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

ABINEL SANTIAGO CERQUEIRA JUNIOR

ANÁLISE SOBRE A MODELAGEM DE AMEAÇAS APLICADA EM ATAQUES CIBERNÉTICOS DO TIPO APT (*ADVANCED PERSISTENT THREATS*) EM UMA ORGANIZAÇÃO PÚBLICA

São Paulo
Abril/2024

ABINEL SANTIAGO CERQUEIRA JUNIOR

ANÁLISE SOBRE A APLICAÇÃO DA MODELAGEM DE AMEAÇAS EM ATAQUES CIBERNÉTICOS DO TIPO APT (*ADVANCED PERSISTENT THREATS*) EM UMA ORGANIZAÇÃO PÚBLICA

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
Abril/2024

Cerqueira Junior, Abinel Santiago

C416a Análise sobre a aplicação da modelagem de ameaças em ataques cibernéticos do tipo APT (*advanced persistent threats*) em uma organização pública / Abinel Santiago Cerqueira Junior. – São Paulo: CPS, 2024.

89 f. : il.

Orientador: Prof. Dr. Carlos Hideo Arima

Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos) – Centro Estadual de Educação Tecnológica Paula Souza, 2024.

1. Modelagem de ameaças. 2. Segurança da informação. 3. *Advanced persistent threat*. 4. Serviço digital. I. Arima, Carlos Hideo. II. Centro Estadual de Educação Tecnológica Paula Souza. III. Título.

ABINEL SANTIAGO CERQUEIRA JUNIOR

ANÁLISE SOBRE A APLICAÇÃO DA MODELAGEM DE AMEAÇAS EM ATAQUES CIBERNÉTICOS DO TIPO APT (*ADVANCED PERSISTENT THREATS*) EM UMA ORGANIZAÇÃO PÚBLICA

Prof. Dr. Carlos Hideo Arima
Orientador – CEETEPS

Profa. Dra. Liria Matsumoto Sato
Examinador Externo – Universidade De São Paulo - USP

Prof. Dr. Napoleão Verardi Galegale
Examinador Interno - CEETEPS

São Paulo, 18 de abril de 2024

A Deus, família e todos que me ajudaram ao longo do caminho.

AGRADECIMENTOS

Agradeço a Deus por absolutamente tudo na minha vida e a minha família por todo apoio, em especial a minha esposa por todo amor, carinho, sabedoria, suporte nos momentos mais desafiadores, por toda paciência e prudência para me ajudar. À minha pequena Isabela que, no exato momento que escrevo essa frase, tem apenas 6 anos de idade e viu o papai escrever, parar para brincar com ela e reescrever este trabalho incansavelmente, por muitas e muitas vezes.

Aos meus pais pelo constante amor e incentivo desde sempre e ao meu querido sogro (em memória) que, além de ter sido um grande amigo, me ensinou a prática do bom comportamento e da gentileza, que buscarei levar comigo ao longo da minha vida.

Agradeço especialmente ao Prof. Dr. Carlos Hideo Arima por todo aprendizado, orientações e conselhos dados durante os dois anos de curso. O Arima é, sem dúvidas, o melhor professor que tive na vida, além de ser uma pessoa espetacular e incrível. Um verdadeiro mestre. Espero manter contato e levar essa amizade por muitos anos para que eu possa retribuir tudo que ele me proporcionou.

Aproveito o espaço para agradecer nominalmente todos os professores que tive maior contato durante as disciplinas cursadas e que me ensinaram tudo que foi necessário para concluir essa etapa: ao Prof. Napoleão pela sua clareza, pragmatismo e objetividade em todas as orientações, a Profa. Líria por sua assertividade durante a etapa de qualificação, à Profa. Marília por seu apoio durante as aulas, aos professores Marcelo Duduchi e Márcia Ito por todo aprendizado e aos professores Rosinei, Fabrício, Eliane e Galhardi pelo aprendizado.

Por fim, agradeço a toda turma do Mestrado Profissional em Gestão e Tecnologia, T10. Torço pelo sucesso de cada um e que todos, sem exceção, consigam atingir seus objetivos na vida pessoal e profissional.

A você que está lendo esta seção, confie em si mesmo e siga em frente, sempre. Muito obrigado por ler até aqui e que Deus te abençoe!

Ouça conselhos e aceite instruções,
e acabará sendo sábio. (Salomão)

RESUMO

CERQUEIRA JUNIOR, A. S. **Análise sobre a aplicação da modelagem de ameaças em ataques cibernéticos do tipo APT (*Advanced Persistent Threats*) em uma organização pública**. 88 f. Dissertação (Mestrado Profissional em Gestão e Desenvolvimento da Educação Profissional). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2024.

O presente trabalho tem por objetivo analisar a aplicação de um processo específico para modelagem de ameaças para análise e prevenção de ataques cibernéticos do tipo Advanced Persistent Threats (APT), em serviços públicos digitais, mantidos por uma organização pública brasileira. A metodologia aplicada nesta pesquisa foi baseada na Design Science Research (DSR), com o apoio de métodos como a pesquisa-ação e entrevistas individuais. Ao todo, 12 especialistas em cibersegurança foram consultados para avaliação do método MCT-RB (Modelling Cyber Threats using a Risk-Based approach) e seu processo de negócio aplicado em um serviço público digital, disponível na internet. Os resultados obtidos permitem observar que a aplicação de uma modelagem de ameaças, específica para APTs, pode apoiar organizações a efetuar o gerenciamento do risco cibernético para prevenção de ameaças cibernéticas, que as tarefas relacionadas ao gerenciamento de risco devem ser observadas e conduzidas pelo gestor do serviço púbico digital responsável, que o método proposto pode ser aplicado para habilitação de um novo serviço ou tecnologia a ser implementada em organizações que adotam a transformação digital em seus produtos e serviços, e que o processo desenvolvido para modelar ameaças pode ser formalizado em processos operacionais de cibersegurança como gestão de vulnerabilidades, gestão de atualizações de segurança, testes de intrusão, processos de detecção e bloqueio de ameaças como o SOC (Security Operations Center), respostas a incidentes de segurança e ações de conscientização aos usuários. Além disso, a modelagem proposta pode apoiar organizações durante a habilitação ou renovação da certificação ISO 27001. Sistemas de Informação e Tecnologias Digitais e Gestão Estratégica de Tecnologia da Informação.

Palavras-chave: Modelagem de ameaças. Segurança da informação. *Advanced Persistent Threat*. Serviço digital.

ABSTRACT

CERQUEIRA JUNIOR, A. S. **Análise sobre a aplicação da modelagem de ameaças em ataques cibernéticos do tipo APT (*Advanced Persistent Threats*) em uma organização pública**. 88 f. Dissertação (Mestrado Profissional em Gestão e Desenvolvimento da Educação Profissional). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2024.

The present work aims to analyze the application of a specific process for threat modeling for the analysis and prevention of Advanced Persistent Threats (APT) cyberattacks in digital public services maintained by a Brazilian public organization. The methodology applied in this research was based on Design Science Research (DSR) with the support of methods such as action research and individual interviews. In all, 12 cybersecurity experts were consulted to evaluate the MCT-RB (Modelling Cyber Threats using a Risk-Based approach) method and its business process applied in a digital public service available on the internet. The results obtained allow us to observe that the application of a specific threat modeling for APTs can support organizations to carry out cyber risk management for the prevention of cyber threats, that the tasks related to risk management must be observed and conducted by the product owner of the digital public service, that the proposed method can be applied to enable a new service or technology to be implemented in organizations that adopt the digital transformation in its products and services and that the process developed to model threats can be formalized in operational cybersecurity processes such as vulnerability management, patch management, penetration testing, threat detection and blocking processes like a SOC (Security Operations Center), security incident responses, and user awareness actions. In addition. the proposed modeling can support organizations during the qualification or renewal of ISO 27001 certification. Information Systems and Digital Technologies and Strategic Management of Information Technology.

Keywords: Threat Model. Information Security. Advanced Persistent Threat. Digital service.

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SIGLAS

APT	*Advanced Persistent Threats*
BPM	*Business Process Model*
CVSS	*Common Vulnerability Scoring System*
DSR	*Design Science Research*
GDPR	*General Data Protection Regulation*
IPS	*Intrusion Prevention System*
LGPD	Lei Geral de Proteção de Dados
MCT-RB	*Modelling Cyber Threats using Risk-Based*
MFA	*Multi-Factor Authentication*
PDTI	Plano Diretor de Tecnologia da Informação
PDSI	Plano Diretor de Segurança da Informação
PRISMA-P	*Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols*
RACI	*Responsible, Accountable, Consulted, Informed*
SGSI	Sistema de Gestão de Segurança da Informação
SIEM	*Security Information and Event Management*
TI	Tecnologia da Informação
TTP	Táticas, Técnicas e Procedimentos
WAF	*Web Application Firewall*

SUMÁRIO

1 INTRODUÇÃO

O volume de dados e informações disponíveis por sistemas produtivos tecnológicos nos dias de hoje permitem que organizações em todo mundo tenham condições e infraestrutura tecnológica para desenvolver e oferecer produtos e serviços que atendam a necessidade de indústrias. A crescente digitalização de serviços oferece um significativo potencial para os negócios, o que permite um aumento na competitividade por meio da ampla oferta de soluções tecnológicas.

Nesse sentido, a transformação digital trouxe profundas mudanças nos modelos de negócios, gerando impactos na forma como as empresas se relacionam com seus consumidores, fornecedores e negócios. Por meio da transformação digital, as organizações mudaram a forma como seus produtos e serviços são apresentados e disponibilizados ao público (MOŞTEANU, 2020; FELICIANO-CESTERO *et al*., 2023).

Contudo, questões legais e regulatórias vinculadas a privacidade e proteção de dados, em especial após a criação do Regulamento 2016/679 na União Europeia, conhecida como *General Data Protection Regulation* (GDPR) relativo ao tratamento de dados pessoais (União Europeia, 2016), motivaram discussões para que organizações de diferentes setores fossem questionadas em relação a proteção de dados pessoais hospedados em serviços digitais. Dessa forma, nota-se que a segurança da informação possui papel relevante para assegurar a proteção de dados pessoais.

No Brasil, após o advento da Lei 13.709/2018, conhecida como a Lei Geral de Proteção de Dados (LGPD), que dispõe sobre a privacidade e o tratamento de dados pessoais no Brasil (BRASIL, 2018), as organizações brasileiras devem observar questões regulatórias referentes a privacidade e proteção de dados. Verifica-se que, após a regulamentação sobre privacidade e proteção de dados, tanto no Brasil como na Europa, as organizações devem aprimorar a segurança da informação para cumprimento de leis e regulamentos.

Um estudo global aponta que, após o início da pandemia em 2020, 81% dos executivos questionados pela pesquisa afirmam que a pandemia forçou as organizações a contornarem os processos de segurança cibernética. Além disso, orçamentos insuficientes, complexidade de regulamentação e relações insuficientes com as áreas de negócio são fatores que pressionaram os responsáveis pela segurança da informação nas organizações em todo

mundo (EY, 2021). Dessa forma, verifica-se que a expressiva adoção da transformação digital e a regulamentação sobre privacidade trouxeram desafios organizacionais no que diz respeito a segurança.

Nos últimos anos, a segurança da informação tem obtido maior destaque nas organizações devido ao expressivo número de tentativas de ataques que têm ocorrido no ambiente digital e por conta das violações de dados resultantes de ataques cibernéticos realizados com sucesso (MOŞTEANU, 2020).

Em 2022, somente o Brasil sofreu 31,5 bilhões de tentativas de ataques apenas no primeiro semestre de 2022 enquanto a região da América Latina e Caribe sofreu 137 bilhões de tentativas de ataques cibernéticos (FORTNET, 2022). Caso alguma tentativa de ataque seja bem-sucedida, organizações de diferentes segmentos podem ser vítimas de violações e vazamento de dados, implicando em custos adicionais ao mercado como um todo.

Segundo a IBM (2022), no Brasil, o custo estimado para as empresas que são afetadas por violações de dados é de R$ 6,45 milhões de reais. Em face dos dados citados acima, é necessário assegurar a proteção e prevenção de ameaças em sistemas digitais por meio da segurança da informação.

Whitman e Mattford (2021) afirmam que a segurança da informação é a salvaguarda e proteção da informação e de seus ativos, que inclui sistemas que armazenam, operam e transmitem informações em um meio digital, enquanto a norma técnica internacional ISO/IEC 27001 (2022) define que seu objetivo é preservar a confidencialidade, integridade e disponibilidade das informações. Nota-se que, baseado nas definições apresentadas, a segurança da informação possui papel estratégico na transformação digital, em especial nos sistemas e tecnologias da informação.

Dessa maneira, as ameaças existentes atualmente devem ser compreendidas para criação de estratégias de defesa cibernética e minimização de vulnerabilidades de segurança. Para isso, a modelagem de ameaças é considerada um processo que tem por objetivo a melhoria contínua de segurança de um ambiente, auxiliando em processos relacionados à segurança da informação ao analisar possíveis ameaças que possam explorar vulnerabilidades existentes em um sistema (YOKOYAMA; ARIMA, 2022; CERQUEIRA JUNIOR; ARIMA, 2023).

Das principais ameaças existentes no ambiente digital, destacam-se os ataques cibernéticos classificados como *Advanced Persistent Threat* (APT), também conhecidos como

ameaças avançadas persistentes, que são ataques cibernéticos executados por grupos altamente especializados cujo objetivo é comprometer a confidencialidade, integridade e a disponibilidade de uma informação ou de uma infraestrutura crítica (TATAM *et al*., 2021).

Para que a segurança da informação de um ativo ou produto digital seja aprimorada contra esse tipo de ataque, faz-se necessário compreender e analisar potenciais ameaças existentes para melhor definição de estratégias de defesa cibernética e, principalmente, no que diz respeito a gestão do risco cibernético a qual determinada organização pode estar exposta devido a oferta e disponibilidade de serviços digitais na internet.

No contexto cibernético, resumidamente, considera-se que o risco é uma medida na qual uma entidade pode estar exposta a uma ameaça, evento ou circunstância (NIST, 2023). Dessa forma, espera-se que os riscos cibernéticos a serem identificados pelas organizações, em especial as organizações públicas, sejam gerenciados e devidamente monitorados.

Pode-se afirmar que o risco cibernético é uma categoria de risco dinâmica, que tem evoluído substancialmente ao longo do tempo (ELING; WIRFS, 2019). Nota-se que, dado o alcance e exposição que os serviços digitais públicos possuem na internet, o risco cibernético de uma organização pública deve ser gerenciado com diligência.

Em face do exposto, ao considerar as ameaças avançadas persistentes contra organizações públicas, a questão de pesquisa definida para este estudo é a seguinte:

Como a aplicação da modelagem de ameaças pode ser utilizada para prevenção de ataques cibernéticos do tipo APT em uma organização pública?

Para responder à questão de pesquisa, o objetivo geral do trabalho é:

- Analisar a aplicação de um processo específico para modelagem de ameaças para análise e prevenção de ataques cibernéticos do tipo APT em serviços públicos digitais.

Os objetivos específicos desta pesquisa são:

- Efetuar revisão sistemática da literatura sobre modelagem de ameaças e APTs;
- Desenvolver um método a ser aplicado em uma organização pública brasileira para modelar ameaças cibernéticas;
- Avaliar a aplicação de um processo de negócio específico para modelar ameaças cibernéticas para prevenção de ataques APT.

Espera-se que o presente estudo possa contribuir para a segurança da informação nas organizações brasileiras, em especial aos tópicos relacionados a ameaças, vulnerabilidades e gestão de riscos cibernéticos em sistemas produtivos tecnológicos administrados por organizações públicas.

Além disso, espera-se que o processo de modelagem de uma ameaça cibernética específica, construído com a aplicação da metodologia *Design Science Research* (DSR), seja implementado e formalizado em processos operacionais relacionados à segurança da informação e segurança cibernética no setor público.

Por fim, visando a criação de um produto tecnológico que colabore com a inovação na área de estudo deste trabalho, espera-se que, a partir do artefato a ser construído utilizando o DSR, um produto técnico/tecnológico seja finalizado de forma a permitir o registro de uma patente junto ao órgão responsável no Brasil.

2 FUNDAMENTAÇÃO TEÓRICA

Para melhor compreensão sobre o tema apresentado nessa pesquisa, o referencial teórico foi divido em cinco subseções, sendo a primeira dedicada para a transformação digital e a segunda para gestão de riscos cibernéticos. A terceira subseção refere-se a modelagem de ameaças, a quarta subseção para APTs e a última subseção dedicada ao mapeamento sistemático sobre modelos de ameaças e APTs.

2.1 Transformação digital no governo brasileiro

A adoção de tecnologias permite que as organizações, de modo geral, tenham maior capacidade de aprimorar seu desempenho empresarial tanto no nível operacional como estratégico. Para tanto, observa-se que o uso de sistemas de informação pode ter papel significativo na criação ou adaptação de estratégias corporativas, principalmente no que diz respeito a inovação nas organizações (ALBERTIN; ALBERTIN, 2008; YOSHIKUNI; ALBERTIN, 2021).

Em face do exposto, nota-se que a Tecnologia da Informação (TI) pode trazer valor estratégico para as organizações e, considerando o cenário atual relacionado a transformação digital, organizações de diversos setores podem se beneficiar de sua adoção.

Apesar de todas as vantagens e benefícios gerados pela transformação digital, o aumento no volume de dados nas organizações criou um desafio especial no tratamento e segurança de dados. Dessa forma, as estratégias de digitalização de serviços devem considerar aspectos relacionados à segurança da informação e a privacidade de dados pessoais (MOŞTEANU, 2020).

Os ataques cibernéticos, de forma geral, impactam diretamente os negócios que estão disponíveis no meio digital, onde o objetivo de cada ataque cibernético pode ser único de acordo com o negócio da empresa. Por exemplo, a extorsão de usuários, a indisponibilidade de serviços ou mesmo a destruição de dados sensíveis são objetivos que podem ser definidos em um ataque cibernético (MOŞTEANU, 2020).

Dessa forma, os serviços digitais podem ser alvos de ataques cibernéticos desde o momento em que estão disponíveis para acesso na internet. Nesse contexto, para aprimorar as questões relacionadas à segurança da informação, os aspectos de gestão que devem ser avaliados pelas organizações são: estratégias de cibersegurança, processos padronizados, conformidade com leis e regulações aplicáveis, apoio da alta liderança e recursos especializados em segurança cibernética (YUSUF; HAFEEZ-BAIG, 2021).

Entretanto, cada organização deve avaliar qual tipo de ameaça cibernética pode causar problemas relacionados à segurança da informação em seus modelos de negócio digitais. Para isso, a modelagem de ameaças é um método eficaz não somente para o aumento da segurança da informação de um negócio, mas principalmente para compreensão do risco cibernético que um serviço digital pode estar exposto.

Tratando-se de administração pública e governo digital, a adoção da transformação digital permite que serviços públicos sejam disponibilizados ao cidadão por meio de aplicativos para dispositivos móveis (como *smartphones* e *tablets*) e para sites na internet mantidos por organizações públicas. No Brasil, o gov.br é a plataforma digital de relacionamento do cidadão com o governo federal brasileiro (BRASIL, 2023).

Para conhecimento, o gov.br foi regulamentado por meio do Decreto Nº 9.756, em 2019, e dispõe sobre as regras e diretrizes para unificar os canais digitais do governo federal para acesso e disponibilidade ao cidadão brasileiro. Atualmente, a plataforma oferece mais de 4 mil serviços públicos na internet e possui mais de 140 milhões de usuários cadastrados (BRASIL, 2023).

Com o avanço da plataforma e a adoção da transformação digital de serviços públicos, em comparação com 198 economias globais, o Índice *GovTech Maturity Index* 2022, divulgado pelo Banco Mundial, destaca que o Brasil foi reconhecido mundialmente como segundo líder em governo digital, ficando à frente de países como Espanha, França, Emirados Árabes Unidos, Japão e Estônia (BANCO MUNDIAL, 2022; BRASIL, 2022).

Em face ao exposto sobre o gov.br, principalmente ao considerar a relevância e alcance que um serviço digital possui, faz-se necessário que cada organização pública, seja uma empresa estatal ou mesmo um órgão público, tenha condições mínimas de identificar e efetuar a gestão dos riscos cibernéticos em serviços públicos disponíveis na internet. Para tanto, a gestão de riscos cibernéticos possui papel relevante para aprimorar a segurança da informação em serviços públicos digitais.

2.2 Gestão de riscos cibernéticos

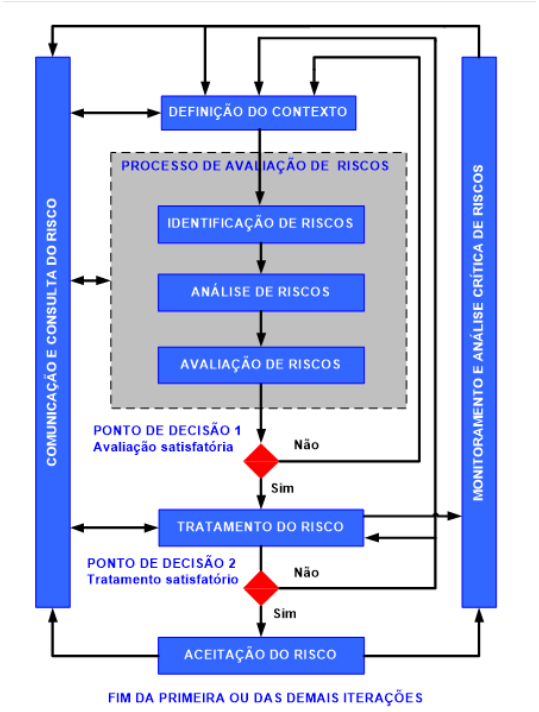
O risco cibernético é um tipo de risco que deve ser gerenciado pelas organizações, de forma que seu potencial impacto pode causar perdas financeiras, danos a reputação e demais consequências negativas a qualquer tipo de instituição, além de trazer preocupações aos indivíduos em relação a privacidade e segurança da informação (NIST, 2023).

Para gerenciar o risco cibernético e reduzir uma provável consequência negativa, como vazamento de dados e danos à imagem institucional, a utilização de referências específicas poderá servir de apoio para que organizações tenham maior entendimento para compreender, avaliar, priorizar e comunicar um risco e, com isso, planejar ações que visem reduzi-lo a um nível aceitável (NIST, 2023).

Das abordagens utilizadas para referência, destacam-se a ISO/IEC 27005 e o NIST *Cybersecurity Framework*, que são documentos que preveem diretrizes e orientações gerais para o processo de gestão do risco cibernético, podendo ser analisadas e aplicadas em qualquer tipo de organização (ABNT, 2023; NIST, 2023).

Sobre o processo, considera-se que a gestão do risco cibernético um processo contínuo que visa, entre outras atividades, identificar e avaliar o risco cibernético em uma organização. Para melhor entendimento, a Figura 1 apresenta o fluxo do processo de gestão de riscos cibernéticos sugerido pela ISO 27005 (ABNT, 2023).

Figura 1 – Fluxo do processo de gestão de riscos cibernéticos



Fonte: Adaptado de ABNT ISO/IEC 27005:2023 (2023)

O processo recomendado pela ISO 27005 indica que seu fluxo, a depender de sua aplicação, pode ser iterativo para o processo de avaliação de riscos e para as atividades relacionadas ao tratamento do risco cibernético. A seguir, cada etapa do processo é apresentada de forma resumida (ABNT, 2023).

a) **Definição do contexto**: a organização deve considerar toda documentação, normas, políticas e demais atividades e processos relacionados à segurança da informação;

b) **Processo de avaliação de riscos**: o processo de avaliação de riscos é subdividido em três atividades: identificação, análise e avaliação de riscos;

c) **Ponto de decisão 1 (avaliação satisfatória)**: antes de se dar entrada nas atividades de tratamento do risco, cabe a organização definir se a avaliação é satisfatória com base no contexto definido anteriormente. Caso a avaliação não seja satisfatória, o processo retorna à etapa de definição do contexto;

d) **Tratamento do risco**: a partir do momento em que o risco é avaliado, a organização deve iniciar o tratamento do risco conforme definições internas;

e) **Ponto de decisão 2 (tratamento satisfatório)**: após o risco cibernético ser tratado pela organização, é necessário verificar se o tratamento aplicado foi satisfatório. Caso o tratamento não seja satisfatório, o fluxo do processo retorna para a etapa de definição do contexto;

f) **Aceitação do risco**: quando o risco cibernético é tratado e sua proposta de tratamento é satisfatória, o risco cibernético é aceito e documentado;

g) **Comunicação e consulta do risco**: as atividades relacionadas à comunicação e consulta do risco são iniciadas após a finalização das atividades do tratamento e aceitação dos riscos. Nesse momento, as partes interessadas são informadas sobre os riscos identificados em um determinado sistema ou tecnologia;

h) **Monitoramento e análise crítica de riscos**: a etapa é iniciada quando as atividades relacionadas ao tratamento e aceitação dos riscos são finalizadas pelas áreas competentes. Os resultados são encaminhados para as partes interessadas iniciarem o monitoramento e reanalisar (se necessário) os riscos tratados.

Dado o contexto apresentado, verifica-se que a gestão do risco cibernético é um processo contínuo e iterativo que deve ser executado pelas organizações para redução de eventual impacto ou consequência negativa de uma ameaça. Com isso, espera-se que a identificação e análise do risco seja efetuada com maior compreensão sobre quais eventos e ameaças cibernéticas podem trazer impactos à segurança da informação em uma tecnologia.

2.3 Modelagem de ameaças

Na segurança da informação, considerando os processos existentes para avaliação dos riscos cibernéticos em uma organização, pode-se afirmar que modelagem de ameaças é um processo diretamente relacionado à gestão de riscos (YOKOYAMA; ARIMA, 2022; CERQUEIRA JUNIOR; ARIMA, 2023).

Uma ameaça cibernética pode ser definida como um evento ou circunstância causada por um agente de ameaça que visa explorar, intencionalmente ou não, uma vulnerabilidade técnica específica. Para que uma ameaça seja analisada com profundidade, aplicam-se diferentes tipos de métodos para análise de uma ameaça ou ataque cibernético (NIST, 2023).

Sob o ponto de vista de proteção e defesa cibernética, os métodos para avaliação e descrição de um ataque devem ser utilizados para representar, por exemplo, a sequência de eventos necessários para que um ataque seja bem-sucedido (LALLIE; DEBATTISTA; BAL, 2020). Para obter entendimento sobre ameaças, os métodos disponíveis que podem ser empregados para avaliação de uma ameaça podem ser classificados como formais, gráficos, automáticos ou manuais (XIONG; LAGERSTRÖM, 2019; TATAM et al., 2021).

Métodos formais são baseados em modelos matemáticos e os modelos gráficos podem ser representados visualmente por meio de um fluxo ou tabela. Nos métodos automáticos, utilizam-se produtos de segurança que realizam testes automatizados em um sistema, enquanto no método manual, a análise de uma ameaça é feita manualmente sem qualquer ferramenta de automação de testes (XIONG; LAGERSTRÖM, 2019).

Dos métodos disponíveis para modelagem de uma ameaça cibernética, destacam-se o CVSS, a árvore de ataque e a superfície de ataque, bem como a utilização do framework Mitre para coleta de informações sobre Táticas, Técnicas e Procedimentos (TTP) de um APT (SHNEIER, 1999, ALHEBAISHI; JAJODIA; SINGHAL (2017); MITRE, 2023, NIST, 2023).

O CVSS (*Common Vulnerability Scoring System*) é um método formal utilizado para medir a severidade de uma vulnerabilidade em sistemas de informação de forma quantitativa, sendo que as versões disponíveis para uso do CVSS são as versões 2.0 e 3.0 (MITRE, 2023; NIST, 2023).

Diferentemente de uma análise de risco, o CVSS é uma métrica que calcula aspectos da ameaça, onde seu valor pode ser mensurado de 0 a 10. A Tabela 1 apresenta a severidade e a pontuação do CVSS referente a vulnerabilidade identificada, onde os detalhes de vulnerabilidade identificada são mantidos na base de vulnerabilidades do NIST (NIST, 2023).

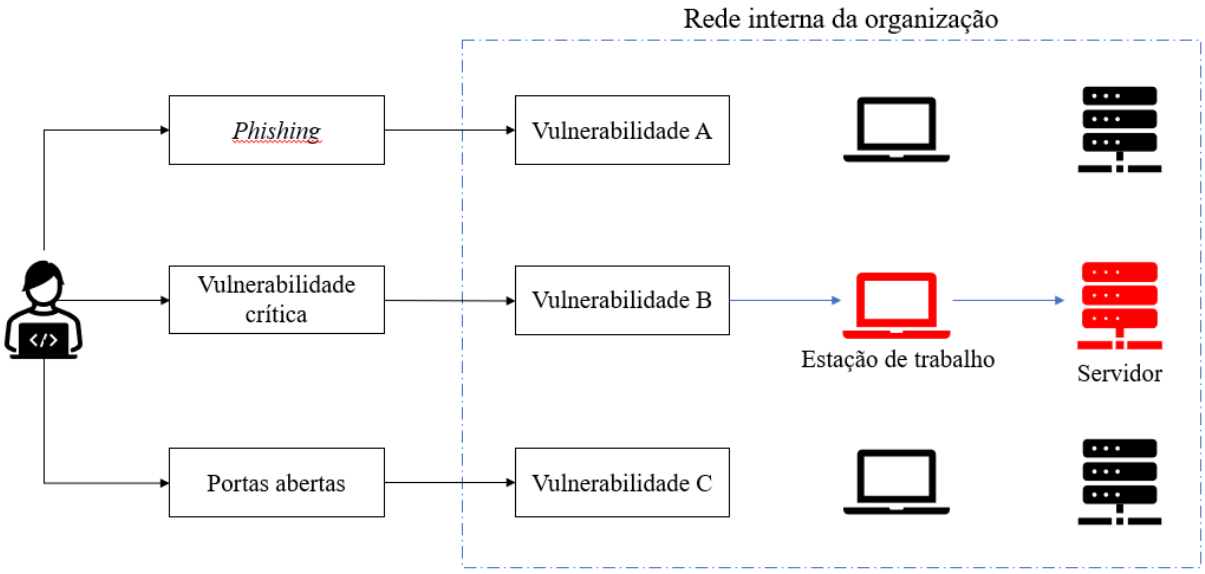
Tabela 1 – CVSS v2 e CVSS v3

Pontuação do CVSS v2.0		**Pontuação do CVSS v3.0**	
Severidade	Pontuação (*rating*)	Severidade	Pontuação (*rating*)
Alto	7.0 - 10.0	Crítico	9.0 - 10.0
Médio	4.0 - 6.9	Alto	7.0 - 8.9
Baixo	0.0 - 3.9	Médio	4.0 - 6.9
		Baixo	0.0 - 3.9

Fonte: Adaptado de NIST (2023)

A superfície de ataque é um método gráfico que permite o mapeamento dos vetores de ataque disponíveis para uma ameaça. Pode-se considerar que o método é a combinação de todos os vetores de ataque disponíveis em um determinado contexto, ou seja, quanto maior o número de vetores de ataque uma organização ou sistema tiver, maior será a superfície de ataque conforme apresentação da Figura 2 (CLOUDFLARE, 2023).

Figura 2 - Superfície de ataque e vetores de ataque



Fonte: Adaptada de Cloudflare (2023)

Nota-se que, a partir do mapeamento da superfície de ataque, recomenda-se que uma organização que possui serviços disponíveis na Internet elimine os possíveis vetores de ataque com o objetivo de aumentar a sua segurança cibernética. Outro método gráfico utilizado para modelar uma ameaça cibernética é a arvore de ataque, que é um método aplicado para apresentar os caminhos que um ameaça pode fazer para obter sucesso em um ataque com um objetivo específico (SHNEIER, 1999; LALLIE; DEBATTISTA; BAL, 2020).

Para ameaças consideradas avançadas, que podem trazer diversos impactos negativos a uma organização, a aplicação de métodos para modelagem de uma ameaça cibernética permite que seja possível descrever como uma ameaça pode obter sucesso em um ataque cibernético. No caso de APTs, considera-se relevante descrever e analisar as Táticas, Técnicas e Procedimentos (TTP) para caracterizar seu comportamento (DELGADO, 2018; TATAM et al., 2021).

Portanto, nota-se a importância de se efetuar a análise e gestão do risco cibernético em sistema mantido por uma organização com o objetivo de identificar o nível de exposição ao risco de tal sistema frente as ameaças.

A partir do momento em que vulnerabilidades técnicas e ameaças cibernéticas são devidamente avaliadas por métodos para modelagem, cabe a organização aplicar os procedimentos e controles de segurança necessários para efetuar a gestão do risco cibernético, seguindo diretrizes e normas definidas para tal categoria de risco para consolidar a prevenção de ameaças.

2.4 Advanced Persistent Threat (APT)

Uma ameaça avançada persistente, conhecida pelo termo APT, é um tipo de ataque cibernético executado por grupos especializados que possuem recursos, ferramentas e infraestrutura tecnológica para mobilizar ataques direcionados com objetivos específicos (CHEN; DESMET; HUYGENS, 2014; TATAM et al. 2021).

O termo APT foi trazido em 2006 pela Força Aérea dos Estados Unidos da América para representar invasores ou ameaças desconhecidas visando facilitar as discussões a respeito. De acordo com o Singh et al. (2019) e Tatam et al. (2021), no contexto da segurança da informação, o termo APT deriva das seguintes características:

- *Advanced* (avançada): considera-se que esse tipo de ameaça é de característica avançada, em especial devido ao amplo número de recursos disponíveis (infraestrutura e capacidade financeira), sua alta habilidade técnica para evasão de controles de segurança (firewalls, entre outros) e a capacidade de manter-se

dentro de organizações e obter dados confidenciais sem qualquer tipo de detecção;

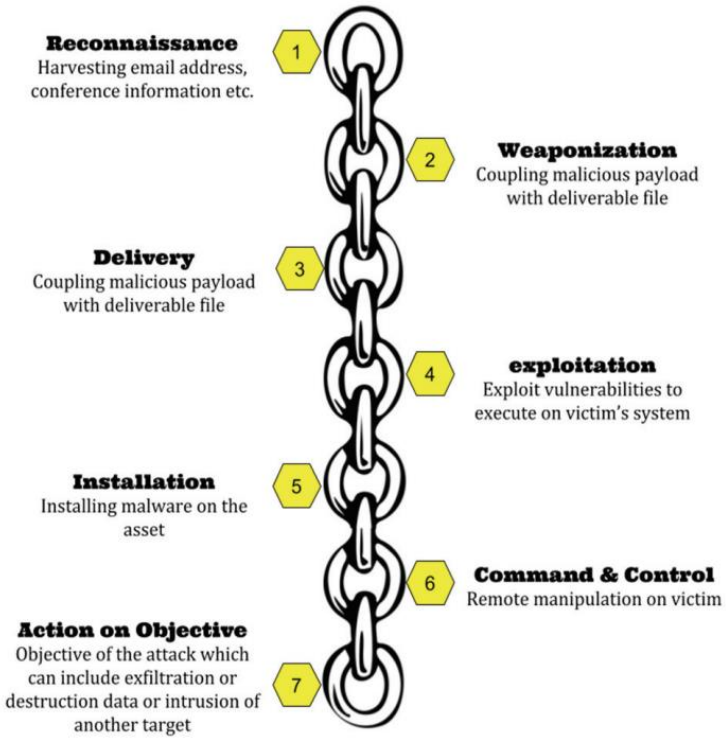
- *Persistent* (persistente): em comparação com outras ameaças, como hackativistas e invasores que não detêm grande conhecimento especializado e experiência em segurança cibernética, um ataque APT tem por característica ser persistente, ou seja, é um ataque que pode durar semanas ou meses até que seu objetivo seja alcançado. Exemplo: causar indisponibilidade em um sistema, efetuar vazamento de dados pessoais, entre outros. Além disso, a ameaça é considerada persistente a partir do momento em que o acesso inicial é obtido em um ataque bem-sucedido, pois sua remoção e proteção a partir do acesso inicial é altamente complexa e difícil;
- *Threat* (ameaça): dada suas características, um ataque APT é considerada uma ameaça cibernética.

Em 2013, o termo obteve projeção mundial devido a um ataque cibernético bem-sucedido relatado pela New York Times, onde estima-se que o ataque teve duração de mais de 30 dias ininterruptos e, além disso, a empresa divulgou que vinha sendo atacada por quatro meses seguidos. Com o objetivo de detalhar o funcionamento do ataque, a empresa resolveu descrever como o ataque ocorreu em matéria publicada. Após a publicação da matéria pelo New York Times, o ataque foi atribuído a unidade militar chinesa, conhecida como APT1 (KARSPERSKY, 2013; NEW YORK TIMES, 2013).

O *framework* Mitre Att&ck é uma base de informações referentes a esse tipo de ataque que contém dados e registros detalhados sobre as principais táticas, técnicas e procedimentos de APT executados mundialmente (MITRE, 2023). Verifica-se que, após obter acesso aos TTPs executados por APTs, é necessário obter melhor entendimento sobre o ciclo de vida de um ataque cibernético.

Para descrever o ciclo de vida de um ataque cibernético, em 2011, após a publicação do método Cyber Kill Chain, os ataques começaram a serem descritos com maior assertividade para mapeamento do ciclo de vida e principais etapas de um ataque cibernético (HUTCHINS et al., 2011; CHEN; DESMET; HUYGENS, 2014; SINGH et al., 2019). Para conhecimento, o Cyber Kill Chain é um método que visa descrever as principais etapas que são efetuadas em um ataque, conforme apresentação da Figura 3.

Figura 3 – Ciclo de vida de um ataque cibernético de acordo com o Cyber Kill Chain



Fonte: adaptado de Hutchins *et al*. (2011) e Bahrami *et al*. (2019)

Para melhor compreensão sobre o ciclo de vida de um ataque proposta pelo *Cyber Kill Chain*, no que diz respeito a cada etapa sugerida pelo método apresentada na Figura 4, o Quadro 1 apresenta a relação entre as etapas do Cyber Kill Chain e sua descrição resumida.

Quadro 1 – Descrição das etapas do *Cyber Kill Chain*

Etapas	**Descrição**
Reconhecimento	Obter informações sobre a organização, como pessoas, tecnologias utilizadas, entre outros.
Escolha de ferramentas (*weaponization*)	Após finalizar a etapa de reconhecimento, o atacante seleciona as ferramentas (*softwares*, códigos etc.) necessárias para execução do ataque.
Entrega ou execução	A execução ou entrega do ataque consiste em enviar o código malicioso (vírus, etc) para a organização, pessoa ou tecnologia para iniciar a exploração
Exploração	A etapa inicia-se com a exploração de uma vulnerabilidade técnica de segurança em um sistema para obtenção do acesso inicial a infraestrutura do alvo.
Instalação	A etapa de instalação tem por objetivo manter o acesso inicial no sistema invadido por um longo período.
Comando e Controle	A etapa referente ao Comando e Controle visa configurar mecanismos para efetuar o controle total do sistema de forma autônoma e remota.
Ações sobre objetivos	A última etapa do *Cyber Kill Chain*, conhecida como Ações sobre Objetivos, busca executar as tarefas necessárias para cumprir os objetivos definidos pelo atacante/invasor.

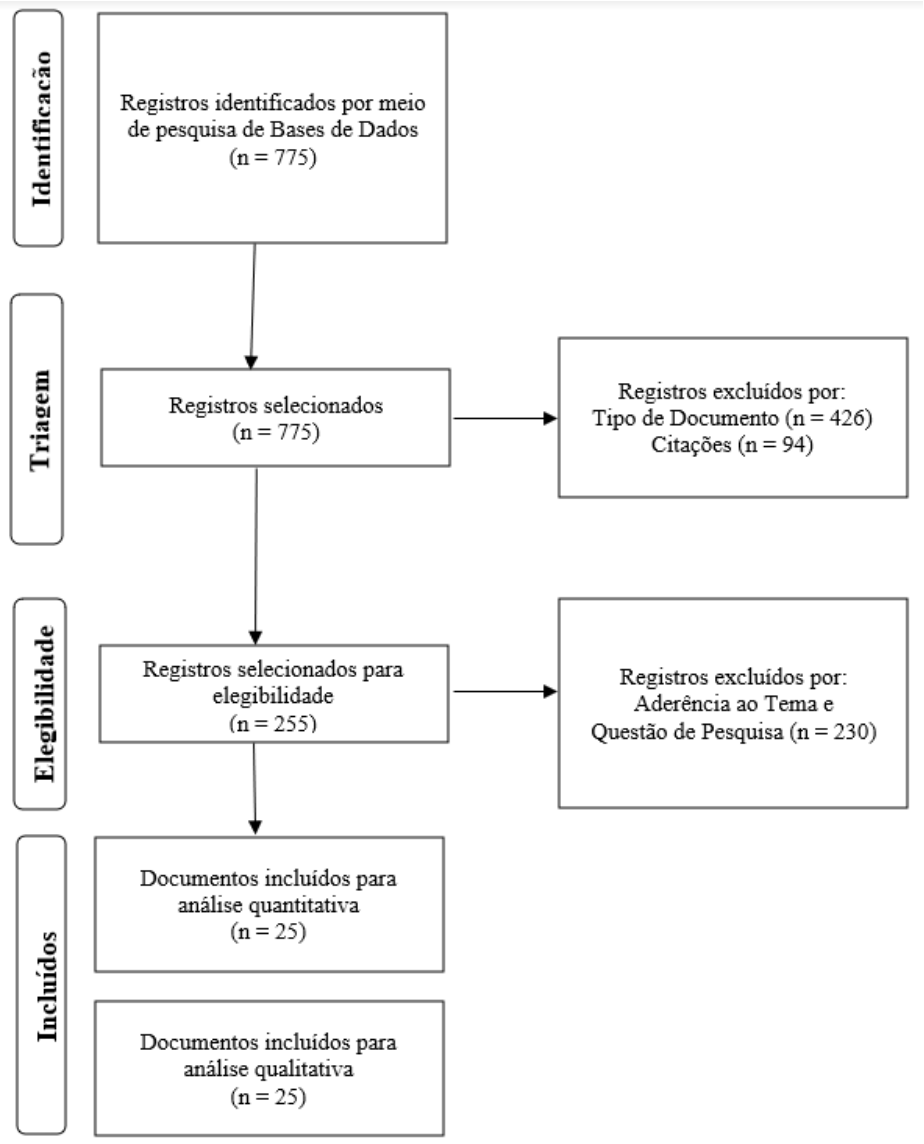
Fonte: adaptada de Hutchins *et al*. (2011) e Chen; Desmet; Huygens (2014)

Nota-se que as sete etapas mapeadas pelo Cyber Kill Chain permitem observar o comportamento e ações que podem ser executadas por uma ameaça altamente qualificada como é o caso de um APT. Desse modo, tendo em vista o objetivo de prevenção contra esse tipo de ataque, verifica-se a relevância de se mapear e analisar o ciclo de vida de um ataque cibernético para elaboração de estratégias de defesa cibernética.

2.5 Mapeamento Sistemático sobre Modelos de Ameaças e APTs

Para o desenvolvimento desta pesquisa, de caráter qualitativo, uma revisão sistemática da literatura foi conduzida com a adoção de um protocolo baseado no PRISMA-P com o objetivo de obter uma análise dos artigos selecionados. Para conhecimento, o PRISMA-P foi construído como um roteiro para apoiar pesquisadores na execução de revisões sistemáticas (MOHER et al., 2015). De acordo com Moher et al. (2015), as etapas sugeridas no fluxograma do PRISMA-P são identificação, triagem, elegibilidade e documentos incluídos para análise, conforme fluxograma apresentado na Figura 4.

Figura 4 – Fluxograma da revisão sistemática da literatura



Fonte: Resultado da pesquisa (2023)

Iniciou-se a etapa de identificação do protocolo com a pesquisa em 5 bases de dados: ACM Digital Library, IEEE Xplore, Science Direct, Scopus e Web of Science. A Tabela 2 apresenta os critérios de inclusão adotados, bem como as palavras-chave e a *string* utilizada em cada base de dados para busca dos resultados. Para conhecimento, adotou-se o período de 5 anos, de 2018 a 2022.

Tabela 2 - Quantidade de resultados por base de dados

Base de Dados	**Quantidade de Resultados**	***String* de busca**
ACM Digital Library	131	*[[All: threat modeling] OR [All: threat model]] AND [All: "advanced persistent threat"] AND [[All: cybersecurity] OR [All: information security]]*
IEEE Xplore	127	*All Fields: (threat modeling OR threat model) AND (advanced persistent threat) AND (cybersecurity OR information security)*
Science Direct	247	*("All Metadata":threat modeling OR "All Metadata":threat model) AND ("All Metadata":advanced persistent threat) AND ("All Metadata":cybersecurity OR "All Metadata":information security)*
Scopus	136	*("threat modeling" OR "threat model") AND ("advanced persistent threat") AND ("cybersecurity" OR "information security")*
Web of Science	134	*All Fields: (threat modeling OR threat model) AND (advanced persistent threat) AND (cybersecurity OR information security)*

Fonte: Resultado da pesquisa (2023)

Após conclusão da etapa de identificação, a etapa de triagem foi executada conforme critérios de exclusão apresentados na Tabela 2. Utilizando-se do Microsoft Excel para execução da triagem e organização dos resultados, considera-se o tipo de documento e o número de citações que cada publicação possui como critérios de exclusão.

Tabela 2 - Critérios de exclusão

Critérios de exclusão	**Descrição**
Tipo de documento	Publicações que não sejam artigos (livros, revistas, entre outros)
Citações	Publicações que tenham acima de 10 citações

Fonte: Resultado da pesquisa (2023)

Após a conclusão da etapa de triagem, iniciou-se a etapa de elegibilidade visando selecionar os artigos aderentes ao tema e questão de pesquisa. Conforme apresentação do Quadro 2, foram selecionados 25 estudos para análise, com o objetivo de responder à questão de pesquisa.

Quadro 2 – Trabalhos selecionados

Título	Autores	DOI
An enhanced deep learning based framework for web attacks detection, mitigation and attacker profiling	Shahid *et al*. (2022)	https://doi.org/10.1016/j.jnca.2021.103270
APT attacks on industrial control systems: A tale of three incidents	Kumar *et al*. (2022)	https://10.1016/j.ijcip.2022.100521
A review of threat modelling approaches for APT-style attacks	Tatam *et al*. (2021)	https://doi.org/10.1016/j.heliyon.2021.e05969
Cyber-attack scoring model based on the offensive cybersecurity framework	Kim; Alfouzan; Kim (2021)	https://doi.org/10.3390/app11167738
Improving SIEM alert metadata aggregation with a novel kill-chain based classification model	Bryant; Saiedian (2020)	https://doi.org/10.1016/j.cose.2020.101817
APT datasets and attack modeling for automated detection methods: A review	Stojanović; Hofer-Schmitz; Kleb (2020)	https://doi.org/10.1016/j.cose.2020.101734
A Game-Theoretic Approach for Dynamic Information Flow Tracking to Detect Multistage Advanced Persistent Threats	Moothedath *et al*. (2020)	https://doi.org/10.1109/TAC.2020.2976040
A New Proposal on the Advanced Persistent Threat: A Survey	Quintero-Bonilla; Martín Del Rey (2020)	https://doi.org/10.3390/app10113874

Título	Autores	DOI
Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics	Zimba *et al*. (2020)	https://doi.org/10.1016/j.future.2020.01.032
Conan: A Practical Real-Time APT Detection System With High Accuracy and Efficiency	Xiong *et al*. (2020)	https://doi.org/10.1109/TDSC.2020.2971484
Alerts Correlation and Causal Analysis for APT Based Cyber Attack Detection	Khosravi; Ladani (2020)	https://doi.org/10.1109/ACCESS.2020.3021499
A review of attack graph and attack tree visual syntax in cyber security	Lallie; Debattista; Bal (2020)	https://doi.org/10.1016/j.cosrev.2019.100219
Insider Threat Modeling: An Adversarial Risk Analysis Approach	Joshi; Aliaga; Insua (2020)	https://doi.org/10.1109/TIFS.2020.3029898
Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack	Ahmad *et al*. (2019)	https://doi.org/10.1016/j.cose.2019.07.001
A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions	Singh *et al*. (2019)	https://doi.org/10.1007/s11227-016-1850-4
Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures	Bahrami *et al*. (2019)	https://doi.org/10.3745/JIPS.03.0126

Título	Autores	DOI
A novel approach for APT attack detection based on combined deep learning model	Do Xuan; Dao (2019)	https://doi.org/10.1007/s00521-021-05952-5
Cyber threat intelligence sharing: Survey and research directions	Wagner *et al.* (2019)	https://doi.org/10.1016/j.cose.2019.101589
Dynamic defense strategy against advanced persistent threat under heterogeneous networks	Lv; Chen; Hu (2019)	https://doi.org/10.1016/j.inffus.2019.01.001
Modified cyber kill chain model for multimedia service environments	Kim; Kwon; Kim (2019)	https://doi.org/10.1007/s11042-018-5897-5
Disguised executable files in spear-phishing emails: detecting the point of entry in advanced persistent threat	Ghafir *et al.* (2018)	https://doi.org/10.1145/3231053.3231097
A Risk Management Approach to Defending Against the Advanced Persistent Threat	Yang *et al.* (2018)	https://doi.org/10.1109/TDSC.2018.2858786
Attacker-Centric View of a Detection Game against Advanced Persistent Threats	Xiao *et al.* (2018)	https://doi.org/10.1109/TMC.2018.2814052
Multi-Stage Attack Detection Using Contextual Information	Aparicio-Navarro *et al.* (2018)	https://doi.org/10.1109/MILCOM.2018.8599708

Título	Autores	DOI
Effective Repair Strategy Against Advanced Persistent Threat: A Differential Game Approach	YANG *et al.* (2018)	https://doi.org/10.1109/TIFS.2018.2885251

Fonte: Resultado da pesquisa (2023)

Após seleção dos artigos, considerando a questão de pesquisa "Como a aplicação da modelagem de ameaças pode ser utilizada para prevenção de ataques cibernéticos do tipo APT em uma organização pública?", verificou-se quais tipos de métodos foram adotados nos trabalhos selecionados após leitura completa, assim como o principal método aplicado ou abordado para efetuar a modelagem de uma ameaça.

Os tipos de métodos apresentados no Quadro 5 considerou a classificação proposta pela revisão sistemática feita por Xiao e Lagerstron (2019), que consideram quatro tipos de métodos para modelagem de uma ameaça cibernética: manual, automatizado, formal e gráfico. O Quadro 3 apresenta, resumidamente, os métodos abordados pelos autores dos trabalhos para modelagem de ameaças cibernéticas.

Quadro 3 – Métodos abordados para modelar ameaças cibernéticas

Autores	Manual	Automatizado	Formal	Gráfico	Não se aplica	Principal método
Shahid *et al.* (2022)		X	X			Modelo ou software customizado (baseado em modelos de *deep learning*)
Kumar *et al.* (2022)	X			X		Árvore de ataque (*attack tree*)
Tatam *et al.* (2021)					X	Não se aplica
Kim; Alfouzan; Kim (2021)					X	*Cyber Kill Chain*
Bryant; Saiedian (2020)		X	X			*Cyber Kill Chain*
Stojanović; Hofer-Schmitz; Kleb (2020)	X	X	X			*Attack life-cycle model*
Moothedath *et al.* (2020)		X	X			Modelo ou software customizado (*game-theory*)
Quintero-Bonilla; Martín Del Rey (2020)		X	X			APT *life-cycle* (Fireeye's Mandiant e *Cyber Kill Chain*)
Zimba *et al.* (2020)	X					*Cyber Kill Chain*
Xiong *et al.* (2020)		X				Modelo ou software customizado (*protótipo*)
Autores	**Manual**	**Automatizado**	**Formal**	**Gráfico**	**Não se aplica**	**Principal método**

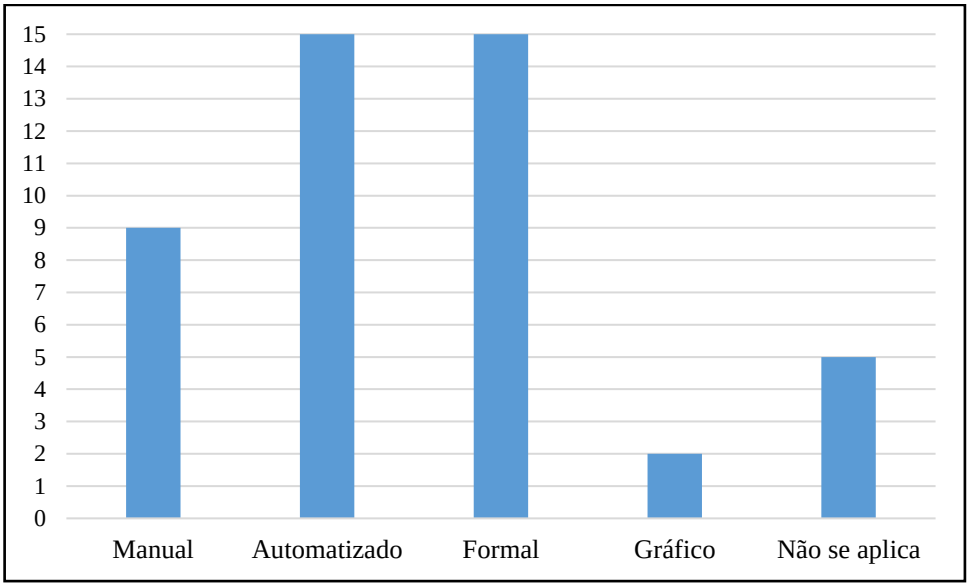
Khosravi; Ladani (2020)	X	X	X			*Intrusion Kill Chain*
Lallie; Debattista; Bal (2020)		X	X	X		Árvore de ataque (*attack tree*)
Joshi; Aliaga; Insua (2020)		X	X			Modelo ou software customizado (*game-theory*)
Ahmad *et al*. (2019)					X	Não se aplica
Singh *et al*. (2019)					X	Não se aplica
Bahrami *et al*. (2019)	X					*Cyber Kill Chain*
Do Xuan; Dao (2019)		X	X			Modelo ou software customizado (baseado em modelos de *deep learning*)
Wagner *et al*. (2019)		X				*Cyber Threat Intelligence (CTI)*
Lv; Chen; Hu (2019)	X	X	X			Modelo ou software customizado (*game-theory*)
Kim; Kwon; Kim (2019)					X	*Cyber Kill Chain*
Ghafir *et al*. (2018)		X	X			Modelo ou software customizado (*protótipo*)
Yang *et al*. (2018)	X		X			Modelo ou software customizado (*game-theory*)
Xiao *et al*. (2018)	X		X			Modelo ou software customizado (*game-theory*)
Aparicio-Navarro *et al*. (2018)		X	X			*Multi-Stage Attack* (MSA)
Yang *et al*. (2018)	X	X	X			Modelo ou software customizado (*game-theory*)

Fonte: Resultado da pesquisa (2023)

Verifica-se que, dos principais métodos aplicados para modelar ameaças cibernéticas, *Cyber Kill Chain* e modelos ou softwares customizados foram os principais métodos abordados em comparação com outros métodos, como a árvore de ataque e *Multi-Stage Attack*. Por se tratar de artigos de revisão ou pesquisa bibliográfica, os artigos de Tatam et al. (2021), Kim, Alfouzan e Kim (2021), Singh et al. (2019) e Bahrami et al. (2019), não sugerem aplicação de métodos específicos.

Para melhor visualização dos tipos de métodos aplicados nos estudos selecionados, a Figura 5 apresenta o gráfico de barras com os 4 tipos de métodos classificados conforme apresentação do Quadro 3.

Figura 5 – Métodos aplicados nos artigos selecionados



Fonte: Resultado da pesquisa (2023)

Dos 25 artigos selecionados, somente a 4 artigos não se aplica qualquer tipo de método, pois são artigos de revisão ou pesquisa bibliográfica. Nota-se que, ao analisar os tipos de métodos apresentados na Figura 5, verifica-se que os métodos automatizados e formais são mais utilizados em comparação com os métodos manual e gráfico, o que sugere a necessidade de se utilizar ferramentas para executar testes automatizados que possuam métricas específicas para modelagem de uma ameaça.

Além dos métodos disponíveis para efetuar a modelagem de ameaças, o tipo de controle de segurança abordado por cada artigo foi para análise. Considerando que os tipos de controles de segurança podem ser classificados como preventivo, detectivo e corretivo (TSEGAYE; FLOWERDAY, 2014; MOURATIDIS et al. 2023) e que podem ser aplicados em conjunto para mitigar riscos, o Quadro 4 apresenta os tipos de controle de segurança abordados.

Quadro 4 – Tipo de controle de segurança por artigo

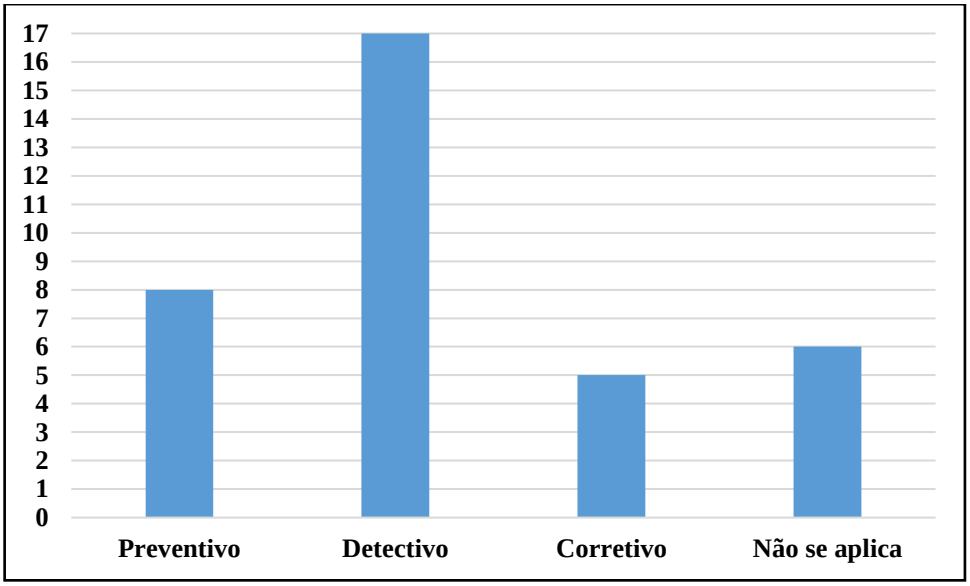
Autores	Preventivo	Detectivo	Corretivo	Não se aplica
Shahid *et al*. (2022)	X	X		
Kumar *et al*. (2022)	X			
Tatam *et al*. (2021)				X
Kim; Alfouzan; Kim (2021)				X
Bryant; Saiedian (2020)		X		
Stojanović; Hofer-Schmitz; Kleb (2020)		X		
Moothedath *et al*. (2020)		X		
Quintero-Bonilla; Martín Del Rey (2020)				X
Autores	**Preventivo**	**Detectivo**	**Corretivo**	**Não se**

				aplica
Zimba *et al*. (2020)		X		
Xiong *et al*. (2020)		X		
Khosravi; Ladani (2020)		X		
Lallie; Debattista; Bal (2020)				X
Joshi; Aliaga; Insua (2020)	X	X		
Ahmad *et al*. (2019)	X	X	X	
Singh *et al*. (2019)				X
Bahrami *et al*. (2019)				X
Do Xuan; Dao (2019)		X		
Wagner *et al*. (2019)		X	X	
Lv; Chen; Hu (2019)	X	X		
Kim; Kwon; Kim (2019)	X	X	X	
Ghafir *et al*. (2018)		X		
Yang *et al*. (2018)	X		X	
Xiao *et al*. (2018)		X		
Aparicio-Navarro *et al*. (2018)		X		
Yang *et al*. (2018)	X	X	X	

Fonte: Resultado da pesquisa (2023)

Nota-se que os controles detectivos foram abordados com maior frequência em comparação com os controles preventivos e corretivos. Por se tratar de artigos de revisão ou de pesquisa bibliográfica, os artigos de Tatam et al. (2021), Kim, Alfouzan e Kim (2021), Quintero-Bonilla e Martín Del Rey (2020), Singh et al. (2019) e Bahrami et al. (2019) não apresentaram controles de segurança recomendados ou aplicados. Para representação gráfica do Quadro 6, a Figura 6 apresenta os resultados consolidados referentes aos controles de segurança.

Figura 6 – Tipos de controle de segurança



Fonte: Resultado da pesquisa (2023)

Os controles detectivos destacam-se em comparação com os demais tipos de controle de segurança, com 15 artigos no total. Dos 25 artigos selecionados, 5 artigos apresentam controles preventivos e corretivos. Levando-se em consideração os três tipos de controles de segurança, para modelar ameaças do tipo APT, considera-se o uso de controles detectivos de suma importância para visibilidade e detecção, em tempo real, de ameaças cibernéticas que podem comprometer a segurança da informação de uma organização.

Conclui-se que, após revisão sistemática da literatura, a identificação dos principais métodos utilizados para modelar uma ameaça cibernética do tipo APT, e a definição sobre qual tipo de controle de segurança pode ser aplicado em um determinado ambiente, pode auxiliar na elaboração de estratégias de defesa cibernética para redução do risco cibernético em serviço digital de uma organização.

3 METODOLOGIA

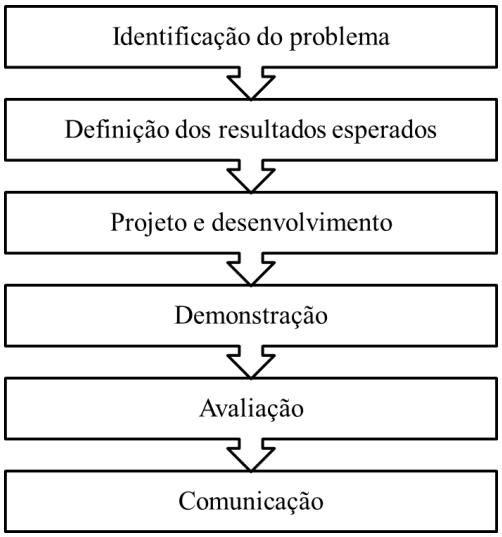
A metodologia de pesquisa adotada para a pesquisa foi baseada na DSR, com a utilização de outros métodos de pesquisa em diferentes etapas do DSR, como a pesquisa-ação, a observação direta do participante e as entrevistas.

3.1 Design Science Research (DSR)

O DSR é um método de pesquisa que tem como objetivo a resolução de problemas por meio da construção e aplicação de um artefato, que pode ser representado através de um constructo, método, modelo ou instanciação (PEFFERS, 2007; DRESCH, 2015; HEVNER, 2019).

A escolha do método justifica-se pela sua aplicação em sistemas de informação, e por considerar as etapas de avaliação e comunicação do artefato. Para sua devida execução, o fluxo do processo adotado para a presente pesquisa considerou a proposta apresentada por Peffers (2007), conforme ilustração referente às etapas do DSR apresentada na Figura 7.

Figura 7 – Fluxo do DSR



Fonte: adaptado de Peffers (2007)

As etapas do DSR apresentadas no fluxo são: identificação do problema, definição dos resultados esperados, projeto e desenvolvimento, demonstração, avaliação e comunicação.

Apesar de ser ilustrado como um processo sequencial, sua execução pode ser realizada de forma iterativa se necessário (PEFFERS, 2007). O Quadro 5 apresenta as etapas e os métodos e ferramentas utilizados na pesquisa.

Quadro 5 - Estrutura básica para execução da pesquisa-ação

Etapas	**Métodos e Ferramentas**
Identificação do problema	Questão de pesquisa Pesquisa bibliográfica Revisão sistemática da literatura Observação participante Pesquisa documental
Definição dos resultados esperados	Reuniões individuais com gestores Pesquisa documental *Sketching* (esboço)
Projeto e desenvolvimento	Análise documental e do ambiente Pesquisa-ação Observação participante Construção do artefato Pré-teste com conversas individuais com especialistas internos da organização Matriz RACI
Demonstração	Apresentação dos resultados após aplicação do método e processo construídos
Avaliação	Entrevistas individuais Avaliação descritiva
Comunicação	Publicação de artigos em congressos e periódicos

Fonte: Resultado da pesquisa (2023)

Considerando as etapas, métodos e ferramentas apresentadas no Quadro 5, as subseções a seguir apresentam as informações relacionadas a cada etapa assim como detalhamento a respeito.

3.1.1 Identificação Do Problema

A identificação do problema a ser investigado na presente pesquisa iniciou-se com a observação participante na organização analisada. A partir da observação direta e da pesquisa bibliográfica sobre o tema, a questão de pesquisa foi elaborada e a revisão sistemática da literatura foi efetuada em bases de dados conhecidas internacionalmente. Ressalta-se que durante a identificação do problema dentro da organização, ao realizar a pesquisa documental sobre processos de cibersegurança em vigência, observou-se a ausência de um método ou processo de negócio específico para analisar ameaças cibernéticas em sistemas implementados.

3.1.2 Definição dos resultados esperados

A definição dos resultados esperados foi feita a partir da coleta de informações disponíveis na organização que autorizou a execução da pesquisa. Além da pesquisa documental, reuniões individuais com gestores e o *sketching* (esboço) foi realizado considerando a questão de pesquisa elaborada na etapa de identificação do problema.

3.1.3 Projeto e desenvolvimento

O método escolhido para executar a etapa de projeto e desenvolvimento foi a pesquisa-ação, devido sua característica exploratória, e por ser um método qualitativo que busca a resolução de problemas (CERQUEIRA JUNIOR et al., 2023). Além da pesquisa-ação, com o apoio da ferramenta Bizagi Modeler, o *sketching* foi utilizado para criação e desenho de um processo específico para modelar ameaças. Com a aplicação da pesquisa-ação, uma nova análise documental e do ambiente que a organização pública está inserida foi efetuada para auxiliar a construção do método e processo proposto neste trabalho.

Após finalização da construção do processo, utilizando-se da observação participante, três especialistas internos da organização foram consultados para sugestões e melhorias do

processo construído, permitindo que o processo de negócio construído fosse aprimorado com a inclusão de novas tarefas, e com o estabelecimento da matriz RACI, para cada parte interessada responsável no processo.

3.1.4 Demonstração

A etapa de demonstração do artefato foi conduzida junto aos especialistas da organização, utilizando a observação participante e conversas individuais. Ao realizar a demonstração, o pré-teste foi feito ao demonstrar o funcionamento e aplicação do método construído na etapa de projeto e desenvolvimento. A partir do momento em que o método e o processo de negócio foram desenvolvidos, os resultados foram apresentados aos especialistas internos e externos.

3.1.5 Avaliação

A etapa de avaliação do método foi realizada com a aplicação de uma avaliação descritiva e entrevistas individuais com especialistas internos da organização e especialistas externos. Ao todo, para finalização deste trabalho, 6 especialistas internos e 6 especialistas externos foram entrevistados para avaliação interna e externa, respectivamente.

3.1.6 Comunicação

A etapa de Comunicação como a última, a princípio, está sendo executada por meio da dissertação, porém, será realizada por meio de publicação de artigos científicos em congressos e periódicos.

4 RESULTADOS E DISCUSSÃO

Os resultados da pesquisa foram divididos em quatro partes: construção do método, a execução do projeto e desenvolvimento, a demonstração dos resultados e a avaliação dos especialistas sobre o método e do processo de negócio construído para modelar ameaças cibernéticas.

4.1 Construção do método

Para o desenvolvimento do MCT-RB (*Modelling Cyber Threats using Risk-Based approach*), método específico para modelar ameaças cibernéticas do tipo APT com uma abordagem baseada em riscos, utilizou-se a fundamentação teórica, os resultados da revisão sistemática da literatura sobre o tema apresentado, uso da notação BPMN 2.0 e técnicas de *sketching* (esboço).

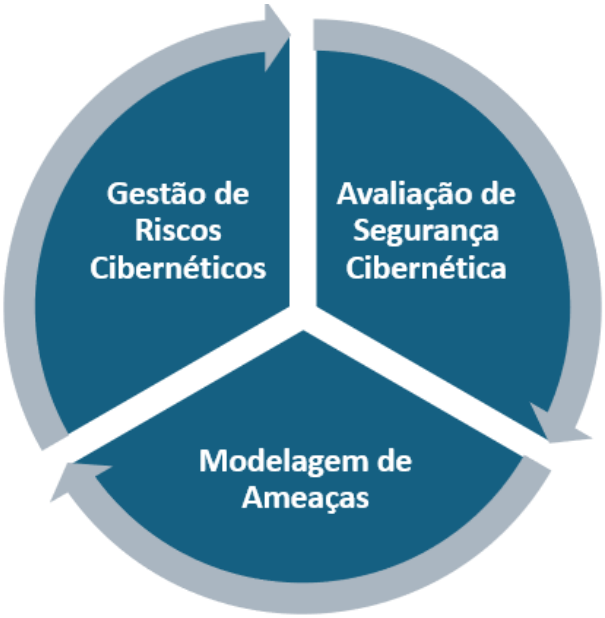
Dessa forma, o MCT-RB contém 4 tipos de métodos para modelar ameaças: métodos automatizados, manuais, gráficos e formais. O método automatizado no MCT-RB faz uso de ferramentas de cibersegurança para efetuar testes automatizados para identificação de vulnerabilidades. Os métodos manuais contidos no MCT-RB são executados a partir de análises e pesquisa em bases de conhecimento e frameworks de cibersegurança por parte da equipe de Segurança Operacional.

Os métodos gráficos que estão inseridos na aplicação do MCT-RB, que são a superfície de ataque e a árvore de ataque, são representações visuais sobre as ações maliciosas que uma ameaça cibernética pode realizar em um determinado sistema. Com isso, os métodos gráficos trazem visibilidade sobre uma ameaça específica. Por fim, o uso de métodos formais no MCT-RB busca utilizar métricas conhecidas e aplicadas na área de segurança da informação. Nesta pesquisa, o CVSSv3 foi utilizado para cumprir essa finalidade.

Resumidamente, a Figura 8 apresenta o MCT-RB por meio de um ciclo segmentado com três etapas distintas: Avaliação de Segurança Cibernética, Modelagem de Ameaças e Gestão de Riscos. Em suma, o método construído pode ser executado de forma cíclica e seu processo de negócio pode ser adaptado conforme a estrutura organizacional da instituição

pública. Entende-se que, além das organizações públicas, o método pode ser adaptado para empresas privadas conforme necessidade.

Figura 8 – Método MCT-RB (*Modelling Cyber Threats using Risk-Based approach*)



Fonte: Resultado da pesquisa (2024)

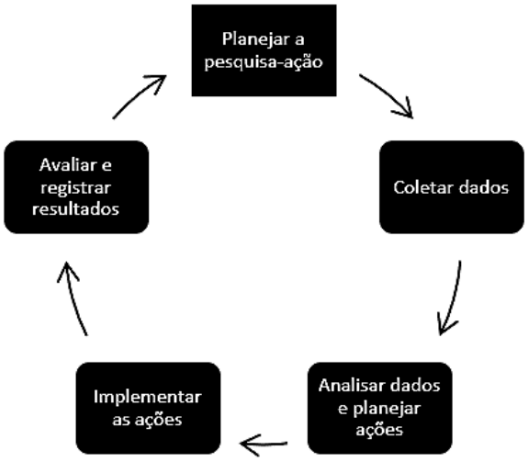
A avaliação de segurança cibernética consiste em efetuar testes automatizados ou manuais de segurança em um determinado sistema, aplicação ou infraestrutura para identificar fragilidades e possíveis vulnerabilidades de segurança. A modelagem de ameaças tem como objetivo realizar uma análise sobre que tipo de ameaça pode ser capaz de explorar vulnerabilidades presentes no sistema avaliado. Por fim, a gestão de riscos visa obter uma visão executiva sobre o grau de exposição ao risco cibernético de um sistema a uma ameaça previamente avaliada.

4.2 Execução do projeto e desenvolvimento

Para aplicação do método proposto, a organização que autorizou a execução da pesquisa exigiu que qualquer informação confidencial seja mantida em confidencialidade conforme recomendação e legislação aplicável. Cabe ressaltar que a justificativa para escolha da empresa que hospeda tal sistema se deu por critério de conveniência dos autores.

A Figura 9 apresenta a estrutura básica para condução da pesquisa-ação, que é dividida em cinco etapas em um processo cíclico: “Planejar a pesquisa-ação”, “Coletar dados”, “Analisar dados e Planejar ações”, “Implementar as ações” e “Avaliar e Registrar resultados” (MELLO et al., 2012; CERQUEIRA JUNIOR et al., 2023).

Figura 9 - Estrutura utilizada para execução da pesquisa-ação



Fonte: Adaptado de Mello *et al*. (2012) e Cerqueira Junior *et al*. (2023)

Durante a condução da pesquisa-ação, optou-se por executar dois ciclos para melhoria contínua do artefato, sendo o primeiro ciclo dedicado para aplicação da modelagem da ameaça antes da etapa referente à avaliação dos controles de segurança, enquanto o segundo ciclo foi executado com ênfase na gestão do risco cibernético restrito a ameaça analisada. Segue Quadro 6 descrevendo cada etapa e ferramenta utilizada nos ciclos da pesquisa-ação.

Quadro 6 - Ciclos da Pesquisa-ação

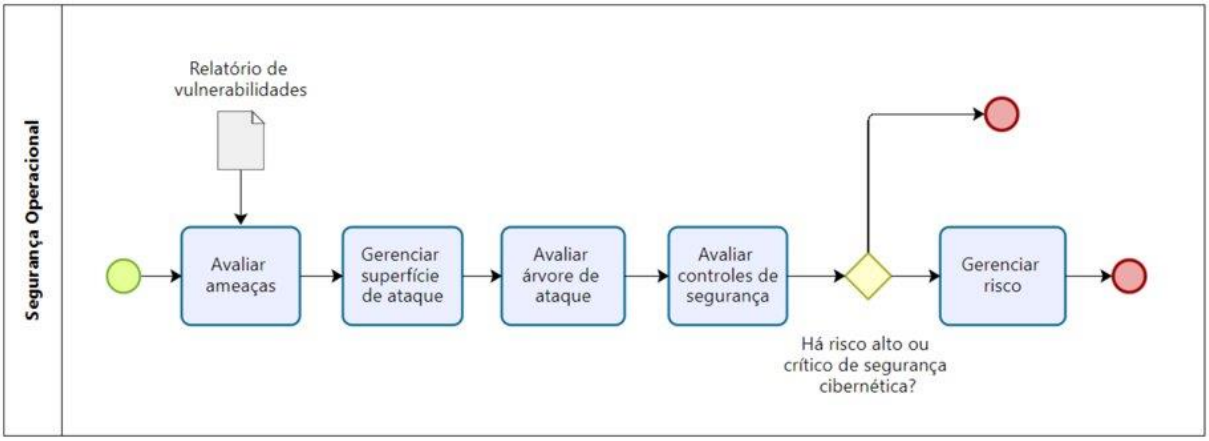
Pesquisa-ação conduzida pelos autores			
Método	**Etapa**	**Objetivos**	**Técnicas e ferramentas**
Pesquisa-ação	Planejar pesquisa-ação	1º ciclo: desenhar artefato para o processo da modelagem de ameaça.	*Sketching* (esboço), ferramenta para desenho de processo e análise documental (artigos científicos e bases técnicas).
		2º ciclo: analisar procedimentos internos da organização para gestão de riscos cibernéticos.	Análise documental da organização.
	Coletar dados	1º ciclo: obter informações sobre sistemas da organização.	Análise documental da organização.
		2º ciclo: obter informações sobre avaliação de risco cibernético em sistemas da organização.	Análise documental da organização.
	Analisar dados e planejar ações	1º ciclo: definir sistema a ser avaliado sob a perspectiva da ameaça	Análise documental (bases técnicas de segurança e *framework* do Mitre).
		2º ciclo: analisar resultados da modelagem de ameaças	
	Implementar ações	1º ciclo: executar modelagem de ameaça	Análises automatizadas de segurança da informação.
		2º ciclo: executar avaliação de riscos cibernéticos	Análise dos resultados da modelagem aplicada e avaliação de riscos
	Avaliar e registrar resultados	1º e 2º ciclos: coletar resultados e aprimorar etapas do artefato	Observação participante sobre avaliações de especialistas da organização.

Fonte: Resultado da pesquisa (2023)

Após a execução dos ciclos da pesquisa-ação, três especialistas da organização foram consultados para avaliação do processo. Além disso, os autores da pesquisa revisaram o processo criado inicialmente após análise dos registros feitos pelos especialistas para melhorias e adaptações.

A Figura 10 apresenta o artefato criado inicialmente para que os ataques cibernéticos do tipo APT sejam analisados por meio da aplicação de uma modelagem específica para este tipo de ataque. Nota-se que, nesta versão inicial do processo, cabe a equipe de Segurança Operacional executar todas as etapas da modelagem para definir se a gestão do risco cibernético residual considerado alto será efetuada pela área responsável pelo risco.

Figura 10 - Artefato para modelar ameaças



Fonte: Resultado da pesquisa (2024)

Neste processo, a modelagem inicia com a relação completa de todas as vulnerabilidades identificadas pela equipe de Segurança Operacional em um determinado produto ou serviço (aplicativo, site, entre outros). Antes de iniciar a análise do risco cibernético, as quatro tarefas que a Segurança Operacional deve executar são:

1. Avaliar ameaças: a equipe de segurança operacional analisa as vulnerabilidades informadas em um relatório consolidado sob a perspectiva de um APT (APT3, APT29, entre outros). Nessa etapa, a partir do resultado da análise das vulnerabilidades, espera-se que a defesa cibernética de um sistema seja avaliada com base nas fragilidades existentes, considerando qual ameaça pode ser capaz de explorar alguma falha de segurança e que TTPs podem ser executadas pela ameaça avaliada.

2. Gerenciar superfície de ataque: após a avaliação das ameaças, a Segurança Operacional deverá iniciar as atividades relacionadas à gestão da superfície de ataque. Essa tarefa consiste em obter uma visão técnica de quais vetores de ataque podem ser utilizados pela ameaça e verificar que tecnologias e funcionalidades devem ser controladas e monitoradas com maior atenção pela organização.

3. Avaliar árvore de ataque: após a avaliação da superfície de ataque, a tarefa de "Avaliar árvore de ataque" consiste em verificar, visualmente, que caminhos prováveis uma ameaça pode escolher ao executar um ataque cibernético de acordo com o seu objetivo claro e definido.

4. Avaliar controles de segurança: com isso, a tarefa tem como objetivo identificar e avaliar os controles de segurança implementados na organização para responder ao risco cibernético identificado no Relatório de Vulnerabilidades. Para cumprimento da tarefa, faz-se necessário avaliar se o risco residual, mesmo após a aplicação dos controles de segurança, será alto ou crítico com base na severidade do CVSS indicado para uma vulnerabilidade.

5. Gerenciar risco: caso o risco residual seja alto ou crítico, a tarefa se inicia com as devidas ações para tratamento do risco cibernético. Entretanto, caso o risco residual não seja alto ou crítico com base no CVSS identificado, encerra-se a modelagem.

A seguir, nas próximas subseções, são apresentados os resultados obtidos durante a aplicação do artefato para melhor compreensão da modelagem efetuada.

4.2.1 Primeiro ciclo: aplicação do processo em um sistema

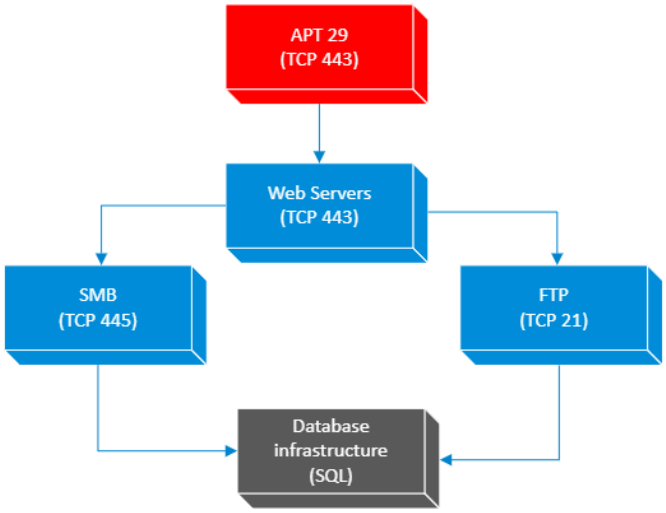
Tendo em vista coletar os resultados do artefato, um sistema digitalizado em 2015, em funcionamento, foi selecionado para que o artefato fosse aplicado em um ambiente real. Maiores detalhes do funcionamento do sistema, tais como, arquitetura, número de servidores e número de acessos simultâneos, foram omitidos por confidencialidade.

Para iniciar a modelagem da ameaça, o Relatório de Vulnerabilidades foi produzido para identificação das fragilidades encontradas nos servidores que compõem o produto, onde o CVSSv3 foi utilizado como um tipo de método formal para avaliar a severidade da vulnerabilidade.

Com isso, o grupo APT 29 foi selecionado para aplicação da modelagem por suas características, além de utilizarem diferentes TTPs para obter acesso completo a servidores e sistemas expostos na internet, como técnicas de exploração e análises de vulnerabilidade (MITRE, 2023). Após a avaliação do APT 29, a tarefa "Gerenciar a superfície de ataque" foi iniciada. Na superfície de ataque, cinco vetores de ataque foram identificados.

Após o mapeamento da superfície de ataque, bem como o conhecimento detalhado de cada vulnerabilidade identificada, a tarefa "Avaliar árvore de ataque" inicia-se, considerando quais caminhos uma ameaça pode realizar para efetuar o ataque cibernético com sucesso. A Figura 11 apresenta, resumidamente, a árvore de ataque construída para representar a ameaça e a infraestrutura que pode ser atacada.

Figura 11 - Árvore de ataque para infraestrutura construída

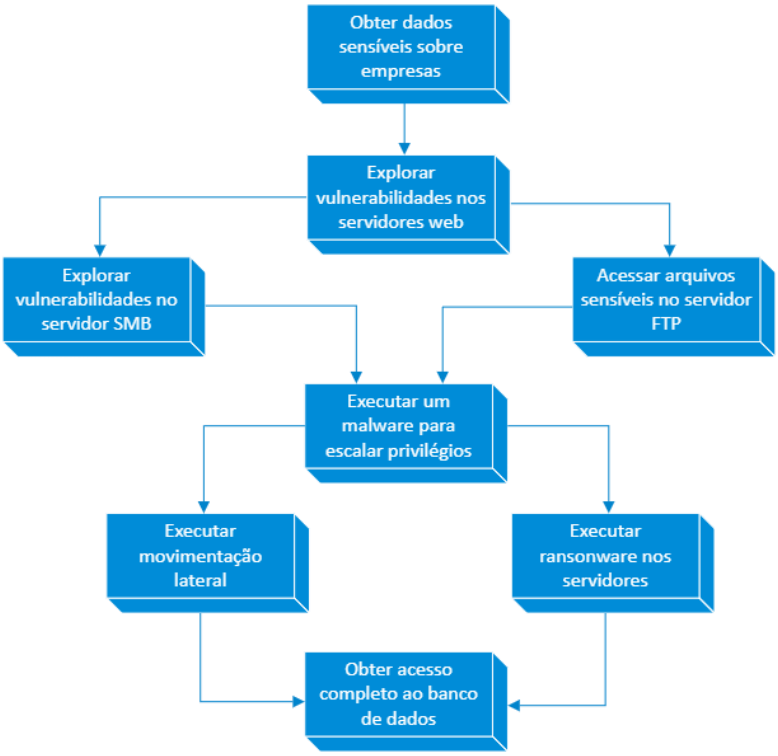


Fonte: Resultado da Pesquisa (2023)

Nesse exemplo, um dos caminhos que o atacante pode adotar para realizar o ataque com objetividade é obter acesso ao sistema por meio da porta TCP 443, disponível para acesso na internet. Após consulta em bases de segurança cibernética, verificou-se que o APT29 adota táticas, técnicas e procedimentos específicos para tentativas de ataques em servidores web na porta TCP 443 (FIREEYE, 2023; MITRE, 2023).

Ao analisar as informações geradas na tarefa "Avaliar ameaças", com o objetivo de descrever prováveis caminhos que o APT29 pode seguir, a Figura 12 apresenta a árvore de ataque com as ações e objetivos que a ameaça pode realizar, caso obtenha sucesso em seu ataque.

Figura 12 - Árvore de ataque com ações e objetivos



Fonte: Resultado da pesquisa (2023)

Após a avaliação da árvore de ataque, inicia-se a tarefa de analisar os controles de segurança. Toda atividade relacionada à gestão de riscos cibernéticos é apresentada na próxima subseção.

4.2.2 Segundo ciclo: avaliação dos controles de segurança

A avaliação dos controles de segurança, realizada pela equipe de segurança operacional, foi executada conforme as diretrizes e orientações disponíveis na organização pesquisada. Dessa forma, todos os resultados referentes aos controles de segurança foram coletados de acordo com as definições pré-estabelecidas pela organização, como a definição do risco cibernético sendo categorizado como um risco operacional da organização e a utilização de uma pontuação referente à probabilidade e impacto de um risco inerente ou residual.

4.2.3 Recomendações dos especialistas internos após a execução do projeto

Ao final da execução dos dois ciclos da pesquisa-ação, a avaliação do artefato foi feita por especialistas da própria organização que autorizou a pesquisa. Os comentários feitos durante a avaliação dos especialistas foram registrados com o uso da observação participante.

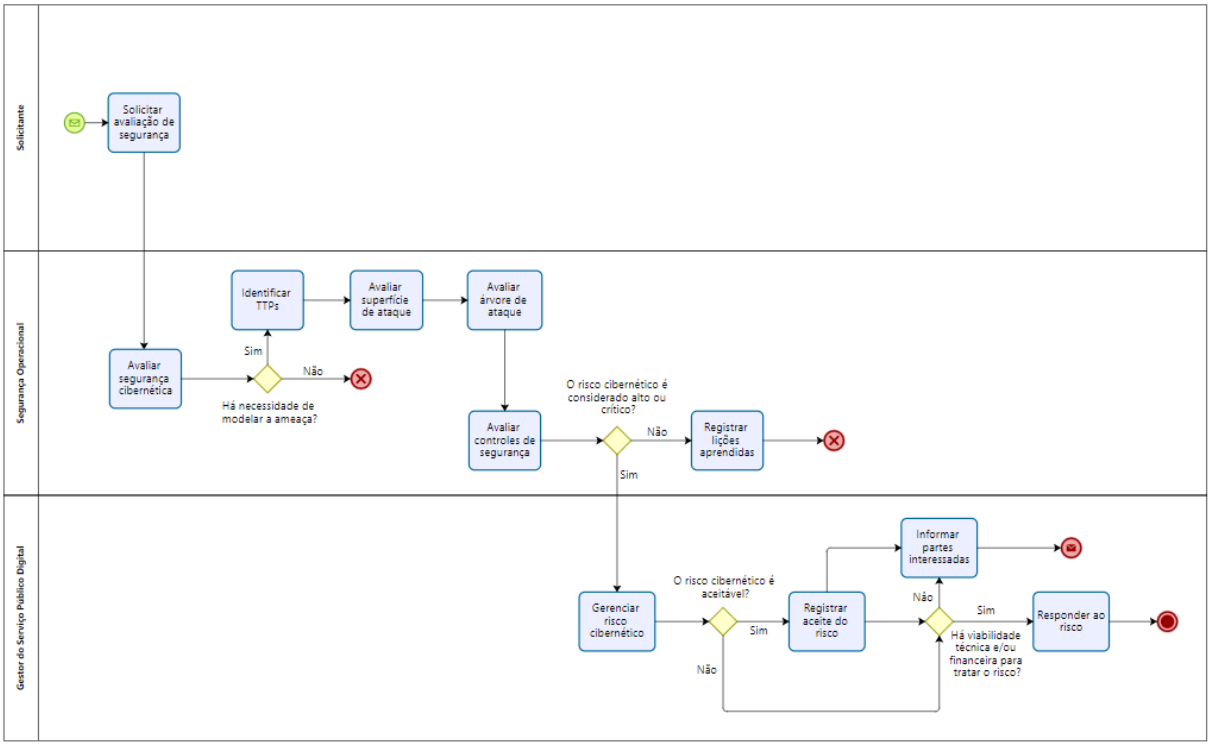
Todos os especialistas são analistas de segurança da informação, possuem mais de 10 anos de experiência na área e possuem, no mínimo, pós-graduação lato sensu completa na área de TI ou segurança da informação.

Em relação ao processo da modelagem, sugere-se que a tarefa “Gerenciar superfície de ataque” seja substituída por “Avaliar a superfície de ataque”. Após, a execução da tarefa “Avaliação dos controles de segurança” pode ser executada pelo time de segurança operacional da organização, e, para que eventual risco residual alto ou crítico seja devidamente tratado, recomenda-se que a área de negócio que administra o sistema seja responsável pela execução da tarefa “Gerenciar o risco”. Por fim, todos os especialistas concordam que a modelagem de ameaça apresenta pode ser aprimorada e utilizada em algum processo interno de segurança da informação.

4.2.4 Processo de negócio construído

Considerando todas as recomendações obtidas pelos especialistas da organização, e, após nova revisão dos autores quanto ao fluxo e tarefas do processo, criou-se a versão do artefato aprimorada utilizando a notação BPMN 2.0, conforme ilustração da Figura 13.

Figura 13 – Processo de negócio construído



Fonte: Resultado da pesquisa (2024)

O Quadro 7 apresenta as partes envolvidas e a função de cada parte envolvida no processo de negócio construído.

Quadro 7 – Partes envolvidas no processo construído

Partes envolvidas	Função no processo
Solicitante	Solicita a modelagem de ameaças em um serviço público digital
Segurança Operacional	Realiza a avaliação de segurança cibernética, a modelagem da ameaça e efetua a tarefa inicial referente a etapa de gestão do risco cibernético do MCT-RB
Gestor do Serviço Público Digital	Responsável pelas tarefas de gestão do risco cibernético somente após avaliação dos controles de segurança feita pela Segurança Operacional.

Fonte: Resultado da pesquisa (2024)

Em comparação com o processo criado inicialmente, o Relatório de Vulnerabilidades foi suprimido do processo e substituído pela tarefa “Avaliar segurança cibernética” com o intuito de esclarecer de que forma as vulnerabilidades serão identificadas pela Segurança Operacional. Dessa maneira, a Segurança Operacional possui autonomia para definir que

serviços públicos devem ser avaliados. Além disso, planos, políticas ou qualquer outro instrumento de governança em segurança cibernética, como um “Plano Interno de Segurança Cibernética” pode ser inserido como insumo no processo para consulta no início do fluxo, podendo se referir a outros instrumentos de governança corporativa estabelecidos em uma organização pública, como o Plano Diretor de Tecnologia da Informação (PDTI) ou o Plano Diretor de Segurança da Informação (PDSI).

Verifica-se que as tarefas referentes à solicitação e avaliação de segurança cibernética foram adicionadas ao processo, bem como a substituição da tarefa “Avaliar ameaças” por “Identificar TTPs” para que a modelagem da ameaça seja mais assertiva, objetiva e específica quanto às ações que uma ameaça pode executar em um sistema vulnerável.

Nota-se que, após a inclusão de novas tarefas e, principalmente, após a tarefa de “Avaliar controles de segurança”, verifica-se que as atividades referentes à gestão do risco cibernético devem ser executadas pelo Gestor do Serviço Público Digital, que é a parte interessada responsável pela gestão do produto ou sistema avaliado. Observa-se também que cabe ao Gestor informar as partes interessadas sobre o aceite do risco e a inviabilidade de tratamento do risco. Inclusive, ressalta-se que essas tarefas estão diretamente relacionadas à etapa de Gestão do Risco Cibernético proposta no método MCT-RB.

Na sequência, segue a descrição de cada tarefa indicada no fluxo do processo de negócio construído.

1. Solicitar avaliação de segurança: o Solicitante inicia a tarefa de solicitação à Segurança Operacional para iniciar uma avaliação (*assessment*) de segurança com o objetivo de identificar vulnerabilidades de segurança em um serviço público digital. A solicitação poderá ser registrada em sistema informatizado, e-mail ou qualquer outro meio adequado conforme indicação ou diretriz da organização.

2. Avaliar segurança cibernética: após receber a solicitação de avaliação por parte do Gestor, inicia o processo de forma proativa ou mesmo seguindo orientações estabelecidas em um instrumento de governança, como um PDSI, a Segurança Operacional deverá iniciar a avaliação de segurança cibernética de um sistema com base nos relatórios de vulnerabilidades produzidos por ferramentas automatizadas de segurança, que são tecnologias especializadas para identificar vulnerabilidades e seu nível de severidade conforme indicação do CVSSv3. A métrica a ser utilizada pode ser adequada e selecionada conforme a necessidade da organização, tal como, utilização do CVSSv2, CVSSv3 ou outra métrica. No entanto, se após

a Avaliação de Segurança Cibernética a Segurança Operacional definir que a modelagem não é necessária, o processo poderá ser encerrado.

3. Identificar TTPs: a Segurança Operacional analisa as vulnerabilidades informadas em um relatório consolidado sob a perspectiva de um APT ou outra ameaça cibernética. Nessa etapa, a partir do resultado da avaliação de segurança cibernética, espera-se que a defesa cibernética de um sistema seja avaliada com base nas fragilidades existentes, considerando qual ameaça pode ser capaz de explorar alguma falha de segurança e que TTPs podem ser executadas por um APT específico. Exemplo: APT1, APT3, entre outros.

4. Avaliar superfície de ataque: visa identificar os vetores de ataque disponíveis a uma ameaça de acordo com as vulnerabilidades identificadas anteriormente na tarefa de "Avaliar Segurança Cibernética". Recomenda-se que a superfície de ataque seja mapeada por meio de tecnologias automatizadas, como sistemas de detecção e identificação de vulnerabilidades ou aplicações que permitam esse tipo de abordagem.

5. Avaliar árvore de ataque: diante da visibilidade trazida pela superfície de ataque, a tarefa de "Avaliar árvore de ataque" consiste em verificar, visualmente, que caminhos prováveis uma ameaça pode efetuar ao realizar um ataque cibernético de acordo com o seu objetivo.

6. Avaliar controles de segurança: após a conclusão das tarefas referentes às etapas de Avaliação de Segurança Cibernética e à Modelagem de Ameaça propostas no método MCT-RB, a Segurança Operacional verifica os controles de segurança aplicados e disponíveis para implementação em um sistema. Além da verificação de controles de segurança, a Segurança Operacional irá descrever a severidade do risco cibernético identificado inicialmente (que é o risco inerente), o evento de risco, as causas, efeitos e consequências, a severidade do risco residual, e irá definir a categoria do risco de acordo com as definições internas da organização. Os controles de segurança podem ser definidos de acordo com frameworks de segurança cibernética, tais como, Mitre Att&ck, CIS Controls, ISO 27002, entre outros.

7. Registrar lições aprendidas: caso o risco residual seja moderado, médio ou baixo ou se o apetite ao risco definido pela organização for atingido, a Segurança Operacional registra as lições aprendidas em um sistema e encerra o processo. Exemplos de sistemas que podem ser utilizados para essa finalidade são sistemas de gestão de segurança, sistemas de

gestão de riscos corporativos, sistemas de gestão de riscos cibernéticos ou qualquer outra aplicação ou tecnologia que permita esse tipo de registro.

8. Gerenciar risco cibernético: caso o risco residual seja alto ou crítico, o Gestor do Serviço Público Digital é notificado formalmente sobre o risco cibernético identificado, e inicia a tarefa "Gerenciar risco" com as devidas tratativas para responder ou aceitar o risco cibernético de acordo com as definições internas da organização. Das estratégias disponíveis para o Gestor gerenciar o risco cibernético, ele pode aceitar o risco de acordo com o apetite de risco estabelecido pela organização ou aceitá-lo por inviabilidade técnica ou financeira para respondê-lo. Além de aceitar o risco, o Gestor pode optar por responder o risco, se houver viabilidade técnica ou financeira.

9. Registrar aceite do risco: após consultar o nível de apetite de risco estabelecido pela organização e a viabilidade técnica ou financeira para responder ao risco, o Gestor poderá optar por aceitar o risco cibernético.

10. Informar partes interessadas: após consultar as equipes operacionais e demais stakeholders (fornecedores, entre outros) para verificar a viabilidade técnica ou financeira para responder ao risco, o Gestor poderá iniciar as tratativas para responder o risco cibernético. Ressalta-se que, nesta tarefa, o Gestor deverá informar as partes interessadas sobre o aceite do risco e a inviabilidade de tratamento do risco identificado e encerrar o processo.

11. Responder ao risco: após consultar as equipes operacionais e demais *stakeholders* (fornecedores, entre outros) para verificar a viabilidade técnica ou financeira para responder ao risco, o Gestor poderá iniciar as tratativas para responder o risco cibernético.

Para apresentar a responsabilidade de cada parte envolvida no processo de negócio construído, a Matriz RACI (*Responsible*, *Accountable*, *Consulted*, *Informed*) foi utilizada como instrumento de apoio para estabelecer as responsabilidades de cada parte interessada (CABANILLAS; RESINAS; RUIZ-CORTÉS, 2012). Segue resumo que descreve cada função designada na Matriz RACI criada.

- **R (*Responsible*):** parte responsável pela execução da tarefa;
- **A (*Accountable*):** parte responsável que presta contas pelos resultados da tarefa;
- **C (*Consulted*):** parte consultada para execução da tarefa;

- **I (*Informed*):** parte informada do resultado da tarefa.

Dessa maneira, o Quadro 8 apresenta a Matriz RACI preenchida de acordo com as tarefas disponíveis no processo.

Quadro 8 – Matriz de responsabilidade (RACI)

Tarefa	Solicitante	Segurança Operacional	Gestor do Serviço Público Digital
1. Solicitar avaliação de segurança	**R/A**	**I**	**I**
2. Avaliar segurança cibernética		**R/A**	
3. Identificar TTPs		**R/A**	
4. Avaliar superfície de ataque		**R/A**	
5. Avaliar árvore de ataque		**R/A**	
6. Avaliar controles de segurança		**R/A**	
7. Registrar lições aprendidas	**I**	**R/A**	**I**
8. Gerenciar risco cibernético		**C**	**R/A**
9. Registrar aceite do risco	**I**	**I**	**R/A**
10. Informar partes interessadas	**I**	**I**	**R/A**
11. Responder ao risco	**I**	**I**	**R/A**

Fonte: Resultado da pesquisa (2024)

Dessa forma, um processo de negócio específico para modelar ameaças cibernéticas foi construído com base nas etapas sugeridas pelo método MCT-RB. Ressalta-se que práticas de BPM foram adotadas para desenho e modelagem do processo, bem como utilizou-se a Matriz RACI para designar as responsabilidades das partes envolvidas no processo.

4.3 Demonstração

A demonstração do processo foi realizada para especialistas internos da organização, bem como especialistas externos. A seguir, os resultados identificados na etapa de Projeto e desenvolvimento foram apresentados aos especialistas conforme fluxo indicado do processo de negócio do método MCT-RB, que foi construído na etapa de Projeto e Desenvolvimento.

4.3.1 Avaliação de Segurança Cibernética

Ao iniciar o processo, a avaliação de segurança cibernética é iniciada e as vulnerabilidades são identificadas e classificadas quanto a severidade de acordo com o rating (pontuação) indicado pelo CVSS. Cabe reforçar que, na organização estudada, o nível de severidade (crítico, alto, médio ou baixo) é utilizado para definição do nível de risco cibernético de cada vulnerabilidade. A seguir, seguem as vulnerabilidades identificadas.

- **Portas abertas**: algumas portas abertas de serviços não conhecidos pelo time de segurança operacional foram identificadas em servidores que compõem o produto. Para conhecimento, o CVSS não se aplica a esse tipo de vulnerabilidade;
- **Servidor web desatualizado (CVSS 10.0)**: foi identificado que o servidor web, que hospeda o site do produto, está desatualizado e sem suporte do fabricante.;
- **Sistema operacional desatualizado (CVSS 10.0)**: em alguns servidores, foi identificado que o sistema operacional está desatualizado e sem suporte do fabricante;
- **Serviços desatualizados e inseguros (vulnerabilidades com CVSS 4.0 e CVSS 5.4)**: os serviços SMB e FTP, identificados durante a análise de vulnerabilidade, atualmente, são considerados desatualizados e inseguros;

- **Criptografia não segura (CVSS 4.6)**: as cifras e a versão do protocolo SSL/TLS, em uso em servidores internos do sistema, são consideradas inseguras.

Com as vulnerabilidades identificadas e sua severidade indicada, as tarefas relacionadas à modelagem das ameaças cibernéticas são iniciadas.

4.3.2 Modelagem da Ameaça

Nessa modelagem, o objetivo do APT é obter dados confidenciais de um serviço público digital. Para verificar a aplicabilidade da modelagem, o APT 29 foi selecionado e, após nova consulta no *framework* do Mitre, o Quadro 9 apresenta as TTPs que podem ser executadas pelo APT 29 de acordo com as vulnerabilidades identificadas anteriormente (MITRE, 2023).

Quadro 9– Mapeamento de TTPSs do APT29

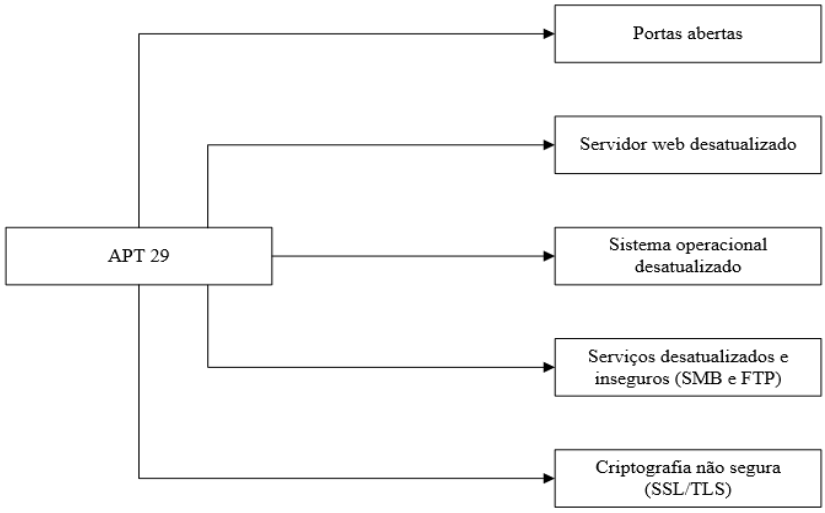
Táticas, técnicas e procedimentos mapeados de acordo com as vulnerabilidades			
APT	**Táticas**	**Técnicas**	**Procedimentos**
APT 29	Reconhecimento	T1595: *Active Scanning: Vulnerability Scanning*	O grupo APT29 realiza uma varredura generalizada em sistemas na internet para identificar vulnerabilidades para exploração.
	Acesso inicial	T1190: *Exploit Public-Facing Application*	A ameaça pode tentar explorar uma fragilidade em um sistema disponível para acesso na internet, para acessar inicialmente uma rede interna.
	Acesso inicial	T1113: *External Remote Services*	A ameaça pode obter informações sobre a rede (IPs públicos, portas TCP, etc) e quais tecnologias estão disponíveis para acesso na internet.
	Execução	T1059: *Command and Scripting Interpreter*	A partir do momento em que obtém o acesso inicial, a ameaça pode utilizar de programas do próprio sistema para executar comandos (vírus, entre outros).
	Exfiltração	T1048: *Exfiltration Over Alternative Protocol*	Os adversários podem roubar dados exfiltrando-os - do sistema alvo para o sistema do APT - através de um protocolo

			de rede específico.

Fonte: Resultado da pesquisa (2024)

Conforme avaliação da ameaça feita na tarefa “Identificar TTPs”, a tarefa “Avaliar a superfície de ataque” foi efetuada e, como resultado, a Figura 14 apresenta a superfície de ataque disponível para o APT29. Nota-se que há um conjunto de vetores de ataque que podem ser utilizados pelo APT29 para execução de um ataque cibernético.

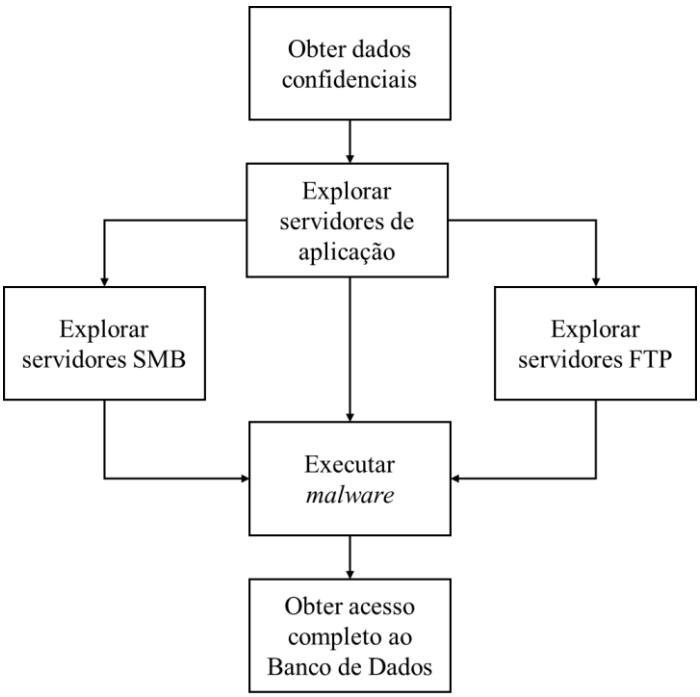
Figura 14 - Superfície de ataque do APT29 para o sistema analisado



Fonte: Resultado da pesquisa (2023)

Após o mapeamento da superfície de ataque, a tarefa "Avaliar árvore de ataque” inicia-se, considerando que caminhos uma ameaça pode seguir para efetuar o ataque cibernético com sucesso, de acordo com um objetivo previamente estabelecido, conforme apresentação da árvore de ataque representada pela Figura 15. Nessa modelagem, caso o ataque seja bem-sucedido, o APT29 conseguirá obter acesso completo ao banco de dados que é acessado pelo serviço público digital disponível para acesso via internet.

Figura 15 - Árvore de ataque



Fonte: Resultado da pesquisa (2024)

Após a avaliação da árvore de ataque, inicia-se a tarefa de avaliar os controles de segurança para prevenção desse tipo de ataque cibernético. Toda atividade relacionada à gestão de riscos cibernéticos será apresentada na próxima seção.

4.3.3 Gestão de Riscos Cibernéticos

A tarefa “Avaliar controles de segurança” foi executada conforme as definições e normativos vigentes na organização pesquisada. Uma análise qualitativa e quantitativa foi feita, de acordo com as informações apresentadas nas tarefas anteriores, e considerando os controles já aplicados e que estão disponíveis para uso na organização. O Quadro 10 apresenta as informações referentes à identificação de eventos de riscos cibernéticos, como o evento de risco, as causas, os efeitos e sua categoria baseada em definições internas da organização para riscos corporativos.

Nota-se que a categoria do risco identificado é de natureza operacional e que, conforme definições internas da organização, as demais categorias de risco não serão apresentadas por questões de confidencialidade.

Quadro 10 - Identificação de eventos de riscos cibernéticos

Identificação de eventos de riscos cibernéticos			
Eventos de Risco	**Causas**	**Efeitos e Consequências**	**Categoria do Risco**
Serviço público digital com vulnerabilidades de risco alto e crítico em um sistema	1. Tecnologias desatualizadas 2. Inventário desatualizado 3. Tecnologias sem suporte do fabricante	1. Exploração de vulnerabilidades conhecidas 2. Vazamento de dados 3. Danos à imagem da empresa como prestadora de serviços ligados a tecnologia	Operacional

Fonte: Resultado da pesquisa (2023)

A seguir, considerando o cálculo da probabilidade e impacto do risco inerente e residual, sendo que o valor definido está no intervalo de 1 a 5 pontos, a Tabela 4 apresenta a probabilidade e impacto do risco identificado de acordo com a avaliação feita. Na organização, considera-se um risco baixo com a pontuação de 1 a 4. Para riscos moderados, a pontuação de 4 a 6, e para riscos altos, a pontuação de 6 a 12.

Tabela 4 – Risco inerente e risco residual

Classificação do risco	**Probabilidade (de 1 a 5)**	**Impacto (de 1 a 5)**
Risco inerente	4	3
Risco residual	2	2

Fonte: Resultado da pesquisa (2023)

Nota-se que, após a avaliação dos controles de segurança, a probabilidade e o impacto do risco residual são menores em comparação com o risco inerente. O Quadro 11 apresenta os 10 controles de segurança já aplicados para proteção do sistema avaliado, bem como os controles que estão disponíveis para aplicação pela organização. Cabe reforçar que as medidas de mitigação disponíveis no *framework* do Mitre foram adotadas como referência para listagem dos controles que a organização dispõe (MITRE, 2024).

Quadro 11 – Resposta ao risco cibernético

Resposta ao risco cibernético			
Nível de risco inerente	**Estratégia para resposta ao risco**	**Controle de segurança atual**	**Nível de risco residual**
Risco alto	Mitigar	M1016 – Verificação de vulnerabilidades M1030 - Segmentação de Rede M1031 - Prevenção de invasões de rede e utilização de IPS (*Intrusion Prevention System*) M1032 - Autenticação multifator M1035 - Limitar acesso a recursos pela rede M1037 - Filtrar tráfego de rede (*firewalls* de rede ou *firewall* de aplicação) M1042 - Desativar ou remover recurso ou programa M1049 - *Antivírus*/*Antimalware* M1050 - Proteção contra *exploits* (*firewalls* de rede ou *firewall* de aplicação) M1051 - Atualizar Software	Risco baixo

Fonte: Resultado da pesquisa (2024)

Na sequência, segue descrição sobre cada controle de segurança aplicado ou disponível na organização para mitigar as vulnerabilidades identificadas conforme apresentação do Quadro 12.

Quadro 12 – Descrição dos controles de segurança

Código do controle no Mitre	Nome do Controle	Descrição do Controle
M1016	Verificação de vulnerabilidades	Consiste em verificar vulnerabilidades de segurança em um sistema de forma manual ou automatizada.
M1030	Segmentação de Rede	Visa implementar segmentação de rede para separar redes internas e externas por meio de *switches*, roteadores, firewalls, entre outros.
M1031	Prevenção de invasões de rede e utilização de IPS	Refere-se a uma tecnologia de segurança que realiza a identificação e prevenção de uma ameaça em uma rede.
M1032	Autenticação multifator (*Multi-Factor Authentication*, conhecido como MFA)	É um mecanismo que habilita múltiplos fatores de autenticação e não somente um único fator. Exemplo: uso de senha e token via aplicativo ou smartphone, senha e digital biométrica, entre outros.
M1035	Limitar acesso a recursos pela rede	Refere-se em limitar o acesso de recursos ou serviços disponíveis em uma rede.
M1037	Filtrar tráfego de rede (*firewalls* de rede ou *firewall* de aplicação)	Consiste em criar regras de acesso em um firewall de rede ou aplicação, que irá permitir o acesso ou bloqueio de um tráfego de rede, além de efetuar o bloqueio de um tráfego considerado malicioso conforme configuração implementada.
M1042	Desativar ou remover recurso ou programa	Tem como objetivo desativar ou remover recurso habilitado em um sistema.
M1049	Antivírus/*Antimalware*	Refere-se a uma tecnologia que realiza uma varredura baseada em uma lista de ameaças (vírus, *malware*, etc). Além disso, esse controle é capaz de detectar, em tempo real, a ação de uma ameaça em um servidor, computador, estação de trabalho ou em um smartphone para bloqueio e prevenção de ações maliciosas.

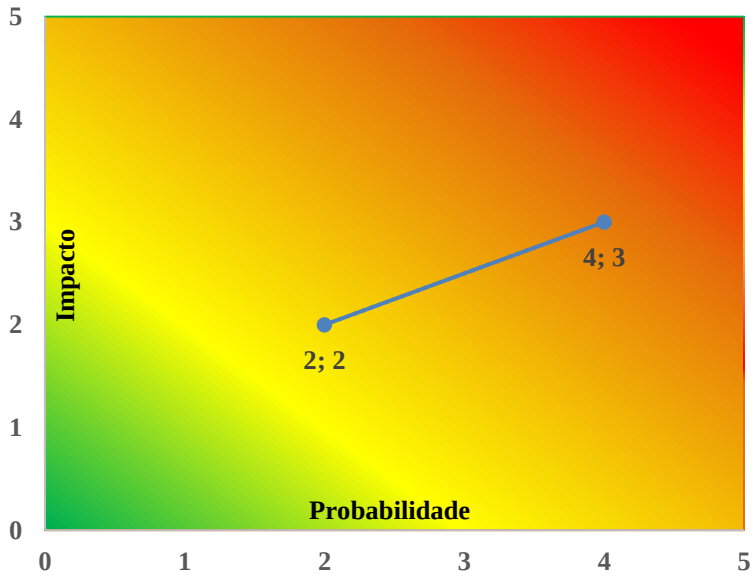
Código do controle no Mitre	Nome do Controle	Descrição do Controle
M1050	Proteção contra *exploits* (*firewalls* de rede ou *firewall* de aplicação)	A proteção de *exploits* se refere a uma medida de segurança aplicada e disponível para configuração nos *firewalls* de rede ou *firewalls* de aplicação (conhecido no mercado de cibersegurança como *Web Application Firewall* ou simplesmente WAF) contra diversas ameaças (*malwares*, códigos de exploração, entre outros).
M1051	Atualizar Software	Esse controle de segurança se refere ao processo de aplicação de atualizações (*patches*) em tecnologias.

Fonte: Resultado da pesquisa (2024)

Em relação aos controles de segurança identificados na organização, verificou-se que o desenho de cada controle de segurança disponível possui procedimentos de controles adequados e formalizados, e que a operação de cada controle de segurança conta com procedimentos que são executados pelas áreas responsáveis. Dessa forma, considerando as informações coletadas na avaliação dos controles de segurança, observa-se que o nível do risco pode ser reduzido para o nível moderado.

Conforme apresentação da Figura 16, ao considerar os valores do risco inerente e residual, optou-se por criar o mapa de calor com o apoio da ferramenta Microsoft Excel, para apresentar visualmente a redução do nível do risco após avaliação dos controles de segurança.

Figura 16 - Mapa de calor do risco inerente e residual



Fonte: Resultado da pesquisa (2023)

Ao final da avaliação dos controles de segurança disponíveis, verifica-se que, ao analisar o mapa de calor, o risco residual encontra-se no nível moderado, indicando um nível

de risco cibernético aceitável de acordo com as definições internas da organização que mantém o sistema avaliado. Com isso, o processo da modelagem de ameaça é encerrado conforme fluxo desenvolvido.

4.4 Avaliação

A avaliação descritiva do método e do processo de negócio criado nesta pesquisa e aplicado em um serviço público digital foi efetuada por meio de uma entrevista individual com 6 (cinco) especialistas internos da organização e 6 (seis) especialistas externos à organização. Na sequência, o Quadro 13 apresenta as 3 (três) perguntas realizadas aos especialistas, bem como as referências utilizadas para elaboração das questões.

Quadro 13 - Questões e referências para entrevista

Questões	Referências
1. Considerando que: - Os ataques cibernéticos do tipo APT são promovidos por grupos altamente organizados e experientes; - As medidas de segurança que são adotadas atualmente na sua organização. De que forma o método apresentado para modelar ameaças pode proteger um sistema hospedado na sua organização?	Tatam *et al*. (2021)
2. Na sua opinião, que controles de segurança são necessários para prevenção de APTs?	ISO 27001 (2022); NIST (2024)
3. O método apresentado pode ser formalizado em algum processo de cibersegurança na sua organização? Caso positivo, quais processos?	ISO 27001 (2022); NIST (2024)

Fonte: Resultado da pesquisa (2024)

A seguir, cada subseção descreve as respostas e comentários realizados pelos especialistas e, para facilitar o entendimento, uma subseção é dedicada para a avaliação dos especialistas internos da organização, e outra subseção à avaliação dos especialistas externos. Ressalta-se que todos os especialistas consultados possuem experiência profissional ou acadêmica na área de segurança da informação e possuem pós-graduação (*lato sensu* ou

stricto sensu). Todos os dados pessoais dos participantes foram preservados conforme exigência da organização pesquisada, bem como dos próprios participantes da pesquisa.

4.4.1 Avaliação interna

Os resultados referentes à avaliação interna foram consolidados por meio de anotações e transcrição das entrevistas. Desse modo, os principais pontos abordados durante o questionamento efetuado serão destacados nos próximos parágrafos. Abaixo, o Quadro 14 apresenta o perfil dos especialistas internos da organização.

Para cumprir as exigências de privacidade da organização, nota-se que a coluna "Código" se refere ao termo utilizado nos trechos de entrevistas incluídos ao longo do texto, para identificar e anonimizar todos os especialistas internos da organização.

Quadro 14 – Especialistas internos

Setor	Função	Escolaridade	Experiência no setor	Código
Administração Pública	Analista	Pós-graduado (*lato sensu*)	Mais de 10 anos	AP-A1
	Assessor	Pós-graduado (*lato sensu*)	Mais de 10 anos	AP-AS
	Coordenador	Pós-graduado (*lato sensu*)	Mais de 10 anos	AP-C
	Gerente	Pós-graduado (*lato sensu*)	Mais de 10 anos	AP-G
	Líder de Equipe	Pós-graduado (*lato sensu*)	Mais de 10 anos	AP-L1
	Líder de Equipe	Pós-graduado (*lato sensu*)	Mais de 10 anos	AP-L2

Fonte: Resultado da pesquisa (2024)

Sobre a maneira como o método pode proteger um sistema hospedado na organização, os especialistas destacaram o papel relacionado ao risco cibernético e sua coerência com o ambiente da administração pública, desde a importância do método, ao Gestor do Serviço Público Digital, no sentido de informá-lo sobre um determinado risco identificado, como a visibilidade trazida a partir do mapeamento do risco cibernético: *"Eu acredito que o método apresentado pode ser útil na organização na medida em que os gestores dos serviços digitais entendam a aplicação, os ganhos e a importância do método"* [AP-L2].

De acordo com um especialista, o método pode ser integrado ao SGSI (Sistema de Gestão de Segurança da Informação) da organização: *"[...] A implementação desse método é conjugada ao SGSI, né? Ao sistema de gestão de segurança da informação. Integrando ali,*

principalmente as análises de risco e as análises dos requisitos técnicos [...] tem um potencial de apoiar bastante a execução do ciclo e até ajudar a obter resultados mais efetivos" [AP-C].

Outros pontos abordados nas respostas da primeira pergunta foram a possibilidade de reduzir um risco cibernético, bem como a precisão na definição dos controles de segurança que devem ser aplicados. De acordo com os especialistas, a visibilidade da ameaça trazida por meio do processo aplicado permite a análise de riscos com maior assertividade.

A respeito dos controles de segurança que são necessários para prevenção de APTs, dois especialistas comentaram que o controle de segurança dependerá do APT, devido ao uso de técnicas de engenharia social e utilização de *phishing* como vetor de ataque para acesso inicial: *"[...] depende, né? Então depende qual a linha que aquele APT segue. [...] Então, se eu tenho um APT que segue mais essa linha de uma engenharia social, eu vou trabalhar mais em controles em cima de conscientização de um usuário"* [AP-G].

De forma geral, os especialistas internos listaram controles de segurança relacionados a tecnologias de cibersegurança e processos ou políticas de gestão de segurança da informação, além de ações de treinamento e conscientização aos usuários. Dos controles de cibersegurança, 7 (sete) tecnologias foram citadas: *firewall* de rede, WAF, *firewall* de banco de dados, IPS, SIEM (*Security Information and Event Management*), criptografia e *proxy* para servidores.

Em relação aos controles processuais e políticas que a organização pode adotar para prevenção de APTs, 5 (cinco) controles foram citados: gestão de vulnerabilidades, atualizações de segurança ou de software, processo de configuração segura de tecnologias (processo conhecido na área de cibersegurança, como *hardening*), processos e políticas relacionadas à gestão de acessos, e aplicação do uso de privilégios mínimos para usuários de sistemas.

Na última questão, se o método apresentado pode ser formalizado em algum processo de cibersegurança na organização, todos os especialistas concordaram que o mesmo pode ser formalizado: *"Sim, com certeza. Eu acho que o método apresentado com certeza pode ser implementado nos processos, e eu já cito quais a gente poderia: colocar num processo de patch de segurança [...]. Num novo processo que a gente vai construir também, [...] que é o processo de gestão de vulnerabilidades mais amplo, que a gente quer englobar não só as*

análises de vulnerabilidade que a gente faz, mas também um processo de gestão junto ao SOC [...] para poder melhorar a nossa detecção de vulnerabilidades" [AP-L1].

Dos processos de cibersegurança citados, ao todo, 5 (cinco) foram citados pelos especialistas: gestão de riscos cibernéticos, gestão de atualizações de segurança, gestão de vulnerabilidades, testes de intrusão (*pentest*), e processos relacionados a detecção e bloqueio de ataques e ameaças vinculados ao SOC (*Security Operations Center*), conhecido como Centro de Operações de Segurança.

Sobre o processo de gestão de vulnerabilidades, segue destaque: *"O método apresentado no trabalho, a gente pode sim integrar ele dentro do nosso processo de gestão de vulnerabilidades"* [AP-G]. Especificamente, sobre o processo aplicado em APTs: *"Para que a gente consiga evoluir a maturidade do processo, [...] olhando os APTs, e principalmente APTs, que estão ali com foco em exploração de serviços governamentais, a gente consegue traçar uma estratégia melhor para conseguir combater, né? E evitar ataques bem-sucedidos. Então sim, o modelo apresentado atende perfeitamente. Pode ser integrado ao processo de vulnerabilidade aqui dentro da nossa organização"* [AP-G].

Um dos especialistas destacou que o processo apresentado no presente trabalho pode ser utilizado para criar estudos de caso sobre ações de monitoramento e detecção de ameaças cibernéticas: *"[...] eu diria (que) seria já nos processos do SOC, por exemplo, né? Processos como por exemplo, modelagem de ameaças, quanto a criação de cases. Modelagem de ameaças ali para a criação de cases de uso. [...] Case de uso de monitoramento, por exemplo. Poderia com certeza agregar"* [AP-AS].

Um especialista atuante na área de processos de cibersegurança destacou que a etapa do método referente à gestão do risco pode ser ajustada, no que diz respeito a nomenclatura e interações com demais áreas de riscos da organização. Destaca-se a resposta dada pelo Coordenador a respeito do método apresentado: *"Pensando aqui na nossa organização, eu acho que este seria um processo à parte. Eu acho que ele seria um processo independente, né, que receberia insumos dos outros processos da casa, mas eu o encaixaria dentro do que não seria formalmente um processo, mas sim um sistema. Eu o encaixaria dentro do SGSI que é executado anualmente"* [AP-C].

Por fim, os especialistas internos comentaram a relevância do processo construído, com destaque para facilidade no entendimento do método, a clareza trazida em cada etapa, e a possibilidade de se aplicar o método em outras organizações públicas: *"[...] implementar esse*

processo de uma forma geral na organização, acho que ficaria bem, bem interessante. Tem [...] potencial para trazer mais rigor para as atividades" [AP-C].

A notificação do risco cibernético ao gestor do serviço público e o desenho do processo de negócio construído pode auxiliar na estratégia de organizações públicas para responder esse tipo de risco: *"[...] é um método extremamente relevante. Ele certamente vai agregar nesta organização e outras organizações públicas também. Ele pode ser generalizado para outras esferas públicas e até privadas. Ele considera as ameaças e usa uma base teórica muito bem fundamentada para considerar essas ameaças que são cada dia mais frequentes e difundidas nos meios tecnológicos. Ele se preocupa com a proteção da organização e mitigação de riscos. Então, ele tem uma relevância muito grande. O trabalho, na minha visão, foi muito bem estruturado, tem uma formulação teórica consistente e utiliza as melhores práticas de segurança. E o referencial também é muito adequado para este tipo de disciplina, que é segurança da informação"* [AP-L2].

Além disso, o desenho do fluxo do processo e a inclusão do gestor do serviço público digital auxilia na gestão do risco cibernético: *"Eu acredito que está bem fácil de entender. O desenho está bastante completo e mostrando ali o envolvimento que existe entre órgãos gestores e órgãos de aplicação. Nem sempre isso é muito claro. Dentro das organizações, nem sempre a organização tem um nome, onde fica toda a responsabilidade por um sistema, por uma aplicação que pode ser invadido"* [AP-A].

4.4.2 Avaliação externa

A avaliação externa foi efetuada com 6 (seis) especialistas em segurança da informação, e contou com a participação de profissionais de diferentes segmentos, a saber: jurídico, financeiro, educacional, TI e segurança cibernética. A seguir, o Quadro 15 apresenta o perfil dos especialistas externos.

Quadro 14 – Especialistas externos

Setor	Função	Escolaridade	Experiência em Segurança da Informação e/ou TI	Código
Jurídico	Coordenador	Pós-graduado (*stricto sensu*)	Mais de 10 anos	J-C
Jurídico	Analista	Pós-graduado (*lato sensu*)	Mais de 10 anos	J-AN
Educação	Coordenador	Pós-graduado (*stricto sensu*)	Mais de 10 anos	E-C
Cibersegurança	Gerente	Pós-graduado (*lato sensu*)	Mais de 10 anos	C-G
Financeiro	Gerente	Pós-graduado (*lato sensu*)	Mais de 10 anos	F-G
TI	Consultor	Pós-graduado (*lato sensu*)	Mais de 10 anos	T-C

Fonte: Resultado da pesquisa (2024)

Optou-se por convidar especialistas de diversos segmentos para avaliar o método e o processo de negócio ser construído com maior assertividade. Além deste aspecto, a participação de especialistas presentes em segmentos diferentes assegura a aspecto interdisciplinar da avaliação, o que permite verificar a consistência e aplicabilidade do método em diferentes mercados, além do setor público brasileiro.

Sobre a primeira pergunta, que se refere de que forma o método pode proteger um sistema hospedado na organização, 1 (um) especialista do setor jurídico indicou a inexistência de um processo de caráter preventivo que tenha um fluxo de tarefa relacionando a notificação do gestor do produto quanto ao risco cibernético. Dessa forma, ele considera o processo relevante nesse sentido.

Os outros 5 (cinco) especialistas destacaram a clareza da modelagem para efetuar o mapeamento de riscos e vulnerabilidades para planejar ações de segurança para prevenção de uma ameaça. Abaixo, segue transcrição de um especialista que atua como Gerente em uma empresa de cibersegurança na América Latina:

"*Basicamente, você tem um mapeamento desses riscos e você tem uma visão clara de quais são os riscos de alto, baixo, médio ou até mesmo riscos que você pode assumir dentro da organização como riscos aceitáveis para o nível de negócio. Então, nesse sentido, você pode ter uma ideia é do quão elevado está o seu nível de vulnerabilidade frente a esse tipo de atacante. Então você pode ter eventualmente uma visão de quais atividades mais críticas você precisa realizar. Você tem uma priorização dessas atividades, né? E quais atividades você deve num plano diretor de segurança, por exemplo, tirar de prioridade, ou readequar o orçamento para elas, alguma coisa do tipo. Então, tendo essa visibilidade e mapeamento obviamente, incluindo essa visão dos riscos baseado nessa vulnerabilidade, com base na*

modelagem que foi feita você tem a capacidade de direcionar a sua maturidade de segurança de um nível x para o nível y de uma maneira mais organizada." [C-G].

Um dos especialistas que atua como consultor internacional de segurança cibernética no mercado de TI destacou que a aplicação do método traz completa visibilidade sobre a ameaça analisada.

A respeito da segunda pergunta, referente aos controles de segurança, todos os especialistas destacam controles tecnológicos de segurança cibernética de prevenção e detecção, como utilização de *firewalls* de rede, WAF, SIEM e tecnologias de detecção e prevenção de ameaças, como a utilização de tecnologias que dispõem de centrais de visibilidade, como soluções de *antimalware* para atuação manual ou automática pela equipe de Segurança Operacional.

Dos controles relacionados aos processos de segurança da informação, os seguintes foram citados pelos especialistas: monitoramento contínuo por meio de um SOC, testes de intrusão, gestão de atualizações de segurança, gestão de vulnerabilidades, gestão de acessos com a inclusão de políticas de privilégios mínimos aos usuários, a aplicação de diretrizes para implementação de MFA (múltiplo fator de autenticação), e processos relacionados a ações de conscientização de segurança da informação aos usuários da organização.

Um dos especialistas que atua no mercado financeiro destaca que, além de processos estruturados, deve-se aplicar a matriz RACI para assegurar a eficácia de cada processo de negócio implementado em cibersegurança:

[...] *Em primeiro lugar, com certeza, processos bem estruturados. Uma coisa fundamental, principalmente em grandes organizações, é você ter as os responsáveis, os owners ali por cada caixa do processo, né? É ter uma RACI bem estabelecida. Garantia a homogeneidade do ambiente para não poder se gerar Locks ali de falta de compatibilidade de soluções. Isso para mim é importantíssimo para você conseguir estruturar [...] os seus controles de segurança, né? É isso, digamos, falando de uma fase inicial dos controles de segurança propriamente ditos. [...] com certeza o nível de compliance mediante algum framework, para mim é fundamental. Esse nível de compliance é fundamental para um gestor conseguir ter a visibilidade do quão vulnerável ou não tá, e quais medidas precisam ser precisam ser deliberadas, quais ações precisam ser deliberadas para conseguir chegar no nível de compliance. Com certeza também um outro controle que é fundamental é a gestão da vulnerabilidade como um todo"* [F-C].

Em relação à terceira pergunta, referente a possibilidade de formalizar o processo construído em algum processo de cibersegurança na organização em que atua, todos os especialistas concordaram que o processo pode ser formalizado internamente. Dos processos mais citados, 3 (três) especialistas destacaram gestão de vulnerabilidades e gestão de atualizações, enquanto 5 (cinco) apontaram que o processo pode ser aplicado na habilitação de um novo serviço ou tecnologia: "*Eu acredito que no processo de mapeamento de risco, no geral, e principalmente no processo de habilitação de um serviço*" [C-G].

Um especialista afirmou que o processo apresentado pode ser utilizado para apoio na certificação de organizações ao padrão ISO 27000 enquanto outro especialista, que atua no setor jurídico, afirma que o processo pode ser formalizado para apoio em respostas a incidentes de segurança. O especialista que atuam no setor educacional destaca que o processo pode ser utilizado para implementação de novos equipamentos em centros educacionais, como equipamentos de tecnologia para laboratórios e novas sistemas a serem disponibilizados aos alunos.

Um dos especialistas, que trabalha como gerente em um grande banco privado brasileiro, destaca que o método é aderente à realidade do mercado financeiro e às práticas do mercado de cibersegurança: "*eu vejo que esse método, justamente como ele trabalha de uma forma preventiva, eu acho que [...] ele pode ajudar para trazer uma maturidade no processo de avaliação de não conformidades e riscos que, dentro de um ciclo de vida de um asset, são detectadas. E também ele pode trazer a modelagem necessária para a implementação de ferramentas*" [F-G].

Um dos especialistas destaca que o Brasil frequentemente é referência no que diz respeito a número de ataques cibernéticos e que o método apresentado poderá auxiliar na proteção de dados do cidadão durante o processo de transformação digital que o governo brasileiro tem conduzido. Segue comentário a respeito:

"Eu acho muito legal que esse tipo de processo seja seguido em boa parte das organizações públicas que a gente tem hoje e, efetivamente, a gente tem visto uma transformação digital muito bacana. Quando a gente olha para o Brasil, em geral, a gente tem visto o país tem se tornado uma referência global nesse sentido [...]. E a diversificação de ataque e de ameaça, ela é muito grande. [...] Quando a gente olha para o mercado de ameaças, no geral, o Brasil está sempre no top 10 tanto quanto o alvo, tanto quanto gerador

de ataques. Isso significa que num mercado onde fora da deep web, por exemplo, você já consegue contratar um tipo de ataque através do Google, por exemplo, pagando bitcoin, alguma coisa do tipo. Isso significa que as empresas precisam cada vez mais resguardar e preservar não só a sua marca no geral, que também se fortalecer com isso, mas principalmente o serviço que ela presta aos seus clientes. E quando a gente fala de serviço público, isso é ainda mais crítico, porque nós estamos tratando de dados confidenciais de pessoas. Nós estamos tratando eventualmente de informações, de doenças que essa pessoa teve durante a vida e, principalmente, nós estamos tratando de informações sensíveis que pode fazer essa pessoa se tornar um alvo no futuro também. Então, eu acho muito bacana que esse trabalho de modelagem de é de risco e de ameaça seja apresentado e desejo que efetivamente seja realizado em todas essas organizações" [C-G].

Resumidamente, todos os especialistas externos concordam que o método apresentado pode auxiliar organizações públicas brasileiras para efetuar ações preventivas em segurança da informação. Características como clareza, objetividade e as funções referentes à gestão do risco cibernético foram destacadas ao longo das entrevistas.

5 CONCLUSÃO

A presente pesquisa sobre a aplicação de um processo de negócio específico para modelagem de ameaças em uma organização pública brasileira foi realizada conforme disposições e exigências feitas pela organização que autorizou tal pesquisa, observando critérios de confidencialidade e privacidade. Ao analisar os resultados encontrados, pode-se afirmar que o estudo trás as seguintes contribuições:

- A aplicação de um processo específico para modelar ameaças cibernéticas permite maior visibilidade sobre uma ameaça, para que ações e estratégias de prevenção de ataques cibernéticos sejam devidamente executadas pelas áreas operacionais;
- O risco cibernético deve ser mapeado e integrado ao risco corporativo de um negócio;
- O gestor do serviço público digital de uma organização pública deve ser notificado e, principalmente, ser o responsável pelo gerenciamento do risco cibernético em seus serviços ou produtos digitais que estão sob sua responsabilidade;
- O processo de negócio desenvolvido para modelar ameaças pode ser implementado em processos operacionais de segurança da informação em organizações que adotam a transformação digital em seus produtos e serviços;
- O processo de modelagem de ameaças pode ser formalizado em processos de gestão de vulnerabilidades, gestão de atualizações de segurança, testes de intrusão, processos de detecção e bloqueio de ameaças, respostas a incidentes de segurança e ações de conscientização aos usuários;
- A modelagem de ameaças pode ser aplicada para habilitação de um novo serviço ou tecnologia a ser implementada em uma organização;
- Os usuários de uma organização devem realizar treinamentos contínuos de conscientização de segurança para prevenção de APTs;
- O método apresentado para modelar ameaças pode ser utilizado para apoiar organizações em processos de habilitação ou renovação de certificações internacionais como a ISO 27001.

O método apresentado pode ser aplicado, preferencialmente, em organizações que possuam condições de aplicar controles de segurança preventivos, detectivos e corretivos para mitigar o risco cibernético relacionado às ameaças cibernéticas do tipo APT.

O presente estudo apresenta limitações quanto aos critérios quantitativos para avaliação do risco cibernético e ao tamanho da amostra da avaliação. Considera-se que os resultados encontrados são limitados às organizações públicas que tenham condições similares.

Para estudos futuros, sugere-se que tal método e processo sejam aplicados em um conjunto de serviços digitais em organizações de diferentes segmentos de mercado, bem como em novas organizações públicas e privadas para seu contínuo aprimoramento.

REFERÊNCIAS

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. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

ALBERTIN, Alberto Luiz; ALBERTIN, Rosa Maria de Moura. **Benefícios do uso de tecnologia de informação para o desempenho empresarial.** Revista de Administração Pública, v. 42, p. 275-302, 2008.

ALHEBAISHI, Nawaf et al. **Threat modeling for cloud data center infrastructures.** In: Foundations and Practice of Security: 9th International Symposium, FPS 2016, Québec City, QC, Canada, October 24-25, 2016, Revised Selected Papers 9. Springer International Publishing, 2017. p. 302-319.

APARICIO-NAVARRO, Franciso J. et al. **Multi-stage attack detection using contextual information.** In: MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM). IEEE, 2018. p. 1-9. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005: Segurança da informação, segurança cibernética e proteção à privacidade - Orientação para gestão de riscos de segurança da informação**. Rio de Janeiro. 2023.

BAHRAMI, Pooneh Nikkhah et al. **Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures.** Journal of information processing systems, v. 15, n. 4, p. 865-889, 2019. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

BANCO MUNDIAL, **2022 GovTech Maturity Index Update. 2022**. Disponível em: https://www.worldbank.org/en/programs/govtech/2022-gtmi. Acesso em: 25 nov. 2023.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Brasil é reconhecido como segundo líder em governo digital no mundo**. [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos, 21 nov. 2022. Disponível em: https://www.gov.br/governodigital/pt-br/transformacao-digital/lista-servicos-digitais/servicos-digitais. Acesso em: 23 nov. 2023.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **GOV.BR já oferece 4 mil serviços públicos digitais para o cidadão**. [Brasília]: Ministério da Gestão e da Inovação em Serviços Públicos, 22 ago. 2022. Disponível em: https://www.gov.br/governodigital/pt-br/noticias/gov-br-ja-oferece-4-mil-servicos-publicos-digitais-para-o-cidadao. Acesso em: 25 nov. 2023.

BRASIL. **Decreto nº 9.756 de 11 de abril de 2019**. Gov.br. Brasília, DF: Presidência da República, [2019]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9756.htm. Acesso em: 14 nov. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 14 abr. 2023.

BRYANT, Blake D.; SAIEDIAN, Hossein. **Improving SIEM alert metadata aggregation with a novel kill-chain based classification model.** Computers & Security, v. 94, p. 101817, 2020. DOI: https://doi.org/10.1016/j.cose.2020.101817. Acesso em: 16 nov. 2023.

CABANILLAS, Cristina; RESINAS, Manuel; RUIZ-CORTÉS, Antonio. **Automated resource assignment in BPMN models using RACI matrices.** In: OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. p. 56-73.

CERQUEIRA JUNIOR, Abinel Santiago et al. **Pesquisa-ação na engenharia de produção: um estudo exploratório sobre sua aplicação na indústria.** Brazilian Journal of Production Engineering, [S. l.], v. 9, n. 1, p. 127–143, 2023. DOI: https://doi.org/10.47456/bjpe.v9i1.40096. Disponível em: https://periodicos.ufes.br/bjpe/article/view/40096. Acesso em: 28 ago. 2023.

CERQUEIRA JUNIOR, Abinel Santiago; ARIMA, Carlos Hideo. **Threat modeling: a study on its application in digital transformation from the perspective of risk.** Revista de Gestão e Secretariado (Management and Administrative Professional Review), v. 14, n. 1, p. 1158-1169, 2023. DOI: https://doi.org/10.7769/gesec.v14i1.1581. Acesso em: 17 set. 2023.

CHEN, Ping; DESMET, Lieven; HUYGENS, Christophe. **A study on advanced persistent threats.** In: Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15. Springer Berlin Heidelberg, 2014. p. 63-72.

CLOUDFLARE, **O que é um vetor de ataque?** Disponível em: https://www.cloudflare.com/pt-br/learning/security/glossary/attack-vector/. Acesso em: 18 de set. de 2023.

DELGADO, Pablo. **Developing an adaptive threat hunting solution: The elasticsearch stack.** 2018. Disponível em: http://hdl.handle.net/10657/3108. Acesso em: 10 set. 2023.

DRESCH, Aline et al. **Design science research**. Springer International Publishing, 2015.

DO XUAN, Cho; DAO, Mai Hoang. **A novel approach for APT attack detection based on combined deep learning model.** Neural Computing and Applications, v. 33, p. 13251-13264, 2021. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

ELING, Martin; WIRFS, Jan. **What are the actual costs of cyber risk events?.** European Journal of Operational Research, v. 272, n. 3, p. 1109-1119, 2019.

EY, **Cybersecurity: How do you rise above the waves of a perfect storm?** 30 de Julho de 2021. Disponível em: https://www.ey.com/en_br/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm. Acesso em: 30 nov. 2023.

FELICIANO-CESTERO, María M. et al. **Is digital transformation threatened? A systematic literature review of the factors influencing firms' digital transformation and internationalization.** Journal of Business Research, v. 157, p. 113546, 2023.

FORTNET, **Brasil é o segundo país que mais sofre ataques cibernéticos na América Latina**. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/brasil-e-o-segundo-pais-que-mais-sofre-ataques-ciberneticos-na-a. Acesso em: 08 de ago. de 2023.

GHAFIR, Ibrahim et al. **Disguised executable files in spear-phishing emails: Detecting the point of entry in advanced persistent threat.** In: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. 2018. p. 1-5. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

HEVNER, Alan; VOM BROCKE, Jan; MAEDCHE, Alexander. **Roles of digital innovation in design science research.** Business & Information Systems Engineering, v. 61, p. 3-8, 2019.

HUTCHINS, Eric M. et al. **Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.** Leading Issues in Information Warfare & Security Research, v. 1, n. 1, p. 80, 2011.

IBM, **Estudo IBM: consumidores pagam o preço por violações de dados**. Disponível em: https://www.ibm.com/blogs/ibm-comunica/estudo-ibm/. Acesso em: 18 de set. de 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection -Information security management systems -Requirements**. Geneva: ISO/IEC, 2022.

JOSHI, Chaitanya; ALIAGA, Jesus Rios; INSUA, David Rios. **Insider threat modeling: An adversarial risk analysis approach.** IEEE Transactions on Information Forensics and Security, v. 16, p. 1131-1142, 2020.

KASPERSKY, **O que é APT**. Disponível em: https://www.kaspersky.com.br/blog/o-que-e-apt/754/. Acesso em: 30 nov. 2023.

KHOSRAVI, Mehran; LADANI, Behrouz Tork. **Alerts correlation and causal analysis for APT based cyber attack detection.** IEEE Access, v. 8, p. 162642-162656, 2020. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

KIM, Hyeob; KWON, HyukJun; KIM, Kyung Kyu. **Modified cyber kill chain model for multimedia service environments.** Multimedia Tools and Applications, v. 78, p. 3153-3170, 2019. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

KIM, Kyounggon; ALFOUZAN, Faisal Abdulaziz; KIM, Huykang. **Cyber-attack scoring model based on the offensive cybersecurity framework.** Applied Sciences, v. 11, n. 16, p. 7738, 2021.

KUMAR, Rajesh et al. **APT attacks on industrial control systems: A tale of three incidents.** International Journal of Critical Infrastructure Protection, v. 37, p. 100521,

2022.

LALLIE, Harjinder Singh; DEBATTISTA, Kurt; BAL, Jay. **A review of attack graph and attack tree visual syntax in cyber security.** Computer Science Review, v. 35, p. 100219, 2020.

LV, Kun; CHEN, Yun; HU, Changzhen. **Dynamic defense strategy against advanced persistent threat under heterogeneous networks.** Information Fusion, v. 49, p. 216-226, 2019. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: xx out. 2023.

MELLO, Carlos Henrique Pereira et al. **Pesquisa-ação na engenharia de produção: proposta de estruturação para sua condução.** Production, v. 22, p. 1-13, 2012.

MITRE, **Active Scanning**. https://attack.mitre.org/techniques/T1595/. Acesso em: 15 set. 2023.

MITRE, **APT29**, Disponível em: https://attack.mitre.org/groups/G0016/. Acesso em: 12 set. 2023.

MITRE, **Command and Scripting Interpreter**. Disponível em: https://attack.mitre.org/techniques/T1059/. Acesso em: 15 set. 2023.

MITRE, **Exfiltration Over Alternative Protocol**. Disponível em: https://attack.mitre.org/techniques/T1048/. Acesso em: 15 set. 2023.

MITRE, **Exploit Public-Facing Application**. https://attack.mitre.org/techniques/T1190/. Acesso em: 15 set. 2023.

MOOTHEDATH, Shana et al. **A game-theoretic approach for dynamic information flow tracking to detect multistage advanced persistent threats.** IEEE Transactions on Automatic Control, v. 65, n. 12, p. 5248-5263, 2020. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

MOȘTEANU, Narcisa Roxana. **Challenges for organizational structure and design as a result of digitalization and cybersecurity.** The Business & Management Review, v. 11, n. 1, p. 278-286, 2020.

MOURATIDIS, Haralambos et al. **Modelling language for cyber security incident handling for critical infrastructures.** Computers & Security, v. 128, p. 103139, 2023.

NEW YORK TIMES. **Hackers in China Attacked The Times for Last 4 Months**. Disponível em: https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html. Acesso em: 30 nov. 2023.

NIST, **The NIST Cybersecurity Framework 2.0**, Disponível em: https://doi.org/10.6028/NIST.CSWP.29.ipd. Acesso em: 13 nov. 2023.

NIST, **National Vulneability Database-Vulnerability Metrics**, Disponível em: https://nvd.nist.gov/vuln-metrics/cvss. Acesso em: 12 set 2023.

QUINTERO-BONILLA, Santiago; MARTÍN DEL REY, Angel. **A new proposal on the advanced persistent threat: A survey.** Applied Sciences, v. 10, n. 11, p. 3874, 2020. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

SHAHID, Waleed Bin et al. **An enhanced deep learning based framework for web attacks detection, mitigation and attacker profiling.** Journal of Network and Computer Applications, v. 198, p. 103270, 2022.

SINGH, Saurabh et al. **A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions.** The Journal of Supercomputing, v. 75, p. 4543-4574, 2019. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

STOJANOVIĆ, Branka; HOFER-SCHMITZ, Katharina; KLEB, Ulrike. **APT datasets and attack modeling for automated detection methods: A review.** Computers & Security, v. 92, p. 101734, 2020. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

TATAM, Matt et al. **A review of threat modelling approaches for APT-style attacks.** Heliyon, v. 7, n. 1, 2021. DOI: https://doi.org/10.1016/j.heliyon.2021.e05969. Acesso em: 16 nov. 2023.

TSEGAYE, Tamir; FLOWERDAY, Stephen. **Controls for protecting critical information infrastructure from cyberattacks.** In: World Congress on Internet Security (WorldCIS-2014). IEEE, 2014. p. 24-29.

UNIÃO EUROPEIA, **Regulamento Geral sobre a Proteção de Dados (RGPD)**, de 27 de Abril de 2016. Disponível em: https://eurlex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 30 nov. 2023.

WAGNER, Thomas D. et al. **Cyber threat intelligence sharing: Survey and research directions.** Computers & Security, v. 87, p. 101589, 2019. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

WHITMAN, Michael E.; MATTORD, Herbert J. **Principles of information security**. Cengage learning, 2021.

XIAO, Liang et al. **Attacker-centric view of a detection game against advanced persistent threats.** IEEE transactions on mobile computing, v. 17, n. 11, p. 2512-2523, 2018. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

XIONG, Chunlin et al. CONAN: **A practical real-time APT detection system with high accuracy and efficiency.** IEEE Transactions on Dependable and Secure Computing, v. 19, n. 1, p. 551-565, 2020. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

YANG, Lu-Xing et al. **A risk management approach to defending against the advanced persistent threat.** IEEE Transactions on Dependable and Secure Computing, v. 17, n. 6, p. 1163-1172, 2018. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

YANG, Lu-Xing et al. **Effective repair strategy against advanced persistent threat: A differential game approach.** IEEE Transactions on Information Forensics and Security, v. 14, n. 7, p. 1713-1728, 2018. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

YOKOYAMA, Rodrigo; ARIMA, Carlos Hideo. **Modelagem de ameaça, análise de risco e suas aplicações na literatura.** International Journal of Development Research, v. 12, n. 04, p. 55049-55055, 2022.

YOSHIKUNI, Adilson Carlos; ALBERTIN, Alberto Luiz. **Effects of strategic information systems on competitive strategy and performance.** International Journal of Productivity and Performance Management, v. 67, n. 9, p. 2018-2045, 2018.

YUSIF, Salifu; HAFEEZ-BAIG, Abdul. **A conceptual model for cybersecurity governance.** Journal of applied security research, v. 16, n. 4, p. 490-513, 2021.

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. DOI: https://doi.org/10.1016/j.cose.2019.07.001. Acesso em: 16 nov. 2023.

APÊNDICE A | MÉTODO MCT-RB (Modelling Cyber Threats using Risk-Based approach)

MÉTODO MCT-RB

Modelling Cyber Threats using Risk-Based approach

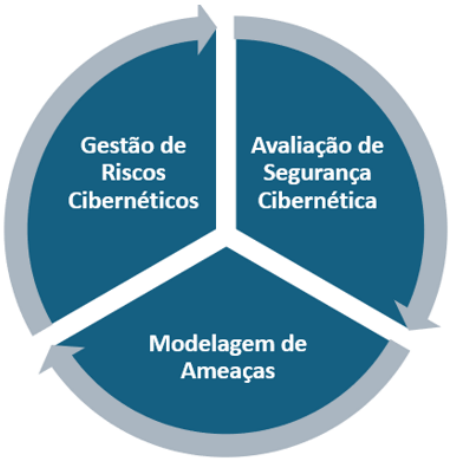
BREVE INTRODUÇÃO AO TEMA

Com o avanço da plataforma e a adoção da transformação digital de serviços públicos, em comparação com 198 economias globais, o Índice GovTech Maturity Index 2022, divulgado pelo Banco Mundial, destaca que o Brasil foi reconhecido mundialmente como segundo líder em governo digital, ficando à frente de países como Espanha, França, Emirados Árabes Unidos, Japão e Estônia (Banco Mundial, 2022; Brasil, 2022).

Uma ameaça cibernética pode ser definida como um evento ou circunstância causada por um agente de ameaça que visa explorar, intencionalmente ou não, uma vulnerabilidade técnica específica. Para que uma ameaça seja analisada com profundidade, aplicam-se diferentes tipos de métodos para análise de uma ameaça ou ataque cibernético (Nist, 2023).

As Ameaças Persistentes Avançadas, tradução literal de "*Advanced Persistent Threat*" (APT), são ataques cibernéticos executados por **grupos experientes e altamente organizados**, cuja intenção é **comprometer** os 3 pilares da Segurança da Informação, que são: **confidencialidade, integridade e disponibilidade** de uma informação ou infraestrutura crítica (Tatam *et al*, 2021).

MÉTODO MCT-RB (*Modelling Cyber Threats using Risk-Based approach*)



Fonte: Resultado da pesquisa (2024)

MÉTODO MCT-RB (*Modelling Cyber Threats using Risk-Based approach*)

O método é dividido em três etapas, conforme descrição a seguir:

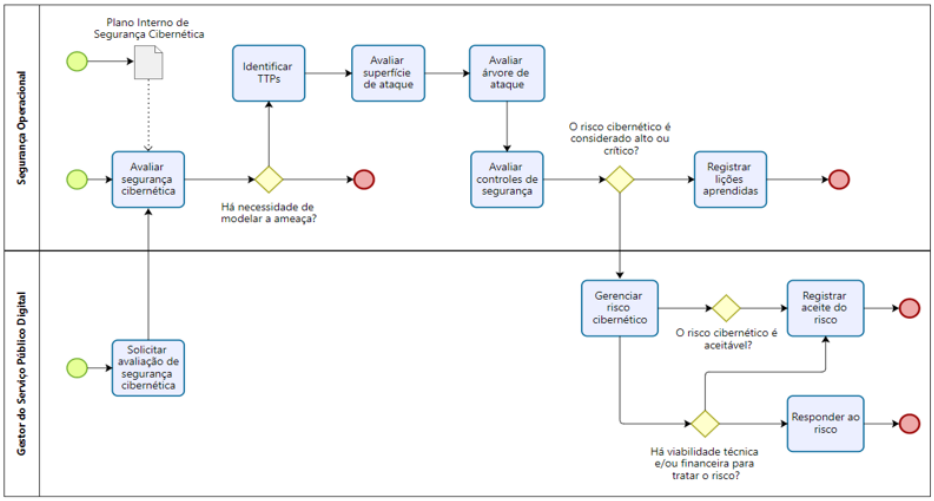
1. **Avaliação de segurança cibernética**: consiste em efetuar testes de segurança em um determinado sistema, aplicação ou infraestrutura para verificar fragilidades e possíveis vulnerabilidades de segurança

2. **Modelagem de ameaças**: tem como objetivo realizar uma análise sobre que tipo de ameaça pode ser capaz de explorar vulnerabilidades presentes no sistema avaliado

3. **Gestão de riscos cibernéticos**: visa obter uma visão executiva sobre o grau de exposição ao risco cibernético referente à ameaça analisada.

PROCESSO DE NEGÓCIO

A partir da construção do método, o processo de negócio abaixo foi desenvolvido utilizando boas práticas de BPM (*Business Process Model*).



Fonte: Resultado da pesquisa (2024)

APÊNDICE B | FORMULÁRIO PARA VALIDAÇÃO INTERNA

Modelagem de ameaças aplicada em APTs em uma organização pública | Validação Interna

Você está sendo convidado a participar da pesquisa "**Uma análise sobre a modelagem de ameaças aplicada em ataques cibernéticos do tipo APT (*Advanced Persistent Threats*) em uma organização pública**" e sua seleção foi por ser especialista interno da organização. Esta pesquisa está sendo desenvolvida pelo pesquisador Abinel Santiago Cerqueira Junior, sob orientação do Prof. Dr. Carlos Hideo Arima, no âmbito do Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos do Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS).

Sua contribuição muito engrandecerá nosso trabalho pois participando desta pesquisa você nos trará uma visão específica pautada na sua experiência sobre o assunto. Esclarecemos, contudo, que sua participação não é obrigatória. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição proponente.

O objetivo deste estudo é "**analisar a aplicação de um processo específico para modelagem de ameaças para análise e prevenção de ataques cibernéticos do tipo APT em serviços públicos digitais**".

As informações obtidas por meio **desta pesquisa serão confidenciais e asseguramos o sigilo sobre sua participação**. Os dados serão divulgados de forma a não possibilitar sua identificação, protegendo e assegurando sua privacidade.

A pesquisa é anônima e possui somente 3 questões.

Com base na leitura prévia do documento enviado juntamente com o link desta pesquisa, o tempo estimado para respondê-la é de aproximadamente 10 minutos.

1. Declaro que entendi os objetivos de minha participação nessa pesquisa e concordo em participar em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD). *

- ◯ Concordo e ciente

2. Qual seu cargo na organização selecionada para a pesquisa? *

- ◯ Gerente ou Coordenador
- ◯ Líder de Equipe
- ◯ Analista

3. Quantos anos de trabalho você possui na empresa? *

- ◯ 1 a 5 anos
- ◯ 5 a 10 anos
- ◯ Mais de 10 anos

4. Considerando que:

   -Os ataques cibernéticos do tipo APT são promovidos por grupos altamente organizados e experientes;
   -As medidas de segurança que são adotadas atualmente na sua organização.

   De que forma o método apresentado para modelar ameaças pode proteger um sistema hospedado na sua organização? *

   Insira sua resposta

5. Na sua opinião, que controles de segurança são necessários para prevenção de APTs? *

   Insira sua resposta

6. O método apresentado pode ser formalizado em algum processo de cibersegurança na sua organização? Caso positivo, quais processos? *

   Insira sua resposta

APÊNDICE C | FORMULÁRIO PARA VALIDAÇÃO EXTERNA

Modelagem de ameaças aplicada em APTs em uma organização pública | Validação Externa

Você está sendo convidado a participar da pesquisa "**Uma análise sobre a modelagem de ameaças aplicada em ataques cibernéticos do tipo APT (*Advanced Persistent Threats*) em uma organização pública**" e sua seleção foi por ser especialista externo. Esta pesquisa está sendo desenvolvida pelo pesquisador Abinel Santiago Cerqueira Junior, sob orientação do Prof. Dr. Carlos Hideo Arima, no âmbito do Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos do Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS).

Sua contribuição muito engrandecerá nosso trabalho pois participando desta pesquisa você nos trará uma visão específica pautada na sua experiência sobre o assunto. Esclarecemos, contudo, que sua participação não é obrigatória. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição proponente.

O objetivo deste estudo é "**analisar a aplicação de um processo específico para modelagem de ameaças para análise e prevenção de ataques cibernéticos do tipo APT em serviços públicos digitais**".

As informações obtidas por meio **desta pesquisa serão confidenciais e asseguramos o sigilo sobre sua participação**. Os dados serão divulgados de forma a não possibilitar sua identificação, protegendo e assegurando sua privacidade.

Sua contribuição será muito importante devido a sua experiência e conhecimento sobre o assunto.

A pesquisa é anônima e possui somente 3 questões.

Com base na leitura prévia do documento enviado juntamente com o link desta pesquisa, o tempo estimado para respondê-la é de aproximadamente 10 minutos.

1. Declaro que entendi os objetivos de minha participação nessa pesquisa e concordo em participar em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD). *

- ◯ Concordo e ciente

2. Qual sua maior graduação acadêmica? *

- ◯ Doutorado
- ◯ Mestrado
- ◯ Pós Graduação / MBA
- ◯ Bacharelado / Tecnólogo

3. Qual sua experiência profissional e/ou acadêmica na área de segurança cibernética ou segurança da informação? *

- ◯ 1 a 5 anos
- ◯ 5 a 10 anos
- ◯ Mais de 10 anos

4. Considerando que:

-Os ataques cibernéticos do tipo APT são promovidos por grupos altamente organizados e experientes;
-As medidas de segurança que são adotadas atualmente na sua organização.

De que forma o método apresentado para modelar ameaças pode proteger um sistema hospedado na sua organização? *

Insira sua resposta

5. Na sua opinião, que controles de segurança são necessários para prevenção de APTs? *

Insira sua resposta

6. O método apresentado pode ser formalizado em algum processo de cibersegurança na sua organização? Caso positivo, quais processos? *

Insira sua resposta