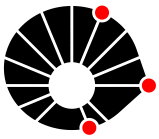

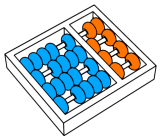

Categorização dos Desafios de Segurança em Nuvem relacionados à tecnologia de Virtualização

M. G. Andrietta *P. L. Geus*

Relatório Técnico - IC-PFG-21-52
Projeto Final de Graduação
2021 - Dezembro

UNIVERSIDADE ESTADUAL DE CAMPINAS
INSTITUTO DE COMPUTAÇÃO

Categorização dos Desafios de Segurança em Nuvem relacionados à tecnologia de Virtualização

Murilo Guidetti Andrietta[1], Paulo Lício de Geus[1]

[1] Instituto de Computação Universidade Estadual de Campinas (UNICAMP), Caixa Postal 6176
13083-970 Campinas-SP, Brasil

m147472@dac.unicamp.br e pgeus@unicamp.br

Resumo. Ao longo dos últimos anos, organizações de variados ramos industriais têm aderido ao uso da Nuvem Computacional, pois os benéficos dessa arquitetura são cada vez mais evidentes. A tecnologia de Virtualização funciona como base para o sucesso desse ambiente em termos de flexibilidade e escalabilidade. Contudo, mesmo com a crescente que se tem verificado, a segurança ainda figura como um fator limitante para muitos atores em suas jornadas de migração para a Nuvem. Muitos autores de artigos científicos, *white papers* e relatórios técnicos, têm empregado esforços para contribuir com o aumento de segurança em um escopo de ameaças relacionadas à Virtualização dentro do ecossistema computacional mencionado, mas fica nítida a falta de padronização durantes as apresentações dos desafios considerados em cada um desses trabalhos. O presente Relatório objetiva propor uma nova forma de categorizar os desafios de segurança em Nuvem, especificamente relacionados à Virtualização, de maneira simples e sistemática.

Palavras-Chave: Computação em Nuvem; Virtualização, Segurança Computacional, Categorização.

1. Introdução

1.1 Contextualização Geral – Computação em Nuvem

Ao longo dos últimos anos, vem se tornando cada vez mais evidente que "a tecnologia de Computação em Nuvem tem deixado para trás todas as outras estruturas/mecanismos de sistemas distribuídos em termos de competitividade, popularidade e sucesso" [1]. De fato, "organizações em uma variedade de indústrias estão lutando para justificar possuir o seu próprio *hardware* enquanto a Computação em Nuvem continua a crescer como uma solução popular para atender às suas necessidades computacionais" [2]. Somente como um exemplo ilustrativo, "Em um estudo recente de corporações do setor de tecnologia pela *International Data Group*, 77% das empresas têm agora alguma parcela de sua infraestrutura implantada junto a um provedor de Nuvem" [2].

A empresa *McAfee*, reconhecida por comercializar soluções de segurança computacional, divulga relatórios periódicos que buscam trazer luz acerca da adoção e dos riscos de se migrar para Nuvem. Em um desses relatórios, pode-se encontrar a Figura 1, abaixo, que traz os benefícios experimentados por companhias que utilizam serviços gerais na Nuvem [3].

Figura 1 – Benefícios experimentados por companhias que utilizam serviços gerais na Nuvem.

Algumas das principais plataformas que oferecem serviços de Nuvem são Microsoft Azure [4], Amazon AWS [5], Google Cloud [6] e IBM Cloud [7].

Em termos de conceituação básica, Ali, Khan e Vasilakos [8] utilizaram o *National Institute of Standards and Technology* (NIST) para trazer a Figura 2, a seguir, e resumir as principais características, modelos de desenvolvimento e oferecimento de serviços em Nuvem.

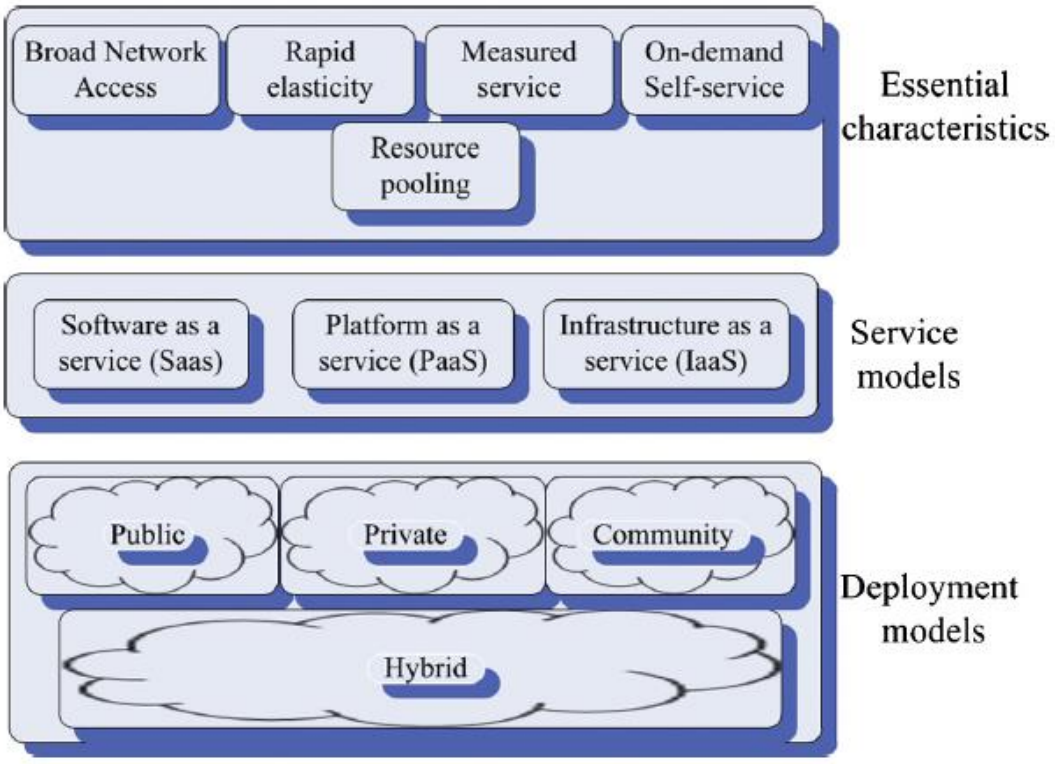

Figura 2 – Definição de Computação em Nuvem de acordo com NIST.

De acordo com a Figura 2, e baseando-se nas explicações presentes no *The NIST Definition of Cloud Computing* [9], a Nuvem Computacional deve possuir como características essenciais um amplo acesso à rede (uma vez que todos os serviços são utilizados via *internet*), uma capacidade intrínseca de elasticidade (significando que os recursos provisionados devem se ajustar às necessidades dos clientes – potencialmente de maneira automática), a possibilidade de metrificar o uso de recursos (de tal forma que os usuários possam monitorar facilmente a utilização de seus ativos), uma oferta sob demanda (o que implica em clientes solicitando componentes computacionais e serviços quando desejarem) e, por fim, uma arquitetura de oferecimento de recursos *multi-tenant* e

compartilhada (talvez o ponto de maior relevância sob a perspectiva de viabilizar a Nuvem Computacional da forma como todos a conhecem).

Os Modelos de Serviços disponíveis no momento da aquisição partem de uma arquitetura contendo apenas recursos de infraestrutura (como processamento, memória, rede e outros componentes fundamentais) conhecida como IaaS, passa por uma opção trazendo um ambiente voltado ao desenvolvimento de *software* (possuindo portanto, além dos componentes básicos, também bibliotecas, linguagens de programação, etc.) chamada de PaaS e chega finalmente a um nível mais alto com opções pré-prontas de aplicações que podem ser utilizadas para diversas finalidades, o modelo SaaS.

Por fim, mas não menos importante, os Modelos de Implantação de Computação em Nuvem estão relacionados ao nível de privacidade, aquisições físicas e custo desejados. No modelo Público, muito em virtude da característica *multi-tenant*, já mencionada, os usuários dependem do provedor de Nuvem contratado para questões de segurança, uma vez que tudo a ser utilizado é disponibilizado por esse provedor. Já o modelo Privado implica basicamente na construção de uma Nuvem particular, o que aumenta custos consideravelmente, mas também traz maior controle sobre dados e operações executadas. A opção Comunitária é uma forma de se criar uma Nuvem Computacional na qual os *tenants* são conhecidos e acordam / dividem entre si as responsabilidades e o uso dos recursos. Por fim, a Nuvem Híbrida é o modelo que mescla dois ou mais dos modelos mencionados acima.

1.2 Contextualização Específica – Virtualização

A subseção anterior demonstrou que a Computação em Nuvem é uma tecnologia em franca ascensão. Existe, contudo, uma outra tecnologia, um pouco mais elementar, mas sem dúvida alguma fundamental, que possibilita a existência de toda a arquitetura de Nuvem e merece, por isso, uma atenção especial: a Virtualização. De fato, Odun-Ayo, Ajayi e Okereke [10] escreveram em seu artigo que a maioria das atividades na Nuvem Computacional são centradas em Virtualização, enquanto Kumar e Rathore [11] disseram que essa tecnologia está na base de toda infraestrutura de Nuvem, endossando a importância citada.

Em termos de conceituação básica, a "Virtualização pode ser vista como a utilização de recursos computacionais para imitar outros recursos computacionais ou um computador inteiro." [10] Além disso, trata-se de uma tecnologia com inúmeras vantagens tanto para usuários como para fornecedores de serviços. Por exemplo, Singh [12] traz alguns dos principais benefícios como sendo:

- Possibilidade de execução de múltiplos sistemas operacionais em um mesmo *hardware* físico;
- Melhoria no gerenciamento de energia;
- Melhoraria na utilização de recursos;
- Possibilidade de balanceamento de carga;
- Manutenção;
- Aumento na disponibilidade dos sistemas;
- Isolamento.

Somente pela lista de vantagens apresentada acima, pode-se imaginar o interesse dos provedores de Nuvem em adotar a Virtualização em suas operações básicas. Por exemplo, do ponto de vista de segurança, a combinação do isolamento mencionado com o fato de que a tecnologia referida "cria uma camada de abstração entre a máquina hospedeira e sistema hospedado" [11], deixa evidente a possibilidade do oferecimento de soluções minimamente coesas, isoladas e encapsuladas em um ambiente *multi-tenant*. Outro ponto interessante foi destacado pelos autores Zhu, Yin, Cai e Li [13] que disseram que a Virtualização "permite a alocação dinâmica e a modificação de múltiplas *Virtual Machines* com uma única máquina física hospedeira como base, ou então a migração de uma única *Virtual Machine* entre diferentes hospedeiros", o que está muito alinhado ao primeiro item da lista apresentada acima e traz como consequência direta tanto a melhoria na utilização de recursos, quanto o aumento na disponibilidade dos sistemas. Essas características, inegavelmente, são de extrema relevância para o oferecimento de soluções escaláveis, elásticas e sob demanda, o que está totalmente de acordo com os conceitos definidos previamente pelo *National Institute of Standard Technology*.

Para enriquecer um pouco mais o *background* dos conceitos de Virtualização, vale a pena mencionar a forma como a literatura classifica os seus tipos. A Figura 3, a seguir, é proveniente de trabalho de Tamane [19] e mostra a divisão mencionada.

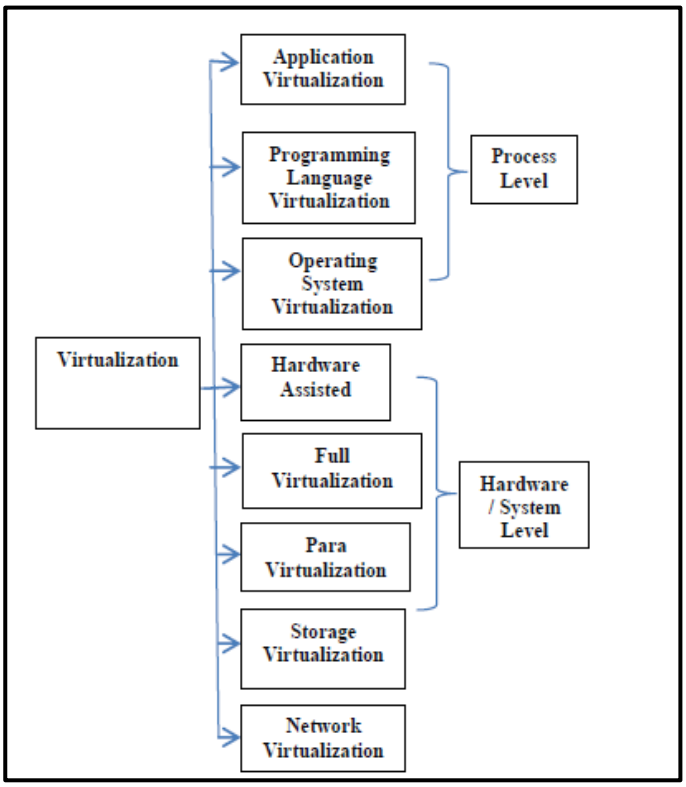

Figura 3 – Tipos de Virtualização de acordo com o trabalho de Tamane [19].

Como se percebe, a Virtualização pode estar presente em praticamente todos os recursos computacionais. A divisão da Figura 3 é, inclusive, bastante abrangente e leva o conceito discutido para além dos limites da Nuvem Computacional. Apenas para que fique um pouco mais didático, é importante mencionar que a seção mapeada como *Hardware / System Level* é tradicionalmente a mais aplicada do ponto de vista dos Provedores de Serviços de Nuvem. Nesse escopo, *Full Virtualization* compreende uma completa simulação de todo o h*ardware* incluindo instruções privilegiadas, interrupções, acesso de memória e assim por diante. Todos esses elementos seriam executados diretamente pelas *Virtual Machines*. Na *Para-Virtualization*, por sua vez, uma interface de *software* é disponibilizada para as *Virtual Machines*, sendo essa muito similar, mas não idêntica ao *hardware*. Por fim, quando se fala de *Hardware-Assisted Virtualization*, faz-se referência a um suporte arquitetural de

hardware para criar um *Hypervisor* que executa um sistema operacional convidado de maneira isolada. [14]

1.3 Problemática

Até o presente momento, o objetivo desse Relatório Técnico foi demonstrar a importância da tecnologia de Virtualização para Computação em Nuvem, bem como a relevância e crescimento dessa última em termos mercadológicos. O foco esteve sempre nas vantagens de cada um desses elementos. Contundo, é evidente que também existem pontos de atenção e preocupação que inibem organizações e usuários de migrarem seus ativos para esse ambiente. Por mais que a Figura 1, apresentada na subseção de Contextualização Geral, traga como vantagem de adesão da Nuvem uma melhoria na segurança (o que de fato é verdade quando se considera o estado anterior de servidores e infraestrutura computacional para grande parte dos usuários), muitos autores, como Kumar e Rathore [11], afirmam que "apesar de ser muito conveniente e eficiente, a Computação em Nuvem não está sendo adotada por todas as potenciais indústrias devido a preocupações com segurança." Além disso, em seu levantamento bibliográfico, Ousmane, Ibrahima e Doudou [15] disseram que "Shahzad et al. expuseram vulnerabilidades associadas à Nuvem Computacional" e "Kanika et al. exploraram vários tipos de vulnerabilidades e ataques associados com a virtualização", o que corrobora o argumento apresentado.

Ao analisar materiais pertinentes sobre o tema (como artigos científicos, relatórios técnicos, *white papers etc.*), fica claro que existe uma quantidade gigantesca de vulnerabilidades e ataques possíveis de se efetuar em ambiente de Nuvem. Isso acontece por inúmeros motivos, mas talvez o principal seja o rico e vasto ecossistema computacional necessário para viabilizar o oferecimento de serviços na Nuvem. De fato, são muitos os pontos de ataque disponíveis nessa situação, pois há uma grande quantidade de códigos sendo executados, infraestruturas sendo utilizadas e todo um conceito de compartilhamento isolado e encapsulado que são desafiados constantemente (seja entre *Hypervisor* e *Virtual Machines*, lateralmente entre as próprias Virtual Machines, ou por diversos outros atores que participam da arquitetura presente). Apenas para ficar no escopo de *software*, vale ressaltar que a existência uma única linha de código insegura é o suficiente para que agentes maliciosos

sejam capazes de comprometer o sistema inteiro. E infelizmente, não vale o argumento de que os códigos comerciais de *Hypervisors* e de provedores de Nuvem são insistentemente verificados e corrigidos, pois até mesmo a própria aplicação que o usuário utiliza é um vetor possível de ser explorado em ataques.

Ao se concluir que a quantidade de vulnerabilidades presentes em ambiente de Nuvem é estatisticamente muito alta, fica mais fácil entender o porquê de muitos pesquisadores que se debruçam sobre desafios de segurança (aqui especificamente relacionados à tecnologia de Virtualização) não classificarem as ameaças estudadas de maneira padronizada e sistemática. Acaba sendo muito comum que as categorizações apresentadas nos artigos científicos levem em conta os ataques de interesse para aquele trabalho específico, o que poupa tempo dos autores e traz o foco para as soluções que estão sendo propostas, por exemplo. Isso não significa que não existam materiais empregando esforços em classificar os problemas desse escopo, mas é um fato que não existe um consenso / padronização na hora de apresentar as ameaças categorizadas.

As Figuras 4 [15], 5 [16], 6 [16] e 7 [AA], a serem apresentadas a seguir, trazem exemplos completamente distintos quanto a classificação dos desafios de segurança em Nuvem, relacionados à tecnologia de Virtualização.

Vulnerabilities	Techniques	Type of attacks
Shared cache	Prime+Probe	Access-driven
Page sharing	Prime+Probe	Access-driven
Huge page	Prime+Probe	Access-driven
Page sharing, inclusive cache	Flush+Reload	Access-driven
Page sharing, inclusive cache	Flush+Reload	Access-driven
Page sharing	Flush+Reload	Access-driven
Xen scheduler	timing attack	Scheduler
Linux 2.6 scheduler	timing attack	Scheduler
4.4BSD	timing attack	Scheduler
History	Brute force attack	Migration and rollback
Hypervisor	-	VM escape
Hypervisor on OpenStack	-	VM escape
Compute node	-	VM escape

Figura 4 – Apresentação das vulnerabilidades relacionadas à virtualização e computação em Nuvem por Ousmane, Ibrahima e Doudou [15].

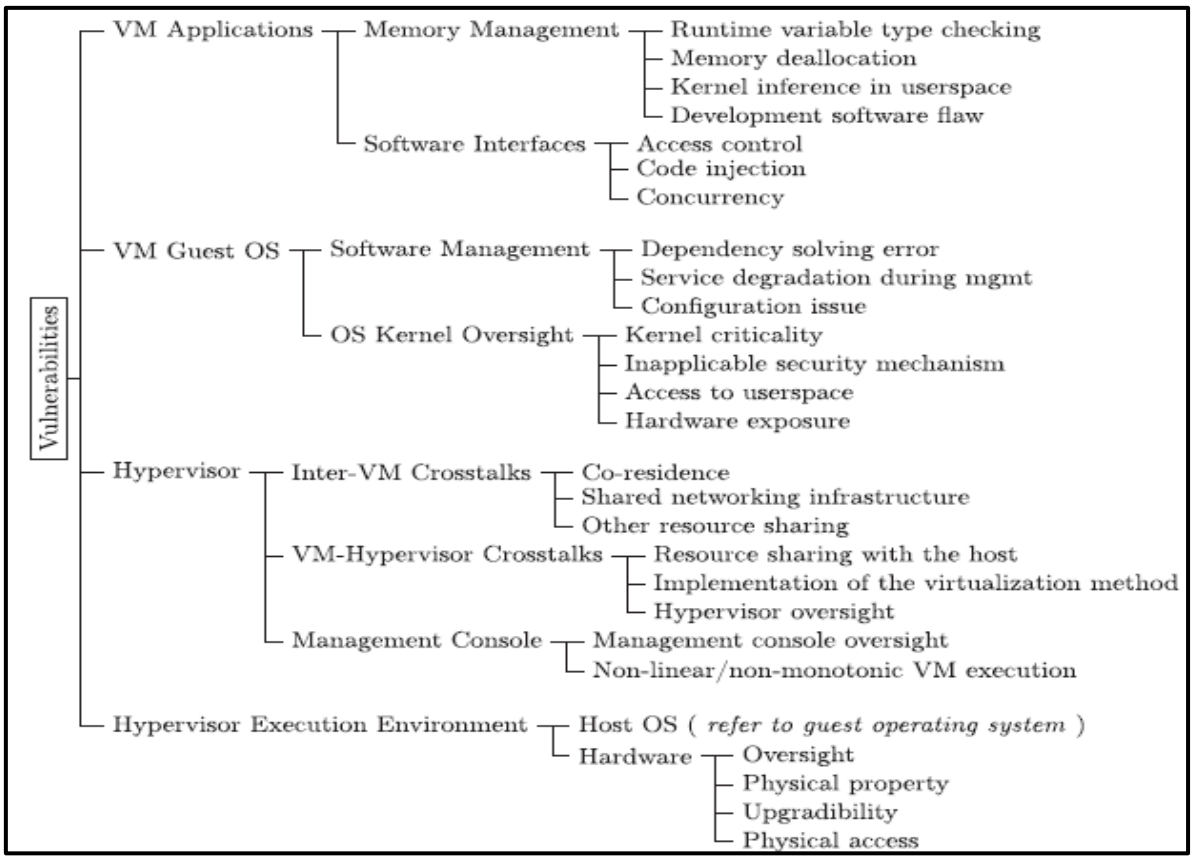

Figura 5 – Apresentação das vulnerabilidades relacionadas à virtualização e computação em Nuvem por Compastié, Badonnel, Festor, e He [16].

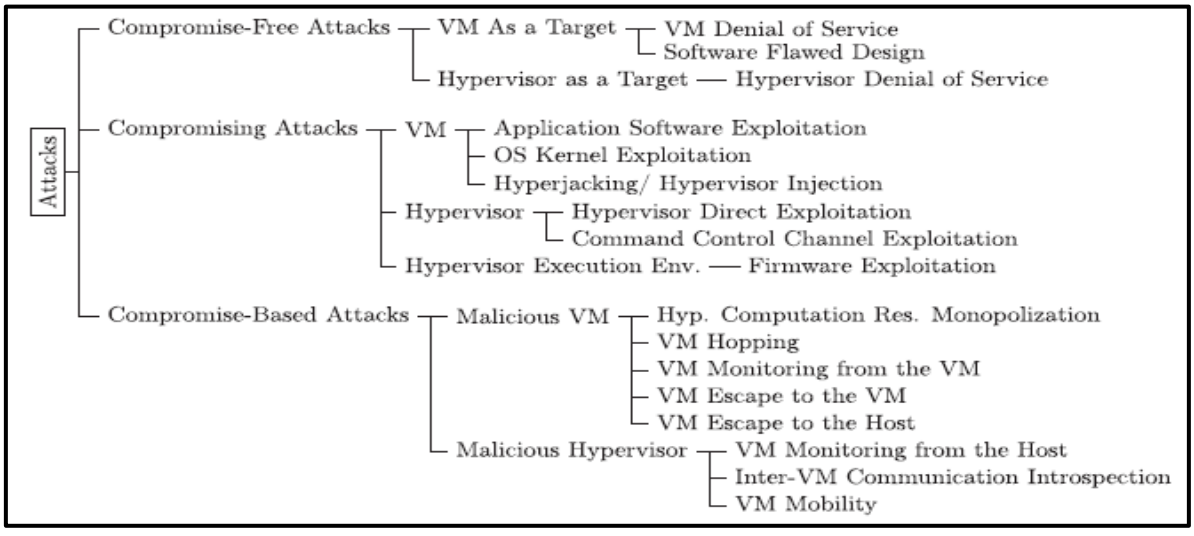

Figura 6 – Apresentação dos ataques relacionados à virtualização e computação em Nuvem por Compastié, Badonnel, Festor, e He [16].

	KVM	Xen
Virtual Hardware Logic Errors	5	20
Device State Management Errors	1	11
Resource Availability Errors	4	15

Figura 7 – Apresentação das vulnerabilidades relacionadas à virtualização e computação em Nuvem por Zhu, Yin, Cai e Li [13].

Como se pode perceber, a apresentação dos problemas de segurança em Nuvem, relacionados à tecnologia de Virtualização, embora com alguma intersecção entre si, não são nem de perto padronizadas. A proposta da Figura 4, proveniente do artigo dos autores Ousmane, Ibrahima e Doudou [15], tenta sumarizar uma lista de ataques / vulnerabilidades previamente divididas em ataques entre as Virtual Machines propriamente e de Virtual Machines para *Hypervisor*. As Figuras 5 e 6 podem ser encontradas no artigo dos autores Compastié, Badonnel, Festor, e He [16]. A primeira delas busca criar uma classificação sistemática de vulnerabilidades possíveis para os problemas do escopo mencionado, enquanto a segunda sumariza os ataques dessa origem, tentando se basear nas vulnerabilidades previamente classificadas. A Figura 6 traz como categorias: ataques não dependentes de sistemas comprometidos, ataques com potencial de comprometer sistemas e ataques baseados em sistemas comprometidos. Por fim, a Figura 7, dos autores Zhu, Yin, Cai e Li [13], traz uma divisão de problemas relacionados à Virtualização em Nuvem de acordo com o comportamento dos *softwares* virtualizadores que tentam imitar o *hardware* original. Percebe-se nessa figura as menções aos *Hypervisors* KVM e Xen, o que ilustra claramente uma categorização dos problemas enviesada pelo assunto do artigo em questão.

Com esse raciocínio, definiu-se a problemática base para o desenvolvimento desse Relatório Técnico como sendo a falta de padronização das classificações de vulnerabilidades relacionadas à tecnologia de Virtualização em ambiente de Nuvem Computacional.

2. Proposta, Objetivos e Justificativa

Com base na problemática apresentada na seção de Introdução do presente Relatório Técnico, definiu-se como proposta a confecção de uma Categorização dos Desafios de segurança em Computação em Nuvem, especificamente relacionados à tecnologia de Virtualização.

A classificação criada ao final do trabalho objetiva ser simples e direta, ao mesmo tempo em que se apresenta sistemática e completa. A simplicidade é uma meta, pois facilita a disseminação e o reuso do material em futuros artigos. A sistematização, por sua vez, é fundamental para evitar que qualquer problema deixe de ser considerado, além de possibilitar que desafios ainda não mapeados no presente possam ainda assim ser contemplados com a utilização da lógica aqui desenvolvida.

Todo o desenvolvimento se alicerça no fato de que não existe um padrão de classificações para esse escopo de problemas de segurança que seja adotado amplamente nos artigos científicos publicados atualmente.

3. Materiais e Métodos

Para viabilizar a criação da categorização proposta, inicialmente, foram definidos um conjunto de levantamentos bibliográficos que mapeassem áreas de interesse para a execução do trabalho. Os seguintes temas foram considerados pertinentes:

- Computação em Nuvem;
- Tecnologia de Virtualização;
- Desafios de Segurança relacionados à Virtualização em ambientes de Nuvem;
- Categorizações existentes para os desafios mencionados.

Os levantamentos bibliográficos se iniciaram por volta do mês de agosto do ano de 2021. Houve uma preocupação com a reputação das fontes utilizadas e com a variabilidade de buscadores acessados, almejando-se sempre maior confiabilidade e diversidade possíveis. Em geral, os materiais utilizados foram provenientes de artigos científicos encontrados nas plataformas IEEE [17], ScienceDirect [18] e Google Scholar [19]. Além disso, *white papers* e páginas *web* de empresas referências nos temas de interesse também foram considerados.

Após a etapa descrita, e com o embasamento necessário, foi efetuado um processo de síntese e elaboração criativa que culminaram em versões incrementais da categorização proposta. Ao final do segundo semestre de 2021, a classificação final foi transcrita para o presente Relatório Técnico, como via de apresentação formal da lógica desenvolvida.

Todas as etapas do processo tiveram o acompanhamento e a orientação do professor responsável pela disciplina, Professor Doutor Paulo Lício de Geus, com o qual houve reuniões periódicas objetivando direcionamentos específicos.

4. Resultados e Discussões

4.1 Eixos e Elementos da Categorização Proposta

A construção da categorização dos desafios de segurança em Computação em Nuvem, especificamente relacionados à tecnologia de Virtualização, teve como base primária a tríade de segurança computacional: Disponibilidade, Confidencialidade e Integridade. A razão por trás desse *design* é trazer simplicidade para a classificação proposta, bem como mapear quaisquer problemas existentes ou futuros, através de uma divisão clássica presente nas mais incipientes definições sobre o tema de segurança. A Figura 8, abaixo, ilustra o tripé mencionado.

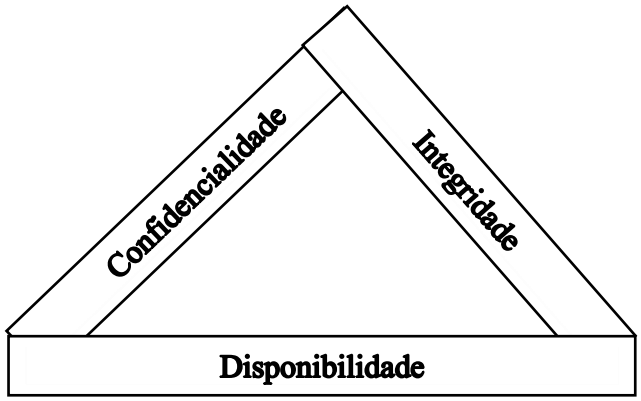

Figura 8 – Tríade de Segurança Computacional utilizada como base para categorização criada.

Uma vez definidos os eixos que embasam a classificação proposta, considerou-se os seguintes elementos pertencentes a uma arquitetura tradicional de Computação em Nuvem:

- Usuário,
- Provedor de Serviços em Nuvem,
- Rede,
- Servidor,
- *Hypervisor*,
- *Virtual Machine* e
- Contratos e Regulamentações.

O objetivo do mapeamento desses elementos é criar uma relação entre eles e os eixos presentes no tripé de segurança computacional. Isso foi feito para possibilitar uma categorização sistemática das vulnerabilidades e ataques presentes na proposta desse trabalho, de tal forma que seja possível identificar com exatidão ambos o escopo e a porção da arquitetura entre Usuário e Provedor de Serviços em Nuvem para um dado risco computacional.

É importante efetuar um detalhamento mais aprofundado acerca de cada um dos elementos mencionados. Por Usuário, entende-se todo e qualquer indivíduo, ou grupo de indivíduos (representando empresas ou outras organizações pertinentes), que tenha contratado e esteja utilizando serviços em Nuvem. O Provedor de Serviços de Nuvem, por sua vez, figura como o fornecedor desses mesmos serviços aos Usuários. A Rede deve ser entendida como o canal de comunicação entre os dois últimos elementos, funcionando através de protocolos padrão como TCP/IP, por exemplo. O Servidor representa a máquina física em que os Usuários possuam aplicações / operações em Nuvem em um determinado período. As *Virtual Machines* operam simulando virtualmente um computador real e são utilizadas pelos Usuários. O *Hypervisor* é a solução de código utilizada pelo Provedor para gerenciar as *Virtual Machines* e conectá-las ao Servidor físico. E, por fim, os Contratos e Regulamentações comprimem o acordo de responsabilidade dividida entre Usuário e Provedor de Serviços em Nuvem, assim como as regulamentações nacionais ou transnacionais vigentes.

4.2 Categorização dos Desafios de Segurança em Nuvem relacionados à Tecnologia de Virtualização

As Figura 9, 10 e 11, nas páginas seguintes, trazem a proposta de Categorização dos Desafios de Segurança em Nuvem relacionados à Tecnologia de Virtualização para cada um dos três eixos no tripé de segurança computacional anteriormente definido: Disponibilidade, Confidencialidade e Integridade.

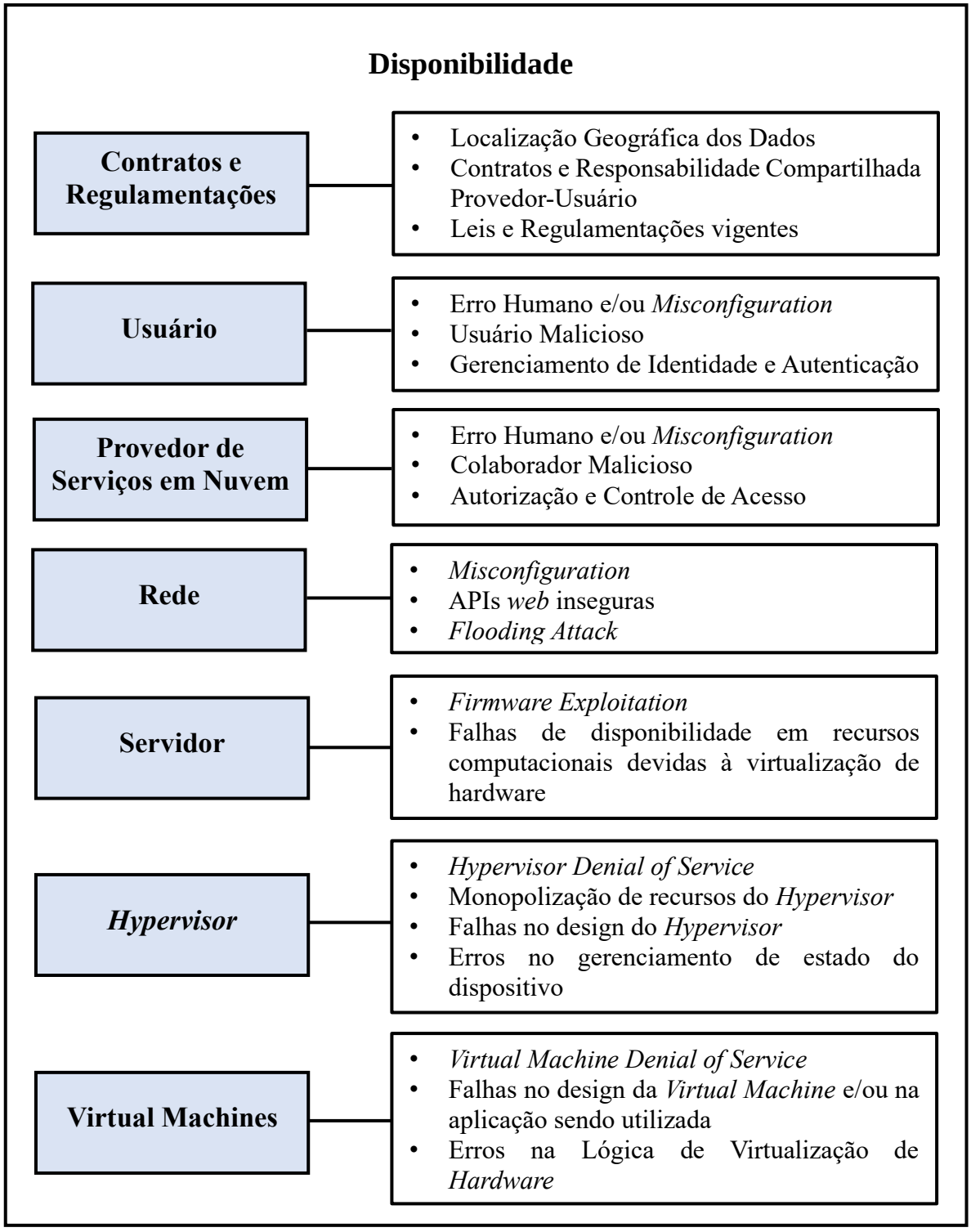

Figura 9 – Categorização dos Desafios de Segurança em Nuvem relacionados à Tecnologia de Virtualização – Escopo de Disponibilidade.

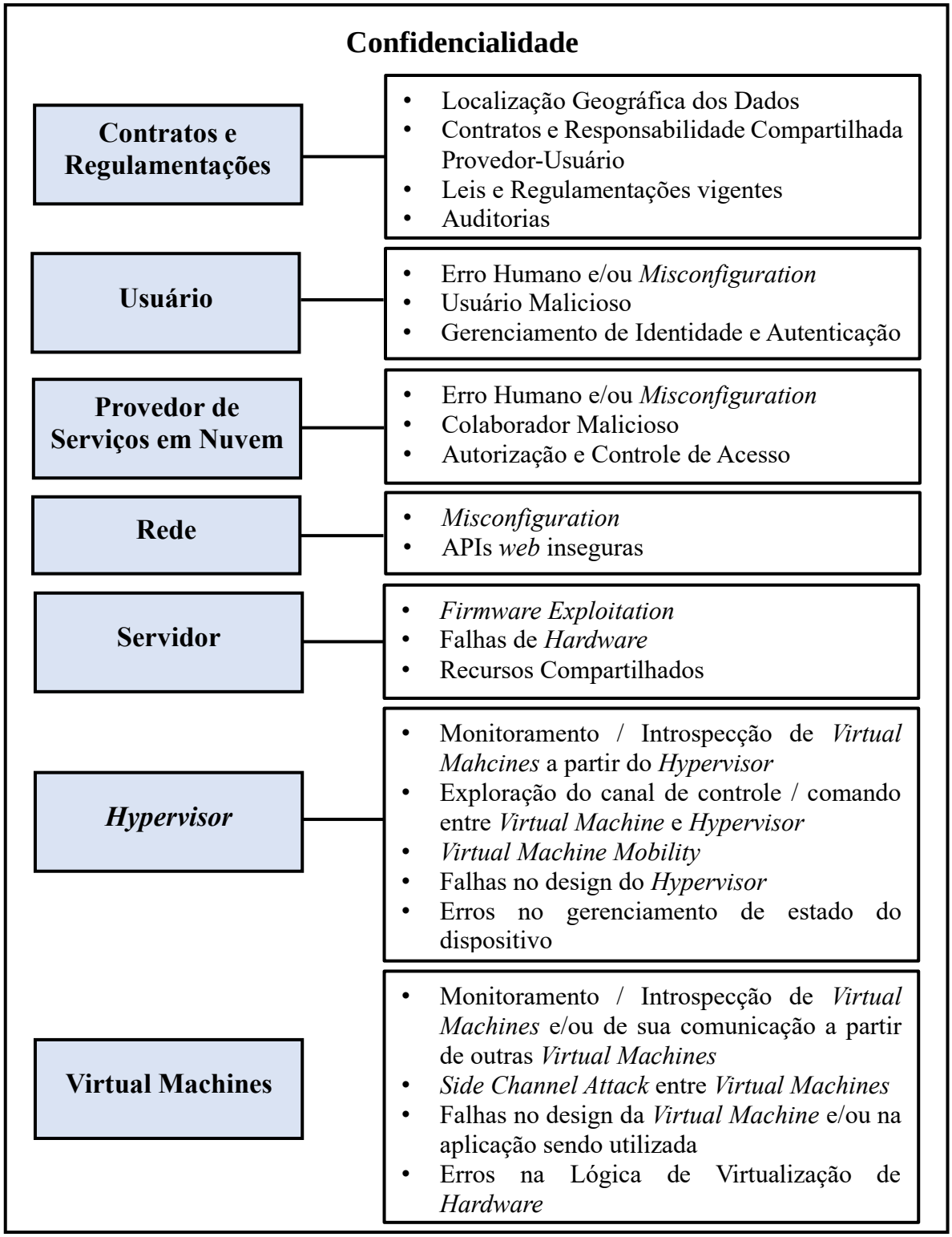

Figura 10 – Categorização dos Desafios de Segurança em Nuvem relacionados à Tecnologia de Virtualização – Escopo de Confidencialidade.

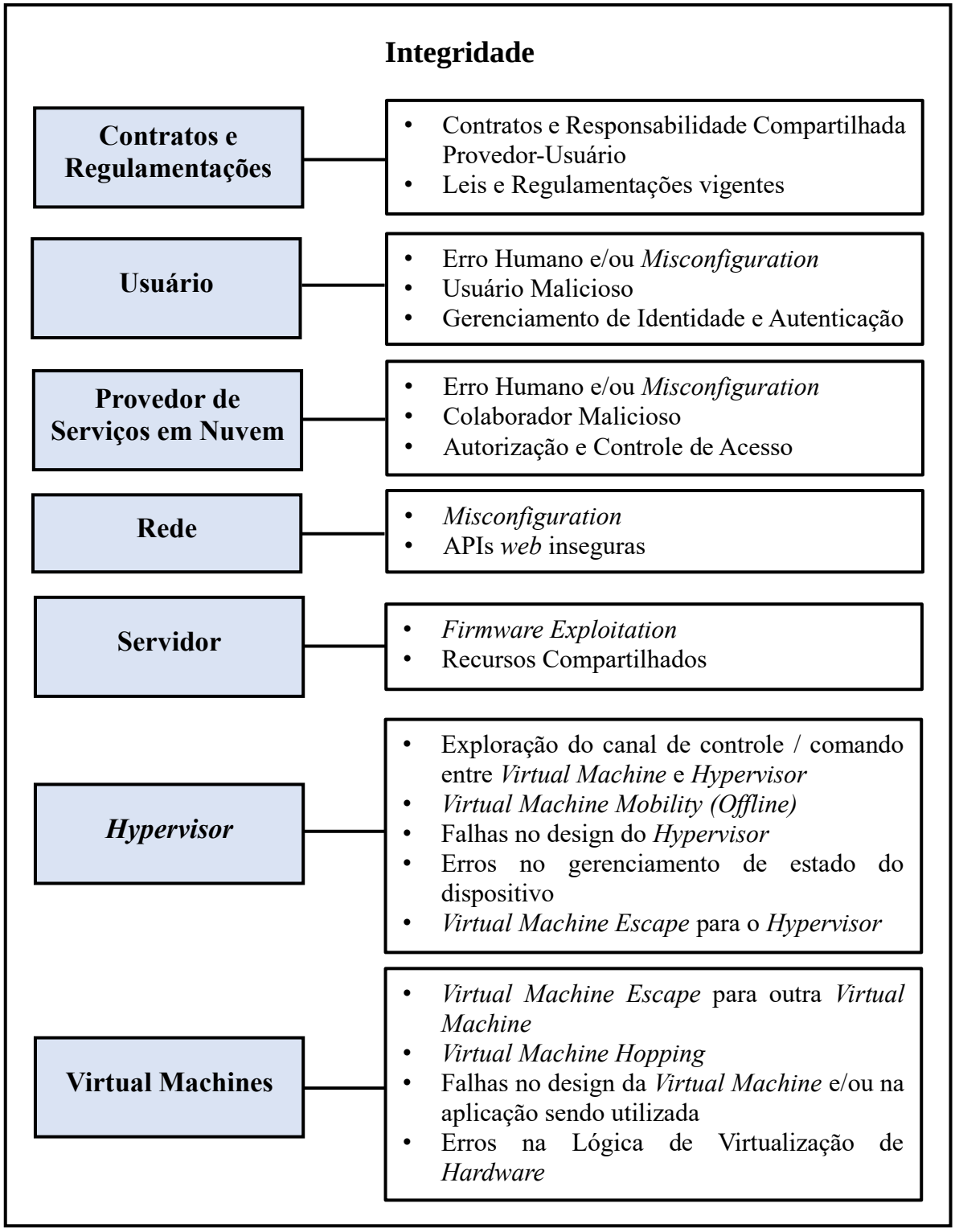

Figura 11 – Categorização dos Desafios de Segurança em Nuvem relacionados à Tecnologia de Virtualização – Escopo de Integridade.

4.3 Discussão dos Resultados

Iniciando a análise pelos desafios de segurança no eixo de Disponibilidade, nota-se, no elemento de Contratos e Regulamentações, que foram levados em conta políticas de negócio e fatores contratuais entre o Provedor de Serviços em Nuvem e o Usuário, além de leis vigentes que permeiam transações comerciais dessa natureza. A questão da localização geográfica dos servidores pertencentes ao Provedor é um exemplo bastante abrangente, pois ilustra decisões de negócio entre os envolvidos, e, potencialmente, pode levar dados sensíveis e estratégicos de uma determinada companhia para fora dos limites legais permitidos de acordo com legislações nacionais ou políticas da própria empresa contratante. Ainda dentro desse escopo, vale ressaltar o acordo firmado entre as partes na contratação dos serviços de Nuvem, uma vez que a responsabilidade da segurança do sistema final será compartilhada e, assim como no exemplo geográfico, pode influenciar na disponibilidade ou não das informações.

Do ponto de vista dos Usuários e Provedores de Serviços em Nuvem, a disponibilidade pode ser afetada por erros operacionais humanos (inclusive relacionados a *misconfiguration*), pessoas com intenções maliciosas ou então problemas no gerenciamento de autenticação e autorização ao uso do sistema de interesse. O exemplo de *misconfiguration* é bastante pertinente, pois mesmo se tratando de algo não necessariamente intencional (o que diminui consideravelmente as probabilidades de ataques quando comparados com desafios intencionais), ainda assim configura uma porta de entrada para atacantes externos, que muitas vezes estão buscando exatamente oportunidades dessa natureza. Funcionários maliciosos, pertencentes a qualquer um dos elementos considerados da arquitetura, possuem acesso privilegiado ao sistema e, por isso, também representam um risco. Por fim, problemas de autenticação e autorização, por estarem diretamente relacionados com acesso ao sistema, são mais uma vez considerados como potenciais portas de entrada por atacantes.

No elemento da Rede, problemas de *misconfiguration* estão tão presentes quanto os já descritos para Usuários e Provedores. APIs *web* inseguras contribuem para ataques por possuírem vulnerabilidades e livre acesso ao sistema. E por fim, *Flooding Attacks*

configuram uma estratégia conhecida dos *hackers* para sobrecarregar a arquitetura com uma quantidade de requisições muito superior à capacidade de resposta, influenciando em falhas de disponibilidade.

Servidores físicos comprimem muitas vulnerabilidades de *hardware* relacionadas ao escopo de desafios de segurança em virtualização. Algumas falhas decorrentes da virtualização de sensores (não disponíveis em um *loop* indefinidamente, como um recurso físico estaria, por exemplo), ilustram um dos problemas possíveis de serem abordados por *hackers*. A exploração do *firmware*, por sua vez, consiste em buscar brechas por falta de atualizações nos recursos materiais - outra maneira viável de atacar o sistema em questão.

O *Hypervisor* é um elemento-chave para a arquitetura discutida. Devido a sua grande influência sobre as *Virtual Machines,* muitos canais que podem ser utilizados como meios de ataque. Além do clássico *Denial of Service*, que consiste em sobrecarregar o *Hypervisor* muito além de sua capacidade, falhas em sua própria implementação podem ser utilizadas por atacantes para os mais diversos tipos de acometimentos. Outra forma já utilizada por agentes maliciosos, foi a danificação do *Scheduler* desse elemento, modificando o relógio do computador e fazendo com que a alocação de recursos para *Virtual Machines* se desse de maneira tendenciosa. Mais um exemplo de vulnerabilidade dentro desse escopo é o possível mal gerenciamento do estado dos dispositivos controlados pelo *Hypervisor*, ou seja, o manuseio incorreto de registradores e afins no momento de interação com *Virtual Machines*.

Virtual Machines, por sua vez, correspondem ao último elemento a ser descrito nessa seção da análise. Para influenciar negativamente na disponibilidade através desse artefato, é possível explorar falhas no *software* da própria *Virtual Machine* ou da aplicação que esteja sendo executada pelo Usuário. Erros na lógica de virtualização, mesmo que não influenciem diretamente no tempo em que o serviço usado esteja disponível, podem ser portas para ataques de *hackers* experientes. Por fim, tal qual o *Hypervisor*, também é possível sobrecarregar *Virtual Machines* com mais requisições do que a sua capacidade, causando problemas na disponibilidade final.

A partir daqui a análise se debruça sobre os desafios de segurança dentro do eixo de Confidencialidade. Trazendo o foco para os elementos de Contratos e Regulamentações,

Usuário, Provedor de Serviços em Nuvem, Rede e Servidor é possível notar que todos eles possuem uma intersecção de causa-raiz muito semelhante à análise já efetuada para o eixo de Disponibilidade. Embora as causas sejam similares, contudo, os problemas causados possuem impactos diferentes dos explicados nos últimos parágrafos. No escopo aqui presente, a preocupação recaí sobre o sigilo das informações e dados manuseados e não no tempo em que o serviço está disponível ou não. Dessa forma, é preciso interpretar *APIs* inseguras que revelem mais do que deveriam, erros humanos que exponham conteúdos secretos e falhas de *hardware* que, mesmo não intencionais, causem danos de segredos irreversíveis, só para citar alguns exemplos. Já na área que foge da intersecção com os parágrafos anteriores, pode-se mencionar, dentro de Contratos e Regulamentações, o papel das auditorias, que são responsáveis por verificar toda e qualquer informação das empresas alvo. Outro ponto são os recursos compartilhados (especialmente caches) nos servidores físicos, representando talvez uma das ameaças mais fundamentais de toda a arquitetura de Nuvem, já que possibilitam a atacantes a tentativa de interação com tais informações.

Do ponto de vista do *Hypervisor*, existe a possibilidade de que *hackers*, a partir desse elemento, monitorem e infiram informações acerca das *Virtual Machines* que estejam sendo controladas. Os atacantes também podem explorar o canal especial usado para comunicação entre o *Hypervisor* e as *Virtual Machines*, visando interceptar a troca de dados entre eles. Outro problema já relatado, é o de *Virtual Machine Mobility* que implica em agentes maliciosos buscando acesso aos arquivos que representam as máquinas virtuais quando o *Hypervisor* está realizando migrações físicas decorrentes das necessidades de elasticidade e escalabilidade em Nuvem. Além de tudo isso, como já explanado anteriormente, falhas no *design* do *software* do componente em questão, bem como erros no gerenciamento do estado de registradores e afins, também compreendem vetores de riscos quando transladados para o escopo de Confidencialidade.

As *Virtual Machines*, propriamente, contribuem com riscos para a Confidencialidade pois também são alvos de *hackers* para efetuar monitoramentos e inferências acerca de seus pares. Ataques mais sofisticados utilizam inclusive canais paralelos para buscar sucesso em *Side Channel Attacks*. Da mesma forma como explicado para o eixo de Disponibilidade,

falhas no *design* da *Virtual Machine* e/ou na aplicação sendo utilizada pelo Usuário, bem como erros na lógica da virtualização aplicada são portas de entrada que também podem ser exploradas por atacantes.

A última parte da análise (acerca do escopo de Integridade), assim como anteriormente, traz uma grande intersecção com os eixos já discutidos. Mais uma vez, os elementos de Contratos e Regulamentações, Usuário, Provedor de Serviços em Nuvem, Rede e Servidor possuem causas-raiz muito próximas das já explanadas nesse Relatório Técnico. Contudo, aqui também vale a citação de que os problemas em cada um desses casos possuem impactos diferentes daqueles sob os escopos de Confidencialidade ou Disponibilidade. Nesse ponto, em especial, as ameaças estão voltadas para o comprometimento de informações. Deve-se interpretar funcionários maliciosos, por exemplo, como responsáveis por danificar dados ou o próprio sistema dentro da arquitetura, e assim por diante.

O *Hypervisor*, por sua vez traz dois elementos distintos dos já apresentados até aqui: *Virtual Machine Escape* e *Virtual Machine Mobility (Offline).* O primeiro caso trata de um cenário onde o atacante utiliza de sua própria *Virtual Machine* para executar processos capazes de escaparem do escopo original e alcançarem o *Hypervisor* (com potencial claro de corromper dados desse elemento, bem como o de outros elementos controlados por ele). A segunda ameaça se difere da *Virtual Machine Mobility* anteriormente apresentada, pois possuí foco em corromper arquivos correspondentes a *Virtual Machines* enquanto elas estão desligadas. Ambos os cenários apresentados merecem atenção especial quando se utiliza de sistemas em Nuvem.

As *Virtual Machines* também representam um vetor de ataque quando o assunto é Integridade. Além dos problemas na intersecção dos já apresentados, como são os casos de falhas em *design* de *softwares* das próprias *Virtual Machines* ou da aplicação utilizada pelo Usuário e erros na lógica de virtualização de *hardware*, é possível que *hackers* efetuem ataques de *escape* com alvo a outras *Virtual Machines* ou então a dispositivos virtuais (situação conhecida como *Virtual Machine Hopping*), sempre com foco em comprometer seus pares.

5. Conclusão

Tendo em vista todos os aspectos apresentados durante a concepção desse Relatório Técnico, pode-se concluir que a Categorização dos Desafios de segurança em Nuvem, relacionados à tecnologia de Virtualização, aqui apresentada é uma maneira simples e sistemática de classificar os desafios propostos. A proposta visa aglutinar grandes categorias de problemas de segurança (Disponibilidade, Confidencialidade e Integridade) dividindo-as em facetas correspondentes a cada um dos elementos presentes em uma arquitetura tradicional de uso da Nuvem (Contratos e Regulamentações, Usuário, Provedor de Serviços de Nuvem, Rede, Servidor, *Hypervisor* e *Virtual Machines*), de tal forma que possa ser utilizada na literatura para padronizar a apresentação dos problemas existentes e futuros dentro do escopo considerado.

Por esses motivos, conclui-se que o trabalho é capaz de contribuir com o meio científico e, por isso, pode ser considerado um sucesso. A criação de novas classificações focando em nichos de problemas diferentes, porém dentro de um ambiente de Nuvem, será avaliada e pode compreender trabalhos futuros.

6. Referências

[1] BEHL, A. *Emerging Security Challenges in Cloud Computing.* Artigo Científico. *Centre of Excellence, Advance Services - Cisco Systems. New Delhi, India*. (2011)

[2] CAIN, C., RAYMOND, D. e RANSBOTTOM , J. S. *The State of the Public Cloud: Security Concerns with Cloud Computing.* Artigo Científico. *Virginia Tec*. (2020).

[3] McAfee. *Cloud Adoption and Risk Report. Business Growth Edition.* Relatório Técnico. (2019)

[4] MICROSOF AZURE. Disponível em: < https://azure.microsoft.com/en-us/ >. Acesso em: 11/11/2021.

[5] AMAZON AWS. Disponível em: < https://aws.amazon.com/ >. Acesso em: 11/11/2021.

[6] GOOGLE CLOUD. Disponível em: < https://cloud.google.com/ >. Acesso em: 11/11/2021.

[7] IBM CLOUD. Disponível em: < https://cloud.ibm.com/ >. Acesso em: 11/11/2021.

[8] ALI, M., KHAN, S. U., VASILAKOS, A.V. *Security in Cloud Computing: Opportunities and Challenges.* Artigo Científico. *North Dakota State University, Kuwait University* e *COMSATS Institute of Information Technology*. (2015)

[9] MELL, P. and GRANCE, T. *The NIST Definition of Cloud Computing.* Relatório Técnico. (2011)

[10] ODUN-AYO, I., AJAYI, O. e OKEREKE, C. *Virtualization in Cloud Computing: Development and Trends.* Artigo Científico. *Covenant University e University of Lagos Nigeria.* (2017)

[11] KUMAR, V. e RATHORE, R. S. *Security Issues with Virtualization in Cloud Computing*. Artigo Científico. *Galgotias College of Engineeringand Technology*. (2018)

[12] SINGH, M. *Virtualization in Cloud Computing - A Study*. Artigo Científico. *Government of NCT of Delhi.* (2018)

[13] ZHU, G., YIN, Y., CAI, R. e Li, K. *Detecting Virtualization Specific Vulnerabilities in Cloud Computing Environment*. Artigo Científico. *University of Georgia*. (2017).

[14] TAMANE, S. *A Review on Virtualization: Cloud Technology.* Artigo Científico. *MGMs, Jawaharlal Nehru Engineering College.* (2015)

[15] OUSMANE, S. B., IBRAHIMA, N. e DOUDOU, F. *A Review of Virtualization, Hypervisor and VM allocation Security: Threats, Vulnerabilities, and Countermeasures*.

Artigo Científico. *Cheikh Anta Diop University* e *Nara Institute of Science and Technology*. (2018)

[16] COMPASTIÉ, M., BADONNEL, R., FESTOR, O. e HE, R. *From virtualization security issues to cloud protection opportunities: An in-depth analysis of system virtualization models*. Artigo Cientìfico. *University of Lorraine* e *Orange Labs*. (2020).

[17] IEEE. Disponível em: <https://ieeexplore.ieee.org/Xplore/home.jsp> Acesso em: 20/11/2021.

[18] *ScienceDirect*. Disponível em: <https://www.sciencedirect.com/>. Acesso em: 20/11/2021.

[19] *Google Scholar*. Disponível em: <https://scholar.google.com.br/>. Acesso em: 20/11/2021.