Mecanismo de Priorização em Segurança da Informação para um ambiente de Computação em Nuvem Pública

Rodrigo Blefari, Fatec São Caetano do Sul, sr.blefari@gmail.com
Pedro P. Paulon, Fatec São Caetano do Sul, pedro.peoss@gmail.com
Kaique Alves Lima, Fatec São Caetano do Sul, kaiqui82@gmail.com
Edna M. Duarte, Fatec São Caetano do Sul, edna.duarte@fatec.sp.gov.br

Resumo

As organizações estão passando por um momento de grande transição, principalmente, no que tange seus ambientes computacionais. A utilização de computação em nuvem pública vem aumentando, muito por conta das vantagens oferecida, em relação ao antigo modelo de infraestrutura própria. Em conjunto com essa mudança, há também uma série de novos desafios em especial para segurança da informação. Nesse contexto, foi desenvolvido este artigo que tem como objetivo: utilizar o Modelo de Causa e Efeito e a Teoria dos Grafos, para fornecer um mecanismo de priorização de ações relacionadas à Segurança da Informação em um ambiente de Computação em Nuvem, tendo como base as boas práticas fornecidas pelo NIST 800-144. Assim, caracteriza-se como uma pesquisa bibliográfica, que por fim, apresenta um modelo conceitual que explora a multidisciplinaridade como fator diferencial e que poderá atender às expectativas de segurança da informação para diferentes segmentos de mercado com relação a priorização.

Palavras-chave: Priorização, Segurança da Informação, Modelo de Causa e Efeito, Teoria dos Grafos, Computação em Nuvem.

Abstract

Organizations are going through a moment of great transition, especially about their computing environments. The use of public cloud computing has been increasing, largely because of the advantages it offers, compared to the old proprietary infrastructure model. Along with this change, there are also several new challenges in particular for information security. In this context, this article was developed that aims to: use the Cause and Effect Model and the Graph Theory, to provide a mechanism for prioritizing actions related to Information Security in a Cloud Computing environment, based on the best practices provided by NIST 800-144. Thus, it is characterized as bibliographic research, which finally presents a conceptual model that explores multidisciplinarity as a differential factor and that can meet the information security expectations for different market segments regarding prioritization.

Keywords: Prioritization, Information Security, Cause and Effect Model, Graph Theory, Cloud Computing.

1. Introdução

Até pouco tempo atrás as empresas se viam com a necessidade de comprar computadores cada vez mais potentes, que em pouco tempo se tornavam defasados ou obsoletos, para realizar as tarefas para quais foram adquiridos. Atualmente, um novo modelo de mercado surgiu para atender a esta demanda, a Computação em Nuvem ou *Cloud Computing*, que tem a capacidade de suprimir a maioria das necessidades das corporações de uma forma extremamente eficaz. Por meio de seus pilares de disponibilidade, elasticidade e *pay-per-use* (pague pelo uso), a computação em nuvem, conseguiu atingir em cheio os novos modelos de negócio chamados de *startups*, que passam por expansões meteóricas em um curto espaço de tempo, e ainda, as empresas mais tradicionais. Para todas essas empresas esse novo modelo possibilita uma redução substancial de seu *Capital Expenditure* – CAPEX, migrando esse investimento para *Operational Expenditure* – OPEX, por meio de um serviço totalmente personalizado capaz de adequar as necessidades do negócio e suas variações de demanda.

Paralelo a toda essa revolução proporcionada pela computação em nuvem ocorreu também a transferência do perímetro do ambiente computacional das organizações, que antes se limitavam a sua infraestrutura física e agora enfrentam os desafios de estarem muito além dessa barreira. Além disto, há a contínua evolução de ataques cibernéticos, os quais o modelo antigo de proteção não mais se mostra eficaz. Com isto, pequenas, médias e grandes empresas, e até mesmo usuários pessoais vivem hoje, a necessidade de se obter mecanismos de proteção que se enquadrem nessa nova realidade.

De acordo com Gonzalez e Miers (2013), as ameaças aos ambientes de informática não estão relacionados ao local onde estão estas estruturas, ou seja, a computação em nuvem por si só não é a fonte desses novos problemas, mas existe uma carência de mecanismos capazes de mitigar os riscos, e diante disso este artigo, que é um recorte de uma monografia desenvolvida no Curso Superior de Tecnologia em Segurança da Informação da FATEC São Caetano do Sul, se propõe a desenvolver os conceitos que não só possibilitem a criação de um mecanismo de segurança por meio de conhecimentos multidisciplinares, mas também fomentar a evolução de desenvolvimento de ferramentas deste tipo no formato *open source*, para que pesquisadores com interesse neste tema e com conhecimento necessário possam contribuir para a melhoria contínua deste processo. Desta forma, este artigo tem como objetivo utilizar o Modelo de Causa e Efeito e a Teoria dos Grafos, para fornecer um mecanismo de priorização de ações relacionadas à Segurança da Informação em um ambiente de Computação em Nuvem, tendo como base as boas práticas fornecidas pelo NIST 800-144.

Ainda, é possível observar que há uma carência muito grande de produção de conteúdo

conceitual sobre segurança da informação em português. Apesar de cada dia, mais e mais profissionais, se capacitarem nesse universo, a grande maioria acaba por ingressar na parte operacional. Este aspecto somado a grande expansão do uso de nuvens públicas, que segundo pesquisa realizada pelo Gartner em 2019, somente em 2020, haverá um aumento de investimentos da ordem de 30 bilhões de dólares nesse seguimento de serviços, gera a necessidade de pesquisas, com foco no desenvolvimento de um modelo conceitualmente sobre o tema. Além disso, este crescimento cria vulnerabilidades da mesma proporção do ponto de vista da cibersegurança.

Assim, grandes empresas do segmento de segurança cibernética participam de uma corrida para atender às demandas crescentes de proteção desses ambientes, pois as cifras são altas e esse movimento de migração já é uma realidade, não muito recente. Se levar essa perspectiva para o usuário comum ou até a pequena organização, que não dispõe de capital para investir em soluções caras, é possível observar um problema ainda maior, a falta de ferramentas de código aberto com modelo de licenciamento gratuito.

Tendo em vista todos esses fatores, a falta de estudos que sirvam como base para a criação desses mecanismos de baixo custo e que sejam destinados a proteger estes ambientes de setores específicos orientados por criticidade, faz com que seja latente a necessidade de se fomentar conceitos e estruturas que atendam a expansão e evolução destes meios de defesa cibernética. Assim, realizar a correlação entre o *baseline* fornecido pelo NIST 800-144 e as vulnerabilidades às quais os aspectos avaliados estão sujeitos, possibilitará criar uma ordem de prioridade de vulnerabilidades relacionadas a sua criticidade para que sejam tratadas de forma adequada e em tempo. A combinação das diferentes disciplinas envolvidas neste estudo, poderá fornecer um conjunto consolidado, capaz de realizar uma análise complexa, e fornecer uma resposta clara e objetiva do objeto avaliado.

Diante disto, esse estudo caracteriza-se como uma pesquisa bibliográfica que desenvolveu um mecanismo de priorização pautada em artigos, capítulos de livros e documentos da área de conhecimento de Segurança da Informação. No qual, o primeiro mecanismo escolhido para esta abordagem foi o Diagrama de *Ishikawa* ou Modelo de Causa e Efeito, pois ele é capaz de estruturar de uma forma segmentada, múltiplos aspectos de possíveis vulnerabilidades de segurança e, para o modelo proposto, associar estas causas a um efeito desejado. Vale ressaltar, que o efeito é a ordem em que estas causas devem ser tratadas. Esta estrutura associada ao segundo mecanismo adotado, a Teoria dos grafos, consegue incorporar um método matemático que é capaz de fornecer um resultado numérico sobre qual

dessas vulnerabilidades são de maior severidade ao negócio. Sendo que esta base de informação, a respeito da nota atribuída a severidade de uma vulnerabilidade, está associada a um terceiro elemento que se incorpora ao projeto; a base de dados das *Common Vulnerabilities and Exposures* – CVEs. Sua escolha se deve a característica de classificar as vulnerabilidades por meio de uma nota de severidade elencada a *Common Vulnerability Scoring System* – CVSS, e assim, ser uma forma simples de estabelecer uma ordem de criticidade, além de fornecer orientação para resolução dessas vulnerabilidades, na maioria dos casos. Como *baseline* norteador foi utilizado o documento de referência do *National Institute of Standards and Technology* - NIST 800-144 *Guidelines on Security and Privacy in Public Cloud Computing*, dele foram incorporadas as premissas que norteiam todas as análises necessárias para este tipo de ambiente, além de prover uma base para a correlação com boas práticas a um segmento de mercado específico e com isso fornece uma avaliação mais precisa e personalizada.

Com isto, este artigo foi estruturado em 5 seções, começando com a introdução que apresentou a contextualização do tema, o objetivo, a justificativa e a metodologia. Em seguida, na segunda seção, foi fornecido o embasamento teórico para o desenvolvimento e compreensão da pesquisa, pontuando uma introdução do Modelo de Causa e Efeito, Teoria dos grafos e Segurança da Informação. Na terceira seção, foi realizada uma breve contextualização da Computação em Nuvem e apresentado o documento que foi utilizado como base de todo o desenvolvimento da pesquisa, o NIST 800-144. Na quarta seção, foi apresentado o mecanismo de priorização desenvolvido. E por fim, na quinta seção, foram pontuadas as considerações finais sobre o tema pesquisado.

2. Associando os conceitos do Modelo de Causa e Efeito e Teoria dos Grafos à Segurança da Informação

O Diagrama de Ishikawa conhecido também como Diagrama Espinha de Peixe, de acordo com Peinado e Graeml (2007), é um modelo gráfico usado com a finalidade de segregar raciocínios em diversos processos para representar as possíveis causas relacionadas a cada um dos aspectos avaliados e a relação entre o possível efeito positivo ou negativo gerado por estas causas.

Criado pelo engenheiro químico japonês Kaoru Ishikawa, em 1943, o Modelo de Causa e Efeito foi originalmente proposto com o intuito de auxiliar na solução de problemas na produção industrial, e seu uso foi aprimorado durante os anos, sendo hoje mais aplicado nesse ramo, utilizando-se da metodologia 6M: Método, Material, Mão-de-obra, Máquina,

Medida e Meio Ambiente.

Ainda, para os autores, nessa metodologia, se separa cada M em uma espinha do peixe, após deve-se elencar dentro de cada parâmetro, as possíveis causas do problema ou efeito a ser analisado, e com isso é possível obter uma visão mais ampla dos processos separadamente, auxiliando na resolução do problema. Cabe ressaltar que não há limitações quanto ao uso do Modelo de Causa e Efeito, sendo possível sua aplicação por pessoas que não possuam um conhecimento profundo sobre os aspectos avaliados, pois o próprio método se enquadra como uma ferramenta prática para prover insumos de análise e aperfeiçoamento de resultados, e assim, ser uma forma muito eficaz e estruturada para a solução de problemas em diversos setores e tipos de organizações. Desta forma, nesta pesquisa, o Modelo de Causa e Efeito foi utilizado, para separar os pontos de atenção especificados pelo NIST 800-144, em relação à segurança da informação para Computação em Nuvem Pública, e com isso foi possível mensurar separadamente o risco para cada um destes pontos, tendo como base a pontuação de severidade fornecida pelas *Common Vulnerabilities and Exposures* - CVE's, às quais estejam susceptíveis, e com isto obter uma ordem de priorização de ações de proteção para os segmentos avaliados.

Segundo Boaventura e Jurkiewicz (2017) na antiga Prússia no século XVIII, o matemático Leonhard Paul Euler em uma visita a cidade de Königsberg, residência de diversos intelectuais, tomou conhecimento de um problema aparentemente simples, mas sem solução: um rio cortava a cidade, e no meio dele havia duas ilhas ligadas por uma ponte, que possuía seis pontes que a ligavam a margem, de acordo com Nogueira (2015). O problema era encontrar um trajeto que atravessasse a ponte uma única vez e retornasse a origem de partida. Euler observou que o número de pontes em cada ilha, era sempre ímpar, e provou aos intelectuais que para conseguir realizar o trajeto, deveria haver um número par ligando a margem as pontes, segundo Boaventura e Jurkiewicz (2017). Mais de 280 anos atrás ocorria o primeiro registro de um problema relacionado a grafos em que ele trouxe uma nova perspectiva a um problema que provou não haver solução.

A representação gráfica dos grafos torna a compreensão do problema mais simples. Uma forma de representar graficamente, é rotular cada vértice, a fim de que, por esses dados possa identificá-lo. Ao trabalhar com grafos para expressar determinadas situações em que seja necessário rotular, utiliza-se conjuntos para que os elementos sejam bem definidos e distintos, de acordo com Boaventura e Jurkiewicz (2017). O modelo de grafo em floresta contempla problemas que são acíclicos, ou seja, nem todos os vértices possuem ligação entre

si; e não conexos, pois não existe caminho entre quaisquer vértices. Esta abordagem foi utilizada na elaboração desta pesquisa, para tratar dos diversos temas como: governança, *compliance*, *trust*, arquitetura, IAM, isolamento de *software*, proteção de dados, resposta a incidentes e disponibilidade, dentro de um único assunto Computação em Nuvem Pública.

Ainda, há muito tempo os negócios evoluíram, empresas se adaptaram às novidades que surgiram no mercado, e podemos dizer que a informação é um dos ativos mais importantes de uma organização, e que vem sendo mais valorizado a cada dia. Se foi o tempo em que a informação era tratada de forma mais centralizada, atualmente esse ativo está presente em todos os setores e processos das organizações, sendo compartilhado e permitindo a implantação de modelos de gestão mais ágeis e eficientes, garantindo uma vantagem competitiva. A informação, para Fontes (2006), é um ativo de grande importância na empresa, e necessita estar adequadamente protegida. Podemos então, afirmar que o dado pode ser, uma troca de informações em uma comunicação ou informações de maior relevância dentro das organizações, fato é que, em ambos os casos, esses dados devem ser protegidos.

Logo, para garantir que o dado esteja seguro, e garantir que a informação seja regida pelos pilares de confidencialidade, integridade e disponibilidade, é necessário a utilização não só de ferramentas de *software* e equipamentos voltados para a segurança da informação, mas também políticas de segurança e uma gestão da informação que esteja alinhada para o cumprimento das normas que regem aquele dado. Para que isso seja feito de forma eficiente também é necessário se ter em mente os conceitos de ameaça, vulnerabilidade e riscos que os dados possam estar sujeitos no ambiente organizacional. Sêmola (2014) diz que vulnerabilidades são fragilidades presentes ou associadas aos ativos que manipulam e/ou processam os dados, (...) e ameaças são agentes ou condições que afetam os dados e seus ativos, explorando vulnerabilidades, gerando incidentes e impactando os negócios da empresa. Com isto, podemos concluir que as ameaças exploram vulnerabilidades, gerando riscos que impactam as organizações.

Diante disto, este trabalho leva essa visão para a computação em nuvem, baseando-se no NIST-800 144, utilizando o Modelo de Causa e Efeito e a Teoria dos Grafos, como uma forma de elencar os pontos de atenção descritos no documento, e desta forma mostrar dentro de um contexto, a quais vulnerabilidades a organização pode estar exposta, apontando as CVEs relacionadas a cada ponto de atenção elencado, e também retornando as boas práticas descritas no NIST para a segurança em Computação em Nuvem Pública, auxiliando

na priorização de ações de segurança da informação, com o objetivo de reduzir os riscos aos dados de organizações.

3. A Computação em Nuvem Pública e NIST 800-144

A computação em nuvem nem sempre foi da forma que conhecemos, segundo Gartner (2020), com recursos abrangentes de segurança, controles sofisticados, arquiteturas híbridas que atendem diversos tipos de infraestruturas e escalável para atender as demandas do mercado. Foram necessárias décadas de evolução para que os serviços de nuvem pública fossem tendência no mundo todo.

Na transição dos processos e atividades de negócio das empresas para o mundo digital, novos riscos surgiram por meio de ataques realizados dentro desse meio, com o intuito de roubo de informações, paralização dos processos, dentre outras ações, que prejudiquem as organizações. O fato é que a superfície de ataque aos ativos, dessas empresas, aumentou drasticamente, de acordo com Nakamura e Geus (2007, p. 26) “novas tecnologias e novos sistemas sempre são criados, é razoável considerar que novas vulnerabilidades sempre existirão e, portanto, novos ataques também sempre serão criados”.

Porém, ferramentas e serviços não são suficientes para manter a segurança de uma empresa, afinal em todos os seus processos, pessoas estão envolvidas, e essas podem cometer erros seja por falta de treinamento e conhecimento, ou por malícia, visando adquirir algo em benefício próprio. Para lidar com esse aspecto, é necessário o desenvolvimento e implementação de Políticas de Segurança da Informação - PSI, para Nakamura e Geus (2007, p. 188), ela é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante dentro de todas as organizações, tratando de aspectos humanos, culturais e tecnológicos, e considerando também, os processos e os negócios além da legislação local. E para que essa política seja implementada de forma efetiva, ela deve ter o apoio dos executivos e ser entendida por todos os funcionários da organização.

Com o surgimento de legislações locais voltadas para a segurança da informação, as instituições necessitam estar com todos os seus processos em conformidade com a lei que rege a sua área. Para auxiliar nessa questão existem *frameworks* e *baselines*, como o NIST *Cybersecurity Framework*, que abrange um conjunto de normas e regras que as empresas precisam aplicar em seus processos organizacionais relacionados à segurança da informação para estar em conformidade.

3.1. O NIST 800-144

O *National Institute of Standards and Technology* - NIST, fundado em 1901, parte do U.S. *Departament of Commerce* ou Departamento de Comércio dos Estados Unidos, foi criado com o objetivo de aumentar a competitividade dos Estados Unidos nos mais diversos segmentos industriais provendo métodos de medição, padrões e tecnologia. O NIST 800 144 *Guidelines on Security and Privacy in Public Cloud Computing* foi criado pelos autores Wayne Jansen da Booz Allen Hamilton e Tim Grance, ambos do NIST, com o objetivo de fornecer uma visão geral dos desafios de segurança e privacidade pertinentes à Computação em Nuvem Pública, apontando as considerações que as organizações devem observar quando fazem uso de um ambiente de nuvem pública.

O documento se divide em 6 seções*: Introduction, Background, Public Cloud Services, Key security and Privacy Issues Public Cloud Outsourcing and Conclusion*. A estrutura do documento traz uma contextualização inicial sobre computação em nuvem, os modelos de serviço, como funcionam as regras de divisão e responsabilidade, aprofundando a abordagem do tema para nuvens públicas. Todo este embasamento teórico precede as recomendações de segurança, ponto principal tratado pelo documento, ele se divide em 9 categorias distintas a saber: *Governance, Compliance,Trust, Architecture, Identity and Access Management, Software Isolation, Data Protection, Availability e Incident Response*, em cada um destes tópicos, é realizada uma série de considerações, descritas a seguir, e que devem ser observadas do ponto de vista da segurança.

Para *Governance* devemos ter controle e supervisão pela organização sobre políticas, procedimentos e padrões para o desenvolvimento de aplicativos e aquisição de serviços de tecnologia da informação, bem como o *design*, implementação, teste, uso e monitoramento de serviços implantados ou contratados, além de a ampla disponibilidade de serviços de computação em nuvem, a falta de controles organizacionais sobre os funcionários que contratam esses serviços arbitrariamente pode ser uma fonte de problema. Embora a computação em nuvem simplifique a aquisição da plataforma, ela não alivia a necessidade de governança; em vez disso, tem o efeito oposto, ampliando essa necessidade.

Com relação ao *Compliance* o NIST recomenda que é necessário compreender os vários tipos de leis e regulamentos que impõem obrigações de segurança e privacidade à organização e potencialmente impactam as iniciativas de computação em nuvem, particularmente aquelas envolvendo localização de dados, privacidade e controles de segurança, gerenciamento de registros e requisitos de descoberta eletrônica. Alerta também

para a importância de revisar e avaliar as ofertas do provedor de nuvem com relação aos requisitos organizacionais a serem atendidos e assegurar-se de que os termos do contrato atendam adequadamente aos requisitos. Garantir que os recursos e processos de descoberta eletrônica do provedor de nuvem não comprometam a privacidade ou a segurança dos dados e aplicativos.

Segundo o documento *Trust* é um ponto de atenção em que devemos garantir que os acordos de serviço tenham meios suficientes para permitir a visibilidade dos controles e processos de segurança e privacidade empregados pelo provedor de nuvem e seu desempenho ao longo do tempo, estabelecendo direitos de propriedade claros e exclusivos sobre os dados. Instituir um programa de gerenciamento de risco que seja flexível o suficiente para se adaptar ao cenário de risco em constante evolução e mudança durante o ciclo de vida do sistema, e por fim monitorar continuamente o estado de segurança do sistema de informações para apoiar as decisões de gerenciamento de risco em andamento.

Em *Architecture*, o documento pontua, que é importante compreender as tecnologias subjacentes que o provedor de nuvem usa para fornecer serviços, incluindo as implicações que os controles técnicos envolvidos têm na segurança e privacidade do sistema durante todo o ciclo de vida e componentes do sistema. Nas recomendações para *Identity and Access Management - IAM*, o documento fala sobre a importância de aferir que as proteções adequadas estejam implementadas para proteger a autenticação, autorização e outras funções de gerenciamento de identidade e acesso, e que sejam adequadas para a organização.

No aspecto *Software Isolation* é importante compreender que a virtualização e outras técnicas de isolamento lógico que o provedor de nuvem emprega em sua arquitetura de *software multi-tenant*, e avalie os riscos envolvidos para a organização. Um dos aspectos mais relevantes trazidos pelo documento, *Data Protection* fala sobre avaliar a adequação das soluções de gerenciamento de dados do provedor de nuvem para os dados organizacionais em questão, e a capacidade de controlar o acesso aos dados, a importância em proteger e limpar os dados em repouso, em trânsito e em uso, considerando o risco de reunir dados organizacionais com os de outras organizações cujos perfis de ameaças são altos ou cujos dados coletivamente representam um valor concentrado significativo e também os riscos envolvidos no gerenciamento de chaves criptográficas no ambiente de nuvem e os processos estabelecidos pelo provedor.

Availability, trata da disponibilidade do serviço, trazendo a necessidade de se entender as cláusulas e procedimentos do contrato para disponibilidade, *backup* e recuperação de dados,

além de recuperação de desastres, certificar-se de que atenda aos requisitos de planejamento de contingência e continuidade da organização. Assegurando que durante uma interrupção intermediária, prolongada ou um desastre grave, as operações críticas possam ser retomadas imediatamente e posteriormente as demais operações possam ser reinstituídas de maneira planejada e organizada.

Fechando seus pontos de atenção o documento fala sobre *Incident Response*, abordando a relevância sobre as disposições do contrato e os procedimentos para resposta a incidentes da provedora do serviço, garantindo que atendem aos requisitos da organização e que exista um processo de resposta transparente e mecanismos suficientes para compartilhar informações durante e após um incidente. Ter garantias de que a organização pode responder a incidentes de forma coordenada com o provedor de nuvem de acordo com suas respectivas funções e responsabilidades de seu ambiente computacional.

Por fim traz uma reflexão sobre aspectos considerados críticos no modelo de terceirização das nuvens públicas, o que fecha o ciclo do escopo do documento que é fornecer uma visão geral da computação em nuvem, seus desafios de segurança e privacidade envolvidos, discutir ameaças, riscos de tecnologia e proteções para estes ambientes.

Diante disso, o objetivo do documento se torna completo provendo a visão necessária à uma organização para que possa realizar sua própria análise de forma a: avaliar, selecionar, envolver e supervisionar os serviços de nuvem pública que melhor atendam suas necessidades. Sendo este o elemento que dita as regras para o estabelecimento de prioridade de ações relacionadas à segurança da informação em um ambiente de nuvem pública, utilizado nesta pesquisa. Sendo assim, na próxima seção será apresentado o produto de forma desmembrada, explicando cada parte de seus componentes e sua função para o mecanismo.

4. Resultados e Discussões

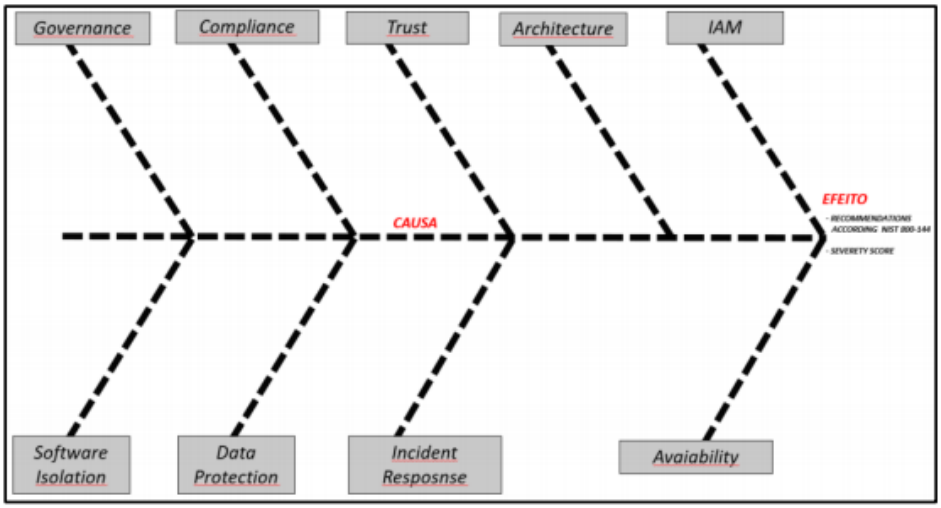
Para que seja capaz de produzir recomendações assertivas e objetivas, todos os conceitos propostos devem operar em sinergia com o objetivo almejado. Isso torna o mecanismo um organismo composto por partes que se inter-relacionam para produzir uma resposta dirigida de acordo com a necessidade de cada usuário. Estas estruturas e o fluxo delas entre si são descritos a seguir.

4.1. Aplicando o Modelo de Causa e Efeito

O primeiro passo é a segregação de todos os pontos de tenção fornecidos pelo NIST 800-144 dentro da estrutura do modelo de causa e efeito para que dessa forma possam ser

realizadas análises mais específicas dentro de cada item pontuado, bem como a vinculação de vulnerabilidades relacionadas àquela estrutura, que será assumida, neste trabalho, como as causas, estruturando as informações para que após a respectiva análise apontem as recomendações e vulnerabilidades que serão os efeitos que devem ser devidamente tratados. O uso desse tipo de estrutura irá incorporar modularidade ao modelo, pois será possível ter a visibilidade de somente um aspecto desejado, agregando personalização e foco à análise. A divisão dessas estruturas pode ser observada na Figura 1, na qual é ilustrada a "causa" e o "efeito" desejado para o modelo proposto.

Figura 1 - Representação do Diagrama de Ishikawa para os pontos de atenção do NIST



Fonte: Autores (2021)

4.1.1. Contextualizando o modelo

Um dos maiores desafios do modelo é fazer com que seja adaptado de forma a gerar resultados personalizados, eliminando ao máximo associações que não façam parte do escopo de atuação do segmento objeto da análise. Contribuindo com esta premissa optou-se, neste trabalho, pela utilização das características de uma licença de software livre, pois para que se torne aplicável a diferentes segmentos de mercado é necessário um aprofundamento dentro das regulações específicas de cada segmento, para então, cruzá-las com as recomendações do NIST 800-144 e identificar quais de fato são relevantes, uma tarefa enorme. Além disto, o fato de ser *software* livre permite que se forme uma comunidade de colaboradores com conhecimentos necessários para a realização dessa evolução do processo e assim tornar o modelo amplamente aplicável. Para esta pesquisa foi descrito a forma como esta análise deve ser feita, criando um processo para que possa ser replicado por outras pessoas. Este tipo de análise inicial deve ser humano, ou seja, realizada por uma pessoa, e esta, deve ser tecnicamente capaz de correlacionar análises complexas sobre as regulações do segmento em

questão, que serão cruzadas com as recomendações do NIST 800-144. Não é possível mecanizar, automatizar ou utilizar qualquer facilitador para uma primeira análise. O resultado de uma análise correta nesse ponto é essencial, pois fornecerá ao modelo o cruzamento das informações que irão prover os melhores resultados possíveis. Com esta correlação bem estabelecida dentro da base de dados do modelo, será possível alinhar as recomendações relevantes do NIST 800-144 para um segmento de mercado específico e com isso obter a composição de palavras-chave que farão a busca por vulnerabilidades na base das CVE's.

Para construir esta correlação, o primeiro passo é dissecar quais são as recomendações fornecidas pelo NIST 800-144 para cada um dos seus pontos de atenção. Assumimos essas recomendações como genéricas no que diz respeito a serviços de Computação em Nuvem Pública, esta primeira etapa, uma vez feita já pode ser implementada ao modelo, obviamente cabendo revisões periódicas ou cada vez que o NIST 800-144 for alterado ou substituído. Feita esta primeira análise e separação, é necessário identificar quais regulações ou recomendações de boas práticas são aplicáveis ao segmento em que se deseja realizar a contextualização e organizá-las dentro dos mesmos pontos de atenção existentes no NIST 800-144.

Com essas informações em mãos, inicia-se o processo de análise e entendimento de cada aspecto apontado pelos documentos e assim realiza-se o cruzamento de recomendações para estabelecer que tipo de recomendação se torna mais relevante para o segmento, bem como quais são as palavras-chave mais importantes para identificar vulnerabilidades nos pontos de atenção requeridos.

Para exemplificar este processo será utilizada as recomendações relacionadas à *Identity and Access Management* – IAM, fornecidas pelo NIST 800-144, serão cruzadas com as recomendações para IAM descritas no NIST 800-66 *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act* (HIPAA) *Security Rule*. Este segundo documento traz diretrizes para a implementação de controles e práticas de segurança que estão descritos na HIPPA, apesar de não ter peso de lei como regulação oficial no Brasil, é amplamente utilizada em empresas nacionais do segmento da saúde, por se tratar de um *baseline* completo e que atende aos diversos pontos críticos do setor, por esta razão, é a referência de mercado para boas práticas no segmento de *HealthCare.*

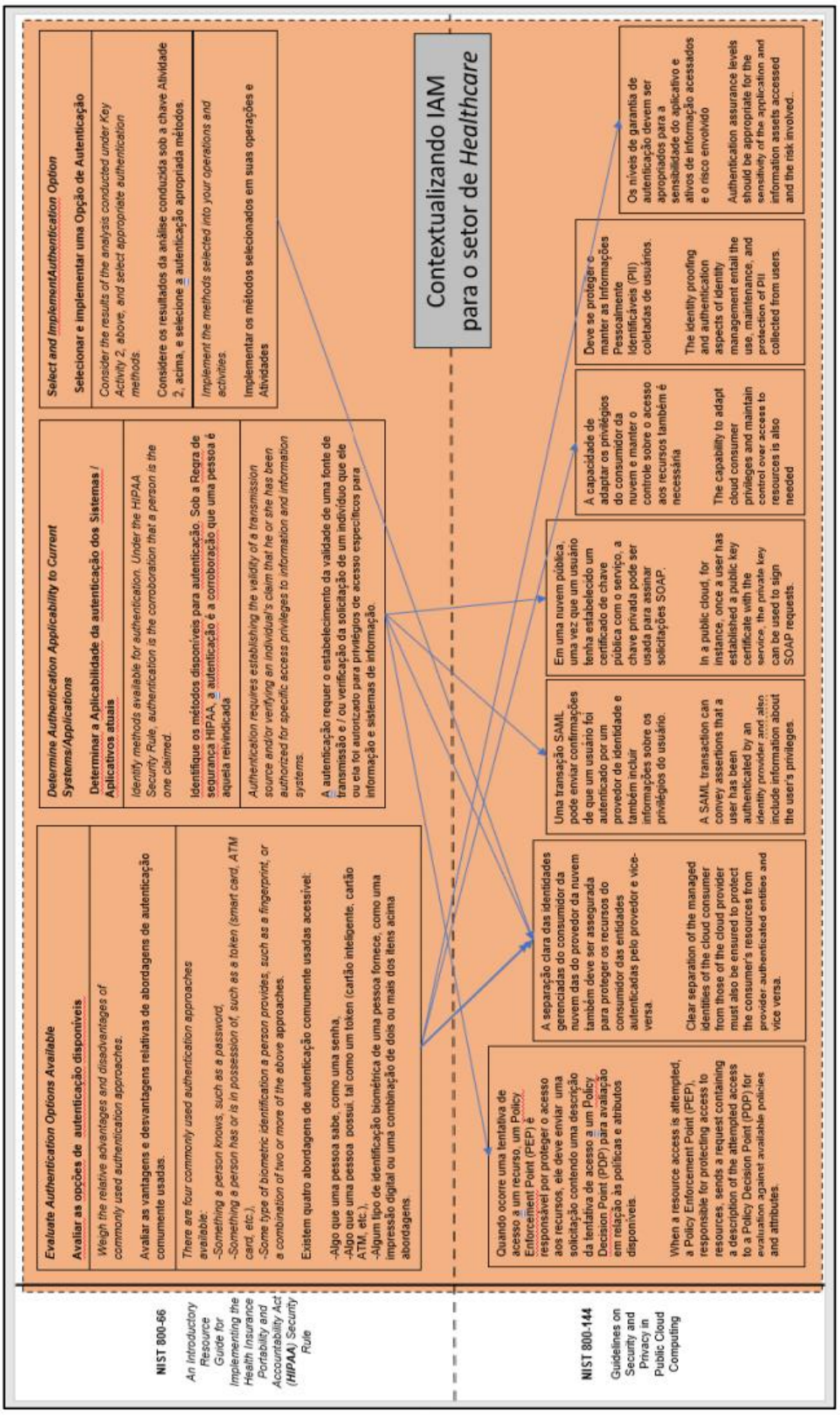
Um dos aspectos declarados pelo NIST 800-66: "A autenticação requer o estabelecimento da validade de uma fonte de transmissão e/ou verificação da solicitação de um indivíduo que ele ou ela foi autorizado para privilégios de acesso específicos para informação e sistemas de informação" (JANSEN et. al 2020, tradução própria). Por sua vez,

uma das recomendações do NIST 800-144 traz o seguinte texto, em português: uma transação SAML pode enviar confirmações de que um usuário foi autenticado por um provedor de identidade e incluir informações sobre os privilégios do usuário. (JANSEN et. al 2020, tradução Própria)

A princípio não é tão clara a relação entre as recomendações, mais ao analisar com atenção é possível perceber que ambas referenciam recomendações correlatas. O NIST 800-66 diz que a autenticação precisa de uma fonte de validação que garanta que aquela pessoa está autorizada a ter um determinado tipo de acesso. No NIST 800-144 está descrito que o *Security Assertion Markup Language* - SAML, que é um padrão aberto para a troca de dados de autenticação e autorização entre partes, pode fazer a confirmação desse tipo de autenticação. Nesse contexto é possível afirmar que esta recomendação do NIST 800-144 é totalmente relevante ao segmento, e que as palavras SAML, IAM, *Identity* e *Access* podem ser inclusas como palavras-chave na busca por vulnerabilidades, este último processo será mais bem descrito a seguir.

A Figura 2 representa uma análise de todos os aspectos de IAM baseado nos dois documentos citados, as setas indicam quais recomendações fazem correlações entre si. É possível identificar pela imagem que algumas recomendações estão mais associadas entre si do que outras, sendo assim, será possível extrair dessa incidência o resultado de quais recomendações do NIST 800-144 são mais relevantes para IAM no setor de *HealthCare*.

Figura 2 - Contextualizando IAM entre NIST 800-144 e NIST 800-66



Fonte: Autores (2021)

4.2. A associação de vulnerabilidades

Um aspecto de grande relevância do modelo é a capacidade de pontuar as vulnerabilidades que estão relacionadas ao que o NIST 800-144 preconiza em suas recomendações, contudo, para que isso ocorra há a necessidade de se realizar uma abstração, somente desta forma será possível obter um resultado efetivo.

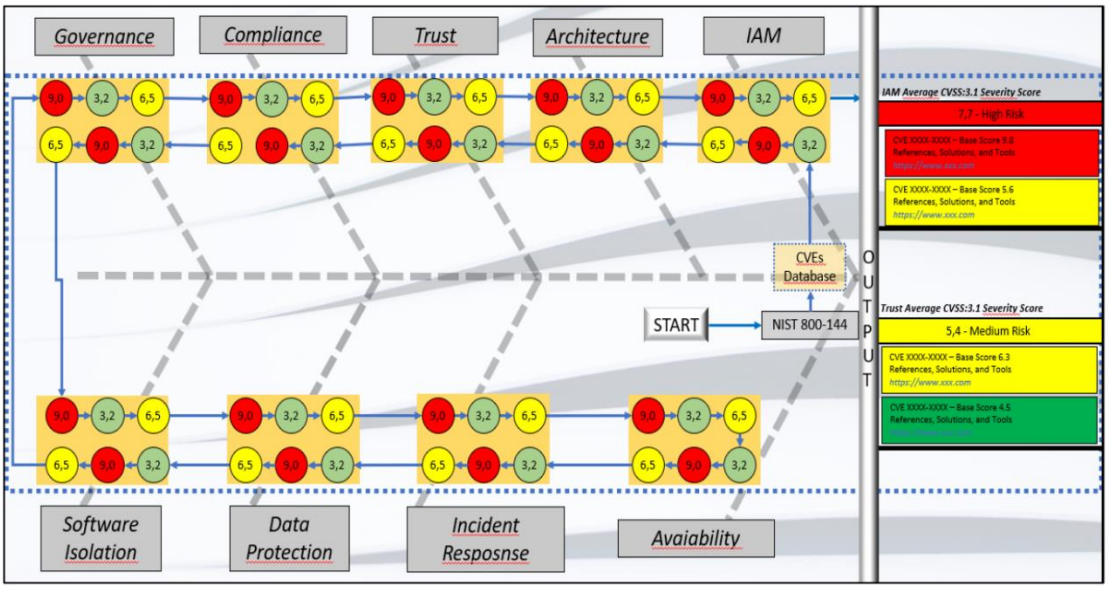
Vale ressaltar, que nesta pesquisa, partimos do princípio de que está sendo utilizada uma nuvem pública como objeto de avaliação. Atualmente, a vasta oferta de diferentes fornecedores deste tipo de serviço, faz emergir um crescente número de vulnerabilidades. Dessa forma, o modelo proposto para busca de vulnerabilidades deverá fazer uso de palavras-chave, este conjunto de palavras será gerado combinando a inserção de dados fornecidos por quem deseja fazer a análise com palavras de relevância para o alvo da análise, um exemplo desse resultado foi descrito no item.

4.2.1. Contextualizando o modelo

Essa combinação de palavras pode ser descrita, da seguinte forma: Um usuário tem interesse em realizar uma análise para o ponto de atenção Y no serviço de nuvem pública X, no caso o *input* fornecido será o fornecedor X e o ponto de atenção Y, a partir desse momento o modelo realiza uma abstração por meio da correlação existente em sua base de dados e as informações fornecidas pelo usuário, em seguida, combina palavras chave que permitam realizar uma busca o mais assertiva possível dentro da base de dados das CVE's conhecidas. Um outro exemplo, pode ser o *input* do usuário: "Fornecedor X, *Data Protection, Healthcare*", a combinação das palavras-chave deve resultar da abstração realizada de acordo com o provedor de nuvem pública X e os critérios correlacionados entre os NIST 800-144 e o *baseline* do segmento de *healthcare* existente na base de dados do modelo de priorização.

Cabe ressaltar, que os círculos coloridos, conforme Figura 3, representam as vulnerabilidades por meio da nota da severidade individual e significam: vermelho - alto risco, amarelo - risco médio e verde - baixo risco. Eles estão distribuídos entre os diferentes pontos de atenção na estrutura do modelo.

Figura 3 - Representação das Vulnerabilidades Identificadas



Fonte: Autores (2021)

4.3. Aplicando a Teoria dos Grafos

Com base no princípio de priorização de ação de segurança da informação de acordo com a criticidade de vulnerabilidades associadas, é feita a implementação da Teoria dos Grafos sobre a estrutura do modelo. A Teoria dos grafos é uma ferramenta poderosa para esta função, pois se trata de um mecanismo capaz de identificar o caminho crítico, esta foi a principal motivação para sua escolha, além do fato de sua implementação na forma algorítmica já existir.

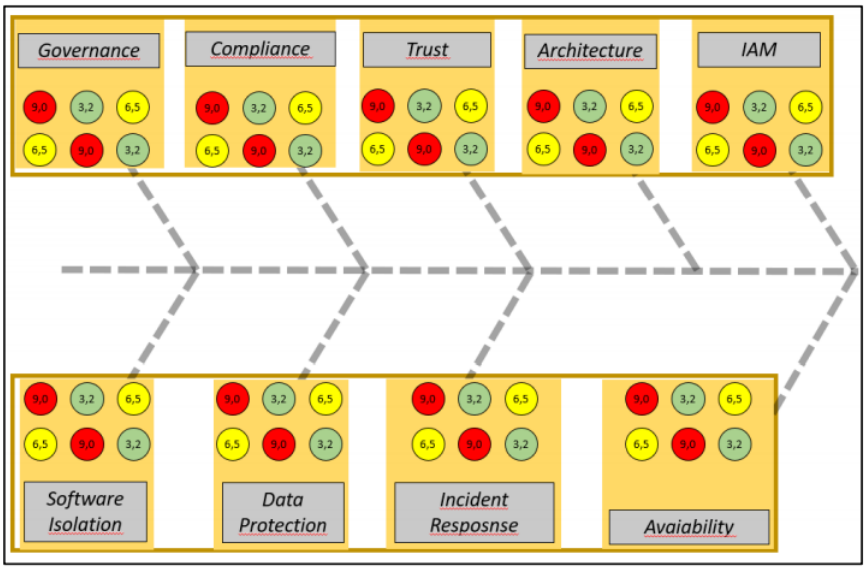
Nesta pesquisa assumimos como crítico, um critério para o modelo proposto, a nota de severidade, sendo que quanto maior a nota maior a criticidade, desta forma é possível identificar a priorização de ação na mitigação das vulnerabilidades.

Para um melhor entendimento da utilização da teoria no modelo proposto, será realizada uma analogia com o percurso de uma trilha. A trilha seria o caminho completo, o que liga de ponta a ponta, o início e fim da jornada, durante o percurso existem algumas cidades por onde passa a trilha, e dentro de cada uma dessas cidades existem bandeiras com valores distintos. O objetivo é percorrer a trilha completa por todas as cidades e coletar todas essas bandeiras, somente uma vez e ao final, separar as bandeiras de acordo com a cidade que foram coletadas e apontar qual das cidades possuí o maior valor médio na soma das bandeiras, e ainda, quais foram as bandeiras coletadas de cada cidade respectivamente.

Colocando nos termos empregados para o modelo de priorização, a trilha é conjunto dos pontos de atenção levantados pelo NIST 800-144, cada um desses pontos de atenção são

as cidades por onde a trilha passa e as bandeiras são as notas de severidade das vulnerabilidades. Como resultado o modelo fornece qual dos pontos de atenção possuí maior criticidade e por tanto deve ter sua tratativa priorizada. A Figura 4 representa a teoria dos grafos sendo aplicada ao modelo por meio de setas azuis simbolizando o percurso, e ao lado um exemplo do resultado de priorização fornecido por este cálculo.

Figura 4 - Representação da Teoria dos Grafos aplicada ao modelo proposto



Fonte: Autores (2021)

4.4. O Fluxo do mecanismo no modelo de priorização

Com o funcionamento de todos os mecanismos da estrutura descritos, será possível realizar a análise do modelo. Para isso, o fluxo será divido em oito etapas sequenciais que correspondem ao ciclo completo de uma análise. Sendo que, dessas etapas apenas na primeira e na última haverá interação do usuário. Na primeira, como provedor de informações para a análise, e na última como consumidor dos resultados obtidos. Todas as demais etapas são o *backend* do modelo, e serão explicadas a seguir para uma compreensão de todo o fluxo de análise.

A primeira etapa consiste na inserção de informações para realização da análise, é nessa etapa que o usuário deve informar qual serviço de nuvem pública está utilizando e qual segmento de mercado é o foco da pesquisa, e escolher quais os pontos de atenção quer avaliar. Com estas informações devidamente fornecidas é possível seguir para segunda etapa, na qual o modelo separa os dados dentro do diagrama de Ishikawa de acordo com os pontos de atenção do NIST 800-144 e todas as suas recomendações.

Na terceira etapa é feita a correlação entre todas as informações relevantes ao

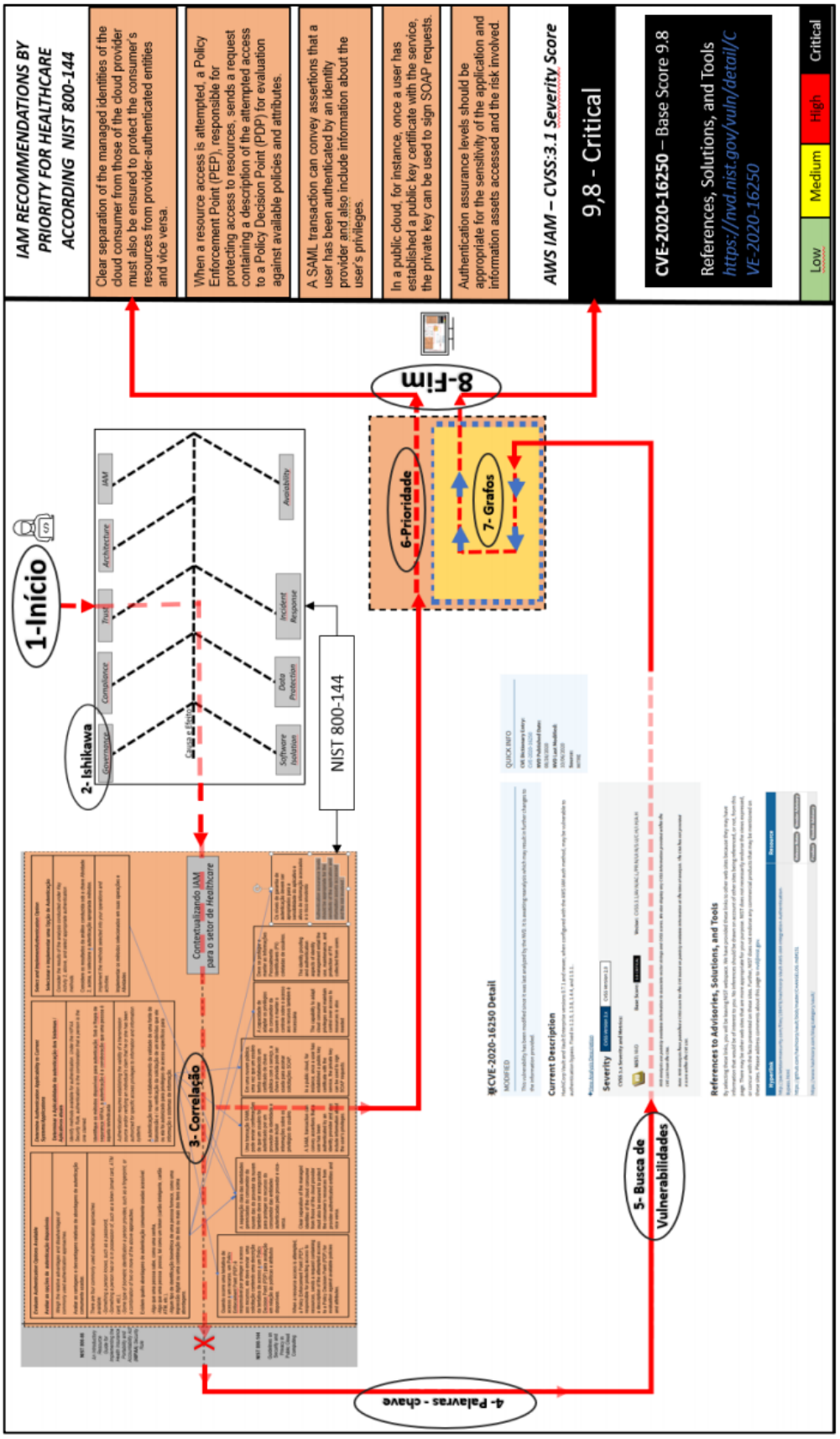
segmento de mercado alvo da análise e os pontos de atenção do NIST 800-144. Esta etapa é o coração do modelo, pois é nela que está concentrada a base de dado mais importante, que fornecerá uma análise focada, segmentada e assertiva. A quarta etapa, corresponde a inserção das palavras-chave nos mecanismos de busca vulnerabilidades, o caminho para esta conexão entre o modelo e a base de dados de CVE's e o consequentemente o score da CVSS será realizada por meio de APIs, que são conectores para acesso a um aplicativo de software ou plataforma baseado na Web.

Na quinta etapa é realizada a busca de vulnerabilidades dentro da base de dados de CVE´s, este mecanismo de busca já existe dentro de uma plataforma web e é dela que o modelo fará uso. As etapas sexta e sétima correspondem a organização da informação que será exibida ao usuário. As recomendações, serão apresentadas por ordem de relevância, para o segmento analisado e as vulnerabilidades encontradas por ordem de severidade sendo a mais severa o topo da lista.

Para estabelecer quais recomendações do NIST 800-144 são mais relevantes ao segmento, o modelo proposto, usará a correlação realizada na terceira etapa, e por meio do resultado da quantidade de incidência de recomendações que cruzarem com o NIST 800-144 será estabelecida uma ordem de prioridade, sendo que, quanto mais uma recomendação incidir sobre um ponto de atenção, maior será a relevância desse aspecto avaliado.

Vale ressaltar que a sétima etapa é a ação da teoria dos grafos. Este mecanismo irá analisar a severidade de todas as vulnerabilidades encontradas, estabelecer dentre os pontos de atenção quais possuem maior valor médio de severidade e ordenar para cada ponto de atenção avaliado as vulnerabilidades correspondentes em ordem decrescente de acordo com nota de severidade atribuída às vulnerabilidades identificadas. Por fim, a oitava etapa é o *frontend* que irá fornecer ao usuário os resultados da sua análise, serão exibidas recomendações do NIST 800-144 por ordem de relevância para o segmento alvo da análise e apresentará as vulnerabilidades identificadas por ordem e severidade separadas por ponto de atenção avaliado. A Figura 5 ilustra esse fluxo de funcionamento e demonstra um exemplo de resultado possível para uma análise. Para o exemplo em questão foi utilizado o ponto de atenção IAM para um serviço de Computação em Nuvem Pública.

Figura 5 - Fluxo de análise e funcionamento do mecanismo completo



Fonte: Autores (2021)

5. Considerações Finais

Partindo do objetivo definido, neste artigo, a saber: Utilizar o modelo de causa e efeito e a teoria dos grafos, para fornecer um mecanismo de priorização de ações relacionadas à segurança da informação em um ambiente computação em nuvem, tendo como base as boas práticas fornecidas pelo NIST 800-144, é possível afirmar que diante do que foi apresentado ele foi alcançado. Durante a pesquisa foram exploradas diferentes formas para que a combinação desses elementos fosse realizada de forma coesa e que atingisse o resultado esperado, e as escolhas, as referências teóricas adotadas neste percurso, bem coma explicação e demonstração com um exemplo de sua utilização, contribuíram para seu alcance.

A compreensão em associar as teorias propostas no projeto se expandiu por meio de cada conceito incorporado ao modelo, sendo necessário desenvolver métodos de interação entre diferentes linhas do conhecimento de forma a permitir que trabalhassem em conjunto de maneira lógica e relevante, exigindo um nível de abstração considerável para realizar esta conexão. Foi um grande desafio estruturar as recomendações do NIST 800-144 de forma que fosse possível estabelecer tópicos que permitissem uma avaliação sobre um aspecto determinado, além disso, trazer a teoria dos grafos para possibilitar diferentes formas de análise, e encontrar qual se adequava melhor ao modelo proposto também foi uma tarefa árdua.

A metodologia escolhida foi fundamental para o resultado, por se tratar de diversas áreas do conhecimento sem uma exploração de bibliografias que correspondessem às nossas expectativas seria impossível ter o entendimento necessário para a criação do mecanismo, e como resultado deste, os *outputs* do mecanismo tiveram uma abordagem que permitiu estabelecer de forma simples uma orientação da ordem de ação das tratativas.

Acreditamos ser de grande relevância para a área acadêmica de segurança da informação uma pesquisa como esta desenvolvida, pois é uma área de estudo que está em constante mutação e boa parte do aprendizado se concentra em atividades operacionais e entendimento técnico, por esta razão consideramos de grande relevância se aprofundar no desenvolvimento de conceitos que possibilitem a criação de ferramentas, métodos ou técnicas para evolução constante desses processos. Ainda, trazer este tipo de desenvolvimento para o universo acadêmico, possibilita, como em nossa proposição, materializar o direito coletivo de segurança da informação, no sentido de que um projeto como este poderá gerar uma ferramenta com licenciamento não pago, e além disto, permitir que um grupo de pesquisadores, que tenham interesse em comum, possam fazer esta ferramenta evoluir e se manter atualizada.

Por fim, como esta pesquisa teve o foco conceitual na construção de um modelo, objetivo que foi alcançado no desenvolvimento do trabalho, ficaram questões que poderão ser discutidas e/ou trabalhadas em um momento futuro, buscando obter as respostas a respeito do efetivo funcionamento do mecanismo e sua aceitação como uma ferramenta eficaz para a priorização de ação em ambientes de Computação em Nuvem Pública, assim, fica nossa sugestão para futuras pesquisas sobre o tema.

Referências

FONTES, Edison. **Segurança da Informação**: O Usuário faz a diferença. São Paulo, SP: Saraiva, 2006.

GARTNER. **Gartner Forecasts Worldwide Public Cloud Revenue to Grow**.2020. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-publiccloud-revenue-to-grow-17-percent-in-2020. Acessado em 10/05/2021.

GONZALEZ, Nelson Mimura; MIERS, Charles Christian; REDÍGOLO, Fernando Frota; ROJAS, Marco Antônio Torrez; CARVALHO, Tereza Cristina Melo de Brito. Segurança das nuvens computacionais: uma visão dos principais problemas e soluções. **Revista USP**, 2013.

JANSEN, Wayne; GRANCE, Timothy; JANSEN, Wayne; GRANCE, Timothy. **NIST Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing**. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-144/final. Acesso em: 24/10/2020

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio de. **Segurança de Redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

NOGUEIRA, Daniel Klug. **Introdução à Teoria dos Grafos**: Proposta para o Ensino Médio, 2015.

PEINADO, Jurandir; GRAEML, Alexandre Reis. **Administração da Produção Administração da Produção**. Administração da Produção (Operações Industriais e de Serviços), 2007.

SÊMOLA, M. **Gestão da Segurança da Informação** - Uma Visão Executiva - 2 ed. São Paulo, SP: Elsevier, 2014.