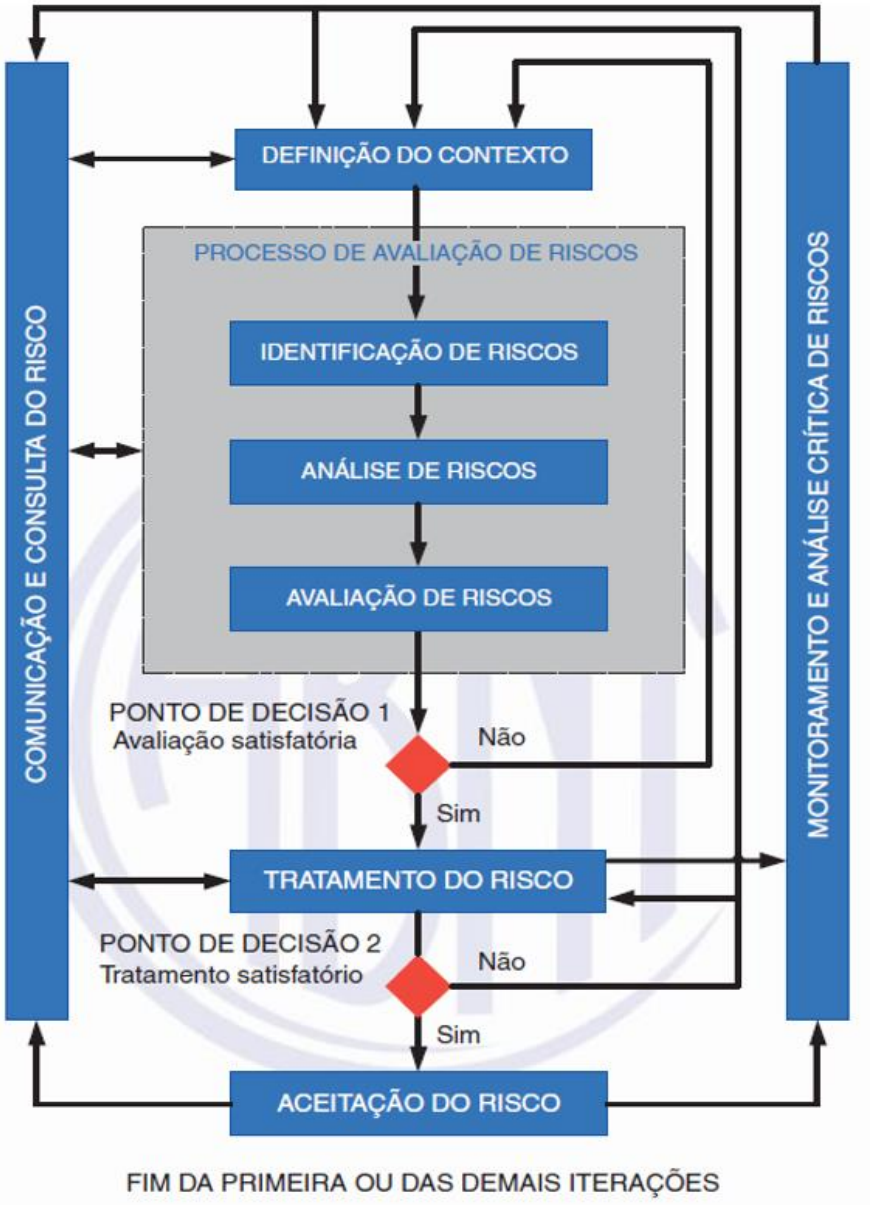
Conforme a ISO/IEC 27005 (2019), convém que o processo defina os contextos interno e externo, avalie os riscos e trate os riscos usando um plano de tratamento a fim de implementar as recomendações e decisões. Convém que a gestão de riscos analise os possíveis acontecimentos e suas consequências, antes de decidir o que será feito e quando será feito, a fim de reduzir os riscos a um nível aceitável.

Recomenda-se que a gestão de riscos de segurança da informação contribua para:

- A identificação de riscos;
- O processo de avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência;
- A comunicação e entendimento da probabilidade e das consequências destes riscos;
- A priorização das ações para reduzir a ocorrência dos riscos;
- O envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e para que elas sejam mantidas informadas sobre a situação da gestão de riscos;
- A eficácia do monitoramento do tratamento dos riscos;
- O monitoramento e análise crítica periódica dos riscos e do processo de gestão de riscos;
- A coleta de informações de forma a melhorar a abordagem da gestão de riscos;
- O treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los.

O processo de gestão de riscos de segurança da informação pode ser aplicado à organização como um todo, a uma área específica da organização (por exemplo, um departamento, um local físico, um serviço), a qualquer sistema de informações, a controles já existentes, planejados ou apenas a aspectos particulares de um controle (ISO 27005, 2019).

Figura 2: Gestão de Risco conforme ISO/IEC 27005:2019



Fonte: ISO/IEC 27005:2019.

Como mostra a Figura 2, o processo de gestão de riscos de segurança da informação pode ser iterativo para o processo de avaliação de riscos e para as atividades de tratamento do risco.

Primeiramente, o contexto é estabelecido. Em seguida, executa-se um processo de avaliação de riscos. Se fornecer informações suficientes para que se determinem de forma eficaz as ações necessárias para reduzir os riscos a um nível aceitável, então a tarefa está completa e o tratamento do risco pode continuar. Por outro lado, se as informações forem insuficientes, executa-se uma outra iteração do processo de avaliação de riscos, revisando-se o contexto (por

exemplo, os critérios de avaliação de riscos, de aceitação do risco ou de impacto), possivelmente em partes limitadas do escopo (ISO 27005, 2019).

O tratamento de riscos envolve um processo cíclico para:

- Avaliar um tratamento do risco;
- Decidir se os níveis de risco residual são aceitáveis;
- Gerar um novo tratamento do risco se os níveis de risco não forem aceitáveis; e
- Avaliar a eficácia do tratamento.

A ISO/IEC 27001 (2013) especifica que os controles implementados no escopo, limites e contexto do SGSI devem ser baseados no risco. A aplicação de um processo de gestão de riscos de segurança da informação pode satisfazer esse requisito.

1. Abordagem da gestão de riscos

Conforme a ISO/IEC 27005 (2019) convém que um método de gestão de riscos apropriado seja selecionado ou desenvolvido e leve em conta critérios como: avaliação de riscos, impacto e aceitação do risco. Além disso, convém que a organização avalie se os recursos necessários estão disponíveis para:

- Executar o processo de avaliação de riscos e estabelecer um plano de tratamento de riscos;
- Definir e implementar políticas e procedimentos, incluindo implementação dos controles selecionados;
- Monitorar controles;
- Monitorar o processo de gestão de riscos de segurança da informação.

2. Critérios para a avaliação de riscos

De acordo com a ISO/IEC 27005 (2019) convém que os critérios para a avaliação de riscos sejam desenvolvidos para avaliar os riscos de segurança da informação na organização, considerando os seguintes itens:

- O valor estratégico do processo que trata as informações de negócio;
- A criticidade dos ativos de informação envolvidos;
- Requisitos legais e regulatórios, bem como as obrigações contratuais;

- Importância, do ponto de vista operacional e dos negócios, da disponibilidade, da confidencialidade e da integridade;
- Expectativas e percepções das partes interessadas e consequências negativas para o valor de mercado (em especial, no que se refere aos fatores intangíveis desse valor), a imagem e a reputação.

Além disso, critérios para avaliação de riscos podem ser usados para especificar as prioridades para o tratamento do risco.

3. Ativo

Segundo a ISO/IEC 27005 (2019) Um ativo é algo que tem valor para a organização e que, portanto, requer proteção. Para a identificação dos ativos convém que se tenha em mente que um sistema de informação compreende mais do que hardware e software.

Convém que a identificação dos ativos seja executada com um detalhamento adequado que forneça informações suficientes para o processo de avaliação de riscos. O nível de detalhe usado na identificação dos ativos influenciará a quantidade geral de informações reunidas durante o processo de avaliação de riscos. O detalhamento pode ser aprofundado em cada iteração do processo de avaliação de riscos.

O limite da análise crítica é o perímetro dos ativos da organização a serem considerados pelo processo de gestão de riscos de segurança da informação.

4. Riscos

O propósito da identificação de riscos é determinar eventos que possam causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer. As etapas descritas nas próximas subseções servem para coletar dados de entrada para a atividade de análise de riscos. Convém que a identificação de riscos inclua os riscos cujas fontes estejam ou não sob controle da organização, mesmo que a fonte ou a causa dos riscos não seja evidente (ISO 27005, 2019).

5. Ameaças de segurança

Conforme a ISO/IEC 27005 (2019), uma ameaça tem o potencial de comprometer ativos (como informações, processos e sistemas) e, por isso, também as organizações. Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais. Convém que tanto as

fontes das ameaças acidentais quanto as das intencionais, sejam identificadas.

Uma ameaça pode surgir de dentro ou de fora da organização. Convém que as ameaças sejam identificadas genericamente e por classe (por exemplo, ações não autorizadas, danos físicos, falhas técnicas) e, quando apropriado, que ameaças específicas sejam identificadas dentro das classes genéricas. Isso significa que nenhuma ameaça é ignorada, incluindo as não previstas, mas que o volume de trabalho exigido é limitado.

Algumas ameaças podem afetar mais de um ativo. Nesses casos, elas podem provocar impactos diferentes dependendo de quais ativos são afetados. Aspectos culturais e relacionados ao ambiente precisam ser considerados quando se examinam as ameaças.

Convém que experiências internas de incidentes e avaliações anteriores das ameaças sejam consideradas na avaliação atual. Pode ser útil a consulta a outros catálogos de ameaças (talvez mais específicos a uma organização ou negócio) a fim de completar a lista de ameaças genéricas, quando relevante.

Quando forem usados catálogos de ameaças ou os resultados de uma avaliação anterior das ameaças, convém que se tenha consciência de que as ameaças relevantes estão sempre mudando, especialmente se o ambiente de negócio ou se os sistemas de informações mudarem.

6. Vulnerabilidades

De acordo com a ISO/IEC 27005 (2019), vulnerabilidades podem ser identificadas nas seguintes áreas:

- Organização;
- Processos e procedimentos;
- Rotinas de gestão;
- Recursos humanos;
- Ambiente físico;
- Configuração do sistema de informação;
- Hardware, software ou equipamentos de comunicação;
- Dependência de entidades externas.

A presença de uma vulnerabilidade não causa prejuízo por si só, pois precisa haver uma ameaça presente para explorá-la. Uma vulnerabilidade que não tem uma ameaça correspondente

pode não requerer a implementação de um controle no presente momento, mas convém que ela seja reconhecida como tal e monitorada, no caso de haver mudanças.

Convém notar que um controle implementado incorretamente, com mau funcionamento ou sendo usado de forma errada pode, por si só, representar uma vulnerabilidade. Um controle pode ser eficaz ou não, dependendo do ambiente no qual ele opera. Inversamente, uma ameaça que não tenha uma vulnerabilidade correspondente pode não resultar em um risco.

Vulnerabilidades podem estar ligadas a propriedades do ativo, as quais podem ser usadas de uma forma ou para um propósito diferente daquele para o qual o ativo foi adquirido ou desenvolvido. Vulnerabilidades decorrentes de diferentes fontes precisam ser consideradas, por exemplo, as intrínsecas e as extrínsecas ao ativo.

2.2.2. NIST 800-30 Avaliação de Risco

O objetivo do NIST 800-30 é fornecer orientação para a realização de avaliações de risco de sistemas e organizações de informações federais. fornece orientação para as organizações na identificação de fatores de risco específicos. A avaliação de riscos é um componente chave de um processo holístico de gerenciamento de riscos em toda a organização. A NIST 800-30 fornece diretrizes similares as diretrizes fornecidas pela noma ISO/IEC 27000 para o tratamento de risco.

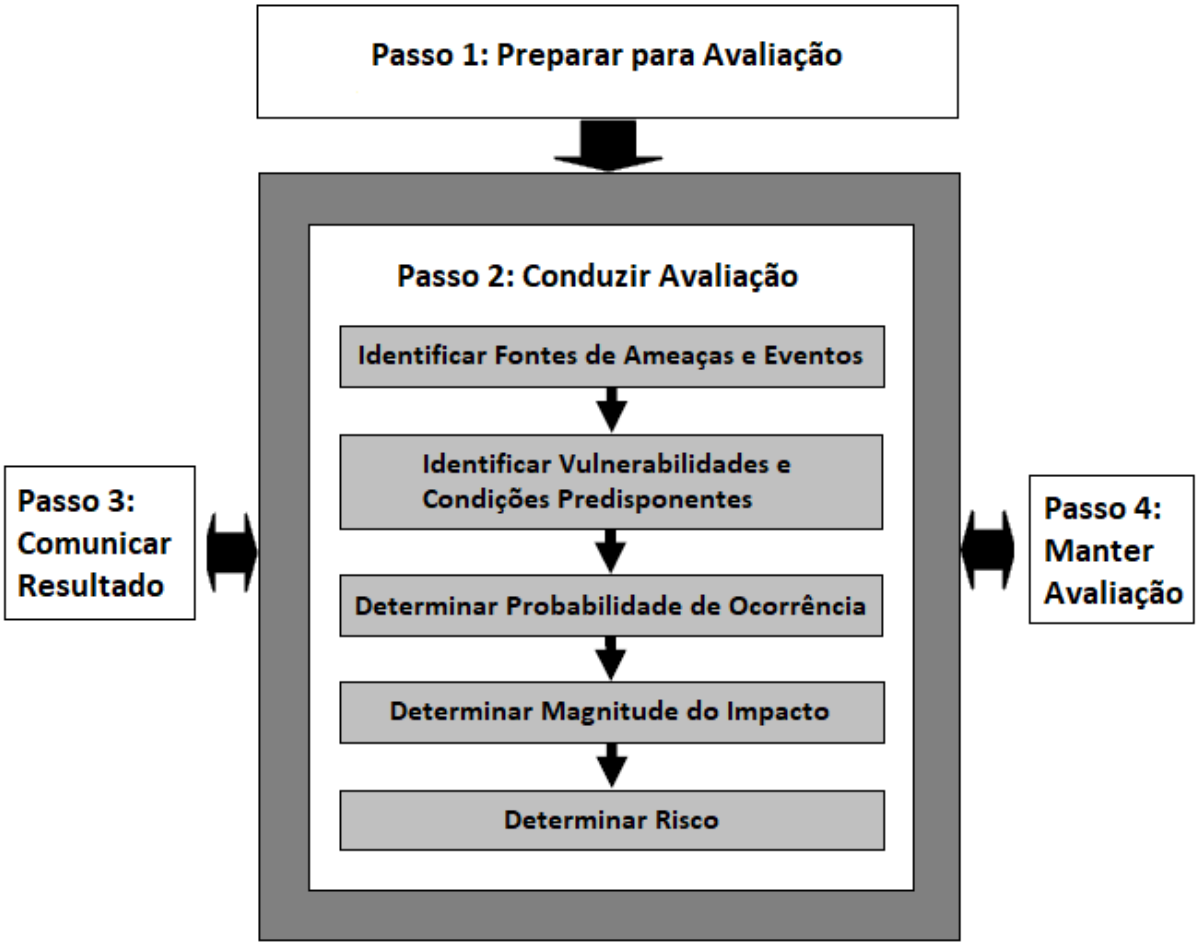
NIST SP 800-30 pode ser usada como um complemento ao processo de avaliação de risco e pode ser aplicada ao framework de risco da ISO 27005 (AL FIKRI, 2019).

O processo de avaliação de risco é composto por quatro etapas:

1. Preparação para a avaliação;
2. Realizar a avaliação;
3. Comunicar os resultados da avaliação;
4. Manter a avaliação.

Cada etapa é dividida em um conjunto de tarefas. Para cada tarefa, a orientação suplementar fornece informações adicionais para organizações que realizam avaliações de risco, a Figura 3 ilustra as etapas básicas do processo de avaliação de risco e destaca as tarefas específicas para conduzir a avaliação:

Figura 3: Processo de Avaliação de Risco



Fonte: Adaptado de NIST 800-30.

São consideradas para este trabalho, eventos de ameaças evidenciadas pela NIST 800-30 e artigos relacionados que apresentam convergência para maior abrangência nos resultados, para o método é utilizado a base existente na norma ISO/IEC 27000.

2.3. Modelagem de ameaça

Modelagem de ameaças pode ser definido como um processo estratégico destinado a considerar possíveis cenários de ataque e vulnerabilidades em um ambiente de aplicativo proposto ou existente com o objetivo de identificar claramente os níveis de risco e impacto (UCEDAVÉLEZ; MORANA, 2015).

Bons modelos de ameaças podem auxiliar na verificação da necessidade de alguns requisitos, por exemplo, o sistema precisa estar seguro contra alguém que possua acesso físico ao dispositivo? A Apple disse sim para o iPhone, que é diferente do mundo tradicional do PC. À medida que ameaças são encontradas e faz-se a triagem para decidir o que fazer com elas, os requisitos são esclarecidos. Com requisitos mais claros, é possível dedicar energia a um conjunto consistente de recursos e propriedades de segurança (SHOSTACK, 2014).

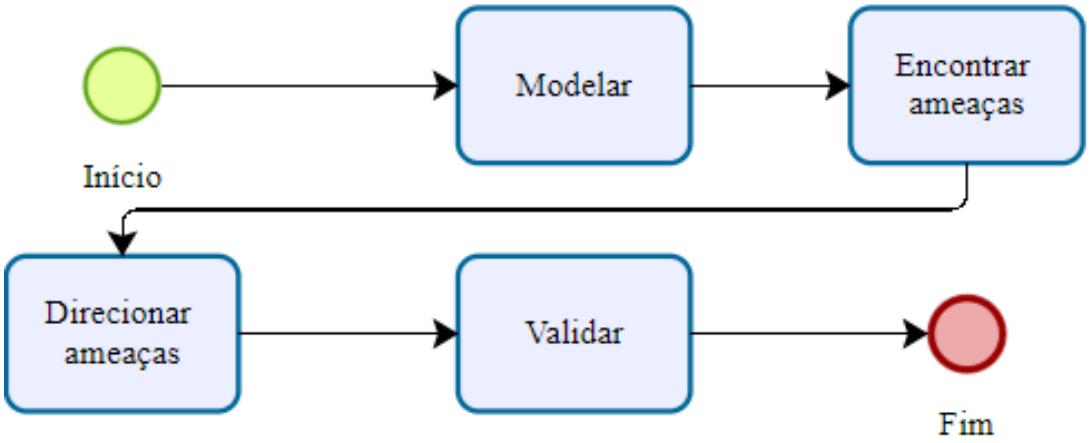
Há uma interação importante entre requisitos, ameaças e mitigações. Ao utilizar modelagem de ameaças, é possível verificar que algumas ameaças não se alinham com os requisitos do negócio e, como tal, podem não valer a pena serem abordadas. Com outras ameaças, resolvê-las seria muito complexo ou caro. Será necessário fazer uma ligação entre abordá-las parcialmente ou aceitando (e comunicando) que essas ameaças não serão tratadas (SHOSTACK, 2014).

A modelagem de ameaças visa revitalizar bastante o esforço de proteção de dados por meio de um processo estratégico e colaborativo (UCEDAVÉLEZ; MORANA, 2015).

Um bom modelo ajuda a lidar com classes ou grupos de ataques, em suma, a modelagem de ameaças é o uso de abstrações para ajudar a pensar sobre os riscos (SHOSTACK, 2014).

O Ciclo de modelagem de ameaça é mostrado na Figura 4:

Figura 4: Ciclo de modelagem de ameaça



Fonte: Adaptado de Shostack. (2014).

Modelagem de ameaça permite que ameaças específicas para o negócio sejam mapeadas no ambiente, analisando funções nativas do aplicativo que possam ser vistas como ameaças e tratadas para que essas funções não estejam disponíveis no momento da implantação ou mitigada no ambiente de produção.

2.3.1. STRIDE

O acrônico STRIDE é atualmente o método de modelagem de ameaças mais maduro entre os outros métodos existentes, desenvolvido por Loren Kohnfelder e Praerit Garg em 1999 e adotado pela Microsoft em 2002. Este método evoluiu ao longo do tempo para incluir novas tabelas específicas de ameaças e as variantes STRIDE por Elemento e STRIDE por Interação (SHEVCHENKO, 2018).

STRIDE por elemento é mais complexo, pois analisa o comportamento e as operações de cada componente do sistema. STRIDE por interação, enumera ameaças contra interações do sistema considerando origem, destino e interação. A Microsoft utiliza no treinamento de seu Ciclo de Vida de Desenvolvimento de Segurança de modelagem de ameaças, os seguintes elementos: entidade externa, processos, fluxo de dados e armazenamento de dados (SHOSTACK, 2014).

O STRIDE por elemento torna o STRIDE mais prescritivo ao observar que certas ameaças são mais prevalentes com certos elementos de um diagrama, por exemplo, é improvável que um armazenamento de dados falsifique outro armazenamento de dados, ao se concentrar em um conjunto de ameaças contra cada elemento, essa abordagem facilita a localização de ameaças (SHOSTACK, 2014).

Cada elemento é a vítima, não o perpetrador. Portanto, se houver adulteração em um armazenamento de dados, a ameaça é para o armazenamento de dados e os dados nele contidos. Se houver falsificação de uma forma que afeta um processo, então o processo é a vítima, independentemente dos detalhes técnicos. O *STRIDE-per-element* tem a vantagem de ser prescritivo, ajudando você a identificar o que procurar. Quando utilizado por especialistas, ele pode encontrar novos tipos de pontos fracos em componentes. Em mãos menos habilidosas, ainda pode encontrar muitos problemas comuns (SHOSTACK, 2014).

De acordo com Shostack (2014) STRIDE é um mnemônico para coisas que dão errado na segurança, significando: *Spoofing* (Falsificação), *Tampering* (Adulteração), *Repudiation* (Repúdio), *Information Disclosure* (Divulgação de informações), *Denial of Service* (Negação de serviço) e *Elevation of Privilege* (Elevação de privilégio). Cada letra que compõe o nome STRIDE é uma categoria. A definição de cada categoria, em português, é explicada na sequência:

- S: Falsificação é fingir ser algo ou alguém que você não é;
- T: Adulterar é modificar algo que você não deve modificar. Pode incluir pacotes na rede (com ou sem fio), bits no disco ou bits na memória;
- R: Repúdio significa alegar que você não fez algo (independentemente se você fez ou não);
- I: Divulgação de informações é sobre a exposição de informações a pessoas não autorizadas;

- D: Negação de serviço são ataques projetados para impedir que um sistema forneça serviço, inclusive travando-o, tornando-o excessivamente lento ou preenchendo todo o seu armazenamento;
- E: Elevação de privilégio é quando um programa ou usuário é tecnicamente capaz de fazer coisas que eles não deveriam fazer.

STRIDE analisa vulnerabilidades contra cada componente do sistema que pode ser explorado por um invasor para comprometer todo o sistema (KHAN et al., 2017).

Com base nas 6 classificações do STRIDE, é possível então classificar as ameaças, inserindo cada ameaça encontrada em sua devida classificação no STRIDE.

Após a classificação das ameaças, se faz necessário avaliar o tratamento para cada ameaça encontrada, escolhendo se a ameaça será mitigada, se a responsabilidade será transferida ou se o risco será aceito. A opção de mitigar a ameaça é sempre a mais favorável, as outras opções devem ser consideradas apenas caso haja tolerância ao risco.

SCANDARIATO et al. (2015) em seu estudo descritivo da técnica de modelagem de ameaças da Microsoft, mostram que o método STRIDE tem uma taxa moderadamente baixa de falsos positivos e uma taxa moderadamente alta de falsos negativos. STRIDE foi aplicado com sucesso a sistemas cibernéticos e ciberfísicos (SHEVCHENKO, 2018).

STRIDE está entre os métodos de modelagem de ameaça mais maduros da atualidade. Este método foi escolhido para este trabalho, como o método principal de modelagem de ameaça, devido a sua ampla utilização no universo acadêmico.

2.3.2. DREAD

O acrônimo DREAD significa *Damage Potencial* (Dano em potencial), *Reproducibility* (Reprodutibilidade), *Exploitability* (Explorabilidade), *Affected Users* (Usuários Afetados) e *Discovery* (Descoberta) (BODEAU; MCCOLLUM; FOX, 2018).

O DREAD pode ser aproveitado para avaliar e classificar a gravidade das ameaças. As metodologias DREAD e STRIDE podem ser usadas em conjunto para avaliações abrangentes de segurança cibernética e ciclo de vida de serviços (ZOGRAFOPOULOS, et al., 2021).

O DREAD fornece um esquema pelo qual os vetores de ameaças identificados usando STRIDE ou outras metodologias são avaliados e priorizados. Cada vetor de ameaça individual é pontuado nos cinco elementos e uma média obtida, que pode ser usada para comparar sua

gravidade e probabilidade com as de outros vetores de ameaça. Assim, o DREAD vai além da modelagem de ameaças para a avaliação de riscos (BODEAU; MCCOLLUM; FOX, 2018).

De acordo com Seifert e Reza, (2016) O modelo DREAD classifica cada ameaça em cinco áreas diferentes e, em seguida, produz uma classificação geral com base nas pontuações. A análise DREAD é baseada na determinação de respostas para as seguintes perguntas para cada ataque:

- Dano: Quanto dano resultaria?
- Reprodutibilidade: Quão difícil é a execução?
- Explorabilidade: O quão fácil é reproduzir o ataque?
- Usuários afetados: Quantas pessoas provavelmente seriam afetadas?
- Descoberta: Quão difícil é encontrar a vulnerabilidade?

Cada item citado recebe um valor equivalente de 1 a 3. Por fim, para calcular o risco, deve-se somar os valores atribuídos a cada uma das propriedades e dividir o valor da soma por 5.

DREAD calcula o risco das ameaças encontradas usando vários fatores, incluindo potencial de dano, reprodutibilidade, explorabilidade, usuários afetados e descoberta. Essas classificações individuais são então calculadas em média para determinar uma pontuação geral para a ameaça. DREAD é um dos mecanismos mais completos para avaliar o risco de ameaça (SEIFERT; REZA, 2016).

STRIDE e DREAD são modelos de modelagem de ameaças bem estabelecidas para a avaliação de segurança de produtos e serviços ao longo de seu ciclo de vida (ZOGRAFOPOULOS, et al., 2021).

DREAD permite que as ameaças apresentadas sejam quantificadas de modo que fique claro a magnitude do risco apresentado ao ambiente, tornando possível a priorização de ameaças críticas. Este método foi escolhido para ser utilizado neste trabalho devido a contribuição em conjunto com o método STRIDE, pois o STRIDE não quantifica a ameaça, informando o grau de perigo apresentado.

3. METODOLOGIA

A metodologia de pesquisa empregada neste estudo é baseada em DSRM e em um processo da Pesquisa-Ação Canônica (CAR).

O foco deste estudo é a geração e aplicação de um artefato que possibilite identificar, descrever e avaliar os impactos da aplicação do método modelagem de ameaça, utilizando normas de gestão de risco, em computadores empresariais com auxílio de um sistema para monitoramento. O DSRM em conjunto com CAR possibilita alcançar este objetivo e proverá subsídio para pesquisas futuras.

3.1. *Design Science Research Methodology*

O método DSRM foi escolhido como o método principal para a realização deste estudo pois, segundo Dresch (2015) pesquisas, com enfoque prescritivo, encontram suporte para sua condução, por meio do emprego do método de pesquisa denominado *Design Science Research*.

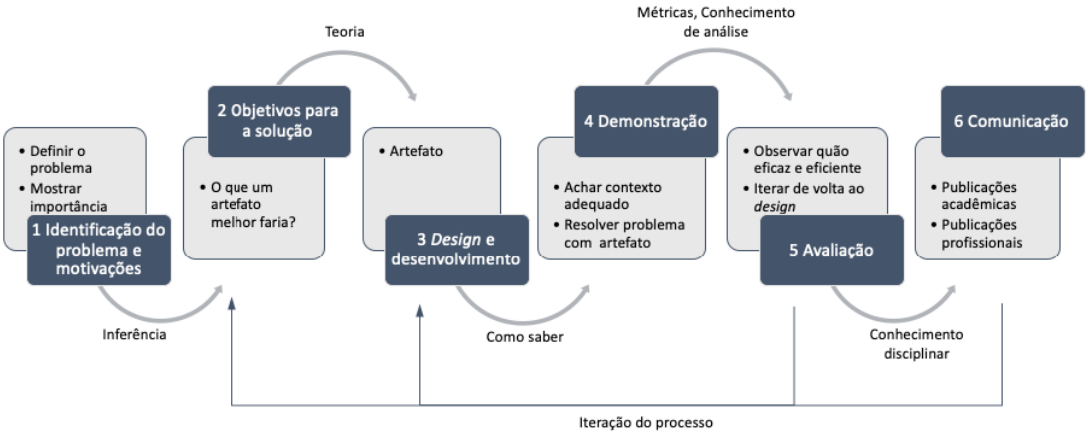
O DSRM tem embasamento na produção de pesquisa com o processo de *Design Science* e na apresentação por meio de modelo mental para tratar da realidade construída a partir da compreensão do problema, conforme Peffers et al. (2006).

A *design Science research* tem se apresentado como um método de pesquisa que dedica atenção para o desenvolvimento de estudos que tenham como objetivo a prescrição, o projeto e, também, a construção de artefatos. Esse método de pesquisa tem como base epistemológica a *design science*, conceito que se diferencia das ciências tradicionais, por se ocupar do artificial, ou seja, tudo aquilo que foi projetado e concebido pelo homem (DRESCH; LACERDA; ANTUNES, 2015).

A DSRM tem apresentado uma grande evolução como abordagem nas áreas de ciências exatas. Esta evolução se deve a sua característica em constituir um processo rigoroso para projetar artefatos para resolver problemas, avaliar o que foi projetado ou o que está funcionando, e comunicar os resultados obtidos (LACERDA *et al*., 2013).

O processo de DSRM possui seis etapas: (2.1) identificação e motivação do problema; (2.2) definição dos resultados esperados; (2.3) *design* e desenvolvimento; (2.4) demonstração; (2.5) avaliação e (2.6) comunicação. A Figura 5 ilustra as etapas do processo DSRM.

Figura 5: Etapas do processo de *Design Science Research Methodology*



Fonte: Adaptado de PEFFERS et al. (2006).

A primeira etapa do método proposto é a identificação e motivação do problema e da definição dos pontos que motivam a realização da pesquisa.

A identificação do problema específico da pesquisa e a justificativa do valor do artefato a ser produzido, como solução a ser construída e desenvolvida com aplicabilidade prática, motivando pesquisadores e leitores para se interessarem pela proposta de solução e pelo raciocínio associado ao entendimento do problema, contemplam os recursos necessários ao conhecimento teórico e prático do problema e da importância da solução proposta (HEVNER; CHATTERJEE, 2010).

Esta primeira etapa direciona a definição do problema de pesquisa específico e justificativa o valor de uma solução. Uma vez que a definição do problema é usada para desenvolver um artefato que possa efetivamente fornecer uma solução, pode ser útil atomizar o problema conceitualmente para que a solução possa capturar sua complexidade. Justificar o valor de uma solução ajuda produzir duas coisas: motiva o pesquisador e o público da pesquisa a buscar a solução e a aceitar os resultados e ajuda a entender o raciocínio associado à compreensão do problema pelo pesquisador (PEFFERS et al., 2007).

O problema está identificado na fundamentação teórica do presente estudo, por meio dos artigos estudados e aderência à questão da pesquisa apresentados neste estudo, que consiste em identificar, descrever e avaliar os impactos da aplicação do método modelagem de ameaça, utilizando normas de gestão de risco, em computadores empresariais com auxílio de um sistema para monitoramento.

Os outros passos do DSRM são detalhados no capítulo 4, em conjunto com a pesquisa empírica realizada para o estudo.

3.2. Pesquisa-ação Canônica

A Pesquisa-ação Canônica visa abordar problemas organizacionais e, ao mesmo tempo, contribuir para o conhecimento acadêmico, um conjunto de princípios útil para atingir esses objetivos potencialmente conflitantes e, assim, promover o rigor e a relevância do CAR (DAVISON; MARTINSONS; KOCK, 2004)

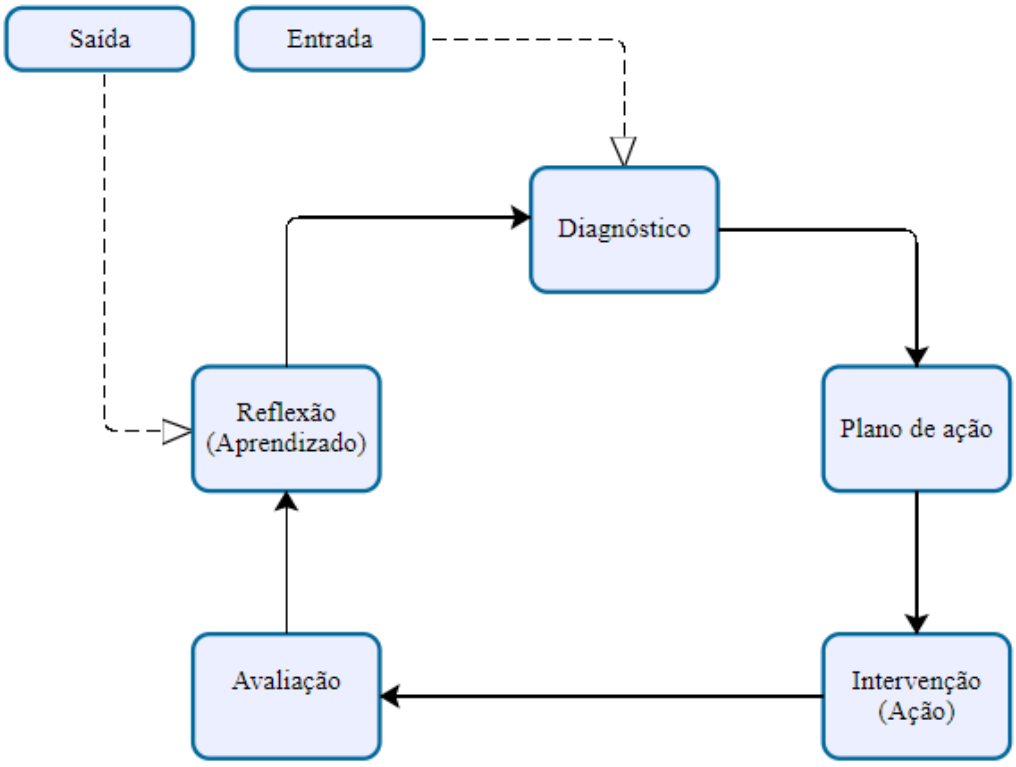
O princípio que é adaptado e utilizado neste estudo é:

Princípio do Modelo de Processo Cíclico

A natureza do modelo de processo cíclico sugere um fluxo unidirecional, com diagnóstico seguido de planejamento, intervenção e assim por diante. Embora isso seja desejável, nossa experiência sugere que alguma iteração entre os estágios pode ser necessária. (DAVISON; MARTINSONS; KOCK, 2004)

Os Passos para a utilização deste princípio pode ser conferido a partir da Figura 6:

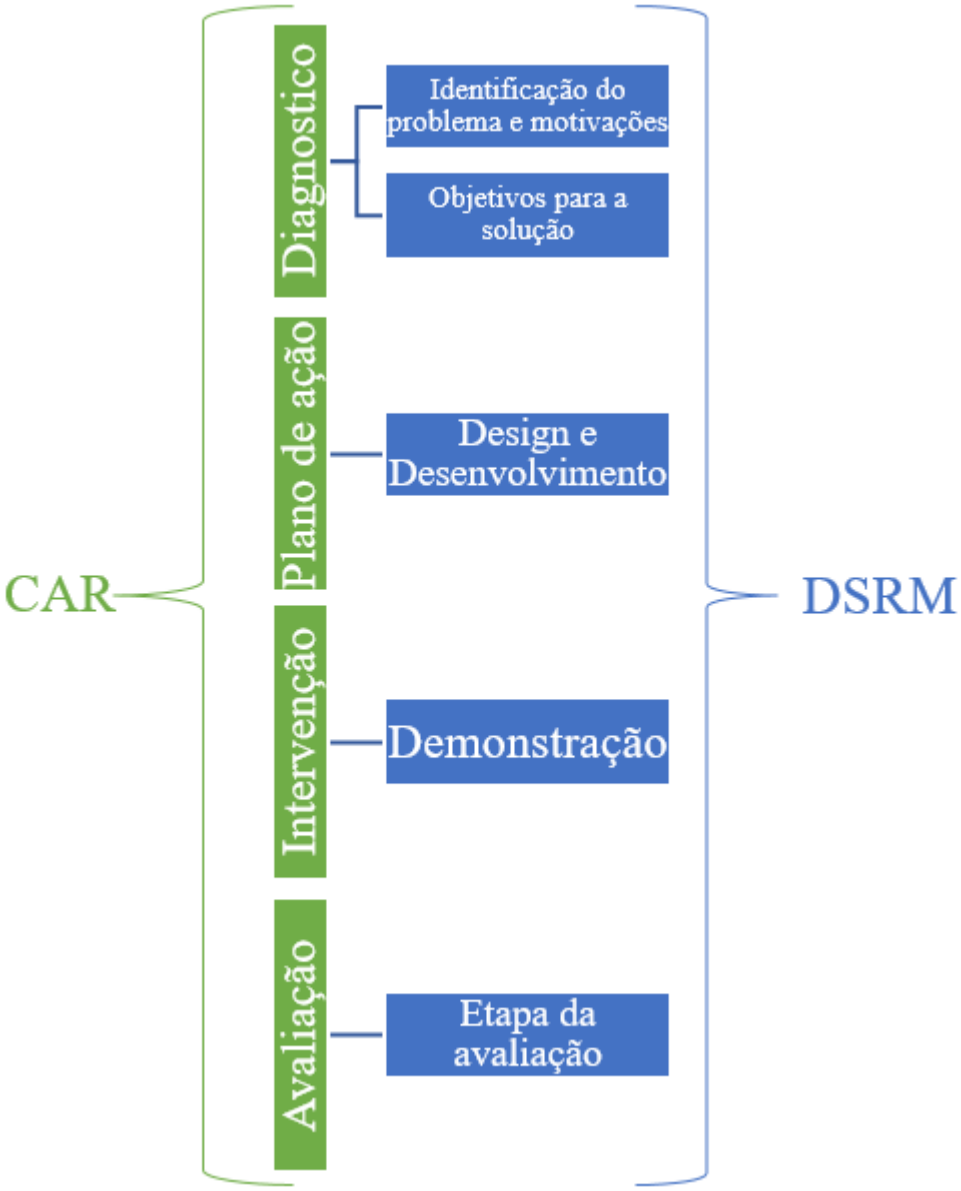
Figura 6: Passos da Pesquisa-Ação Canônica



Fonte: Adaptado de DAVISON; MARTINSONS; KOCK (2004).

Neste estudo, pode-se considerar que o diagnóstico foi realizado na parte da identificação do problema e motivação e em objetivos para solução, o plano de ação está contido em design e desenvolvimento, intervenção na etapa de demonstração e a avaliação na etapa de avaliação do processo de DSRM. Conforme mostra Figura 7.

Figura 7: Similaridades dos passos de CAR e DSRM



Fonte: Resultado da pesquisa.

A metodologia proposta para o trabalho propõe como base a utilização do DSRM em conjunto com a execução de um ciclo do Princípio do Modelo de Processo Cíclico.

4. PESQUISA EMPÍRICA

No capítulo 3 foi apresentado uma visão geral da metodologia. Este capítulo apresenta a proposta de aplicação da metodologia em resposta ao objetivo proposto no trabalho.

A pesquisa foi conduzida baseada na metodologia de DSRM, aplicando as seis etapas, cujos resultados são apresentados a seguir. A etapa de identificação do problema e motivações para a pesquisa referenciadas na DSRM estão cobertas pelo capítulo 1 de introdução e pelo capítulo 2 de fundamentação teórica, por meio da literatura científica estudada e da aderência à questão da pesquisa.

As próximas seções discutem as etapas de Definição dos resultados esperados, *design* e desenvolvimento, demonstração, avaliação e comunicação.

4.1. Definição dos resultados esperados

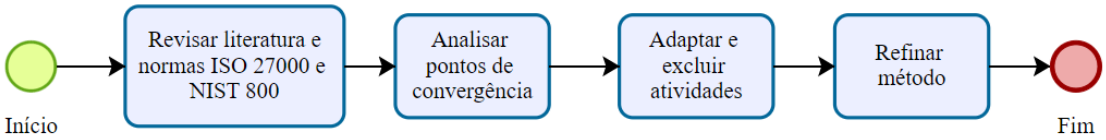
Esta etapa trata dos objetivos da solução, inferir os objetivos de uma solução a partir da definição do problema e do conhecimento do que é possível e viável. Os objetivos podem ser quantitativos, por exemplo, termos em que uma solução desejável seria melhor do que as atuais, ou qualitativos, por exemplo, uma descrição de como se espera que um novo artefato suporte soluções para problemas até então não abordados. Os objetivos devem ser inferidos racionalmente a partir da especificação do problema. Os recursos necessários para isso incluem o conhecimento do estado dos problemas e das soluções atuais, se houver, e sua eficácia (HEVNER; CHATTERJEE, 2010).

De acordo com Peeffers (2007), essa etapa visa inferir os objetivos de uma solução a partir da definição do problema. Os objetivos podem ser quantitativos, por exemplo, termos em que uma solução desejável seria melhor que a atual, ou qualitativos, por exemplo, onde um novo artefato é esperado para apoiar soluções para problemas até então não abordados. Os objetivos devem ser inferidos racionalmente a partir da especificação do problema. Os recursos necessários para isso incluem conhecimento do estado dos problemas e das soluções atuais e sua eficácia, se houver.

O resultado esperado neste trabalho consiste em uma aplicação de modelagem de ameaça com foco na segurança e atualização de programas para *endpoints*, utilizando o método STRIDE e DREAD com embasamento na norma ISO/IEC 27005 e controles existentes que possam contribuir, contidos nas normas ISO/IEC 27002 e NIST 800-30, e a criação de um sistema para monitoramento dos resultados encontrados.

As principais atividades utilizadas para o desenvolvimento da solução proposta neste trabalho são apresentadas na Figura 8, são elas: revisão da literatura e norma ISO/IEC 27000 e NIST 800; Análise dos pontos de convergência; Adaptação e exclusão de atividades; e Refinamento do método.

Figura 8: Processo de desenvolvimento do método



Fonte: Resultado da pesquisa.

4.1.1. Revisar Literatura e Normas ISO/IEC 27000 e NIST 800

Faz-se necessário o entendimento do que se concerne as principais metodologias de modelagem de ameaça vigentes e normas ISO/IEC 27002, ISO/IEC 27005 e NIST 800-30. A partir da observação da literatura e sugestões contidas nas normas ISO/IEC 27002, ISO/IEC 27005 e NIST 800-30, buscou-se a identificação e o entendimento das atividades envolvidas no processo de modelagem proposto.

Nesta atividade, foram consideradas tantos as metodologias em um cenário geral, quanto as metodologias ou trabalhos que utilizam modelagem de ameaças, que podem ser consultados no capítulo 2.

4.1.2. Análise dos pontos de convergência

Como estratégia para a apresentação de um método aplicável a padronização da segurança de um ambiente operacional, procurou-se identificar os pontos em que as metodologias analisadas convergiam. Em outras palavras, para a definição de um método base, foram mapeadas as atividades que estão presentes na ISO/IEC 27002 e na aplicação do STRIDE. A partir desta estratégia, foi definida um método baseado nas atividades da ISO/IEC 27002 e NIST 800-30, e na metodologia STRIDE e DREAD.

4.1.3. Adaptação e exclusão das atividades

O objetivo principal desta atividade foi analisar as atividades que compunham a metodologia de modelagem de ameaça inicial em termos de sua adequação ao objetivo proposto. Para isto, as atividades foram contrastadas com as propriedades inerentes ao paradigma de modelagem de ameaça e foram alvos de duas decisões estratégicas: adaptação da atividade ou exclusão da atividade.

4.1.4. Refinamento metodológico

Após busca na literatura sobre possíveis soluções ao problema apresentado, foi definido como potencial solução o desenvolvimento de um artefato que auxiliará em uma abordagem sistemática para controle e identificação das ameaças encontradas.

4.2. *Design* e desenvolvimento

A etapa de *Design* e desenvolvimento envolvem os processos necessários para a criação do artefato. O objetivo desta etapa é criar o artefato. Tais artefatos são potencialmente constructos, modelos, métodos, instanciações ou *Design Propositions*. Conceitualmente, um artefato de pesquisa de *design* pode ser qualquer objeto projetado no qual uma contribuição de pesquisa esteja incorporada ao *design* (HEVNER et al., 2004).

Esta atividade inclui determinar a funcionalidade desejada do artefato e sua arquitetura e, em seguida, criando o artefato real. Recursos necessários para passar dos objetivos para o *design* e o desenvolvimento incluem o conhecimento da teoria que pode ser usado como solução (PEFFERS et al., 2007).

O princípio fundamental é ter processo de pesquisa para adquirir conhecimento e compreensão de um problema, reconhecer os recursos necessários para passar dos objetivos ao projeto, sendo que o desenvolvimento inclui o conhecimento da teoria que possa ser aplicada por artefato (HEVNER; CHATTERJEE, 2010). O Quadro 1 resume as descrições dos tipos de artefatos geralmente documentados na DSRM.

Quadro 1: Tipos de artefatos da DSRM

Tipos de artefatos	Descrição
Constructos	Constructos ou conceitos formam o vocabulário de um domínio. São os conceitos usados para descrever os problemas dentro do domínio e para especificar as respectivas soluções. Os constructos definem os termos usados para descrever e pensar sobre as tarefas, sendo valiosos tanto para os profissionais quanto para os pesquisadores.
Modelos	Os modelos podem ser entendidos como um conjunto de proposições ou declarações que expressam as relações entre os constructos. São considerados representantes da realidade que apresentam tanto as variáveis de determinado sistema como suas relações. Um modelo pode também ser considerado uma descrição, isto é, uma representação de como as coisas são. As relações entre os elementos do modelo precisam ser claramente definidas.
Métodos	Métodos são um conjunto de passos necessários para desempenhar determinada tarefa. Podem ser representados graficamente ou encapsulados em heurísticas e algoritmos específicos. Os métodos podem estar ligados aos modelos, e as etapas do método podem utilizar partes do modelo como uma entrada que o compõe. Os métodos favorecem sobremaneira tanto a construção quanto a representação das necessidades de melhoria de um determinado sistema. Além disso, favorecem a transformação dos sistemas em busca de sua melhoria. Os métodos são criações típicas das pesquisas fundamentadas em *design Science*.

Instanciações	As instanciações são os artefatos que operacionalizam outros artefatos (constructos, modelos e métodos). A operacionalização visa também demonstrar a viabilidade e a eficácia dos artefatos construídos. As instanciações informam como implementar ou utilizar determinado artefato e seus possíveis resultados no ambiente real. Elas podem se referir a um determinado artefato ou à articulação de diversos artefatos para a produção de um resultado em um contexto. A partir dessa lógica, é possível afirmar que o artefato instanciação consiste em um conjunto coerente de regras que orientam a utilização dos artefatos (constructos, modelos e métodos) em um determinado ambiente real, que compreende desde as fronteiras da organização ou da indústria onde se encontra até os contornos da realidade econômica na qual a organização está inserida. Logo, a instanciação pode ter um papel particularmente relevante, pois orienta a utilização de outros artefatos considerando múltiplos fatores, assim como o tempo e prazo para implementação da solução.
Design Propositions	As *design propositions* correspondem a um *template* genérico que pode ser utilizado para o desenvolvimento de soluções para uma determinada classe de problemas. O artefato que for uma contribuição teórica originária do *design science resarch* é apresentado como a generalização de uma solução para uma determinada classe de problemas, tornando-se um conhecimento que pode ser aplicado para diversas situações similares, desde que consideradas suas particularidades.

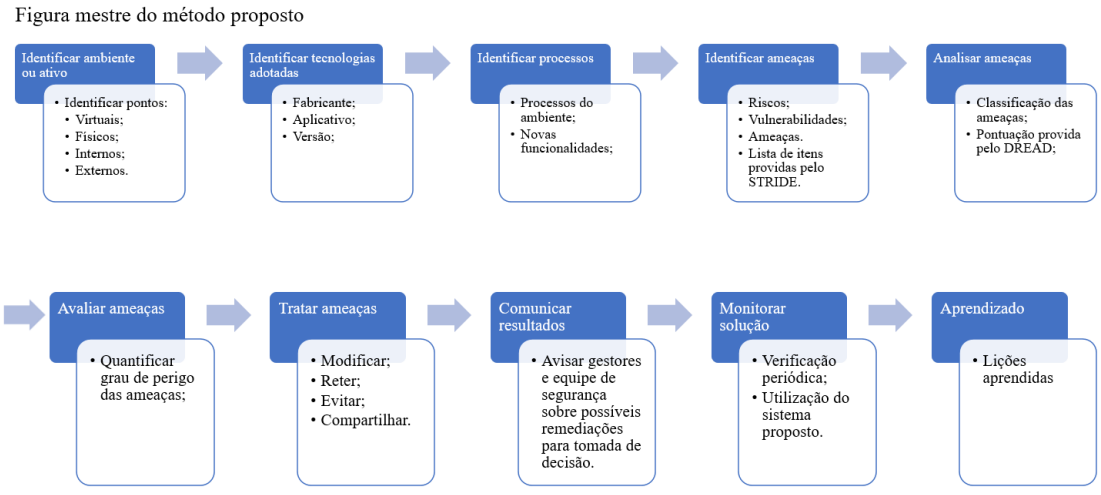
Fonte: Adaptado de DRESCH; LACERDA; MIGUEL (2015).

Esta atividade define a solução (artefato) que seja uma contribuição de pesquisa e a criação real do artefato. Os processos abaixo definem a abordagem sistemática para identificação e tratamento das ameaças apresentadas pelo ambiente ou ativo, assim como a criação de um sistema para monitoração.

O Artefato esperado para este trabalho é um método, por utilizar a variação do modelo de modelagem em conjunto com normas de segurança, apresentado em conjunto com o sistema para controle de versões.

A figura mestre do método proposto pode ser conferida na Figura 9:

Figura 9: Figura mestre do método proposto



Fonte: Resultado da pesquisa.

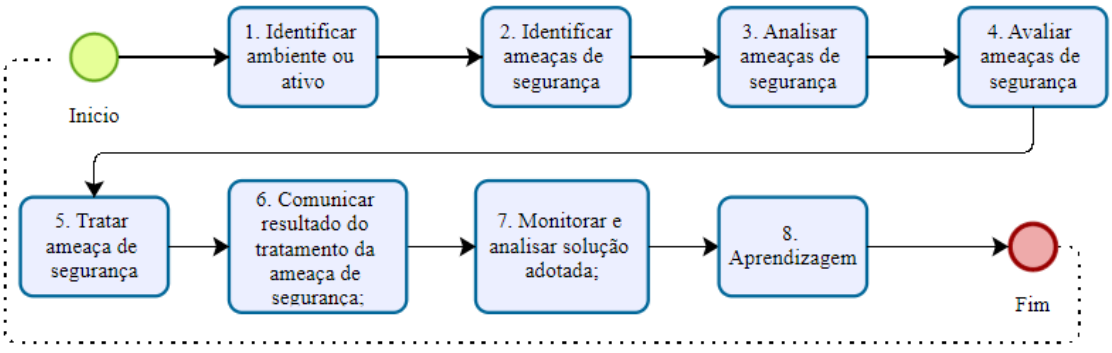
4.2.1. Processos

O Método aplicável para o objetivo proposto pode ser compreendida a partir dos seguintes processos e atividades, elaborada com base nos controles contidos na ISO/IEC 27005 e a utilização do método de modelagem de ameaça:

1. Identificar ambiente ou ativo;
    - Identificar as tecnologias adotadas;
    - Identificar os processos do sistema;
2. Identificar ameaças de segurança;
3. Analisar ameaças de segurança;
4. Avaliar ameaça de segurança;
5. Tratar ameaça de segurança;
6. Comunicar resultado do tratamento da ameaça de segurança;
7. Monitorar e analisar solução adotada;
    - Criação de um sistema para monitoramento.
8. Aprendizagem

A Figura 10 apresenta os processos que representam o método:

Figura 10: Processos do método



Fonte: Resultado da pesquisa.

Uma comparação dos fluxos entre o método sugerido, metodologia de modelagem de ameaça e da ISO 27005 podem ser visualizadas no apêndice E.

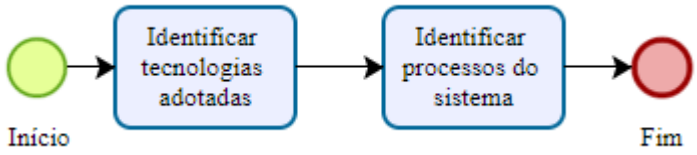
Em caso de tratativa de ameaças identificadas em versões de softwares que estão em produção, deve-se iniciar o processo a partir do passo 3, da Figura 10.

4.2.1.1. Identificar ambiente ou ativo

O primeiro processo destina-se a obter a compreensão do sistema sob análise. Para identificação efetiva das ameaças de segurança, é necessário compreender quais são os ativos do sistema, seus processos e interações. Para a realização da etapa de modelagem da arquitetura do ambiente ou ativo, é recomendado consultar documentações que descrevam o ambiente tecnicamente.

Com isto, o método proposto neste trabalho define as seguintes atividades a serem realizadas: Identificar os ativos do sistema e identificar os processos do sistema. A Figura 11 mostra a representação deste processo:

Figura 11: Processos da identificação do ambiente ou ativo



Fonte: Resultado da pesquisa.

1. Identificar as tecnologias adotadas

Esta atividade visa identificar as diversas tecnologias adotadas pelo sistema. Nesta atividade, deve-se identificar quais tecnologias são utilizadas ou implantadas para a utilização do sistema e seu produto. Deve-se identificar o fabricante, sistema operacional, versão do produto etc. Permitindo que sejam verificadas ameaças relacionadas ao programa em específico.

A tecnologia adotada para este trabalho foi o Sistema Operacional Windows 10, da Microsoft, onde são analisadas unicamente o seu sistema operacional, não sendo levado em consideração a utilização de outros programas de terceiros. Programas que interferem no funcionamento e proteção do Windows poderão ser analisados em trabalhos futuros.

2. Identificar os processos do sistema

Esta atividade visa identificar os processos realizados pelo sistema e processos que afetam ou modificam o sistema.

Nesses processos pode-se incluir tarefas manuais por profissionais de tecnologia, assim como processos automáticos, que possuem como objetivo modificar algo no próprio sistema ou no produto que é gerado pelo sistema; como uma atualização ou a adição de alguma

funcionalidade. Por exemplo, no caso deste estudo, a alteração de um processo que envolve a atualização de um programa ou sistema contido na imagem, o sistema operacional Windows, afeta um processo crítico do dispositivo de implantação de sistema e, consequentemente, o produto final, que tem esse sistema atualizado.

4.2.1.2. Identificar ameaças de segurança

Esta atividade visa identificar os pontos de risco, ameaça ou vulnerabilidade do sistema, no caso deste estudo, o sistema operacional e seus programas. Neste processo busca-se a identificação dos riscos, ameaças de segurança e vulnerabilidades no ambiente analisado, como resultado, é gerada uma lista das ameaças de segurança encontradas nos ativos que foram analisados.

4.2.1.3. Analisar ameaças de segurança

Esta etapa visa analisar as ameaças encontrados na etapa anterior. A análise dos riscos, ameaças de segurança e vulnerabilidades é o núcleo principal de modelagem de ameaças, nesta etapa pode-se utilizar o método DREAD para definir o grau de ameaça de cada item contido na lista de ameaças encontradas na etapa anterior.

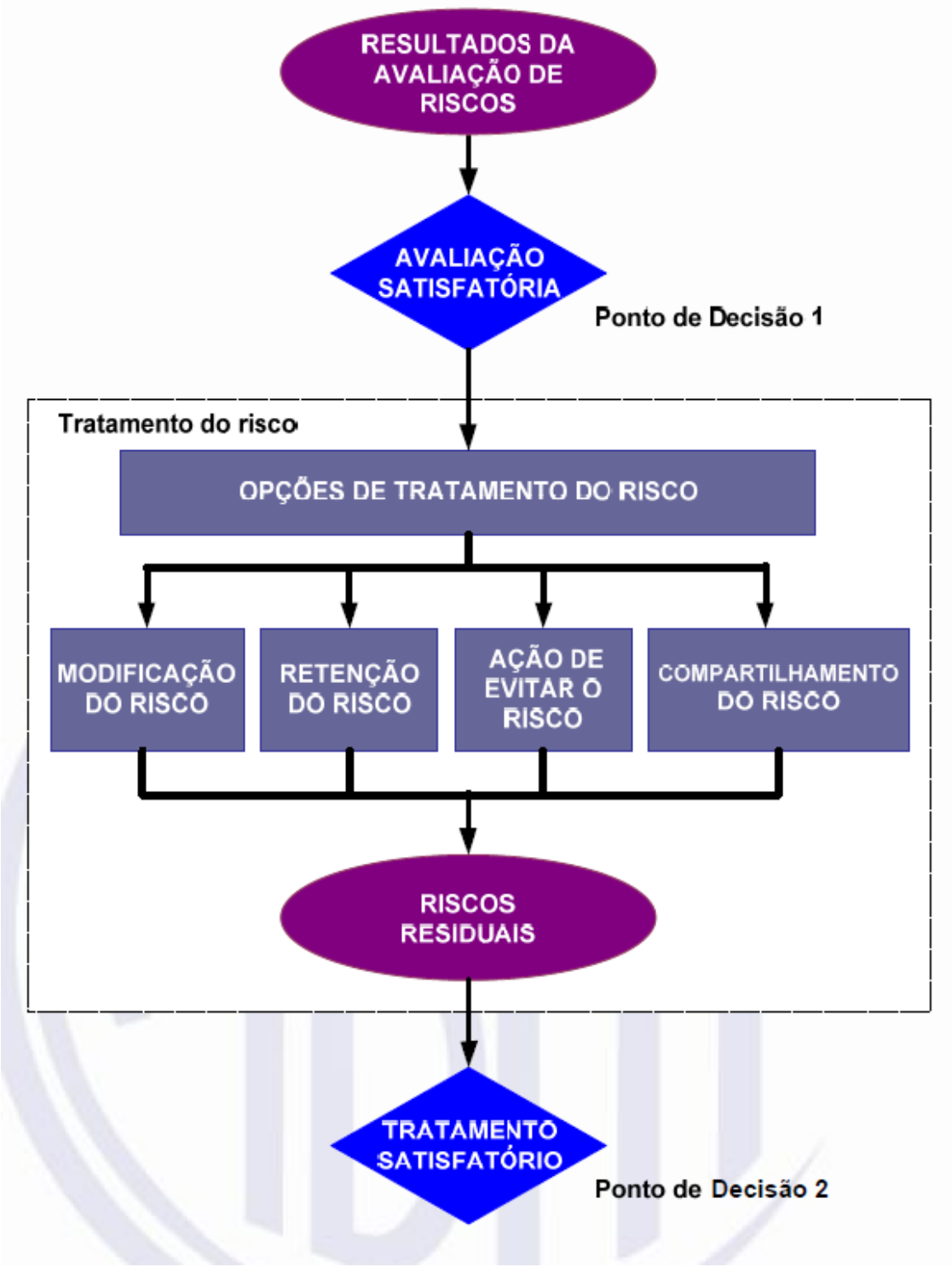
4.2.1.4. Avaliar ameaça de segurança

Nesta etapa objetiva-se avaliar as ameaças evidenciadas nas etapas anteriores. Essa atividade visa quantificar o grau de perigo das ameaças encontradas para mostrar a magnitude apresentada por cada ameaça, consequentemente auxiliando a priorização no tratamento de cada ameaça.

4.2.1.5. Tratar ameaça de segurança

Esta atividade propõe soluções cabíveis para a ameaça de segurança encontrada. Segundo a ISO/IEC 27005 (2019), recomenda-se que controles para modificar, reter, evitar ou compartilhar os riscos sejam selecionados e que seja definido um plano para o tratamento do risco, conforme Figura 12.

Figura 12: Atividade de tratamento do risco



Fonte: ISO/IEC 27005.

1. Modificação do risco

Consoante com a ISO/IEC 27005 (2019), recomenda-se que o nível de risco seja gerenciado por meio da inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e então considerado aceitável. Em geral, os controles podem fornecer um

ou mais dos seguintes tipos de proteção: correção, eliminação, prevenção, minimização do impacto, dissuasão, detecção, recuperação, monitoramento e conscientização.

2. Retenção do risco

De acordo com a ISO/IEC 27005 (2019), convém que as decisões sobre a retenção do risco, sem outras ações adicionais, sejam tomadas tendo como base a avaliação de riscos. Se o nível de risco atende aos critérios para a aceitação do risco, não há necessidade de se implementar controles adicionais e pode haver a retenção do risco.

3. Ação de evitar o risco

Conforme a ISO/IEC 27005 (2019), quando os riscos identificados são considerados demasiadamente elevados e quando os custos da implementação de outras opções de tratamento do risco excederem os benefícios, pode-se decidir que o risco seja evitado completamente, seja pela eliminação de uma atividade planejada ou existente (ou de um conjunto de atividades), seja pelas mudanças nas condições em que a operação da atividade ocorre ou a mudança da solução adotada.

4. Compartilhamento do risco

Concordante com a ISO/IEC 27005 (2019), compartilhamento do risco envolve a decisão de se compartilhar certos riscos com entidades externas. O compartilhamento do risco pode gerar novos riscos ou modificar riscos existentes e identificados, portanto, um novo tratamento do risco pode ser necessário. Convém notar que é possível compartilhar a responsabilidade de gerenciar riscos, entretanto não é normalmente possível compartilhar a responsabilidade legal por um impacto. Os clientes provavelmente atribuem um impacto adverso como sendo falha da organização.

4.2.1.6. Comunicação do resultado do tratamento da ameaça de segurança

De acordo com a ISO/IEC 27005 (2019), a comunicação do risco é uma atividade que objetiva alcançar um consenso sobre como gerenciar e lidar os riscos por meio da troca ou compartilhamento das informações sobre o risco entre os tomadores de decisão e as outras partes interessadas. Como por exemplo, equipe de segurança, equipe responsável pela vulnerabilidade e gestores envolvidos.

4.2.1.7. Monitorar a solução adotada

Esta etapa propõe um monitoramento contínuo sobre a solução e ambiente analisado, evitando assim possíveis novos incidentes de segurança e mantendo o ambiente seguro e atualizado. Recomenda-se que os riscos e seus fatores sejam monitorados e analisados criticamente, a fim de se identificar, o mais rapidamente possível, eventuais mudanças no contexto da organização e de se manter uma visão geral dos riscos.

4.2.1.8. Aprendizagem

O aprendizado obtido com os processos pode ser reaproveitado em outras verificações, mesmo que o aplicativo analisado seja diferente. Neste item pode-se citar o amadurecimento do processo de modelagem de ameaça e do próprio sistema proposto.

4.2.2. Desenvolvimento do sistema para controle e monitoramento

Para a monitoração da solução adotada, atualmente não é possível prescrever uma possível solução automática devido a necessidade de homologação das atualizações dos softwares providas pelos fabricantes antes da replicação ao ambiente. Devido a esta limitação, foi realizado a proposta de um sistema para auxílio no controle de homologação das atualizações do sistema operacional.

O sistema proposto implantará o processo de melhoria contínua na verificação de ameaças, que consiste na melhoria da maturidade do produto, pois fará com que a verificação de ameaça seja feita de modo organizado e em datas definidas, possibilitando que sejam encontradas ameaças que não foram mapeadas em uma verificação anterior. Fará também com que o processo de atualização passe a ser uma tarefa controlada, deixando de ser uma tarefa reativa, onde a atualização acontece apenas quando alguma necessidade é apresentada.

Esta etapa explana o desenvolvimento do sistema, necessário para a monitoração da solução adotada, no caso deste estudo, o controle sobre as versões e ameaças identificadas na modelagem de ameaça.

O artefato foi apresentado aos times de segurança da informação e ao time de apoio a projetos e atualizações, para aprovação e questionamento sobre a viabilidade de utilização do sistema proposto. Após alinhamento com as equipes e concordância das áreas na utilização do artefato, o time de sistemas foi acionado para iniciar a construção do sistema que deve auxiliar no monitoramento de versão dos programas e atualizações do ambiente.

O sistema foi desenvolvido por uma analista do time de sistemas interno do escritório, utilizando as ferramentas providas pela plataforma PowerApps. Foram realizadas 8 reuniões com a analista de sistemas, com duração de 45 minutos cada. O assunto de cada reunião pode ser conferido no Apêndice F.

Para desenvolvimento do sistema foi utilizado a plataforma PowerApps e para desenvolvimento dos gatilhos para envio dos e-mails aos responsáveis, a plataforma PowerAutomate, ambos da Microsoft. O sistema PowerApps possui o próprio banco de dados armazenado na nuvem Sharepoint, utilizando formato padrão providenciado pela Microsoft, sendo feito seu backup automático em períodos escolhidos pelo gestor da ferramenta conforme configuração selecionada pela empresa.

A idealização do sistema foi feita visando o funcionamento interno no escritório pelo aplicativo “Teams” da Microsoft, facilitando assim a interação dos analistas responsáveis com a aplicação, havendo permissão de leitura e escrita apenas para os analistas envolvidos no projeto.

Devido ao objetivo do sistema, os seguintes campos foram considerados essenciais para o funcionamento do sistema: ID, Título do software, Criticidade, Modificado por, Modificado, Versão da aplicação, Versão de homologação, Data de verificação, Data Limite homologação, Periodicidade, ID GMUD, Equipe Responsável, Ponto focal, Gestor responsável, Data modelagem de ameaça, Ameaça atual, Ameaça versão de homologação, CVE, Site de atualização, Observações e Anexos, conforme mostra o Quadro 2.

Quadro 2: Explanação sobre os campos no sistema

Nome do campo no sistema	Explanação sobre o campo
ID	Número atribuído automaticamente ao software para controle no sistema
Título	Nome de exibição do software
Criticidade	Medição do nível de criticidade da atualização do software ao negócio: Baixa, média ou alta
Modificado por	Último profissional que realizou alterações no controle
Modificado	Data da última modificação realizada
Versão da aplicação	Versão atual do software no ambiente em produção
Versão de homologação	Versão em homologação, que está em teste antes de ser implantado ao ambiente
Data de verificação	Data que iniciará a homologação da nova versão do software
Data limite homologação	Data limite para finalização da homologação do software
Periodicidade	Periodicidade em que é realizada a verificação de nova versão ou patch disponível: Mensal, trimestral, semestral ou anual.
ID GMUD	Número da GMUD relacionada a atualização do software
Equipe responsável	Equipe responsável pelo software
Ponto focal	Profissional responsável pela verificação e homologação do programa
Gestor responsável	Gestor do responsável pelo software

Data modelagem de ameaça	Data da última modelagem de ameaça realizada
Ameaça versão atual	Campo apresenta se há, ou não, ameaça no programa atual
Ameaça versão de homologação	Campo apresenta se há, ou não, ameaça no programa em homologação
CVE	Número do CVE relacionado a vulnerabilidade encontrada, se houver
Site de atualização	Site contendo detalhes sobre a disponibilidade e mudanças contidas da nova versão
Observações	Observações, caso exista
Anexos	Anexos necessários para a execução da tarefa, assim como a modelagem de ameaça realizada.

Fonte: Resultado da pesquisa.

Os Campos: ID, Modificado por, Modificado e Data Limite homologação são controlados pelo sistema, não sendo possível sua modificação por ações humanas.

Os campos: Criticidade, Equipe responsável, Periodicidade, Ponto focal e Gestor responsável, não são editáveis na visão do operador, apenas os gestores poderão alterar essas informações no acesso *Web* ao sistema.

Os Campos: Título do software, Versão da aplicação, Versão de homologação, Data de verificação, ID GMUD, Data modelagem de ameaça, Ameaça atual, Ameaça versão de homologação, CVE, Site de atualização, Observações e Anexos podem ser editados pelos operadores.

Para o funcionamento do sistema, a criação de uma Equipe no “Teams” é necessária para o controle de pessoas autorizadas para acesso ao sistema, restringindo assim o acesso de outros profissionais e permitindo acesso apenas a pessoas que serão envolvidas na utilização do sistema.

A necessidade de um histórico de alteração evidenciando o que foi alterado e quem realizou a alteração no sistema foi considerada como item necessário, fazendo com que qualquer alteração no sistema seja registrada, para possível necessidade de verificação futura.

A periodicidade de verificação da nova versão do sistema ditará o tempo que o sistema deve permitir para homologação. Não é viável permitir a atualização automática do aplicativo devido a necessidade de homologação antes de ser implementado no ambiente.

A quantidade de atualizações de cada software irá variar, dependendo: da quantidade de vezes o software é atualizado pela empresa ao ano, se o update é majoritário ou se o update é um patch de segurança . A periodicidade foi estabelecida para garantir que o software está atualizado e para que seja possível aplicar o processo de melhoria contínua, conforme mostra a Tabela 1.

Tabela 1: Periodicidade e tempo de homologação

Periodicidade	Tempo para homologação
Anual	3 meses
Semestral	2 meses
Trimestral	1 meses
Mensal	15 dias

Fonte: Resultado da pesquisa.

Grupos de homologação foram criados para garantir que o Sistema Operacional não conflite com programas já existentes nos computadores, foram criados dois grupos que receberão as atualizações. O primeiro grupo possui apenas profissionais de Tecnologia e o segundo grupo abrange pelo menos um profissional de cada área da empresa.

Os grupos receberão as atualizações em datas diferentes:

- 1º Grupo receberá a atualização assim que estiver disponível;
- 2º Grupo receberá a atualização após 7 dias da implementação realizada no grupo 1.

O fluxograma do sistema deve funcionar do seguinte modo:

1. Na data de atualização do programa, o sistema enviará um alerta ao responsável para verificação de atualização e ameaça do software analisado. O responsável precisa realizar a verificação dentro do período proposto, caso não realize, o gestor imediato será alertado.
    - Caso não exista uma nova versão do programa, o responsável finalizará a tarefa de verificação e o ciclo de verificação será finalizado.
2. Caso exista uma nova atualização esteja disponível, é iniciado testes relacionados a conflitos de software e verificação das alterações do software contidas na nota de atualização, para verificar se há alguma nova característica no software que represente ameaça.
    - Após testes no grupo de homologação e verificação de ameaças, caso o programa seja compatível e não represente ameaça aos sistemas existentes a empresa, o programa é atualizado.
3. Caso a versão disponível represente ameaça a empresa, seja incompatível ou não esteja disponível para *download*, é feito o contato com o fornecedor para verificar os pontos elencados.

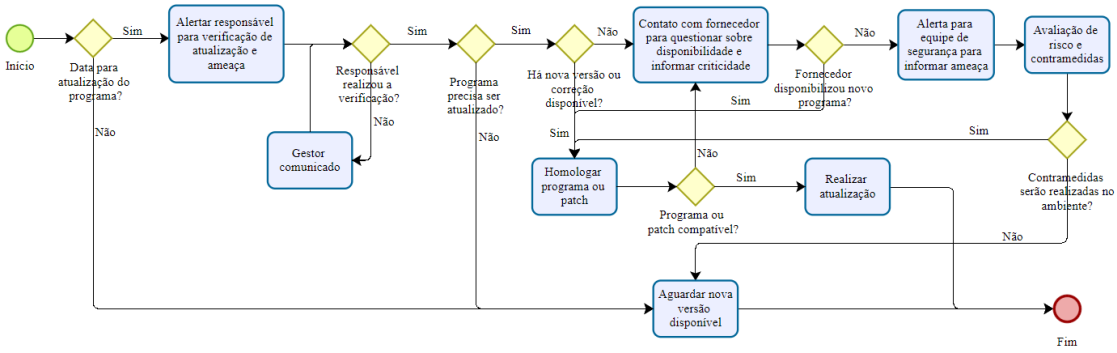
- Após testes de homologação e verificação de ameaças, caso o programa seja compatível e não represente ameaça aos sistemas existentes a empresa, o programa é atualizado.

4. Caso a atualização do fornecedor seja incompatível com algum sistema utilizado ou ainda represente ameaça a empresa, o time de segurança é alertado sobre a impossibilidade de atualização e, se necessário, é realizado a aplicação de patches de segurança para a nova versão.

- Caso não exista um patch de segurança para a nova versão, a equipe de segurança é alertada sobre a ameaça e se dá início a avaliação de risco e contramedida. O time de segurança analisa se há necessidade de aplicação de algum patch de segurança para a versão antiga ou se a atualização para a nova versão será realizada.

O fluxograma do sistema é representado na Figura 13:

Figura 13: Fluxograma do sistema



Fonte: Resultado da pesquisa.

Para o objetivo do sistema, foi necessário a criação de três gatilhos individuais, que farão o envio de comunicação com os profissionais responsáveis:

- Envio de e-mail aos responsáveis para verificação de nova versão. O campo “data de verificação” informará quando o e-mail deverá ser enviado;
- Envio de e-mail ao gestor responsável pela aplicação, caso o responsável não tenha realizado a tarefa de verificação de nova versão. O campo “Data limite homologação” informará quando o e-mail deverá ser enviado;
- Envio de notificação ao time de segurança pelo “Teams”, caso o fornecedor não tenha uma solução relacionada a ameaça encontrada. Quando o campo “Ameaça

versão de homologação” for preenchido com sim, a mensagem no grupo do “Teams” deverá ser enviada.

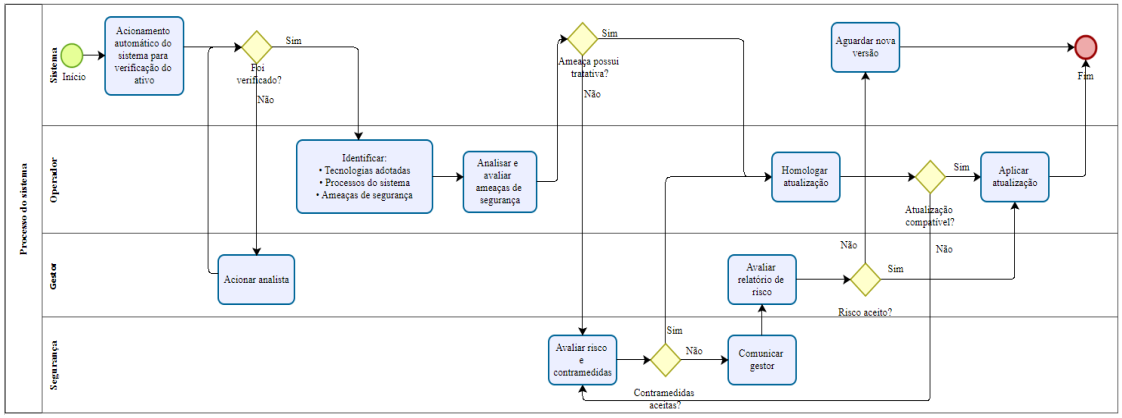
Após criação do sistema, foram inseridas duas tarefas para verificação dos itens encontrados na modelagem de ameaça; Atualização Build e Atualização Patch:

- A tarefa Atualização Build fica responsável pela atualização do build do Windows e criação de uma nova imagem para o ambiente. No momento da criação da imagem, além da atualização do build, é feita a validação do funcionamento dos bloqueios citados encontrados na modelagem de ameaça, para certificar-se de que os bloqueios estão efetivos.
- A tarefa Atualização de patch fica responsável por manter o Sistema Operacional em sua última versão, caso não sejam encontrados pontos de ameaça ou conflito com outros softwares utilizados no escritório em sua homologação.

A inserção do campo CVE, para que, quando necessário, seja preenchido pelo operador responsável pela verificação de ameaças no software. A verificação de CVE para o patch aplicado ao programa é feito através da busca disponível no site da Mitre (MITRE, 2022) ao inserir a versão do programa para checagem de alguma possível ameaça existente e comunicada para a comunidade.

O processo do método proposto e equipes envolvidas é representado pela Figura 14:

Figura 14: Processo do sistema e seus atores



Fonte: Resultado da pesquisa.

De acordo com os processos e o fluxo do sistema, as ameaças são encontradas ao analisar a documentação de atualização disponibilizada pelo fabricante, onde é possível identificar novas funcionalidades que possam representar ameaças para a empresa. Também é

possível manter o aplicativo atualizado, evitando vulnerabilidades já tratadas, mas que tornavam o ambiente vulnerável devido a ausência do patch.

Exemplos das imagens e alertas enviadas pelo sistema podem ser vistos no Apêndice G.

4.3. Demonstração

Na quarta etapa é feita a demonstração do uso do artefato para solucionar o problema em questão, essa etapa pode ser desenvolvida por meio de experimentação, simulação etc.

Para demonstrar a eficácia do artefato, deve-se envolver seu uso em experimentação, simulação, estudo de caso, prova ou outra atividade. Os recursos necessários para a demonstração incluem conhecimento efetivo de como usar o artefato para resolver o problema (PEFFERS et al., 2007).

Pode-se dizer que a demonstração da utilização contempla o seu método, uma vez que os constructos e modelos já apresentados se concretizam em um exemplo prático, neste caso aplicado a um sistema operacional.

O ciclo de teste iniciou-se em junho de 2022, o Sistema Operacional Windows foi eleito como o programa para teste por ser a base para todos os outros programas existentes. Inicialmente foi realizada a modelagem de ameaça para a verificação das ameaças encontradas no Sistema Operacional. Para cada ameaça encontrada, uma análise foi realizada e a remediação prescrita para a resolução do incidente conforme explanado anteriormente neste capítulo.

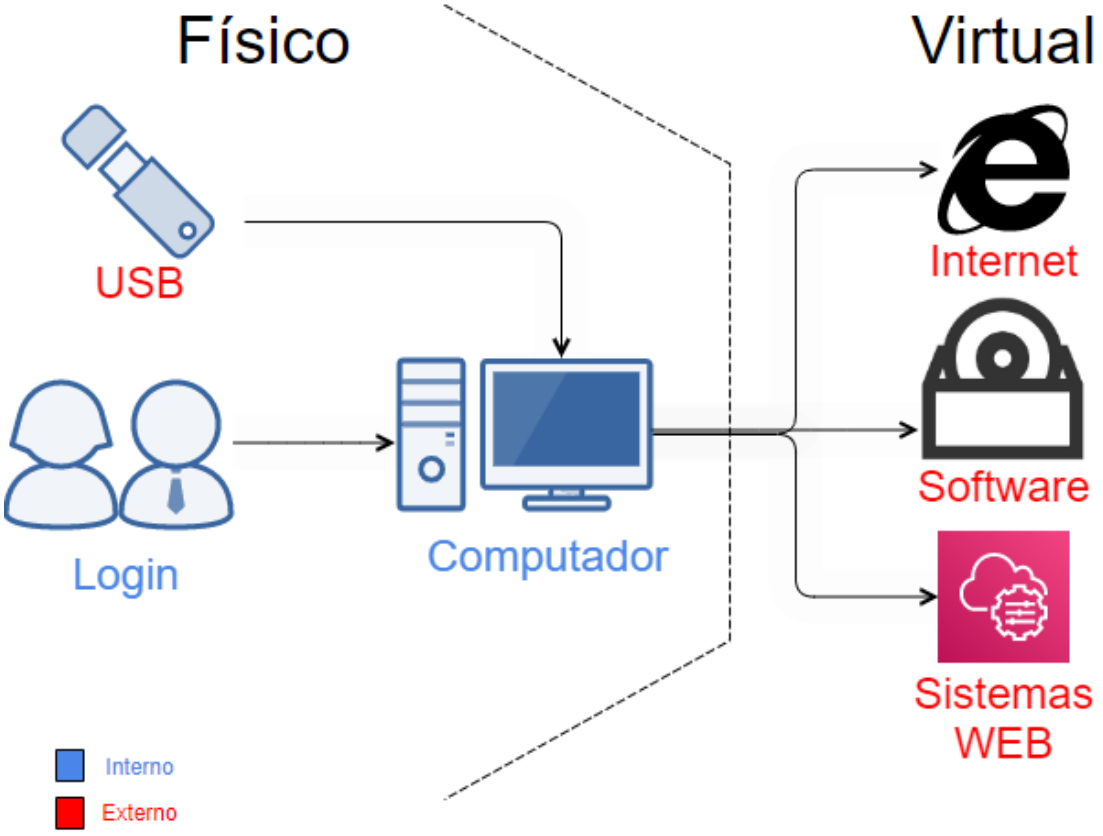
4.3.1. Identificar ambiente ou ativo

Inicialmente foram necessários verificar os processos que estão presentes no ambiente, para melhor entendimento das possíveis ameaças. Os pontos de processos foram divididos entre:

- Pontos virtuais: que apresentarão ameaças relacionadas aos aplicativos e funcionalidades nativas do Sistema Operacional;
- Pontos físicos, onde serão apresentadas ameaças que podem ser exploradas devido a exposição do computador a um ambiente físico, como por exemplo, exploração através de pen drive ou alteração na BIOS;
- Pontos internos, que são pontos apresentados pelo próprio ambiente da empresa, sem influência externa;
- Pontos externos, onde serão apresentados pontos de ameaças que partem de um ambiente externo, não relacionado ao ambiente interno empresarial.

O computador e seu Sistema Operacional possuem os seguintes processos nativos, conforme mostra Figura 15:

Figura 15: Diagrama do ambiente



Fonte: Resultado da pesquisa.

4.3.1.1. Identificar as tecnologias adotadas

Fez-se necessário a verificação do ambiente, no caso deste estudo, o ambiente operacional Windows 10, utilizado pela empresa onde será aplicada a solução proveniente do artefato.

Também foram coletadas informações sobre o modo de login utilizado pelos colaboradores, para melhor entendimento sobre as sugestões que serão realizadas como soluções para a mitigação de ameaças encontradas.

4.3.1.2. Identificar os processos do sistema

Os processos mapeados pelo ambiente que apresentam possíveis ameaças:

- Ao login no computador físico;
- Utilização de hardware externo para gravação de arquivos;

- Desproteção física ao conteúdo do disco rígido;
- Desproteção do ativo, contra ameaças virtuais;
- Desproteção contra perda de informações contidas no computador;
- Divulgação de informações para entidades externas.

4.3.2. Identificar ameaças de segurança

Com base nos processos mapeados pelo ambiente que possam apresentar ameaças, utilizando a modelagem de ameaça STRIDE por elemento, foi possível identificar as seguintes ameaças:

1. Acesso a sites ou sistemas não autorizados pela empresa;
2. Acesso indevido ao dispositivo utilizando conta externa ou de terceiros;
3. Alteração de informações na rede empresarial;
4. Compartilhamento do login empresarial;
5. Divulgação ou perda de conteúdo empresarial;
6. Falta de proteção física ao conteúdo do HD;
7. Instalação de programa que sobrecarrega o sistema;
8. Instalação de programas não autorizados pela empresa;
9. Instalação de software que sobrecarrega a rede empresarial;
10. Perda de informações empresariais em caso de desastres;
11. Programas desatualizados;
12. Proteção do ativo, contra ameaças virtuais;
13. Utilização de login pessoal em programas da empresa;
14. Utilização de pen drive para gravação de arquivos.

Conforme apresentado no Quadro 3:

Quadro 3: Aplicação do método STRIDE por elemento

Windows						
STRIDE por elemento	**Falsificação**	**Adulteração**	**Repúdio**	**Divulgação de informação**	**Negação de serviço**	**Elevação de privilégio**
Entidade Externa:	Acesso indevido ao dispositivo utilizando conta externa ou de terceiros;		Acesso a sites ou sistemas não autorizados pela empresa;	Acesso a sites ou sistemas não autorizados pela empresa;		
			Utilização de login pessoal em programas da empresa;	Utilização de login pessoal em programas da empresa;		
Entidade Interna:		Programas desatualizados;	Compartilhamento do login empresarial;	Divulgação ou perda de conteúdo empresarial;		
Físico:		Falta de proteção física ao conteúdo do HD;		Utilização de pen drive para gravação de arquivos;		
				Perda de informações empresariais em caso de desastres;		
Virtual:		Proteção do ativo, contra ameaças virtuais;			Instalação de software que sobrecarrega a rede empresarial.	Instalação de programas não autorizados pela empresa;
		Alteração de informações na rede empresarial;			Instalação de programa que sobrecarrega o sistema.	

Fonte: Resultado da pesquisa.

4.3.3. Analisar ameaças de segurança

Para ser possível avaliar as ameaças, elas precisam ser analisadas e classificadas corretamente. As ameaças encontradas foram classificadas conforme grau de ameaça, utilizando as pontuações abaixo:

Dano: Quanto dano resultaria?

- Alto (3) – O atacante pode obter controle total do sistema e/ou executar tarefas com privilégios administrativos;
- Médio (2) – Perda de informações sensíveis;
- Baixo (1) - Perda de informações triviais.

Reprodutibilidade: Quão difícil é a execução?

- Alto (3) - O ataque pode ser sempre reproduzido e/ou pode ser reproduzido com facilidade;
- Médio (2) – O ataque só pode ser reproduzido com uma janela de tempo específica e/ou com uma condição particular;
- Baixa (1) – O ataque é extremamente difícil de ser reproduzido, mesmo com amplo conhecimento em segurança.

Explorabilidade: O quão fácil é reproduzir o ataque?

- Alta (3) – Um programador inexperiente pode realizar um ataque em pouco tempo;
- Médio (2) – Um programador experiente pode realizar o ataque;
- Baixo (1) – O ataque requer uma pessoa extremamente capacitada para realizar o ataque.

Usuários afetados: Quantas pessoas provavelmente seriam afetadas?

- Alta (3) – Todos os usuários, configuração padrão e principais clientes são afetados;
- Média (2) – Alguns usuários e configuração não padrão são afetados;
- Baixa (1) – Pequena porcentagem dos usuários são afetados.

Descoberta: Quão difícil é encontrar a vulnerabilidade?

- Alta (3) – A vulnerabilidade é facilmente notável e fontes públicas explicam os meios de ataque;
- Média (2) – A vulnerabilidade está contida em uma funcionalidade pouco acessível do sistema e requer bastante análise para que seja encontrada;
- Baixa (1) – O bug que viabiliza a vulnerabilidade é obscuro, é altamente improvável que os usuários descubram potenciais danos.

Para a classificação de cada ameaça, foi utilizado o método DREAD, conforme mostrado no Quadro 4:

Quadro 4: Análise das ameaças de segurança utilizando o método DREAD

	Dano	Reprodutibilidade	Explorabilidade	Usuários afetados	Descoberta
1. Acesso a sites ou sistemas não autorizados pela empresa;	Alta	Alta	Alta	Alta	Alta
2. Acesso indevido ao dispositivo utilizando conta externa ou de terceiros;	Alta	Baixa	Baixa	Baixa	Baixa
3. Alteração de informações na rede empresarial;	Alta	Alta	Baixa	Média	Baixa
4. Compartilhamento do login empresarial;	Alta	Alta	Alta	Baixa	Alta
5. Divulgação ou perda de conteúdo empresarial;	Alta	Alta	Alta	Média	Alta
6. Falta de proteção física ao conteúdo do HD,	Alta	Alta	Alta	Baixa	Alta
7. Instalação de programa que sobrecarrega o sistema;	Média	Média	Baixa	Baixa	Baixa
8. Instalação de programas não autorizados pela empresa;	Alta	Alta	Alta	Baixa	Alta
9. Instalação de software que sobrecarrega a rede empresarial;	Alta	Baixa	Baixa	Alta	Alta
10. Perda de informações empresariais em caso de desastres;	Média	Média	Baixa	Baixa	Baixa
11. Programas desatualizados;	Alta	Alta	Alta	Alta	Média
12. Proteção do ativo, contra ameaças virtuais;	Alta	Alta	Alta	Alta	Alta
13. Utilização de login pessoal em programas da empresa;	Baixo	Alta	Baixa	Alta	Média
14. Utilização de pen drive para gravação de arquivos;	Alta	Alta	Alta	Alta	Alta

Fonte: Resultado da pesquisa.

4.3.4. Avaliar ameaça de segurança

Após avaliação de cada item utilizando o método DREAD, foi possível avaliar o grau de perigo de cada ameaça encontrada, conforme mostra a Tabela 2:

Tabela 2: Pontuação DREAD

	Pontuação DREAD
1. Acesso a sites ou sistemas não autorizados pela empresa;	3
12. Proteção do ativo, contra ameaças virtuais;	3
14. Utilização de pen drive para gravação de arquivos;	3
5. Divulgação ou perda de conteúdo empresarial;	2,8
11. Programas desatualizados;	2,8

4. Compartilhamento do login empresarial;	2,6
6. Falta de proteção física ao conteúdo do HD;	2,6
8. Instalação de programas não autorizados pela empresa;	2,6
9. Instalação de software que sobrecarrega a rede empresarial;	2,2
3. Alteração de informações na rede empresarial;	2
13. Utilização de login pessoal em programas da empresa;	1,8
2. Acesso indevido ao dispositivo utilizando conta externa ou de terceiros;	1,4
7. Instalação de programa que sobrecarrega o sistema;	1,4
10. Perda de informações empresariais em caso de desastres;	1,4

Fonte: Resultado da pesquisa.

Pode-se definir uma pontuação mínima, por exemplo 2, para que as ameaças encontradas acima desta pontuação sejam tratadas. Para este trabalho, segue-se com a sugestão de mitigação para todas as ameaças encontradas.

4.3.5. Tratar ameaça de segurança

Após verificação das ameaças apresentadas pelo sistema. Cada ameaça possui sua particularidade, logo, algumas poderão apresentar o mesmo tratamento para correção ou um tratamento singular, faz-se necessário prescrever um plano de remediação para cada ameaça encontrada:

1. Acesso a sites ou sistemas não autorizados pela empresa;

- Recomenda-se a instalação de *proxy* nos computadores empresariais e a utilização de *firewall*, para limitar o acesso a sites e sistemas indevidos. O bloqueio a sites indesejáveis também pode ser realizado por um aplicativo antivírus que suporte realizar esse bloqueio.

2. Acesso indevido ao dispositivo utilizando conta externa ou de terceiros;

- Pode-se aplicar restrição para login de domínio, impedindo assim que contas locais ou de outras empresas consigam acessar o computador. Pode-se também limitar o acesso de login ao computador para usuários nominais e restringir horários para permissão de login, fazendo assim com que usuários do mesmo domínio consigam *logar* apenas no horário e no computador designado para eles.

3. Alteração de informações na rede empresarial;

- Sugere-se a restrição de escrita para a maioria dos profissionais da empresa em drivers de redes ou sistemas críticos. Pode-se restringir o acesso de leitura e escrita

de cada profissional conforme suas necessidades para a realização de suas funções na empresa.

4. Compartilhamento do login empresarial;

- Recomenda-se a utilização de autenticação de duplo fator e a utilização de logs do sistema, para monitoramento de login em todos os dispositivos. Essa implantação também poderá evitar que o acesso ao e-mail empresarial por outros dispositivos seja realizado sem a ciência e permissão do usuário. Em alguns autenticadores, há a opção de denunciar tentativas de logins, melhorando ainda mais a segurança, caso a opção seja utilizada.

5. Divulgação ou perda de conteúdo empresarial;

- Recomenda-se a utilização de um software para concentrar os arquivos empresariais criados pelos profissionais, um programa para gestão eletrônica de documentos por exemplo, evitando assim que informações importantes estejam salvas apenas localmente em seu computador.

6. Falta de proteção física ao conteúdo do HD;

- Sugere-se a utilização de programas de encriptação, por exemplo a própria solução do Windows para encriptação, bitlocker, para evitar que informações sejam acessadas por terceiros. Recomenda-se também a utilização de senha para o acesso a BIOS do equipamento, dificultando alterações indesejadas na inicialização do sistema. Pode-se também limitar o acesso de login ao computador para usuários nominais, fazendo assim com que usuários do mesmo domínio consigam *logar* apenas no computador designado para eles.

7. Instalação de programa que sobrecarrega o sistema;

- Recomenda-se a utilização de restrição de instalação de softwares, o UAC do Windows pode auxiliar nesta tarefa, fazendo com que seja necessária uma conta administradora para a instalação de programas.

8. Instalação de programas não autorizados pela empresa;

- Recomenda-se a utilização de restrição de instalação de softwares, o UAC do Windows pode auxiliar nesta tarefa, fazendo com que seja necessária uma conta administradora para a instalação de programas.

9. Instalação de software que sobrecarrega a rede empresarial;

- Recomenda-se a utilização de restrição de instalação de softwares, o UAC do Windows pode auxiliar nesta tarefa, fazendo com que seja necessária uma conta administradora para a instalação de programas.

10. Perda de informações empresariais em caso de desastres;

- Recomenda-se a utilização de um software para concentrar os arquivos empresariais criados pelos profissionais, um programa para gestão eletrônica de documentos por exemplo, evitando assim que informações importantes estejam salvas apenas localmente em seu computador.

11. Programas desatualizados;

- Faz-se necessário verificar e aplicar a atualização para o Sistema Operacional. Este item pode apresentar dificuldade pois recomenda-se que programas sejam homologados antes de serem implantados no ambiente. Em caso de incompatibilidade, o Sistema Operacional pode apresentar mal funcionamento ou novas ameaças devido incompatibilidade com outros programas.

12. Proteção do ativo, contra ameaças virtuais;

- Sugere-se a utilização de um programa antivírus para proteção do Sistema Operacional, pode-se considerar a utilização do próprio antivírus do Sistema Operacional, Microsoft Defender no caso do Windows, mas recomenda-se um antivírus com mais funções de proteção.

13. Utilização de login pessoal em programas da empresa;

- Pode-se aplicar restrição para login de domínio, impedindo assim que contas locais ou de outras empresas consigam acessar o computador. Para acesso a outros programas, recomenda-se que seja criado um bloqueio para este sistema em específico, permitindo apenas o domínio da empresa, evitando que o usuário consiga *logar* em outros programas utilizando logins pessoais ou de outras empresas.

14. Utilização de pen drive para gravação de arquivos;

- Para o bloqueio de transmissão de arquivos, deve-se utilizar uma regra configurável no computador para bloqueio do USB para leitura e escrita, assim como o bloqueio de transmissão de dados via Bluetooth.

Após a análise no ambiente, foi feito um confronto entre os indicadores apresentados na ISO/IEC 27002 e STRIDE, para melhor entendimento sobre as ameaças encontradas, conforme mostrado no Apêndice H.

4.3.6. Comunicação do resultado do tratamento da ameaça de segurança

Após a coleta das ameaças e suas possíveis soluções, o setor responsável pela segurança do ambiente e gestores responsáveis pela segurança foram alertados, assim como a sugestão de suas remediações, apresentadas.

Devido a empresa utilizar um sistema para padronização da imagem do Sistema Operacional, todos os itens, exceto o item 11, puderam ser aplicados diretamente na imagem do sistema operacional, fazendo com que os bloqueios existam ao serem entregues aos usuários, sem a necessidade de configuração manual em cada dispositivo.

4.3.7. Monitorar a solução adotada

Para o item 11, não era possível prescrever uma possível solução automática ou existente no mercado devido a necessidade de gestão e homologação das atualizações providas pelos fabricantes antes da replicação ao ambiente empresarial. Devido a esta limitação, foi adotado o sistema proposto na etapa de *Design* e Desenvolvimento para auxílio no controle de homologação das atualizações do sistema operacional.

Para acesso e utilização do sistema de Controle de Software, foi elaborado um passo a passo disponibilizado para as equipes que utilizarão o sistema. O passo a passo está presente no Apêndice I.

4.3.8. Aprendizagem

Pode-se citar como aprendizado a conscientização da equipe em relação a importância da segurança do ambiente e a extensão da aplicação do método para outros softwares . O artefato incentivou a utilização e agregação ao objetivo apresentado na equipe operacional, que manifesta planos de utilização do artefato, mesmo nesta fase embrionária, conforme mostra evidência no Apêndice N, relacionado a periodicidade no sistema para futuras atualizações e ampliação da utilização do sistema abordando outros softwares. Devido a necessidade de reaplicação do método para evidenciar outras melhorias, não foi possível coletar mais evidências concretas até o momento da finalização desta dissertação.

4.4. Etapa de Avaliação

Nesta etapa, deve-se comparar os resultados obtidos com os requisitos definidos na segunda etapa do método. A avaliação da solução tem o propósito de definir quão bem a solução

atendeu, auxiliou e auxiliará no controle de ameaças presentes e futuras, relacionadas a computadores empresariais.

Observar e medir quão bem o artefato suporta uma solução para o problema. Esta atividade envolve a comparação dos objetivos de uma solução com os resultados reais observados do uso do artefato na demonstração. Requer conhecimento de métricas relevantes e técnicas de análise (PEFFERS et al., 2007).

Dependendo da natureza do local do problema e do artefato, a avaliação pode assumir muitas formas. Pode incluir itens como uma comparação da funcionalidade do artefato com os objetivos da solução da atividade dois acima, medidas de desempenho quantitativas objetivas, como orçamentos ou itens produzidos, resultados de pesquisas de satisfação, feedback de clientes ou simulações. Pode incluir medidas quantificáveis de desempenho do sistema, como tempo de resposta ou disponibilidade. Conceitualmente, tal avaliação pode incluir qualquer evidência empírica apropriada ou prova lógica (HEVNER; CHATTERJEE, 2010).

Conceitualmente, tal avaliação pode incluir qualquer evidência empírica apropriada ou prova lógica. A natureza do local de pesquisa pode ditar se tal iteração é viável ou não (PEFFERS et al., 2007).

A partir da aplicação do método de modelagem de ameaça e sistema proposto, a avaliação foi direcionada para os seguintes grupos:

1. Interna: Utilizadores do método e sistema proposto neste trabalho e gestores;
2. Externa: Especialistas de segurança da informação.

O método contempla entrevistas semiestruturadas com respondentes dos questionários que assim aceitaram participações com as adequadas iterações, para avaliar se o processo possa ser, eventualmente refinado ou reconstruído. As questões da entrevista semiestruturada constam no Apêndice J.

O material apresentado na entrevista foi o mesmo utilizado para ambas as avaliações, internas e externas. Em ambas as reuniões foi explicado o funcionamento dos gatilhos que acionam o envio dos e-mails e o modo como o sistema deve ser operado, conforme foram evidenciados neste trabalho e acordados na reunião 4. O Apêndice K apresenta os slides utilizados na apresentação.

Após a realização do experimento, os participantes responderam a entrevista semiestruturada para avaliar o artefato produzido. Os resultados individuais da entrevista

semiestruturada de avaliação interna estão no Apêndice L e os de avaliação externa no Apêndice M.

Para avaliação interna, foi realizada reuniões individuais com os analistas da equipe operacional e com a equipe de segurança que têm interação com o sistema para apresentar o artefato. A reunião com a equipe de segurança da informação durou 60 minutos e a reunião com o time operacional, 45 minutos.

Na avaliação externa, foram realizadas 4 entrevistas com especialistas em segurança da informação. A reunião com os especialistas durou de 35 minutos a reunião 01 hora 30 minutos.

4.4.1. Avaliação interna

O Quadro 5 apresenta o perfil da formação acadêmica e experiência profissional dos avaliadores internos:

Quadro 5: Perfil da formação acadêmica e experiência profissional

Avaliador	Formação acadêmica	Cargo	Experiência profissional na área de Tecnologia da Informação
Avaliador Interno 1	Análise e Desenvolvimento de Sistemas	Analista Júnior de Atualização e Apoio a Projetos	8 anos de experiência em Service Desk de escritório jurídico, no momento atuando no gerenciamento de softwares do escritório e projetos ligados ao Service Desk.
Avaliador Interno 2	Bacharel em Sistemas de Informação	Analista Pleno de Atualização e Apoio a Projetos	10 anos de experiência profissional na área de TI, passando por áreas técnicas, suporte ao cliente e projetos de TI.
Avaliador Interno 3	Possuo Graduação Tecnológica em Redes de Computadores. Pós-Graduado em CyberSecurity. Possuo certificação Security+ da Comptia Certificado ISO27001, ISO20000 e ITIL pela Exin. Certificado NSE 2 pela Fortinet Segurança Ofensiva pela Rangeforce	Analista Pleno de Segurança da Informação	3 anos na área de segurança da informação
Avaliador Interno 4	Ensino Superior em Ciências da computação	Analista Sênior de ServiceDesk	15 anos na área de ServiceDesk
Avaliador Interno 5	Engenheiro da Computação	Gerente de Operações em tecnologia	20 anos de experiência na área de tecnologia da informação, mais especificamente em infraestrutura.
Avaliador Interno 6	Pós-graduação	Diretor de tecnologia	21 anos de experiência no segmento de tecnologia da informação. Atualmente diretor de tecnologia em empresa de prestação de serviço.

Fonte: Resultado da pesquisa.

Sobre a existência de processos para a segurança virtual e do método de modelagem de ameaça, os resultados médios são apresentados na Tabela 3, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Concordo mais do que discordo; 4 - Concordo plenamente.

Tabela 3: Existência de processos

Existência de processos e utilização do método modelagem de ameaça	Avaliação média
Existência de processos no contexto de proteção e defesa virtual	4
Aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual do ambiente empresarial.	4

Fonte: Resultado da pesquisa.

Sobre a Utilização do método de modelagem de ameaça, os resultados médios são apresentados na Tabela 4, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Concordo mais do que discordo; 4 - Concordo plenamente.

Tabela 4: Utilização do Método modelagem de ameaça

Utilização do método modelagem de ameaça	Avaliação média
Aperfeiçoará a defesa virtual do ambiente empresarial	3,67
Utilização do método de modelagem de ameaça no contexto de proteção e defesa virtual de *endpoints*.	3,83

Fonte: Resultado da pesquisa.

Sobre a criação e utilização de um sistema para controle, os resultados médios são apresentados na Tabela 5, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Concordo mais do que discordo; 4 - Concordo plenamente.

Tabela 5: Viabilidade de um sistema

Sistema	Avaliação Média
Utilização de um sistema para controle de ameaça em softwares.	4

Fonte: Resultado da pesquisa.

Sobre o artefato deste trabalho, o que inclui a utilização do método de modelagem de ameaça e as funcionalidades do sistema proposto, os resultados médios são apresentados na Tabela 6, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Concordo mais do que discordo; 4 - Concordo plenamente.

Tabela 6: Artefato

Artefato	Avaliação média
Considero correto o modo como a aplicação do método de modelagem de ameaça foi aplicado na proteção e defesa virtual de *endpoints*.	3,83
Considero relevante a utilização de gatilhos para alertas relacionados a verificação de novas ameaças	4
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso ao gestor responsável	3,83
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso a equipe de segurança da informação	3,83
Considero relevante a opção de um campo para registro de tratativa de CVEs já existentes.	3,67
Considero relevante o histórico e para evidenciar a tratativa de CVEs já existentes.	4
Considero relevante a possibilidade de análise de histórico de alterações no sistema.	4

Fonte: Resultado da pesquisa.

A equipe de segurança ressaltou que esse sistema auxiliará na gestão de programas, versões, vulnerabilidades e ameaças em nosso ambiente, assim como também contribuirá na coleta de evidências para a ISO 27001. Foi ressaltado como ponto positivo o sistema ser proativo, com um ciclo de vida, realizando a atualização dos programas antes de qualquer incidente, evitando assim que nosso ambiente contenha programas obsoletos que possam conter vulnerabilidades.

A equipe de segurança solicitou acesso ao histórico de alterações do sistema para que possam utilizá-lo para coleta de evidências para a certificação ISO 27001, outras auditorias e possíveis necessidades em relação a verificação de CVE aplicados no ambiente. A possibilidade de verificação se um CVE foi ou não corrigido poderá ser utilizado para mostrar que, antes de sermos afetados, uma vulnerabilidade foi corrigida.

Na reunião com a equipe operacional, a equipe informou que o sistema auxiliará no controle de softwares e versões utilizados no escritório. Devido a grande quantidade de softwares existentes, uma gestão manual de cada software é inviável e não era possível realizar a verificação de versão manualmente. Ressaltaram que a notificação ao responsável para a realização da tarefa e o aviso ao gestor são ponto chaves para a equipe reforçando a necessidade de realização da tarefa. A possibilidade de escolha e controle de datas para verificação evitará que todos os programas possuam a mesma data de verificação, evitando assim acúmulo de tarefas, sendo possível diluir a demanda no decorrer dos dias.

A alta gestão da tecnologia da empresa que avaliou o artefato, o diretor e um gerente de tecnologia, elogiaram o resultado e informaram que esse novo sistema e a aplicação do método poderão auxiliar na defesa cibernética da empresa, sendo considerado desejável a integração desse sistema com outros existentes, como por exemplo, o sistema de Gmud e o sistema de chamados, para maior automação das tarefas. Também citaram a possibilidade de permitir maior autonomia a equipe operacional e maior agilidade no tratamento de ameaças.

4.4.2. Avaliação externa

O Quadro 6 apresenta o perfil da formação acadêmica e experiência profissional dos avaliadores externos:

Quadro 6: Perfil da formação acadêmica e experiência profissional

Avaliador	Formação acadêmica	Cargo	Experiência profissional na área de Tecnologia da Informação
Avaliador Externo 1	Pós-Graduação	Analista Sênior em Segurança da Informação	25 anos em TI e 15 anos em Segurança de Informações
Avaliador Externo 2	Ciências Econômicas, Segurança da Informação	Analista Sênior em Segurança da Informação	Desenvolvimento, suporte, segurança da informação
Avaliador Externo 3	Pós-graduado em Engenharia de Software	*Product Manager* de segurança	Atuo há mais de 20 anos em tecnologia da informação, sendo os últimos 7 anos no segmento bancário com ferramentas de segurança.
Avaliador Externo 4	Pós-graduação em Cyber Security	Analista pleno em segurança	10 anos sendo os últimos 4 em Cyber Segurança

Fonte: Resultado da pesquisa.

Sobre a existência de processos para a segurança virtual e do método de modelagem de ameaça, os resultados médios são apresentados na Tabela 7, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Concordo mais do que discordo; 4 - Concordo plenamente.

Tabela 7: Existência de processos

Existência de processos e utilização do método modelagem de ameaça	Avaliação média
Existência de processos no contexto de proteção e defesa virtual	4
Aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual do ambiente empresarial.	4

Fonte: Resultado da pesquisa.

Sobre a Utilização do método de modelagem de ameaça, os resultados médios são apresentados na Tabela 8, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Concordo mais do que discordo; 4 - Concordo plenamente.

Tabela 8: Utilização do Método modelagem de ameaça

Utilização do método modelagem de ameaça	Avaliação média
Aperfeiçoará a defesa virtual do ambiente empresarial	4
Utilização do método de modelagem de ameaça no contexto de proteção e defesa virtual de *endpoints*.	4

Fonte: Resultado da pesquisa.

Sobre a utilização de um sistema para controle, os resultados médios são apresentados na Tabela 9, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Concordo mais do que discordo; 4 - Concordo plenamente.

Tabela 9: Viabilidade de um sistema

Sistema	Avaliação Média
Utilização de um sistema para controle de ameaça em softwares.	3,75

Fonte: Resultado da pesquisa.

Sobre o artefato deste trabalho, o que inclui a utilização do método de modelagem de ameaça e as funcionalidades do sistema proposto, os resultados médios são apresentados na Tabela 10, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Concordo mais do que discordo; 4 - Concordo plenamente.

Tabela 10: Artefato

Artefato	Avaliação média
Considero correto o modo como a aplicação do método de modelagem de ameaça foi aplicado na proteção e defesa virtual de *endpoints*.	3,75
Considero relevante a utilização de gatilhos para alertas relacionados a verificação de novas ameaças	3,75
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso ao gestor responsável	3,75
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso a equipe de segurança da informação	4
Considero relevante a opção de um campo para registro de tratativa de CVEs já existentes.	4
Considero relevante o histórico e para evidenciar a tratativa de CVEs já existentes.	4
Considero relevante a possibilidade de análise de histórico de alterações no sistema.	3,75

Fonte: Resultado da pesquisa.

Na entrevista realizada com os especialistas em segurança da informação, foi ressaltado a importância de uma análise voltada para o Sistema Operacional pois, uma vez conseguindo

explorar o Sistema Operacional, já é algo muito crítico, e que houve uma grande mudança na arquitetura de segurança por estarmos remoto.

Foi ressaltado como positivo a utilização do método STRIDE com DREAD e normas ISO com NIST, e a facilidade em mudar o escopo da análise, podendo aplicar o método em outros focos. Como a modelagem de ameaça foi feito a partir do zero, foi correto considerar e evidenciar todos os cenários possíveis.

Os gatilhos para aviso a equipe de segurança e ao gestor foram considerados relevantes. O gatilho para a equipe de segurança tornará a tratativa do incidente mais efetivo e o gatilho ao gestor evitará possíveis conflitos entre equipes. Um dos especialistas citou que na empresa em que atua, trabalham com um dono para cada vulnerabilidade, exatamente para evitar conflitos internos.

No ponto relacionado a verificação de ameaças e vulnerabilidades, informaram que, na realidade não é possível atacar todas as ameaças ou implementar todas as correções devido ao volume de vulnerabilidades críticas que aparecem, inclusive já partem do princípio de que, vulnerabilidade média e baixa, não são avaliadas ou tratadas. Ressaltaram que quanto maior a exposição do *exploit*, normalmente, mais rápido será a criação de um patch de segurança.

A utilização de certificado digital, A1 ou A3 por exemplo, foi uma indicação feita por ambos os especialistas, mas o custo para implementação deve ser avaliado pela empresa devido seu potencial de alto custo.

Em instalação de um Sistema Operacional de alto nível, é possível escolher a personalização do menu e bloqueio de teclas de atalho, fazendo com que seja possível customizar o que aparece para o usuário e restringir acesso a programas indesejáveis, como exemplo citado pelo especialista, a restrição do programa *notepad*, mas restrição de software sugerida na modelagem de ameaça já é um nível de proteção interessante.

Em empresas de grande porte, pode-se também bloquear ameaças utilizando um firewall específico por aplicação para bloquear ameaças especificas, que foram reportadas pelo fornecedor por exemplo, mesmo que ainda não exista um patch disponível. O monitoramento do que é trafegado ou digitado em cada máquina pode ser aplicado, por exemplo, em uma empresa bancária onde um profissional tem acesso a uma base de dados que tenha valores de conta ou dados pessoais muito crítico, essa máquina precisa ser monitorada muito severamente, até ao ponto de existir a possibilidade de conseguir capturar telas do computador ao ser mencionado alguma palavra-chave que está na lista de monitoração. Há monitoramentos mais

severos que também analisam o comportamento ou a troca de mensagens de voz, mas isso dependerá do contexto, valor da informação e o ramo da empresa. O custo da implementação dessas soluções deve ser levado em consideração.

O sistema apresentado, por se basear em um ciclo de melhoria contínua que requer verificações constantes, faz com que o produto analisado avance em sua maturidade gradativamente, o sistema está bem focado na atualização de software. Tem um viés de verificação de ameaça no CVE e na modelagem de ameaça e permite a verificação de novas tecnologias necessárias para a proteção da empresa.

A simplicidade do sistema foi considerada positiva, por mais que seja simples, a segurança está mais relacionada ao método e ao modelo do que ao software em si. O software é um *commodity*, a questão é resolver a necessidade do usuário/negócio com o mínimo de custo possível e de forma mais eficiente. O necessário é saber como mitigar risco, reduzir risco de invasão, fraude, acesso indevido, a aplicação do método, e o sistema proposto aplicado ao mercado, com um pouco de ousadia, usará os mesmos conceitos.

O método DREAD foi utilizado para a classificação do risco apresentado pela ameaça, foi sugerido a aplicação de uma matriz de risco, para melhor visualização da criticidade da ameaça para a alta gestão, devido a utilização de cores que representam se uma ameaça foi classificada como alta, média ou baixa.

Reforçaram que sempre deve-se avaliar o equilíbrio entre a usabilidade do usuário e as medidas de segurança, cada empresa precisará decidir o quão seguro precisa ser, pois provavelmente será necessário um aumento no quadro de pessoas da equipe do suporte e podem ocorrer desgastes com usuários. É necessário avaliar todas essas questões e o quanto cada controle poderá trazer de benefício, há sempre uma balança entre o desgaste a usabilidade do usuário e o controle de segurança. Também sugeriram um novo setor na área de arquitetura e padrões, chamada de gestão de infraestrutura, para cuidar e gerenciar todas as atualizações existentes, uma área central não subordinada aos outros setores de tecnologia.

Políticas de segurança podem auxiliar na conscientização dos usuários, para que sigam normas de segurança e ressaltaram a necessidade de responsabilização, pois os usuários sabem que há ações que ele não pode fazer, de acordo com as políticas de segurança da informação definidas. Mas para que seja efetivo, precisa de auxílio e apoio da alta gestão da empresa.

Esse tipo de trabalho acaba auxiliando o entendimento básico de quem não é de segurança, para mostrar o que a equipe de segurança enfrenta: mostra a importância de se

utilizar o duplo fator, tomar cuidado com os arquivos, pensar em algo que pode acontecer, como por exemplo, crash de HD, se a nuvem é segura, onde está sendo feito o backup, mostrando o dia a dia de segurança.

4.5. Comunicação

Peffers et al. (2006) discutem o artefato sob o prisma da novidade, do rigor de seu *design* e da sua eficácia, para comunicar aos públicos relevantes e pesquisadores, como exemplo, profissionais em exercício relacionado ao objeto do artefato, quando apropriado, possam usar a estrutura do estudo na DSRM para novas pesquisas e/ou desenvolverem novos estudos, sem, no entanto, ter a necessidade de seguir em ordem sequencial as etapas descritas na metodologia.

Comunicar o problema e sua importância, o artefato, sua utilidade e novidade, o rigor de seu *design* e sua eficácia para pesquisadores e outros públicos relevantes, como profissionais atuantes, quando apropriado. Em publicações de pesquisa acadêmica, os pesquisadores podem usar a estrutura desse processo para estruturar o artigo, assim como a estrutura nominal de um processo de pesquisa empírica (definição do problema, revisão da literatura, desenvolvimento de hipóteses, coleta de dados, análise, resultados, discussão e conclusão) é uma estrutura comum para trabalhos de pesquisa empírica (HEVNER; CHATTERJEE, 2010).

A comunicação sobre o artefato iniciou-se com a divulgação da análise textual e bibliométrica sobre modelagem de ameaça nos anais do SIMPEP XXVII, posteriormente sendo aceito para publicação na revista *brazilian journal of development*. A modelagem de ameaça, análise de risco e suas aplicações na literatura foi publicada no periódico *International Journal of Development Research.* A aplicação do método de modelagem de ameaça em um sistema operacional foi divulgada no SIMPEP XXIX.

A publicação do método de modelagem de ameaça está em análise para publicação e a solicitação de patente da solução para assegurar autoria e inovação, com número de processo: BR 102023001943-9 está em processo de análise. Pretende-se continuar o desenvolvimento e aprimoramento do método e do sistema apresentado em futuros estudos.

5. CONCLUSÃO

Esta pesquisa iniciou-se com a questão de pesquisa: “Como o método de modelagem de ameaça pode ser aplicado utilizando normas de gestão de risco, com o apoio de um sistema para controle e identificação de riscos de segurança e vulnerabilidades?”. Deste modo, foi realizada pesquisas bibliométricas em busca de achados sobre o tema nas bases de dados cientificas.

Em sua fundação teórica foi apresentado o escopo sobre o tema investigado, incluindo fundamentos relacionados à Gestão de risco e modelagem de ameaça. Na tríade de segurança relacionada a integridade, confidencialidade e disponibilidade, quando executado corretamente, aborda as três tríades garantindo a integridade do ativo, assim como a confidencialidade dos dados tratados pelo ativo e mantendo sua disponibilidade para uso e acesso.

Para a realização da pesquisa, utilizou se uma metodologia baseada no processo DSRM, composto de seis fases de desenvolvimento em conjunto com um elemento da metodologia CAR. O objetivo principal foi desenvolver, adaptar, utilizar e testar processos baseado no método de modelagem de ameaça STRIDE com DREAD, e normas ISO e NIST.

Para mostrar que a solução pode ser utilizada para atingir os objetivos propostos, a abordagem foi aplicada em um projeto real, conforme observado nos capítulos anteriores, o primeiro ciclo de utilização do método de modelagem de ameaça e a utilização do sistema trouxeram alguns benefícios, como a possibilidade de gestão e padronização da versão utilizada para a empresa e, consequentemente, a redução de risco na segurança empresarial. A Modelagem de ameaça é um fluxo contínuo, sendo necessário a realização a cada atualização para verificar possíveis novas ameaças, com um constante aperfeiçoamento e busca por melhorias.

A pesquisa identificou ameaças existentes em um sistema operacional utilizando os métodos STRIDE e DREAD. Verificou-se 14 tipos de ameaças encontradas em um sistema operacional que podem ser devidamente identificadas e mitigadas com a utilização do método de modelagem de ameaça. Entre as 14 ameaças identificadas, 10 estão com pontuação acima de 2 no método STRIDE, apresentando maior risco. Essa classificação das ameaças auxilia na priorização de tratamento das ameaças.

A Padronização e utilização de uma única versão para todos os dispositivos da empresa auxilia na mitigação das ameaças, tornando necessário que os ajustes sejam realizados apenas

uma única vez e replicado para todos os outros computadores. O sistema proposto pode auxiliar no controle de homologação das versões.

O sistema apresentado possui alertas por período customizáveis visando a melhoria contínua do produto, fazendo com que a verificação deixe de ser uma verificação reativa e torne-se uma verificação controlada, assim como gatilhos para alertar gestores e o time de segurança, evidenciando possíveis ameaças em tempo real. O sistema possui histórico de atualizações, possibilitando a análise de alterações no sistema e o processo de homologação individual, possibilita a customização de cada tarefa, incluindo anexos necessários para execução da tarefa. Há também a possibilidade de utilizar o resultado do sistema para amostragem de conformidade em auditorias.

Como resultado dos respondentes dos questionários para a avaliação do artefato, a média do questionário aplicado sobre o método de modelagem proposto e do sistema apresentado ficaram entre 3,67 para internos e 3,75 para externos, de uma pontuação de 1 a 4. As avaliações decorrentes das entrevistas semiestruturadas mostram, de maneira geral, que a aplicação do método de modelagem de ameaça em combinação com o sistema é útil para melhorar a defesa cibernética do ambiente analisado.

As sugestões dos especialistas serão consideradas e são primordiais para fomentar novas ideias ou ajustes em processos na empresa, como por exemplo, a utilização de um Sistema Operacional de alto nível, *firewall* específicos por aplicação e ajuste na política de segurança e conscientização dos usuários. Especialistas também sugeriram a adoção de uma linguagem *open source*, para possibilitar a implantação do sistema proposto em outras empresas.

Como trabalhos futuros, uma verificação com maior abrangência e foco em boas práticas de governança de TI, como ITIL ou COBIT, pode apresentar melhorias ao método aplicado; ambos possuem processos detalhados que tratam de assuntos relacionados à segurança da informação, visando melhorar a disponibilidade, confidencialidade e integridade das informações e poderá adicionar outra tríade que pode ser estudada integralmente: a tríade de pessoas, processos e tecnologia, podendo dar ênfase a pessoas. A pesquisa atual teve como foco apenas os processos que envolvem a atualização de um aplicativo seguido pela tecnologia envolvida nesta atualização, não visando o foco em pessoas. No teor acadêmico, a evolução do método para alcançar o patamar de instanciação ou de um *Design Proposition* deve ser considerado em futuras pesquisas, a etapa de reflexão da Pesquisa-ação canônica e a utilização de outros princípios: o Princípio da Mudança pela Ação e o Princípio da Aprendizagem por Reflexão.

Para a continuidade do presente trabalho, será analisado a necessidade de uma matriz de risco para facilitar a visualização e entendimento do grau da ameaça e a possibilidade de integração com outros sistemas internos, como o sistema de chamados e o sistema de Gmud, para melhor automação das tarefas. Poderão ser adicionados mais programas na lista para serem verificados, atualmente com 16 programas inseridos para a verificação, até a finalização desta etapa da pesquisa. Também será visto a possibilidade de automação do sistema na parte de verificação de ameaça para trabalhos futuros.

Como benefícios futuros, pode-se citar a possibilidade de envolvimento de outras áreas para a aplicação do método de modelagem de ameaça e controle da versão de softwares em outros dispositivos, como servidores, e a possibilidade de alteração ou criação de um sistema similar utilizando os gatilhos que foram criados para esta pesquisa.

REFERÊNCIAS

ABBAS, Syed Ghazanfar et al. **Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach**. Sensors, v. 21, n. 14, p. 4816, 2021.

ABOMHARA, Mohamed; GERDES, Martin; KØIEN, Geir M. **A stride-based threat model for telehealth systems**. Norsk informasjonssikkerhetskonferanse (NISK), v. 8, n. 1, p. 82-96, 2015.

AGENCIABRASIL. **Home office foi adotado por 46% das empresas durante a pandemia. 2020**, Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2020-07/home-office-foi-adotado-por-46-das-empresas-durante-pandemia, acessado em 17/04/22

AGRAWAL, Vivek. **A framework for the information classification in ISO 27005 standard**. In: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). IEEE, 2017. p. 264-269, 2017.

AHMAD, Atif et al. **Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack**. Computers & Security, v. 86, p. 402-418, 2019.

AL FIKRI, Muhamad et al. **Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency**. Procedia Computer Science, v. 161, p. 1206-1215, 2019.

ALHEBAISHI, Nawaf et al. **Threat modeling for cloud data center infrastructures.** International symposium on foundations and practice of security. Springer, Cham, 2016. p. 302-319, 2016.

ALMOHRI, Hussain et al. **On threat modeling and mitigation of medical cyber-physical systems**. In: 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE). IEEE, 2017. p. 114-119, 2017.

AUFNER, Peter. **The IoT security gap: a look down into the valley between threat models and their implementation.** International Journal of Information Security, v. 19, n. 1, p. 3-14, 2020.

BABAR, Sachin et al. **Proposed security model and threat taxonomy for the Internet of Things (IoT).** International Conference on Network Security and Applications. Springer, Berlin, Heidelberg, p. 420-429. 2010.

BODEAU, Deborah J.; MCCOLLUM, Catherine D.; FOX, David B. **Cyber threat modeling: Survey, assessment, and representative framework.** MITRE CORP MCLEAN VA MCLEAN, 2018.

CAGNAZZO, Matteo et al. **Threat modeling for mobile health systems**. 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). IEEE, 2018. p. 314-319, 2018.

CANALTECH. **Qual é a importância do ISO 27001 para a segurança das empresas?**, Disponível em: https://canaltech.com.br/mercado/qual-e-a-importancia-do-iso-27001-para-a-seguranca-das-empresas-227725/ acessado em 15/12/22

CASOLA, Valentina et al. **Toward the automation of threat modeling and risk assessment in IoT systems**. Internet of Things, v. 7, p. 100056, 2019.

CAUCHICK-MIGUEL, Paulo Augusto et al. **Metodologia de pesquisa em engenharia de produção e gestão de operações**. Rio de Janeiro: Elzevir, 2010.

CHANDRAN, Saranya; HRUDYA, P.; POORNACHANDRAN, Prabaharan. **An efficient classification model for detecting advanced persistent threat.** 2015 international conference on advances in computing, communications and informatics (ICACCI). IEEE, 2015. p. 2001-2009, 2015.

CETIC.BR. **Cresce o uso de Internet durante a pandemia e número de usuários no Brasil chega a 152 milhões, é o que aponta pesquisa do Cetic.br**, 2021, Disponível em: https://cetic.br/pt/noticia/cresce-o-uso-de-internet-durante-a-pandemia-e-numero-de-usuarios-no-brasil-chega-a-152-milhoes-e-o-que-aponta-pesquisa-do-cetic-br/ acessado em 17/04/22

CVE. **Windows 10: CVE security vulnerabilities, versions and detailed reports**, 2022, Disponível em: https://www.cvedetails.com/product/32238/Microsoft-Windows-10.html?vendor_id=26 acessado em 12/12/22

DAVISON, Robert; MARTINSONS, Maris G.; KOCK, Ned. **Principles of canonical action research**. Information systems journal, v. 14, n. 1, p. 65-86, 2004.

DE JESUS, Igor Rosa Dias; COSTA, Helder Gomes. **A Nova Gestão Pública como indutora das atividades de Engenharia de Produção nos órgãos públicos**. Production, [s. l.], v. 24, n. 4, p. 887–897, 2014.

DE, Sanghamitra; BARIK, Mridul Sankar; BANERJEE, Indrajit. **Goal based threat modeling for peer-to-peer cloud**. Procedia Computer Science, v. 89, p. 64-72, 2016.

DRESCH, Aline; LACERDA, Daniel Pacheco; ANTUNES, José Antonio Valle Júnior. **Design Science Research: Método de Pesquisa para Avanço da Ciência e Tecnologia**. Editora Bookman, p. 110-113, 2015.

DRESCH, Aline; LACERDA, Daniel Pacheco; MIGUEL, Paulo Augusto Cauchick. **Uma análise distintiva entre o estudo de caso, a pesquisa-ação e a design science research**. Revista Brasileira de Gestão de Negócios, v. 17, n. 56, p. 1116-1133, 2015.

FIGUEIRA, Pedro Tubío; BRAVO, Cristina López; LÓPEZ, José Luis Rivas. **Improving information security risk analysis by including threat-occurrence predictive models**. Computers & Security, v. 88, p. 101609, 2019.

GORE, Ross; PADILLA, Jose; DIALLO, Saikou. **Markov chain modeling of cyber threats**. The Journal of Defense Modeling and Simulation, v. 14, n. 3, p. 233-244, 2017.

GOSSELS, Jonathan; MACKEY, R**. ISO 2700X: A Cornerstone of True Security**. ISSA Journal, p. 33-35, 2007.

GUPTA, Rajesh et al. **Machine learning models for secure data analytics: A taxonomy and threat model. Computer Communications,** v. 153, p. 406-440, 2020.

HEVNER, A. R. et al. **Design Science in Information Systems Research**. MIS Quarterly, v. 28, n. 1, p. 75 – 105, 2004.

HEVNER, A.; CHATTERJEE, S. **Design Research in Information Systems: Theory and Practice**. New York: Springer, 2010. v. 22. p. 335, 2010.

H-INDEX, **O que é índice h (h index)?** disponível em: http://www.fo.usp.br/sdo/wp-content/uploads/Indice_h2.pdf. Acesso em: 03/06/2021.

HOMOLIAK, Ivan et al. **Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures**. ACM Computing Surveys (CSUR), v. 52, n. 2, p. 1-40, 2019.

HSBS. **4 benefícios proporcionados pelas Normas da Série ISO 27000**, Disponível em: https://www.hsbs.com.br/blog-iso-27000/, acessado em 15/12/22

HUDA, Shamsul et al. **A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system (ICS) networks using deep belief network**. Journal of Parallel and Distributed Computing, v. 120, p. 23-31, 2018.

IPEA: 11% dos trabalhadores fizeram home office ao longo de 2020, 2021, disponível em:https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=38289#

:~:text=Considerando%20a%20aus%C3%AAncia%20de%20perspectiva,da%20Funda%C3%A7%C3%A3o%20Getulio%20Vargas%20%2D%20FGV. Acessado em 17/04/22

ISO/IEC. ISO/IEC 27001: **Information security management systems - Overview and vocabulary**, 2013, disponível em: https://www.abntcatalogo.com.br/. Acessado em: 01/09/2021

ISO/IEC. ISO/IEC 27002: **code of practice for information security management**, 2013, disponível em: https://www.abntcatalogo.com.br/. Acessado em: 01/09/2021

ISO/IEC. ISO/IEC 27005: **Information security risk management**, 2019, disponível em: https://www.abntcatalogo.com.br/. Acessado em: 01/09/2021

JOHNSON, Pontus et al. p**wnpr3d: an attack-graph-driven probabilistic threat-modeling approach**. 11th International Conference on Availability, Reliability and Security (ARES). IEEE, 2016. p. 278-283. 2016.

JOHNSON, Pontus; LAGERSTRÖM, Robert; EKSTEDT, Mathias**. A meta language for threat modeling and attack simulations**. Proceedings of the 13th International Conference on Availability, Reliability and Security. p. 1-8, 2018.

KACHAVE, Deepak et al. **Effect of NBTI stress on DSP cores used in CE devices: threat model and performance estimation**. IET Computers & Digital Techniques, v. 12, n. 6, p. 268-278, 2018.

KALUTARAGE, Harsha Kumara; NGUYEN, Hoang Nga; SHAIKH, Siraj Ahmed. **Towards a threat assessment framework for apps collusion.** Telecommunication Systems, v. 66, n. 3, p. 417-430, 2017.

KANDIAS, Miltiadis et al. **An insider threat prediction model**. International conference on trust, privacy and security in digital business. Springer, Berlin, Heidelberg, p. 26-37, 2010.

KARAHASANOVIC, Adi; KLEBERGER, Pierre; ALMGREN, Magnus. **Adapting threat modeling methods for the automotive industry.** In: Proceedings of the 15th ESCAR Conference. p. 1-10. 2017.

KAZANSKY, Becky. **'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance**. Big Data & Society, v. 8, n. 1, p. 2053951720985557, 2021.

KHAN, Rafiullah et al. **STRIDE-based threat modeling for cyber-physical systems**. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE, p. 1-6, 2017.

KHATTAK, Zubair Ahmad; SULAIMAN, Suziah; AB MANAN, Jamalul-Lail. **A study on threat model for federated identities in federated identity management system**. 2010 International Symposium on Information Technology. IEEE, 2010. p. 618-623, 2010.

KRZYKOWSKA-PIOTROWSKA, Karolina et al. **Is Secure Communication in the R2I (Robot-to-Infrastructure) Model Possible?** Identification of Threats. Energies, v. 14, n. 15, p. 4702, 2021.

LACERDA, Daniel Pacheco et al. **Design Science Research: método de pesquisa para a engenharia de produção**. Gestão & produção, v. 20, n. 4, p. 741-761, 2013.

LALLIE, Harjinder Singh et al. **Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic**. Computers & Security, v. 105, p. 102248, 2021.

LEGG, Philip A. et al. **Towards a conceptual model and reasoning structure for insider threat detection**. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, v. 4, n. 4, p. 20-37, 2013.

LUCKETT, Patrick; MCDONALD, J. Todd; GLISSON, William Bradley. **Attack-graph threat modeling assessment of ambulatory medical devices.** arXiv preprint arXiv:1709.05026, 2017.

MA, Zhendong; SCHMITTNER, Christoph. **Threat modeling for automotive security analysis.** Advanced Science and Technology Letters, v. 139, p. 333-339, 2016.

MADAN, Bharat B.; BANIK, Manoj; BEIN, Doina. **Securing unmanned autonomous systems from cyber threats.** The Journal of Defense Modeling and Simulation, v. 16, n. 2, p. 119-136, 2019.

MANSFIELD, Katrina et al. **Unmanned aerial vehicle smart device ground control station cyber security threat model.** In: 2013 IEEE International Conference on Technologies for Homeland Security (HST). IEEE, p. 722-728, 2013.

MARBACK, Aaron et al. **A threat model-based approach to security testing**. Software: Practice and Experience, v. 43, n. 2, p. 241-258, 2013.

MARSHALL, Romney; STEINBART, Paul. **Accounting Information Systems 14 edition** P.278, Editora Pearson, 2018.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed.-São Paulo: Atlas, 2003.

MAVROEIDIS, Vasileios; BROMANDER, Siri. **Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence**. In: 2017 European Intelligence and Security Informatics Conference (EISIC). IEEE, p. 91-98, 2017.

MEYER, Dominik et al. **A threat-model for building and home automation.** 2016 IEEE 14th international conference on industrial informatics (INDIN). IEEE, p. 860-866, 2016.

MIGUEL, Paulo Augusto Cauchick. **Estudo de caso na engenharia de produção: estruturação e recomendações para sua condução**. Production, v. 17, p. 216-229, 2007.

MITRE CVE SEARCH LIST, Disponível em: https://cve.mitre.org/cve/search_cve_list.html acessado em 14/04/2022

MOSKAL, Stephen; YANG, Shanchieh Jay; KUHL, Michael E. **Cyber threat assessment via attack scenario simulation using an integrated adversary and network modeling approach.** The Journal of Defense Modeling and Simulation, v. 15, n. 1, p. 13-29, 2018.

NIST 800-30 - **Guide for Conducting Risk Assessments**, 2012, Disponível em: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final acessado em 07/05/22

NOVAES NETO, Nelson et al. **Developing a global data breach database and the challenges encountered.** Journal of Data and Information Quality (JDIQ), v. 13, n. 1, p. 1-33, 2021.

NOVOKHRESTOV, Aleksey; KONEV, Anton; SHELUPANOV, Alexander. **Model of threats to computer network software.** Symmetry, v. 11, n. 12, p. 1506, 2019.

OLIVO, Cleber K.; SANTIN, Altair O.; OLIVEIRA, Luiz S. **Obtaining the threat model for e-mail phishing.** Applied soft computing, v. 13, n. 12, p. 4841-4848, 2013.

PAN, Jiaye; ZHUANG, Yi. **PMCAP: a threat model of process memory data on the windows operating system**. Security and Communication Networks, v. 2017, 2017.

PAVLÍK, Lukáš. **Possibilities of modelling the impact of cyber threats in cyber risk insurance**. MATEC Web of Conferences. EDP Sciences, 2018.

PEFFERS, Ken. et al. **The design science research process: A model for producing and presenting information systems research**. DESRIST 2006, Claremont, p. 83 – 106, 2006. _____. **Design science research in information systems: advances in theory and practice.** 1st edition. Berlin: Springer, 2012. P. 438, 2012

POTTEIGER, Bradley; MARTINS, Goncalo; KOUTSOUKOS, Xenofon. **Software and attack centric integrated threat modeling for quantitative risk assessment**. Proceedings of the Symposium and Bootcamp on the Science of Security. p. 99-108, 2016.

RABII, Anass et al. **Information and cyber security maturity models: a systematic literature review.** Information & Computer Security, 2020.

REFSDAL, Atle et al. **Cyber-risk management**. Springer International Publishing, 2015.

SALAMH, Fahad E.; KARABIYIK, Umit; ROGERS, Marcus. **A constructive direst security threat modeling for drone as a service.** Journal of Digital Forensics, Security and Law, v. 16, n. 1, p. 2, 2021.

SCANDARIATO, Riccardo; WUYTS, Kim; JOOSEN, Wouter. **A descriptive study of Microsoft's threat modeling technique. Requirements Engineering,** v. 20, n. 2, p. 163-180, 2015.

SEIFERT, Darren; REZA, Hassan. **A security analysis of cyber-physical systems architecture for healthcare**. Computers, v. 5, n. 4, p. 27, 2016.

SHEVCHENKO, Nataliya et al. **Threat modeling: a summary of available methods.** Carnegie Mellon University Software Engineering Institute Pittsburgh United States, 2018.

SHOSTACK, Adam. **Threat Modeling Designing for Security** P.22 a 25, Editora WILEY, 2014.

SIMONJAN, Jennifer; TAURER, Sebastian; DIEBER, Bernhard. **A generalized threat model for visual sensor networks. Sensors,** v. 20, n. 13, p. 3629, 2020.

SION, Laurens et al. **Solution-aware data flow diagrams for security threat modeling.** Proceedings of the 33rd Annual ACM Symposium on Applied Computing. p. 1425-1432, 2018.

SOKOLOWSKI, John A.; BANKS, Catherine M.; DOVER, Thomas J. **An agent-based approach to modeling insider threat**. Computational and Mathematical Organization Theory, v. 22, n. 3, p. 273-287, 2016.

STEINGARTNER, William; GALINEC, Darko; KOZINA, Andrija. **Threat defense: Cyber deception approach and education for resilience in hybrid threats model**. Symmetry, v. 13, n. 4, p. 597, 2021.

STEVENS, Rock et al. **The battle for new york: a case study of applied digital threat modeling at the enterprise level**. In: 27th {USENIX} Security Symposium ({USENIX} Security 18). p. 621-637, 2018.

SULEIMAN, Husam et al. **Integrated smart grid systems security threat model. Information Systems,** v. 53, p. 147-160, 2015.

TORKURA, Kennedy A. et al. **A threat modeling approach for cloud storage brokerage and file sharing systems.** NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. IEEE, p. 1-5, 2018.

TSOHOU, Aggeliki; HOLTKAMP, Philipp. **Are users competent to comply with information security policies? An analysis of professional competence models**. Information Technology & People, 2018.

UCEDAVÉLEZ, Tony; MORANA, Marco M. **Risk Centric Threat Modeling: process for attack simulation and threat analysis**. John Wiley & Sons, 2015.

VÄLJA, Margus et al. **Automating threat modeling using an ontology framework.** Cybersecurity, v. 3, n. 1, p. 1-20, 2020.

VALLANT, Heribert et al. **Threat Modelling and Beyond-Novel Approaches to Cyber Secure the Smart Energy System**. Applied Sciences, v. 11, n. 11, p. 5149, 2021.

VOCESA, **Vazamentos de dados aumentaram 493% no Brasil, segundo pesquisa do MIT**, 2021, disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit/ acessado em 17/04/22

WU, Zehui; WEI, Qiang. **Quantitative analysis of the security of software-defined network controller using threat/effort model.** Mathematical Problems in Engineering, v. 2017, 2017.

XIONG, Wenjun; LAGERSTRÖM, Robert. **Threat modeling–A systematic literature review**. Computers & security, v. 84, p. 53-69, 2019.

YEBOAH-OFORI, Abel; ISLAM, Shareeful. **Cyber security threat modeling for supply chain organizational environments.** Future Internet, v. 11, n. 3, p. 63, 2019.

YOKOYAMA, Rodrigo, ARIMA Carlos H. **Análise textual e bibliométrica sobre modelagem de ameaça / Textual and bibliometric analysis on threat modeling** Brazilian Journal of Development Vol. 8 No 1 p. 7678-7690, 2022.

_____. **Modelagem de ameaça, análise de risco e suas aplicações na literatura**, International Journal of Development Research, 12, (04), P. 55049-55055, 2022.

ZAEEM, Razieh Nokhbeh et al. **Modeling and analysis of identity threat behaviors through text mining of identity theft stories**. Computers & Security, v. 65, p. 50-63, 2017.

ZIMBA, Aaron et al. **Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics**. Future Generation Computer Systems, v. 106, p. 501-517, 2020.

ZOGRAFOPOULOS, Ioannis et al. **Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies**. IEEE Access, v. 9, p. 29775-29818, 2021.

APÊNDICE A – IDENTIFICAÇÃO DO MÉTODO MODELAGEM DE AMEAÇA

Realizou-se em junho de 2021 um levantamento bibliométrico utilizando o programa "Publish or Perish v7", com os parâmetros abaixo:

No título, as palavras chaves *threat* e *model* foram inseridas, como outras palavras chaves, foram utilizadas *System*, *Security*, *Data* e *Attack*. Utilizando-se and entre as palavras chaves. As bases de dados utilizadas foram: Google Scholar, Microsoft Academic e Scopus. Buscou-se publicações no período de 2010 a 2020, que fossem artigos de congressos, dissertações ou teses e que estivessem no idioma inglês ou português, totalizando 391 registros.

Na primeira triagem, foi utilizado a medição baseada em H-Index (H-INDEX, 2021), onde apenas documentos que são considerados relevantes e possuem certa quantidade de citações são categorizados como H-Index. Nesta triagem, foram removidos 348 registros, totalizando 43 registros para verificação.

Foram removidos registros idênticos que apareciam na busca realizada em base de dados diferentes, realizando-se a exclusão de 2 registros. Ao tentar acessar os 41 registros restantes, notou-se que 15 não estavam acessíveis, sendo assim, removidos, totalizando 24 registros para serem verificados.

Com acesso aos 24 artigos, fez-se a verificação se os registros eram relacionados a área de interesse e se poderiam contribuir, de alguma forma, em um dos seguintes parâmetros: conceito teórico, metodologia de pesquisa, relação com o problema pesquisa, resultados e conclusão. Após essa verificação, notou-se que 11 registros não estavam relacionados ao tema, sendo removidos, totalizando 15 registros válidos para análise. (YOKOYAMA, ARIMA, 2022).

APÊNDICE B – IDENTIFICAÇÃO DO MÉTODO MODELAGEM DE AMEAÇA MAIS UTILIZADO

Em agosto de 2021 realizou-se o segundo levantamento bibliométrico utilizando o programa “Publish or Perish v7”, com os parâmetros apresentados na sequência:

No título, as palavras *Threat Modeling* foram inseridas. Como palavras chaves, foram utilizadas as palavras *System*, *Security*, *Data* e *Attack*. Utilizando-se *and* entre as palavras chaves. As *databases* utilizadas foram: Google Scholar, Microsoft *Academic* e Scopus. Registros publicados entre 2016 e 2021, que estivessem disponíveis no idioma inglês ou português. Totalizando 285 registros encontrados.

Na etapa de triagem, foram selecionados artigos de congresso, dissertações ou teses. Realizando a remoção de 2 registros por serem registros de patentes, totalizando 283 registros.

Na próxima triagem, foi utilizado a medição baseada em H-Index (H-Index, 2021), onde apenas documentos que são considerados relevantes e possuem certa quantidade de citações são categorizados como H-Index. Nesta primeira triagem, foram removidos 257 registros. Totalizando 26 registros para verificação após triagem. Não foram encontrados registros idênticos ou repetidos. Ao tentar acessar os 26 registros restantes, notou-se que 3 não estavam acessíveis, sendo removidos. Totalizando 23 registros para serem verificados. Após avaliação dos artigos, foram selecionados todos os 23 artigos para a análise quantitativa e qualitativa. (YOKOYAMA, ARIMA, 2022).

APÊNDICE C – MODELOS EXISTENTES QUE UTILIZAM NORMA

Em abril de 2022 realizou-se o terceiro levantamento bibliométrico utilizando a máquina de busca do site periódicos CAPES.

Inicialmente foram definidos os objetivos da pesquisa, conforme apresentado no Capítulo 1, os quais foram utilizados como fator de inclusão e exclusão dos estudos científicos encontrados. Depois foram definidos os termos de pesquisa, em inglês, bem como a combinação dos termos, aqui chamada de *strings* de busca.

Como sugerido por CAUCHICK-MIGUEL et al. (2018), foi escolhido o uso de termos no idioma inglês devido os metadados comuns aos documentos pesquisados serem em inglês, em especial, os títulos, subtítulos, resumos e palavras-chaves.

Os termos escolhidos para a realização da pesquisa utilizando a máquina de busca do site Periódicos CAPES são apresentados no Quadro seguinte, e é possível observar os dois grupos de associação dos termos, sendo o grupo 1 formado pelos termos sobre modelagem de ameaças e sistemas e o grupo 2 formado pelos termos associados a modelagem de ameaça e normas ISO.

Quadro: Termos utilizados para pesquisa de artigos sobre o tema da pesquisa

Grupo 1	Grupo 2	Grupo 3
Threat Model *Threat Modeling* *Threat Modelling* *System* *identify* *risk* *vulnerability* *control*	*Threat Model* *Threat Modeling* *Threat Modelling* ISO 27000	*Threat Model* *Threat Modeling* *Threat Modelling* NIST 800

Fonte: Resultado da pesquisa.

Foi utilizada a plataforma de pesquisa disponível no site Periódicos CAPES com acesso livre, sem vínculo com instituição de ensino.

Para inclusão dos termos na máquina de pesquisa foram criadas *strings* que agruparam os termos por meio da utilização de operadores booleanos, como é apresentado no Quadro:

Quadro*: String* de busca

STRING 1	*"threat model" and "system" or "identify" or "risk" or "vulnerability" or "control" or "security"*
STRING 2	*"threat modeling" and "system" or "identify" or "risk" or "vulnerability" or "control" or "security"*
STRING 3	*"threat modelling" and "system" or "identify" or "risk" or "vulnerability" or "control" or "security"*

STRING 4	*"threat model" and* "ISO 27000*"*
STRING 5	*"threat modeling" and* "ISO 27000"
STRING 6	*"threat modelling" and* "ISO 27000"
STRING 7	*"threat model" and* "NIST 800"
STRING 8	*"threat modeling" and* "NIST 800"
STRING 9	*"threat modelling" and* "NIST 800"

Fonte: Resultado da pesquisa.

Após a aplicação de cada *string* de buscar na máquina de pesquisa selecionada, foram aplicados filtros disponíveis na plataforma à fim de refinar a pesquisa, tais como apresentado na Tabela.

Tabela: Filtro de refinamento aplicado em cada *string*

String	Refinado por:	Documentos identificados
1	Nível superior: Periódicos revisados por pares Tipo de recurso: Artigo Data de publicação: 2017 até 2021	11
2	Nível superior: Periódicos revisados por pares Tipo de recurso: Artigo Data de publicação: 2017 até 2021	15
3	Nível superior: Periódicos revisados por pares Tipo de recurso: Artigo Data de publicação: 2017 até 2021	15
4	Nível superior: Periódicos revisados por pares Tipo de recurso: Artigo Data de publicação: 2017 até 2021	1
5	Nível superior: Periódicos revisados por pares Tipo de recurso: Artigo Data de publicação: 2017 até 2021	0
6	Nível superior: Periódicos revisados por pares Tipo de recurso: Artigo Data de publicação: 2017 até 2021	0
7	Nível superior: Periódicos revisados por pares Tipo de recurso: Artigo Data de publicação: 2017 até 2021	1
8	Nível superior: Periódicos revisados por pares Tipo de recurso: Artigo Data de publicação: 2017 até 2021	1
9	Nível superior: Periódicos revisados por pares Tipo de recurso: Artigo Data de publicação: 2017 até 2021	1

Fonte: Resultado da pesquisa.

A análise de busca dos termos presentes nas *strings* foi direcionada para o metadado "qualquer campo" de artigos, com exceção das palavras *Threat model, threat modeling e threat modeling* que foram direcionadas para o metadado "título" em todas as buscas. Também foi priorizado artigos revisados por pares, com período de data de publicação de 2017 até 2021.

Estudos duplicados foram excluídos da amostra, bem como artigos que não atendiam o escopo do trabalho. Para a verificar se o artigo atendia ou não ao escopo do trabalho, no primeiro momento foram lidos os títulos e seus resumos e em um segundo momento, os artigos foram

lidos na integra, a fim de identificar a qualidade dos estudos, para então ser realizada a extração de dados dos estudos.

A partir das buscas realizadas nas bases de dados disponíveis na plataforma de pesquisa Periódicos CAPES, com as *strings* descritas, foram retornados 45 artigos, provenientes da busca automática refinada da máquina de pesquisa, a esses artigos foram aplicados critérios de inclusão e exclusão (artigos duplicados, ano de publicação, adequação aos objetivos da dissertação, respostas às questões de pesquisa). Foram identificados 17 artigos duplicados. 5 artigos foram excluídos por estarem fora do tema da dissertação, seguindo para análise do título e do resumo dos 23 artigos.

APÊNDICE D – LISTA DOS ARTIGOS ENCONTRADOS NA BIBLIOMETRIA

Ano	Autores	Título	Assunto
2021	SALAMH, Fahad E.; KARABIYIK, Umit; ROGERS, Marcus.	*A Constructive DIREST Security Threat Modeling for Drone as a Service*	Modelagem de ameaça para recursos de Drone as a Service (DaaS)
2021	ZOGRAFOPOULOS, Ioannis et al.	*Cyber-Physical Energy Systems Security Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies*	Modelagem de ameaça em CPS
2021	ABBAS, Syed Ghazanfar et al.	*Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach*	Modelagem de ameaça em ataques *phishing*
2021	KRZYKOWSKA-PIOTROWSKA, Karolina et al.	*Is Secure Communication in the R2I (Robot-to-Infrastructure) Model Possible Identification of Threats*	Análise de risco em robôs para infraestrutura
2021	KAZANSKY, Becky.	*It depends on your threat model the anticipatory dimensions of resistance to data-driven surveillance*	Estudo relacionado a utilização de modelagem de ameaça e gerenciamento de risco
2021	STEINGARTNER, William; GALINEC, Darko; KOZINA, Andrija	*Threat Defense Cyber Deception Approach and Education for Resilience in Hybrid Threats Model*	Utilização da tecnologia "*Deception*" em modelagem de ameaça hibrida
2021	VALLANT, Heribert et al.	*Threat Modelling and Beyond-Novel Approaches to Cyber Secure the Smart Energy System*	Modelagem de ameaça em sistemas de energia inteligentes
2020	SIMONJAN, Jennifer; TAURER, Sebastian; DIEBER, Bernhard.	*A Generalized Threat Model for Visual Sensor Networks*	Modelagem de ameaças para superfícies de ataque de aplicativos de rede de sensores visuais e seus componentes.
2020	VÄLJA, Margus et al.	*Automating threat modeling using an ontology framework*	Modelagem de ameaça automatizada utilizando ontologia
2020	GUPTA, Rajesh et al.	*Machine Learning Models for Secure Data Analytics: A taxonomy and threat model*	Modelagem de ameaça utilizando *deep learning*
2020	ZIMBA, Aaron et al.	*Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics*	Ameaças relacionadas a APT

2019	YEBOAH-OFORI, Abel; ISLAM, Shareeful.	*Cyber Security Threat Modeling for Supply Chain Organizational Environments*	Modelagem de ameaça para Ambientes Organizacionais da Cadeia de Suprimentos
2019	FIGUEIRA, Pedro Tubío; BRAVO, Cristina López; LÓPEZ, José Luis Rivas.	*Improving information security risk analysis by including threat-occurrence predictive models*	Análise de risco com base em dados históricos
2019	HOMOLIAK, Ivan et al.	*Insight Into Insiders and IT A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures*	*Survey* relacionada a ameaça interna
2019	NOVOKHRESTOV, Aleksey; KONEV, Anton; SHELUPANOV, Alexander.	*Model of Threats to Computer Network Software*	Modelagem de ameaça em rede de computadores
2019	AHMAD, Atif et al.	*Strategically-motivated advanced persistent threat Definition, process, tactics and a disinformation model of counterattack*	Modelagem de ameaça para APT
2019	AUFNER, Peter.	*The IoT security gap a look down into the valley between threat models and their implementation*	Modelagem de ameaça e lacuna existente em relação a IoT
2019	XIONG, Wenjun; LAGERSTRÖM, Robert.	*Threat modeling–A systematic literature review*	Revisão sistemática da literatura
2019	CASOLA, Valentina et al.	*Toward the automation of threat modeling and risk assessment in IoT systems*	Modelagem de ameaça IOT
2018	HUDA, Shamsul et al.	*A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system (ICS) networks using deep belief network*	Modelagem de ameaça utilizando *deep learning*
2018	JOHNSON, Pontus; LAGERSTRÖM, Robert; EKSTEDT, Mathias.	*A meta language for threat modeling and attack simulations*	Modelagem de ameaça visando ataques específicos de domínio.
2018	TORKURA, Kennedy A. et al.	*A threat modeling approach for cloud storage brokerage and file sharing systems*	Modelagem de ameaça para Cloud Broker
2018	MOSKAL, Stephen; YANG, Shanchieh Jay; KUHL, Michael E.	*Cyber threat assessment via attack scenario simulation using an integrated adversary and network modeling approach*	Modelagem de ameaça baseado no comportamento do invasor

2018	BODEAU, Deborah J.; MCCOLLUM, Catherine D.; FOX, David B.	*Cyber threat modeling: Survey, assessment, and representative framework*	Pesquisa sobre modelos de modelagem de ameaça e proposta de novo modelo de modelagem
2018	KACHAVE, Deepak et al.	*Effect of NBTI stress on DSP cores used in CE devices threat model and performance estimation*	Modelagem de ameaça em componentes eletrônicos de temperatura
2018	PAVLÍK, Lukáš.	*Possibilities of modelling the impact of cyber threats in cyber risk insurance*	Modelagem para impacto de ameaça e seguro cibernético
2018	SION, Laurens et al.	*Solution-aware data flow diagrams for security threat modeling*	Modelagem de ameaça em DFD utilizando STRIDE
2018	STEVENS, Rock et al.	*The battle for New York: a case study of applied digital threat modeling at the enterprise level*	*Survey* sobre aplicação de modelagem de ameaça
2018	CAGNAZZO, Matteo et al.	*Threat modeling for mobile health systems*	Modelagem de ameaça em sistemas de monitoramento de saúde
2018	SHEVCHENKO, Nataliya et al.	*Threat modeling: a summary of available methods*	Tipos de modelagem de ameaça
2017	KARAHASANOVIC, Adi; KLEBERGER, Pierre; ALMGREN, Magnus.	*Adapting threat modeling methods for the automotive industry*	Modelagem de ameaça para automotivos
2017	LUCKETT, Patrick; MCDONALD, J. Todd; GLISSON, William Bradley	*Attack-graph threat modeling assessment of ambulatory medical devices*	Modelagem de ameaça em um ambiente fictício de ambulatório
2017	MAVROEIDIS, Vasileios; BROMANDER, Siri.	*Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence*	Modelo de inteligência contra ameaça
2017	GORE, Ross; PADILLA, Jose; DIALLO, Saikou.	*Markov Chain modeling of cyber threats*	Proposta de novo modelo de ameaça
2017	ZAEEM, Razieh Nokhbeh et al.	*Modeling and analysis of identity threat behaviors through text mining of identity theft stories*	Identificação de roubo utilizando data mining

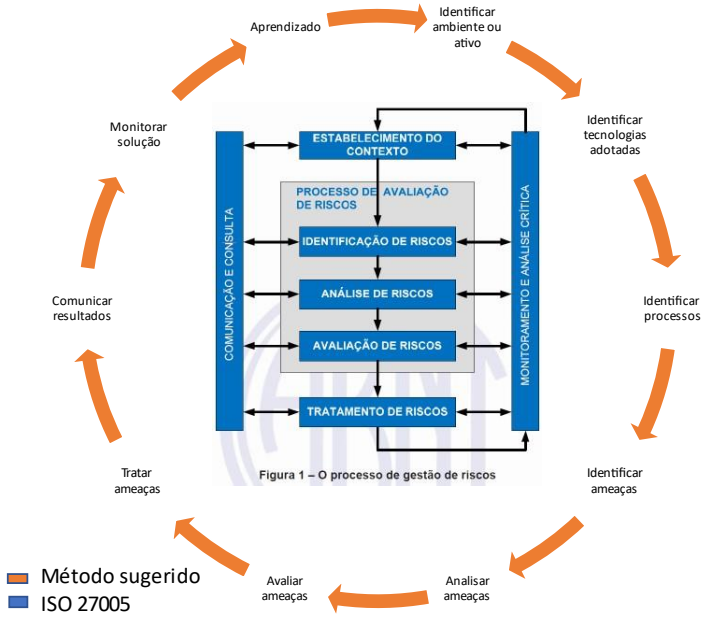
2017	ALMOHRI, Hussain et al.	*On threat modeling and mitigation of medical cyber-physical systems*	Modelagem de ameaça em CPS
2017	PAN, Jiaye; ZHUANG, Yi.	*PMCAP A Threat Model of Process Memory Data on the Windows Operating System*	Proposta de novo modelo de ameaça
2017	WU, Zehui; WEI, Qiang.	*Quantitative Analysis of the Security of Software-Defined Network Controller Using Threat Effort Model*	Modelagem de ameaça em redes definidas por software
2017	KHAN, Rafiullah et al.	*STRIDE-based threat modeling for cyber-physical systems*	STRIDE em CPS
2017	KALUTARAGE, Harsha Kumara; NGUYEN, Hoang Nga; SHAIKH, Siraj Ahmed.	*Towards a threat assessment framework for apps collusion*	Estudo sobre vulnerabilidade relacionada a combinação de multiplicativos em celulares
2016	MEYER, Dominik et al.	*A Threat-Model for Building and Home Automation*	Modelagem de ameaça utilizando arvore de ataque
2016	SOKOLOWSKI, John A.; BANKS, Catherine M.; DOVER, Thomas J.	*An agent-based approach to modeling insider threat*	Modelagem de ameaça para contratados
2016	DE, Sanghamitra; BARIK, Mridul Sankar; BANERJEE, Indrajit.	*Goal Based Threat Modeling for Peer-to-Peer Cloud*	Artigo cita modelagem de ameaça para P2P
2016	JOHNSON, Pontus et al.	*pwnpr3d: an attack-graph-driven probabilistic threat-modeling approach*	Proposta de novo modelo de ameaça
2016	MADAN, Bharat B.; BANIK, Manoj; BEIN, Doina.	*Securing unmanned autonomous systems from cyber threats*	Modelagem de ameaça em sistemas não tripulados
2016	POTTEIGER, Bradley; MARTINS, Goncalo; KOUTSOUKOS, Xenofon.	*Software and attack centric integrated threat modeling for quantitative risk assessment*	Modelagem de ameaça em semáforo

2016	MA, Zhendong; SCHMITTNER, Christoph.	*Threat modeling for automotive security analysis*	Modelagem de ameaça em DFD utilizando STRIDE para automotivos
2016	ALHEBAISHI, Nawaf et al.	*Threat modeling for cloud data center infrastructures*	Modelagem de ameaça para infraestrutura cloud
2015	ABOMHARA, Mohamed; GERDES, Martin; KØIEN, Geir M.	*A STRIDE-Based Threat Model for Telehealth Systems*	Modelagem de ameaça completa para um sistema de *Telehealth*
2015	CHANDRAN, Saranya; HRUDYA, P.; POORNACHANDRAN, Prabaharan.	*An Efficient Classification Model for Detecting Advanced Persistent Threat*	Modelagem de ameaça para APT utilizando floresta randômica
2014	SULEIMAN, Husam et al.	*Integrated smart grid systems security threat model*	Modelagem de ameaça para um centro de energia elétrica que utiliza SCADA
2013	LEGG, Philip A. et al.	*Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection*	Modelagem de ameaça comportamental
2013	MANSFIELD, Katrina et al.	*Unmanned Aerial Vehicle Smart Device Ground Control Station Cyber Security Threat Model*	Modelagem de ameaça para Smartphones
2012	MARBACK, Aaron et al.	*A threat model-based approach to security testing*	Modelagem de ameaça utilizando automação com arvores de ataque
2011	OLIVO, Cleber K.; SANTIN, Altair O.; OLIVEIRA, Luiz S.	*Obtaining the threat model for e-mail phishing*	Modelagem de ameaça para *Phishing*
2010	KHATTAK, Zubair Ahmad; SULAIMAN, Suziah; AB MANAN, Jamalul-Lail.	*A Study on Threat Model for Federated Identities in Federated Identity Management System*	Modelagem de ameaça relacionado a *SingleSignOn*
2010	KANDIAS, Miltiadis et al.	*An Insider Threat Prediction Model*	Modelagem de ameaça comportamental

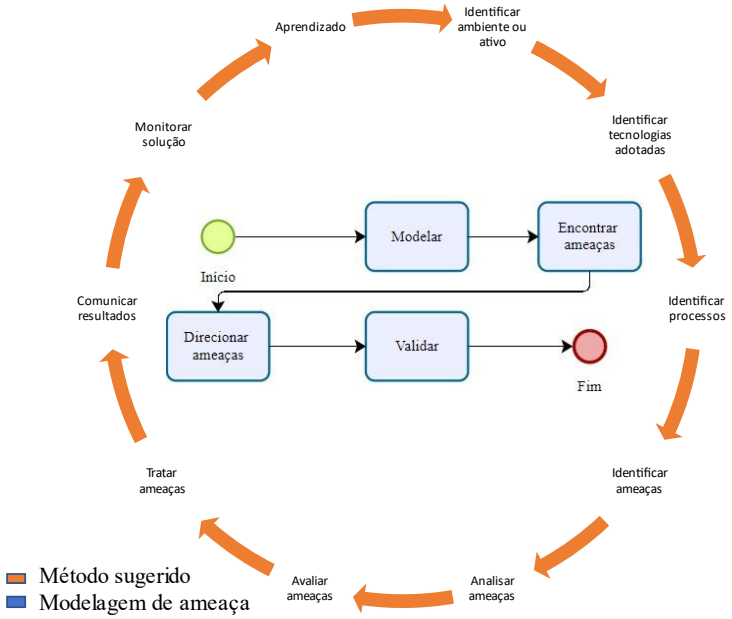
2010	BABAR, Sachin et al.	*Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)*	Modelagem de ameaça para IoT

APÊNDICE E – COMPARAÇÃO DOS FLUXOS DOS PROCESSOS

Método sugerido vs ISO 27005



Método sugerido vs Modelagem de ameaça

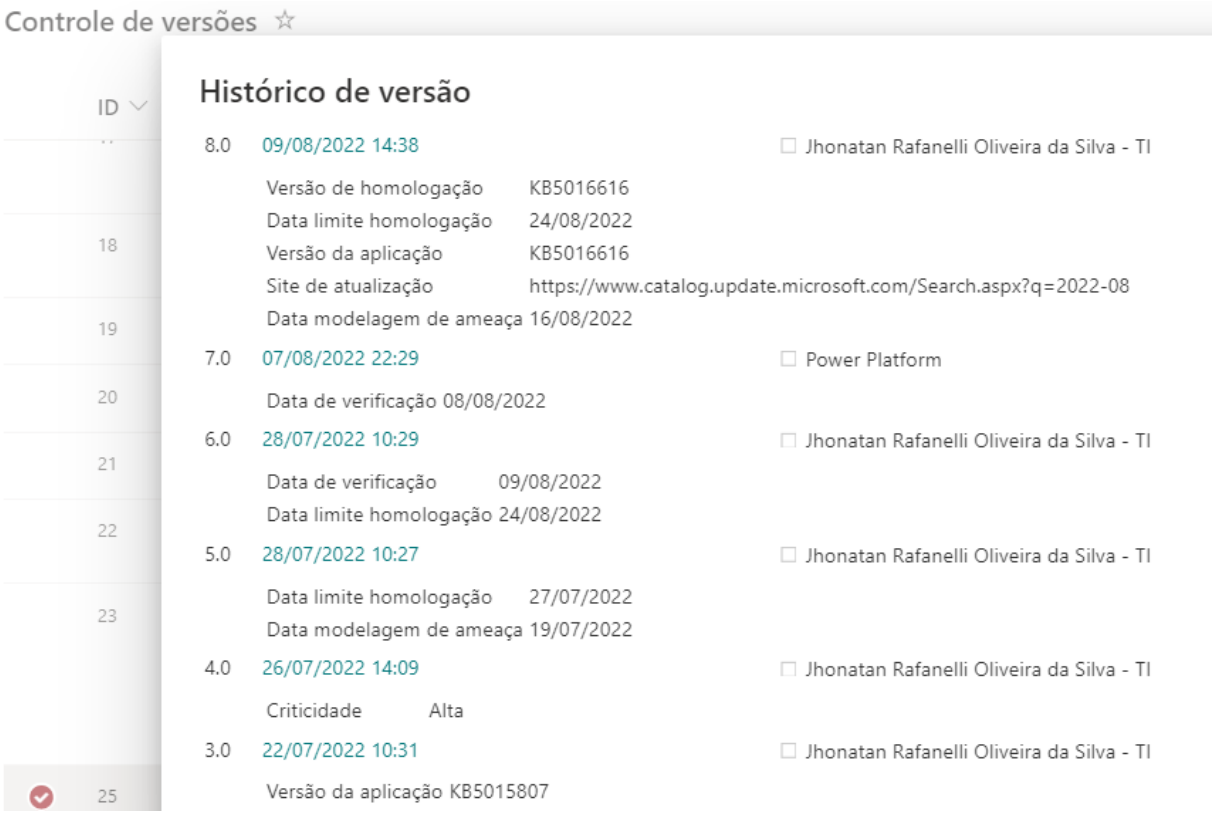


APÊNDICE F – LISTA DE REUNIÕES REALIZADAS PARA CONCEPÇÃO DO SISTEMA

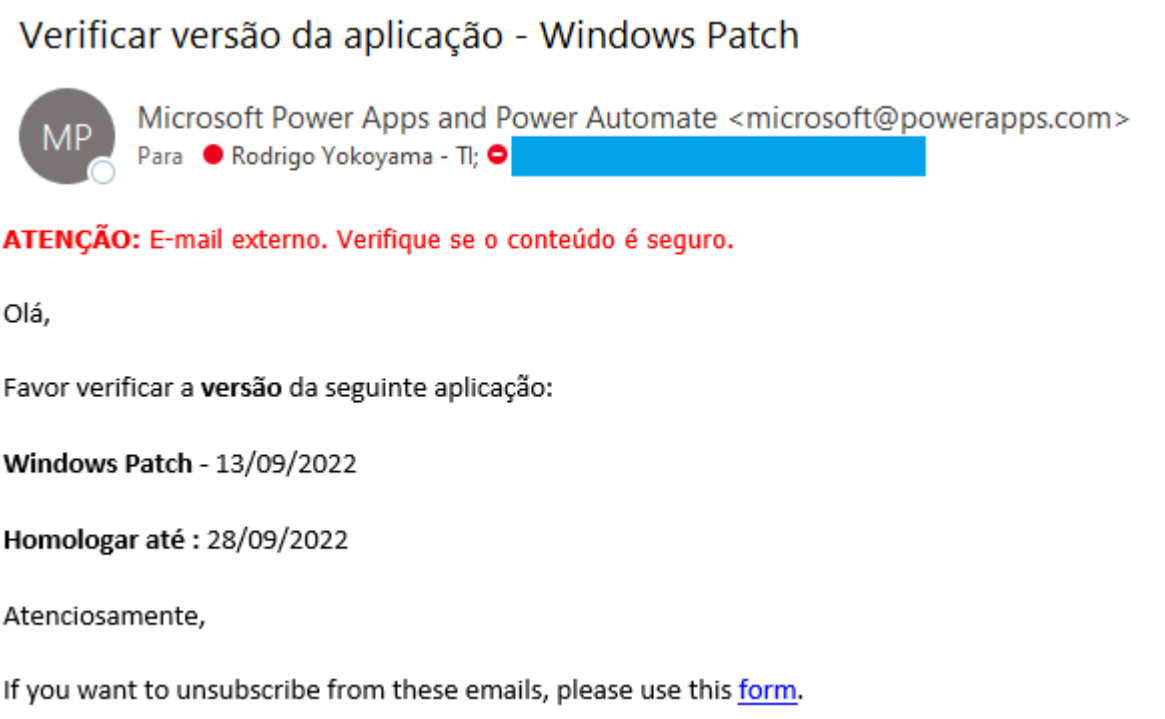
Reunião:	1ª reunião	2ª reunião	3ª reunião	4ª reunião
Duração:	00:45:00	00:45:00	00:45:00	00:45:00
Assunto:	1-Abordado o motivo, premissas e funcionalidade do sistema.	1-Validação dos campos que o sistema deve possuir. 2-Criação da equipe no Teams. 3-Histórico de alterações.	1-Localização dos campos no sistema. 2-Liberação de escrita ao time operacional.	1-Gatilhos e funcionalidades. 2-Tempo para envio de e-mails relacionada a periodicidade de verificação. 3-Fluxograma do sistema.
Reunião:	**5ª reunião**	**6ª reunião**	**7ª reunião**	**8ª reunião**
Duração:	00:45:00	00:45:00	00:45:00	00:45:00
Assunto:	1-Confirmação do funcionamento do fluxo. 2-Inserção de duas tarefas para testes.	1-Verificação dos gatilhos.	1-Correção dos gatilhos. 2-Nova visão para o time operacional. 3-Adicionados campos sugeridos pelo time operacional e de segurança.	1-Verificação final do sistema e confirmação das funcionalidades.

APÊNDICE G – IMAGENS DO SISTEMA E ALERTAS

Histórico de alteração do software:



Verificação de nova versão do programa:



Verificar versão da aplicação - Windows Patch

MP Microsoft Power Apps and Power Automate <microsoft@powerapps.com>
Para Rodrigo Yokoyama - TI; [redacted]

ATENÇÃO: E-mail externo. Verifique se o conteúdo é seguro.

Olá,

Favor verificar a **versão** da seguinte aplicação:

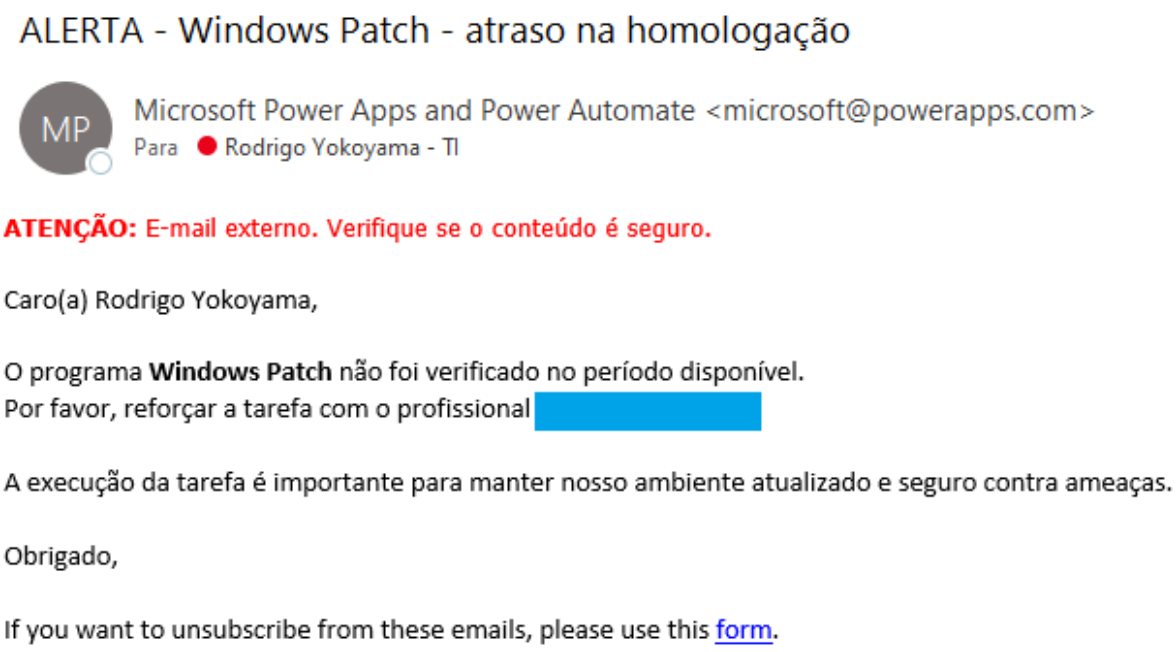
Windows Patch - 13/09/2022

Homologar até : 28/09/2022

Atenciosamente,

If you want to unsubscribe from these emails, please use this form.

Alerta ao gestor:



ALERTA - Windows Patch - atraso na homologação

MP Microsoft Power Apps and Power Automate <microsoft@powerapps.com>
Para Rodrigo Yokoyama - TI

ATENÇÃO: E-mail externo. Verifique se o conteúdo é seguro.

Caro(a) Rodrigo Yokoyama,

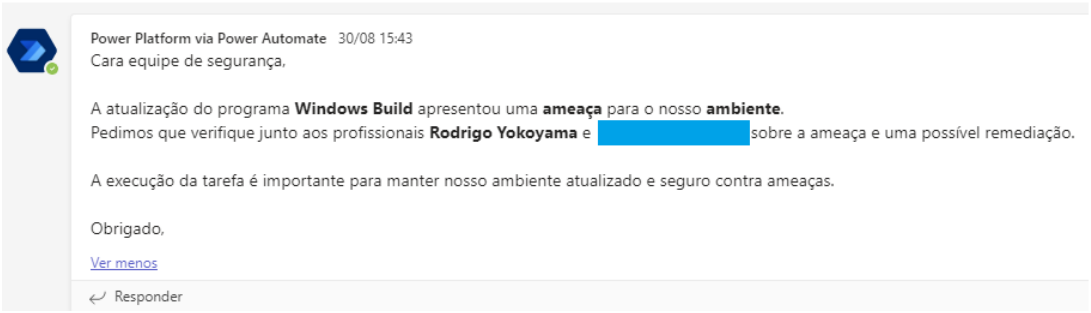
O programa **Windows Patch** não foi verificado no período disponível.
Por favor, reforçar a tarefa com o profissional [redacted]

A execução da tarefa é importante para manter nosso ambiente atualizado e seguro contra ameaças.

Obrigado,

If you want to unsubscribe from these emails, please use this form.

Alerta ao time de segurança:



Power Platform via Power Automate 30/08 15:43
Cara equipe de segurança,

A atualização do programa **Windows Build** apresentou uma **ameaça** para o nosso **ambiente**.
Pedimos que verifique junto aos profissionais **Rodrigo Yokoyama** e [redacted] sobre a ameaça e uma possível remediação.

A execução da tarefa é importante para manter nosso ambiente atualizado e seguro contra ameaças.

Obrigado,

Ver menos

Responder

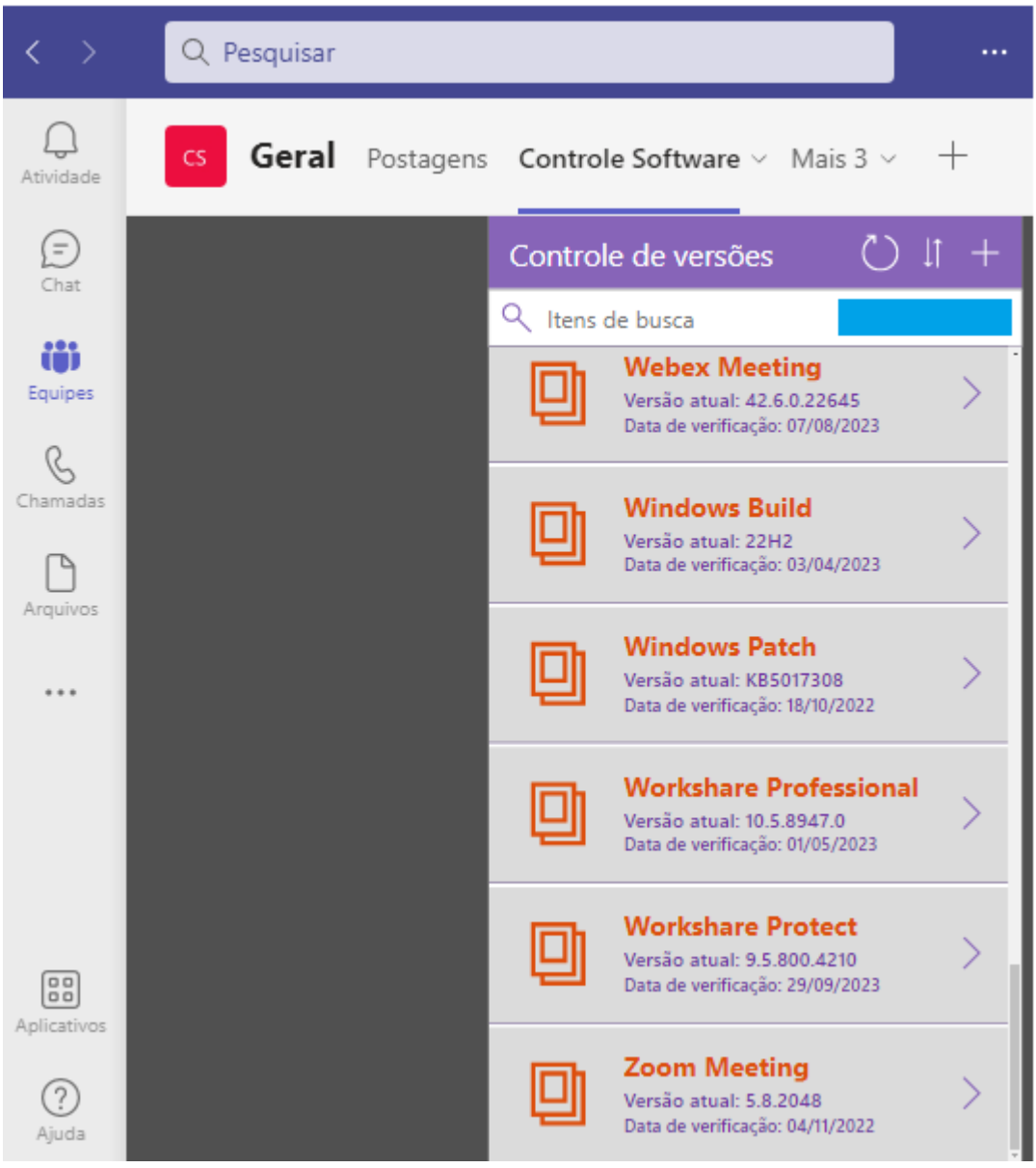
APÊNDICE H – CONVERGÊNCIA ENTRE AMEAÇAS ENCONTRADAS UTILIZANDO ISO 27002 E STRIDE

Convergência entre ameaças encontradas utilizando ISO 27002 e STRIDE:

Windows							
	STRIDE:	**Falsificação**	**Adulteração**	**Repúdio**	**Divulgação de informação**	**Negação de serviço**	**Elevação de privilégio**
ISO 27002:							
Controle de acesso (laptop, rede, devido ao cargo)		X	X	X	Divulgação/compartilhamento do login para terceiros	X	Utilizar login com permissão privilegiada para liberar acesso para conta
Restrição sobre uso e instalação de software		X	X	X	X	X	Instalação de programa com login com permissões administrativas
Transferência de informações		Utilizar conta de terceiros	X	X	Transferir informações confidenciais	X	X
Dispositivos móveis e trabalho remoto		Utilizar conta de terceiros para acesso	X	X	X	X	X
Backup		Utilizar conta de terceiros para acesso	X	X	Transferir informações confidenciais	X	Alguém sem permissão acessar o backup
Proteção contra códigos maliciosos		X	X	X	X	X	Instalação de código malicioso
Gerenciamento de vulnerabilidades		X	Modificar programas	X	X	X	X
Controles criptográficos		Utilizar conta de terceiros	X	X	X	Quebra da encriptação	X
Segurança nas comunicações		Utilizar conta de terceiros	X	X	X	X	X

APÊNDICE I – PASSO A PASSO PARA UTILIZAÇÃO DO SISTEMA

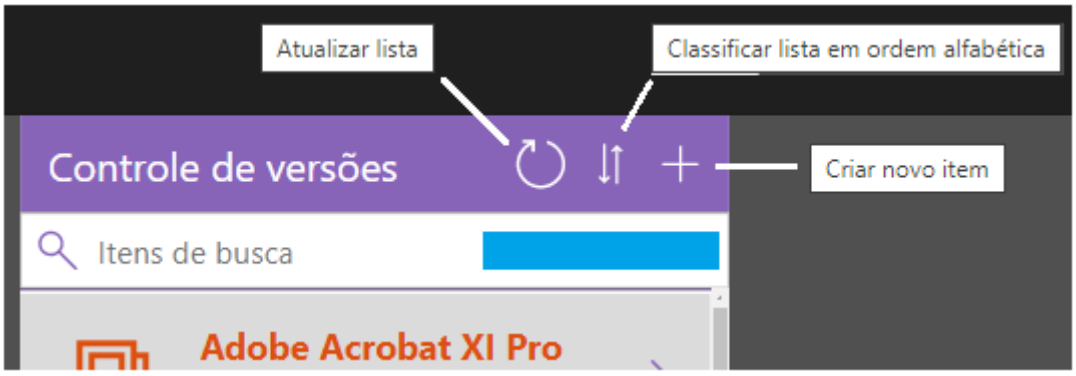
Para acessar o Controle de Software, acesse via Teams a equipe 'Controle de Software', dentro da aba 'Geral' exibir a opção 'Controle de Software':



O Sistema contém três botões no canto superior direito;

1- Atualizar lista
2- Classificar lista em ordem alfabética

3- Criar item



Para expandir as informações de um software específico, clique na seta >

Ao expandir as informações, encontraremos alguns dados do software em questão, como; Versão atual do software no ambiente, periodicidade da próxima atualização, site do instalador do software, existência de alguma ameaça ou CVE, equipe responsável pelo software, analista que realizou a última atualização, entre outros.

Ao editar um sistema, deve-se editar os seguintes campos:

Versão da aplicação: Versão atual em utilização no ambiente

Versão de homologação: Nova versão, que será homologada

Data de verificação: Data que iniciará a homologação do sistema, seguindo o seguinte modelo. Periodicidade Mensal: 10 dias antes. Periodicidade Semestral: 1 mês antes. Periodicidade Anual: 3 meses antes.

ID GMUD: Número da GMUD referente a mudança.

Data modelagem de ameaça: Data que finalizou a aplicação da modelagem de ameaça.

Ameaça versão atual: Deve ser marcado quando houver ameaça na versão atual.

Ameaça versão de homologação: Deve ser marcado quando houver ameaça na nova versão.

(Caso alguma opção esteja em 'Sim', será enviado uma mensagem para a equipe de GSI)

CVE: Informar caso exista algum CVE (pesquisar versão no site)

https://cve.mitre.org/cve/search_cve_list.html

Site de atualização: Site para realizar o download do instalador

(Procurar instaladores offline, de preferência em 64 bits)

Observações: Campo para detalhar alguma observação

Anexos: Campo para anexar evidências, como Checklist ou Modelagem de Ameaça.

Detalhamento completo

ID: Ordenação numérica dos softwares

Nome: Nome de exibição do software

Criticidade: Baixa, Média ou Alta

(Medição do nível de criticidade da atualização do software)

Modificado por: Analista que realizou a atualização
Modificado: Data da última modificação do relatório
Versão da aplicação: Versão atual do software
Versão da homologação: Número da nova versão
Data de verificação: Data que iniciará a homologação da nova versão do software
Data limite da homologação: Data que deverá finalizar a homologação e iniciar a implementação da nova versão.
Periodicidade: Mensal, Semestral, Anual, etc...
(Tempo entre uma atualização e outra)
ID GMUD: Número da GMUD de replicação
Equipe responsável: Equipe responsável pelo software
Ponto Focal: Analista responsável por aquele software
Gestor responsável: Gestor responsável pelo software
Data modelagem de ameaça: Data que finalizou a aplicação da modelagem de ameaça.
Ameaça versão atual: Sim ou Não
Ameaça versão de homologação: Sim ou Não
CVE: Caso exista, nesse campo deverá conter o código do CVE do software.
(*Common Vulnerabilities and Exposures* / Vulnerabilidades e Exposições Comuns)
Site de atualização: Site contendo o instalador do software, para verificar as novas versões.
Observações: Caso exista, detalhar as observações
Anexo: Campo para anexar evidências, como Checklist ou Modelagem de Ameaça.

APÊNDICE J – QUESTIONÁRIO DA ENTREVISTA

Declaro que entendi os objetivos de minha participação na pesquisa e concordo em participar. Registro também que concordo com o tratamento de meus dados pessoais para finalidade específica desta pesquisa, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).

( ) Concordo

Qual a sua formação acadêmica?

Qual a sua experiência profissional na área de Tecnologia da Informação?

Considero relevante a existência de processos no contexto de proteção e defesa virtual do ambiente empresarial.

( ) Concordo plenamente

( ) Concordo mais do que discordo

( ) Discordo mais do que concordo

( ) Discordo plenamente

Considero relevante a aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual do ambiente empresarial.

( ) Concordo plenamente

( ) Concordo mais do que discordo

( ) Discordo mais do que concordo

( ) Discordo plenamente

A utilização do método de modelagem de ameaça aperfeiçoará a defesa virtual do ambiente empresarial

( ) Concordo plenamente

( ) Concordo mais do que discordo

( ) Discordo mais do que concordo

( ) Discordo plenamente

Considero relevante a aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual de *endpoints*.

( ) Concordo plenamente

( ) Concordo mais do que discordo

( ) Discordo mais do que concordo

( ) Discordo plenamente

Considero correto o modo como a aplicação do método de modelagem de ameaça foi aplicado na proteção e defesa virtual de *endpoints*.

( ) Concordo plenamente

( ) Concordo mais do que discordo

( ) Discordo mais do que concordo

( ) Discordo plenamente

Considero relevante a utilização de um sistema para controle de ameaça em softwares.

( ) Concordo plenamente

( ) Concordo mais do que discordo

( ) Discordo mais do que concordo

( ) Discordo plenamente

Considero relevante a utilização de gatilhos para alertas relacionados a verificação de novas ameaças

( ) Concordo plenamente

( ) Concordo mais do que discordo

( ) Discordo mais do que concordo

( ) Discordo plenamente

Considero relevante a utilização de gatilhos para alertas relacionados ao aviso ao gestor responsável

( ) Concordo plenamente

( ) Concordo mais do que discordo

( ) Discordo mais do que concordo

( ) Discordo plenamente

Considero relevante a utilização de gatilhos para alertas relacionados ao aviso a equipe de segurança da informação

( ) Concordo plenamente

( ) Concordo mais do que discordo

( ) Discordo mais do que concordo

( ) Discordo plenamente

Considero relevante a opção de um campo para registro de tratativa de CVEs já existentes.

( ) Concordo plenamente

( ) Concordo mais do que discordo

( ) Discordo mais do que concordo

( ) Discordo plenamente

Considero relevante o histórico e a opção de um campo para notificar a tratativa de CVEs já existentes.

( ) Concordo plenamente

( ) Concordo mais do que discordo

( ) Discordo mais do que concordo

( ) Discordo plenamente

Considero relevante a possibilidade de análise de histórico de alterações.

( ) Concordo plenamente

( ) Concordo mais do que discordo

( ) Discordo mais do que concordo

( ) Discordo plenamente

Possui algum comentário sobre a modelagem de ameaça, sistema ou suas aplicações apresentadas?

Resposta de texto livre.

APÊNDICE K – APRESENTAÇÃO UTILIZADA NA ENTREVISTA

APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

- Objetivo
- Método
- Aplicação
- Sistema
- Conclusões
- Referências

APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

- Objetivo

- Aplicação do método modelagem de ameaça em sistemas operacionais
- Criação de sistema para controle, monitoramento e gestão

Unidade de Pós-Graduação, Extensão e Pesquisa

APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

- Método - STRIDE

De acordo com Shostack (2014) STRIDE é um mnemônico para coisas que dão errado na segurança, significando: Spoofing (falsificação), Tampering (adulteração), Repudiation (repúdio), Information Disclosure (divulgação de informações), Denial of Service (negação de serviço) e Elevation of Privilege (elevação de privilégio). Cada letra que compõe o nome STRIDE é uma categoria. A definição de cada categoria, em português, é explicada na sequência:

- S: Falsificação é fingir ser algo ou alguém que você não é.
- T: Adulterar é modificar algo que você não deve modificar. Pode incluir pacotes na rede, bits no disco ou bits na memória.
- R: Repúdio significa alegar que você não fez algo (independentemente se você fez ou não).
- I: Divulgação de informações é sobre a exposição de informações a pessoas não autorizadas.
- D: Negação de serviço são ataques projetados para impedir que um sistema forneça serviço, inclusive travando -o, tornando-o excessivamente lento ou preenchendo todo o seu armazenamento.
- E: Elevação de privilégio é quando um programa ou usuário é tecnicamente capaz de fazer coisas que eles não deveriam fazer.

APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

- Método - DREAD

O DREAD fornece um esquema pelo qual os vetores de ameaças identificados usando STRIDE ou outras metodologias são avaliados e priorizados. Cada vetor de ameaça individual é pontuado em cinco elementos e uma média obtida, que pode ser usada para comparar sua gravidade e probabilidade com as de outros vetores de ameaça. Assim, o DREAD vai além da modelagem de ameaças para a avaliação de riscos (BODEAU; MCCOLLUM; FOX, 2018)

D – Damage potential – Dano: Quanto dano resultaria?

- Alto (3) – O atacante pode obter controle total do sistema e/ou executar tarefas com privilégios administrativos;
- Médio (2) – Perda de informações sensíveis;
- Baixo (1) - Perda de informações triviais.

R – Reproducibility – Reprodutibilidade: Quão difícil é a execução?

- Alto (3) - O ataque pode ser sempre reproduzido com facilidade.
- Médio (2) – O ataque só pode ser reproduzido com uma janela de tempo específico e/ou com uma condição particular;
- Baixa (1) – O ataque é extremamente difícil de ser reproduzido, mesmo com amplo conhecimento em segurança.

E – Exploitability – Explorabilidade: O quão fácil é reproduzir o ataque?

- Alta (3) – um usuário inexperiente pode realizar um ataque em pouco tempo;
- Médio (2) – Um usuário experiente pode realizar o ataque;
- Baixo (1) – O ataque requer uma pessoa extremamente capacitada para realizar o ataque.

A – Affected users – Usuários afetados: Quantas pessoas provavelmente seriam afetadas?

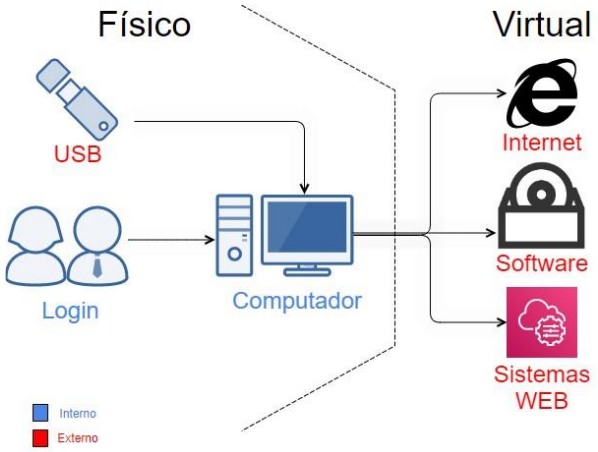
- Alta (3) – Todos os usuários, configuração padrão e principais clientes são afetados;
- Média (2) – Alguns usuários e configuração não padrão são afetados;
- Baixa (1) – Pequena porcentagem dos usuários são afetados

D – Discoverability – Descoberta: Quão difícil é encontrar a vulnerabilidade?

- Alta (3) – A vulnerabilidade é facilmente notável e fontes públicas explicam os meios de ataque;
- Média (2) – A vulnerabilidade está contida em uma funcionalidade pouco acessível do sistema e requer bastante análise para que seja encontrada;
- Baixa (1) – O bug que viabiliza a vulnerabilidade é obscuro, é altamente improvável que os usuários descubram potenciais danos.

APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

- Aplicação - Identificar ambiente ou ativo



APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

- Aplicação - Identificar ameaças de segurança

Windows						
STRIDE por elemento	Falsificação	Adulteração	Repúdio	Divulgação de informação	Negação de serviço	Elevação de privilégio
Entidade Externa:	Acesso indevido ao dispositivo utilizando conta externa ou de terceiros;		Acesso a sites ou sistemas não autorizados pela empresa;	Acesso a sites ou sistemas não autorizados pela empresa;		
			Utilização de login pessoal em programas da empresa;	Utilização de login pessoal em programas da empresa;		
Entidade Interna:		Programas desatualizados;	Compartilhamento do login empresarial;	Divulgação ou perda de conteúdo empresarial;		
Físico:		Falta de proteção física ao conteúdo do HD, em caso de perda ou roubo do equipamento.		Utilização de pen drive para gravação de arquivos;		
				Perda de informações empresariais em caso de desastres;		
Virtual:		Proteção do ativo, contra ameaças virtuais;			Instalação de software que sobrecarrega a rede empresarial.	Instalação de programas não autorizados pela empresa;
		Alteração de informações na rede empresarial;			Instalação de programa que sobrecarrega o sistema.	

APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

- Aplicação - Avaliar ameaça de segurança

	Dano	Reprodutibilidade	Explorabilidade	Usuários afetados	Descoberta
1. Acesso a sites ou sistemas não autorizados pela empresa;	Alta	Alta	Alta	Alta	Alta
2. Acesso indevido ao dispositivo utilizando conta externa ou de terceiros;	Alta	Baixa	Baixa	Baixa	Baixa
3. Alteração de informações na rede empresarial;	Alta	Alta	Baixa	Média	Baixa
4. Compartilhamento do login empresarial;	Alta	Alta	Alta	Baixa	Alta
5. Divulgação ou perda de conteúdo empresarial;	Alta	Alta	Alta	Média	Alta
6. Falta de proteção física ao conteúdo do HD, em caso de perda ou roubo do equipamento;	Alta	Alta	Alta	Baixa	Alta
7. Instalação de programa que sobrecarrega o sistema;	Média	Média	Baixa	Baixa	Baixa

	Dano	Reprodutibilidade	Explorabilidade	Usuários afetados	Descoberta
8. Instalação de programas não autorizados pela empresa;	Alta	Alta	Alta	Baixa	Alta
9. Instalação de software que sobrecarrega a rede empresarial;	Alta	Baixa	Baixa	Alta	Alta
10. Perda de informações empresariais em caso de desastres;	Média	Média	Baixa	Baixa	Baixa
11. Programas desatualizados;	Alta	Alta	Alta	Alta	Média
12. Proteção do ativo, contra ameaças virtuais;	Alta	Alta	Alta	Alta	Alta
13. Utilização de login pessoal em programas da empresa;	Baixo	Alta	Baixa	Alta	Média
14. Utilização de pen drive para gravação de arquivos;	Alta	Alta	Alta	Alta	Alta

APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

- Aplicação - Identificar ambiente ou ativo

	Pontuação DREAD
1. Acesso a sites ou sistemas não autorizados pela empresa;	3
12. Proteção do ativo, contra ameaças virtuais;	3
14. Utilização de pen drive para gravação de arquivos;	3
5. Divulgação ou perda de conteúdo empresarial;	2,8
11. Programas desatualizados;	2,8
4. Compartilhamento do login empresarial;	2,6
6. Falta de proteção física ao conteúdo do HD, em caso de perda ou roubo do equipamento;	2,6
8. Instalação de programas não autorizados pela empresa;	2,6
9. Instalação de software que sobrecarrega a rede empresarial;	2,2
3. Alteração de informações na rede empresarial;	2
13. Utilização de login pessoal em programas da empresa;	1,8
2. Acesso indevido ao dispositivo utilizando conta externa ou de terceiros;	1,4
7. Instalação de programa que sobrecarrega o sistema;	1,4
10. Perda de informações empresariais em caso de desastres;	1,4

APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

- Aplicação - Tratar ameaça de segurança

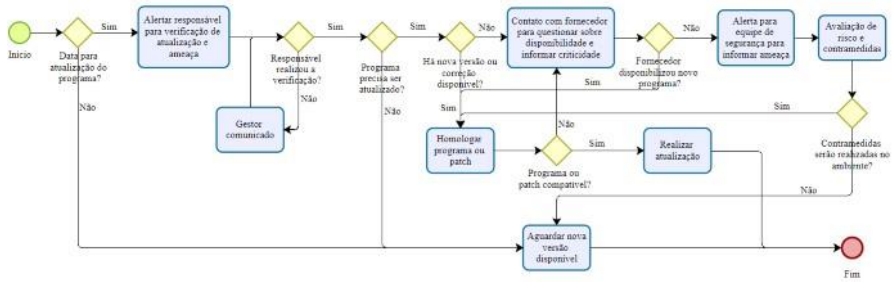
Ameaça	Tratativa
1. Acesso a sites ou sistemas não autorizados pela empresa;	Instalação de proxy nos computadores empresariais; utilização de firewall, para limitar o acesso a sites e sistemas indevi bloqueio a sites indesejáveis também pode ser realizado por um aplicativo antivírus que suporte realizar esse bloqueio.
2. Acesso indevido ao dispositivo utilizando conta externa ou de terceiros;	Restrição para login de domínio, impedindo assim que contas locais ou contras de outras empresas consigam acessar o computador. Limitar o acesso de login ao computador para usuários nominais e restringir horários para permissão de logi
3. Alteração de informações na rede empresarial;	Restrição de escrita para a maioria dos profissionais da empresa em drivers de redes ou sistemas críticos. Restringir o de leitura e escrita de cada profissional conforme suas necessidades para a realização de suas funções na empresa.
4. Compartilhamento do login empresarial;	Utilização de autenticação de duplo fator e utilização de logs do sistema, para monitoramento de login em todos os dispo Essa implantação também poderá evitar que o acesso ao e-mail empresarial pela WEB seja realizado sem a ciência e permissão do usuário.
5. Divulgação ou perda de conteúdo empresarial;	Utilização de uma solução para armazenar os arquivos empresariais criados pelos profissionais, evitando que informações importantes estejam salvas apenas localmente em seu computador.
6. Falta de proteção física ao conteúdo do HD, em caso de perda ou roubo do equipamento;	Utilização de programas de encriptação. Recomenda-se a utilização de senha para o acesso a BIOS do equipamento. Limitar o acesso de login ao computador para usuários nominais, fazendo assim com que usuários do mesmo domínio consigam apenas no computador designado para eles.
7. Instalação de programa que sobrecarrega o sistema;	Restrição de instalação de softwares
8. Instalação de programas não autorizados pela empresa;	Restrição de instalação de softwares
9. Instalação de software que sobrecarrega a rede empresarial;	Restrição de instalação de softwares
10. Perda de informações empresariais em caso de desastres;	Utilização de uma solução para armazenar os arquivos empresariais criados pelos profissionais, evitando que informações importantes estejam salvas apenas localmente em seu computador.
11. Programas desatualizados;	Atualização para o Sistema Operacional, após homologação.
12. Proteção do ativo, contra ameaças virtuais;	Utilização de um programa antivírus para proteção do Sistema Operacional
13. Utilização de login pessoal em programas da empresa;	Restrição para login de domínio, criação de bloqueio, evitando que o computador conectar em outros programas utilizando logins pessoais ou de outras empresas.
14. Utilização de pen drive para gravação de arquivos;	Para o bloqueio de transmissão de arquivos, utilizar regra no computador para bloqueio do USB para leitura e escrita, as como o bloqueio de transmissão de dados via Bluetooth.

APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

- Sistema de controle de software

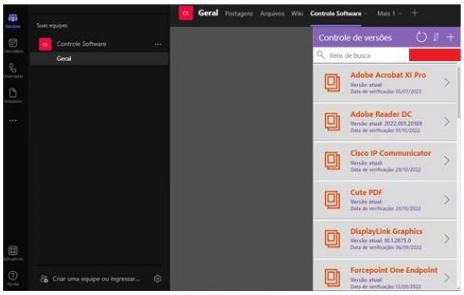
- Gatilhos
  - Envio de e-mail aos responsáveis para verificação de nova versão.
  - Envio de e-mail ao gestor responsável pela aplicação, caso o responsável não tenha realizado a tarefa de verificação de nova versão.
  - Envio de notificação ao time de segurança, caso o fornecedor não tenha uma solução relacionada a ameaça encontrada

Fluxograma



APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

- Sistema de controle de software



APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

- Conclusão - Modelagem de ameaça

- Nesta pesquisa identificou ameaças existentes em um sistema operacional utilizando os métodos STRIDE e DREAD. Verificou-se 14 tipos de ameaças encontradas em um sistema operacional que podem ser devidamente identificadas e mitigadas com a utilização do método de modelagem de ameaça.
- Entre as 14 ameaças identificadas, 10 estão com pontuação acima de 2 no método STRIDE apresentando maior risco.
- Uma abordagem sistemática para controle, identificação e correção das ameaças encontradas pode colaborar com a gestão de risco empresarial, auxiliando assim na verificação de novas versões e homologação antes de ser colocado em produção.
- A Padronização e utilização de uma única versão para todos os dispositivos da empresa poderá auxiliar na mitigação das ameaças, tornando necessário que os ajustes sejam realizados apenas uma única vez e replicado para todos os outros computadores.

APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

• Conclusão - Sistema

- Auxilio para controle de homologação das versões
- Alertas por período customizáveis
- Controle de CVE por software
- Controle de GMUD relacionada a atualização
- Facilidade na utilização
- Gatilhos para alertar gestores e time de segurança
- Histórico de atualizações
- Processo de homologação individual, com passo a passo no anexo
- Possibilidade de utilizar o resultado do controle para amostragem de conformidade em auditorias
- Sistema intuitivo

APLICAÇÃO DO MÉTODO DE MODELAGEM DE AMEAÇA EM UM SISTEMA OPERACIONAL

• Referências

- BODEAU, D. J.; MCCOLLUM, C. D.; FOX, D. B. **Cyber threat modeling: Survey, assessment, and representative framework**. MITRE CORP MCLEAN VA MCLEAN, 2018.
- KHAN et al., **STRIDE-based threat modeling for cyber-physical systems**. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE, 2017. p. 1-6.
- LALLIE et al., **Cyber security in the age of COVID-19: A timeline and analysis of cybercrime and cyber-attacks during the pandemic**, Computers & Security, Volume 105, 2021, 102248, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102248.
- SEIFERT, D.; REZA, H. **A security analysis of cyber-physical systems architecture for healthcare**. Computers, v. 5, n. 4, p. 27, 2016.
- SHEVCHENKO et al. **Threat modeling: a summary of available methods**. Carnegie Mellon University Software Engineering Institute Pittsburgh United States, 2018.
- SHOSTACK, A. **Threat Modeling Designing for Security**. P.22 e 23, Editora WILEY, 2014.
- UCEDAVÉLEZ T.; MORANA M.M, **Risk Centric Threat Modeling**. P; 2 e 3, Editora Willey, 2015.
- XIONG, W.; LAGERSTRÖM, R. **Threat modeling–A systematic literature review** . Computers & security, v. 84, p. 53-69, 2019.
- YOKOYAMA R., ARIMA C.H. **Análise textual e bibliométrica sobre modelagem de ameaça / Textual and bibliometric analysis on threat modeling** Brazilian Journal of Development Vol. 8 No 1 p. 767-787690. doi:10.34117/bjdv8n1-514.
- YOKOYAMA R.; ARIMA C.H. **Modelagem de ameaça, análise de risco e suas aplicações na literatura**, International Journal of Development Research , 12, (04), P. 55049-55055.doi:10.37118/ijdr.24250.04.2022.
- ZOGRAFOPOULOS et al., **Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources , Metrics , and Case Studies**. IEEE Access, vol. 9, p. 29775-29818, 2021, doi: 10.1109/ACCESS.2021.3058403.

APÊNDICE L – RESPOSTAS DOS ENTREVISTADOS INTERNOS

Pergunta	Avaliador interno 1	Avaliador interno 2
Declaro que entendi os objetivos de minha participação na pesquisa e concordo em participar. Registro também que concordo com o tratamento de meus dados pessoais para finalidade específica desta pesquisa, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).	Concordo	Concordo
Qual a sua formação acadêmica?	Análise e Desenvolvimento de Sistemas	Bacharel em Sistemas de Informação
Qual a sua experiência profissional na área de Tecnologia da Informação?	Tenho 8 anos de experiência em Service Desk de escritório jurídico, no momento atuando no gerenciamento de softwares do escritório e projetos ligados ao Service Desk.	Tenho 10 anos de experiência profissional na área de TI, passando por áreas de manutenção, áreas técnicas, suporte ao cliente e projetos de TI.
Considero relevante a existência de processos no contexto de proteção e defesa virtual do ambiente empresarial.	Concordo plenamente	Concordo plenamente
Considero relevante a aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual do ambiente empresarial.	Concordo plenamente	Concordo plenamente
A utilização do método de modelagem de ameaça aperfeiçoará a defesa virtual do ambiente empresarial	Concordo plenamente	Concordo mais do que discordo
Considero relevante a aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual de *endpoints*.	Concordo plenamente	Concordo mais do que discordo
Considero correto o modo como a aplicação do método de modelagem de ameaça foi aplicado na proteção e defesa virtual de *endpoints*.	Concordo plenamente	Concordo mais do que discordo
Considero relevante a utilização de um sistema para controle de ameaça em softwares.	Concordo plenamente	Concordo plenamente
Considero relevante a utilização de gatilhos para alertas relacionados a verificação de novas ameaças	Concordo plenamente	Concordo plenamente

Considero relevante a utilização de gatilhos para alertas relacionados ao aviso ao gestor responsável	Concordo plenamente	Concordo plenamente
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso a equipe de segurança da informação	Concordo plenamente	Concordo mais do que discordo
Considero relevante a opção de um campo para registro de tratativa de CVEs já existentes.	Concordo plenamente	Concordo mais do que discordo
Considero relevante o histórico e para evidenciar a tratativa de CVEs já existentes.	Concordo plenamente	Concordo plenamente
Considero relevante a possibilidade de análise de histórico de alterações no sistema.	Concordo plenamente	Concordo plenamente
Possui algum comentário sobre a aplicação do método de modelagem de ameaça, sistema proposto ou suas aplicações apresentadas?	O sistema é muito importante para o controle dos softwares utilizados, facilitando a verificação e evitando possíveis falhas no processo.	O sistema é muito interessante, bem intuitivo e acredito que ajude muito no controle de softwares e versões, assim como deve "amarrar" os processos, evitando falhas humanas, como o caso de esquecimento. Uma melhoria, poderia ser o filtro de informações, uma forma de filtrar os softwares de determinada área ou ordenar os softwares por data de verificação. Nos demais pontos, fiquei bem impressionado com o fluxo do sistema, facilidade de utilização e prevenção de falhas, comunicando sempre o Gestor atrelado ao software, sobre os processos realizados ou sobre a falta de processos necessários. Olhando para o cenário de uma empresa e/ou escritório, esse sistema evita ameaças e previne falhas, mantendo os softwares atualizados e corrigindo as falhas encontradas nas rotinas de validações.

Pergunta	Avaliador interno 3	Avaliador interno 4
Declaro que entendi os objetivos de minha participação na pesquisa e concordo em participar. Registro também que concordo com o tratamento de meus dados pessoais para finalidade específica desta pesquisa, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).	Concordo	Concordo

Qual a sua formação acadêmica?	Possuo Graduação Tecnológica em Redes de Computadores. Pós-Graduado em CyberSecurity Possuo certificação Security+ da Comptia Certificado ISO27001, ISO20000 e ITIL pela Exin. Certificado NSE 2 pela Fortinet Segurança Ofensiva pela Rangeforce	Ensino Superior em Ciências da computação
Qual a sua experiência profissional na área de Tecnologia da Informação?	3 anos na área de segurança da informação	15 anos na área de Service Desk
Considero relevante a existência de processos no contexto de proteção e defesa virtual do ambiente empresarial.	Concordo plenamente	Concordo plenamente
Considero relevante a aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual do ambiente empresarial.	Concordo plenamente	Concordo plenamente
A utilização do método de modelagem de ameaça aperfeiçoará a defesa virtual do ambiente empresarial	Concordo plenamente	Concordo plenamente
Considero relevante a aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual de *endpoints*.	Concordo plenamente	Concordo plenamente
Considero correto o modo como a aplicação do método de modelagem de ameaça foi aplicado na proteção e defesa virtual de *endpoints*.	Concordo plenamente	Concordo plenamente
Considero relevante a utilização de um sistema para controle de ameaça em softwares.	Concordo plenamente	Concordo plenamente
Considero relevante a utilização de gatilhos para alertas relacionados a verificação de novas ameaças	Concordo plenamente	Concordo plenamente
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso ao gestor responsável	Concordo plenamente	Concordo plenamente
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso a equipe de segurança da informação	Concordo plenamente	Concordo plenamente
Considero relevante a opção de um campo para registro de tratativa de CVEs já existentes.	Concordo plenamente	Concordo plenamente
Considero relevante o histórico e para evidenciar a tratativa de CVEs já existentes.	Concordo plenamente	Concordo plenamente
Considero relevante a possibilidade de análise de histórico de alterações no sistema.	Concordo plenamente	Concordo plenamente

Possui algum comentário sobre a aplicação do método de modelagem de ameaça, sistema proposto ou suas aplicações apresentadas?	A modelagem de ameaças tem um papel muito importante quanto a proteção do ambiente. Este processo de forma estruturada auxilia desde montagem de cenários, identificação de vulnerabilidades e ameaças até a mitigação das mesmas. Trazendo visibilidade sobre o ambiente, sendo possível medir e reduzir a exposição ao risco. Considero de extrema importância para maturidade de um ambiente cada vez mais seguro.	Ao meu ver, o método é super efetivo e detalhado com impactos reais no dia a dia. A ferramenta apresentada será de grande utilidade e faremos um controle de atualização de vulnerabilidade que antes era manual e por vezes nem era feito em softwares mais comuns, mas agora será visto e cuidado com outro nível de atenção

Pergunta	Avaliador interno 5	Avaliador interno 6
Declaro que entendi os objetivos de minha participação na pesquisa e concordo em participar. Registro também que concordo com o tratamento de meus dados pessoais para finalidade específica desta pesquisa, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).	Concordo	Concordo
Qual a sua formação acadêmica?	Engenheiro da Computação	Pós-graduado
Qual a sua experiência profissional na área de Tecnologia da Informação?	Tenho 20 anos de experiência na área de tecnologia da informação, mais especificamente em infraestrutura.	21 anos de experiência no segmento de tecnologia da informação. Atualmente diretor de tecnologia em empresa de prestação de serviço.
Considero relevante a existência de processos no contexto de proteção e defesa virtual do ambiente empresarial.	Concordo plenamente	Concordo plenamente
Considero relevante a aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual do ambiente empresarial.	Concordo plenamente	Concordo plenamente
A utilização do método de modelagem de ameaça aperfeiçoará a defesa virtual do ambiente empresarial	Concordo plenamente	Concordo mais do que discordo
Considero relevante a aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual de *endpoints*.	Concordo plenamente	Concordo plenamente
Considero correto o modo como a aplicação do método de modelagem de ameaça foi aplicado na proteção e defesa virtual de *endpoints*.	Concordo plenamente	Concordo plenamente
Considero relevante a utilização de um sistema para controle de ameaça em softwares.	Concordo plenamente	Concordo plenamente

Considero relevante a utilização de gatilhos para alertas relacionados a verificação de novas ameaças	Concordo plenamente	Concordo plenamente
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso ao gestor responsável	Concordo mais do que discordo	Concordo plenamente
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso a equipe de segurança da informação	Concordo plenamente	Concordo plenamente
Considero relevante a opção de um campo para registro de tratativa de CVEs já existentes.	Concordo plenamente	Concordo mais do que discordo
Considero relevante o histórico e para evidenciar a tratativa de CVEs já existentes.	Concordo plenamente	Concordo plenamente
Considero relevante a possibilidade de análise de histórico de alterações no sistema.	Concordo plenamente	Concordo plenamente
Possui algum comentário sobre a aplicação do método de modelagem de ameaça, sistema proposto ou suas aplicações apresentadas?		A aplicação dos métodos será importante para aumentar a segurança no que tange a atualização dos softwares. O sistema servirá de apoio na atualização e poderá ser utilizado por outros analistas.

APÊNDICE M – RESPOSTAS DOS ENTREVISTADOS EXTERNOS

Pergunta	Avaliador externo 1	Avaliador externo 2
Declaro que entendi os objetivos de minha participação na pesquisa e concordo em participar. Registro também que concordo com o tratamento de meus dados pessoais para finalidade específica desta pesquisa, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).	Concordo	Concordo
Qual a sua formação acadêmica?	Pós-Graduação	Ciências Econômicas, Segurança da Informação
Qual a sua experiência profissional na área de Tecnologia da Informação?	25 anos em TI e 15 anos em Segurança da informação	desenvolvimento, suporte, segurança da informação
Considero relevante a existência de processos no contexto de proteção e defesa virtual do ambiente empresarial.	Concordo plenamente	Concordo plenamente
Considero relevante a aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual do ambiente empresarial.	Concordo plenamente	Concordo plenamente
A utilização do método de modelagem de ameaça aperfeiçoará a defesa virtual do ambiente empresarial	Concordo plenamente	Concordo plenamente
Considero relevante a aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual de *endpoints*.	Concordo plenamente	Concordo plenamente
Considero correto o modo como a aplicação do método de modelagem de ameaça foi aplicado na proteção e defesa virtual de *endpoints*.	Concordo plenamente	Concordo mais do que discordo
Considero relevante a utilização de um sistema para controle de ameaça em softwares.	Concordo plenamente	Concordo mais do que discordo
Considero relevante a utilização de gatilhos para alertas relacionados a verificação de novas ameaças	Concordo plenamente	Concordo mais do que discordo
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso ao gestor responsável	Concordo plenamente	Concordo mais do que discordo
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso a equipe de segurança da informação	Concordo plenamente	Concordo plenamente
Considero relevante a opção de um campo para registro de tratativa de CVEs já existentes.	Concordo plenamente	Concordo plenamente

Considero relevante o histórico e para evidenciar a tratativa de CVEs já existentes.	Concordo plenamente	Concordo plenamente
Considero relevante a possibilidade de análise de histórico de alterações no sistema.	Concordo plenamente	Concordo mais do que discordo
Possui algum comentário sobre a aplicação do método de modelagem de ameaça, sistema proposto ou suas aplicações apresentadas?	Acredito que o método apresentado vai auxiliar principalmente empresas que ainda não possuem uma equipe especializada em segurança, porém mesmo para as que já possuem tal equipe, considero que o método tende a produzir informações relevantes e úteis para o dia a dia, principalmente no quesito vulnerabilidades e correções.	As considerações foram feitas durante a entrevista.

Pergunta	**Avaliador externo 3**	**Avaliador externo 4**
Declaro que entendi os objetivos de minha participação na pesquisa e concordo em participar. Registro também que concordo com o tratamento de meus dados pessoais para finalidade específica desta pesquisa, em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).	Concordo	Concordo
Qual a sua formação acadêmica?	Pós-graduado em Engenharia de Software	Pós-graduação em Cyber Security
Qual a sua experiência profissional na área de Tecnologia da Informação?	Atuo há mais de 20 anos em tecnologia da informação, sendo os últimos 7 anos no segmento bancário com ferramentas de segurança.	10 anos sendo os últimos 4 em Cyber Segurança
Considero relevante a existência de processos no contexto de proteção e defesa virtual do ambiente empresarial.	Concordo plenamente	Concordo plenamente
Considero relevante a aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual do ambiente empresarial.	Concordo plenamente	Concordo plenamente
A utilização do método de modelagem de ameaça aperfeiçoará a defesa virtual do ambiente empresarial	Concordo plenamente	Concordo plenamente
Considero relevante a aplicação do método de modelagem de ameaça no contexto de proteção e defesa virtual de *endpoints*.	Concordo plenamente	Concordo plenamente
Considero correto o modo como a aplicação do método de modelagem de ameaça foi aplicado na proteção e defesa virtual de *endpoints*.	Concordo plenamente	Concordo plenamente
Considero relevante a utilização de um sistema para controle de ameaça em softwares.	Concordo plenamente	Concordo plenamente

Considero relevante a utilização de gatilhos para alertas relacionados a verificação de novas ameaças	Concordo plenamente	Concordo plenamente
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso ao gestor responsável	Concordo plenamente	Concordo plenamente
Considero relevante a utilização de gatilhos para alertas relacionados ao aviso a equipe de segurança da informação	Concordo plenamente	Concordo plenamente
Considero relevante a opção de um campo para registro de tratativa de CVEs já existentes.	Concordo plenamente	Concordo plenamente
Considero relevante o histórico e para evidenciar a tratativa de CVEs já existentes.	Concordo plenamente	Concordo plenamente
Considero relevante a possibilidade de análise de histórico de alterações no sistema.	Concordo plenamente	Concordo plenamente
Possui algum comentário sobre a aplicação do método de modelagem de ameaça, sistema proposto ou suas aplicações apresentadas?	Se tiver a intenção de "produtizar" a solução para uso em empresas diversas, escolheria uma linguagem que possa se incorporar em contextos que não utilizem a plataforma Microsoft permitindo algo *open source.*	O método é eficaz para o que se propõe-se . Empresas sem investimento em Cyber Security e de pequeno porte.

APÊNDICE N – PLANO E UTILIZAÇÃO DO SISTEMA

Cronograma de Atualização de Softwares

Moacir [redacted]
Para ⊞D_SD_ Atualização_Projetos

Prezados, boa tarde.

Segue uma projeção sobre o cronograma das Atualizações de Softwares para 2023;

Software	Novembro	Dezembro	2023	Janeiro	Fevereiro	Março	Abril	Maio	Junho	Julho	Agosto	Setembro	Outubro	Novembro	Dezembro	Periodicidade
Adobe Acrobat XI Pro	.	.		.	.	.	.	.	.	24/7	.	.	.	.	.	1 ano
Adobe Reader DC	21/11	.		.	.	.	.	22/5	.	.	.	.	.	20/11	.	6 meses
Cute PDF	.	.		.	.	.	.	.	.	.	.	4/9	.	.	.	1 ano
DisplayLink Graphics	.	.		.	6/2	.	.	.	.	.	7/8	.	.	.	.	6 meses
Google Chrome	1/11	1/12		1/1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9	1/10	1/11	1/12	1 mês
Izarc	.	.		.	.	13/3	.	.	.	.	.	13/9	.	.	.	6 meses
Java	.	.		.	.	.	.	1/5	.	.	.	.	.	1/11	.	6 meses
Microsoft Office 365	.	.		.	.	.	.	.	12/6	.	.	.	.	.	.	6 meses
Mozilla Firefox	1/11	1/12		1/1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9	1/10	1/11	1/12	1 mês
PDFsam Basic	.	.		.	.	.	.	.	5/6	.	.	.	.	.	5/12	1 ano
SendMail	.	.		.	.	.	10/4	.	.	.	.	.	10/10	.	.	6 meses
VLC media player	.	5/12		.	.	.	.	.	.	.	.	.	.	.	5/12	1 ano
Windows Build	.	.		.	.	.	.	.	.	.	14/8	.	.	.	.	1 ano
Windows Patch	15/11	20/12		17/1	21/2	21/3	18/4	16/5	20/6	18/7	15/8	19/9	17/10	21/11	19/12	1 mês
Workshare Protect	.	.		30/1	.	.	.	.	.	31/7	.	.	.	.	.	6 meses
Zoom Meeting	.	.		.	.	.	.	.	.	.	.	.	23/10	.	.	6 meses
TOTAL	4	4		4	4	4	4	5	5	5	5	5	5	5	5	

Desta forma, não passaremos de 5 atualizações por mês, lembrando que 3 já são mensais (Chrome, Firefox e Windows Patch).

Podemos conversar melhor sobre isso, na reunião de amanhã.

Atenciosamente,

RES: UPDATE - Atualização Office 16.0.[redacted]

Moacir [redacted]
Para ⊞D_SD_ Atualização_Projetos
Cc ⊞D_SD2; ⊞D_SD3

Responder | Responder a Todos | Encaminhar | ...

qua 26/10/2022 15:50

Boa tarde,

Segue update da atualização do Office para a versão (16.0.[redacted]).

Atualizado: 1209
Em andamento: 360
Pendente: 170

Caso encontrem algum problema que pode estar ligado a essa atualização nos avisem.

Atenciosamente,

RES: Atualização Java [redacted]

Moacir [redacted]
Para D_SD_ Atualização_Projetos
Cc D_SD2; D_SD3

Responder | Responder a Todos | Encaminhar | ...

qua 09/11/2022 15:55

Boa tarde,

Segue status da atualização do Java para a versão [redacted]

Atualizado: 943
Em andamento: 472
Pendente: 435

Caso encontrem algum problema que pode estar ligado a essa atualização nos avisem.

Atenciosamente,