VIRTUALIZAÇÃO E SEGURANÇA COM VMWARE EM UM CENTRO DE TELEMÁTICA

Valdinei Carlos Oliveira[1]

Resumo. A virtualização nos últimos anos, tem obtido considerável destaque na estrutura dos *data centers*. A instalação seja do tipo *bare metal* ou *hosted* tem sido usado largamente, face as suas vantagens. Os tipos de virtualização adicionam um dinamismo à uma possível implantação, pois trazem a flexibilidade que o paradigma de *hardware* dedicado não oferece. O Exército Brasileiro, a exemplo de outras instituições, também optou pela virtualização e incentiva tal prática em suas Organizações Militares. Aspectos como controle centralizado, possibilidade de oferecer alta disponibilidade de maneira simples e intuitiva, facilidade de backup, migrações em tempo real, contribuíram bastante para esse crescimento e reconhecimento. Devido a esse rápido crescimento, houve a necessidade de evolução das ferramentas de segurança para acompanhar o rápido crescimento da virtualização e proporcionar assim, uma camada a mais de proteção, face o surgimento de novas vulnerabilidades trazidas pela presença do *hypervisor*. Ataques do tipo fuga para o *hypervisor* e sequestro de máquina virtual, injeção de código, além da necessidade de controle do fator humano, constantemente preocupam os administradores de *data centers*. Logo, é primordial que a segurança, seja o primeiro aspecto a ser considerado em um planejamento para a implantação de um ambiente virtualizado. Caso seja bem executado, um bom planejamento traz vários benefícios, evitando atrasos e retrabalho, contribuindo assim, para um gerenciamento equilibrado, tolerante a desastres e acima de tudo seguro.

Palavras-chave: Virtualização. Para-Virtualização. VMware. Otimização. Segurança.

Abstract. Virtualization in recent years has been gaining considerable prominence in the structure of data centers. The installation, whether bare metal or hosted, has been used widely, given its advantages. The types of virtualization add dynamism to a possible deployment, as they bring the flexibility that the dedicated hardware paradigm does not offer. The Brazilian Army, like other institutions, also opted for virtualization and encourages such practice in its Military Organizations. Aspects such as centralized control, the possibility of offering high availability in a simple and intuitive way, ease of backup, migrations in real time, contributed a lot to this growth and recognition. Due to this rapid growth, there was a need for the evolution of security tools to keep pace with the rapid growth of virtualization and thus provide an additional layer of protection, given the emergence of new vulnerabilities brought about by the presence of the hypervisor. Escape attacks to the hypervisor and hijacking of virtual machines, code injection, in addition to the need to control the human factor, are a constant concern for data center administrators. Therefore, it is essential that security is the first aspect to be considered in planning for the implementation of a virtualized environment. If well executed, good planning brings several benefits, avoiding delays and rework, thus contributing to balanced management, tolerant to disasters and above all safe.

Keywords: Virtualization. Para-virtualization. Vmware. Otimization. Security.

---

[1] Capitão QCO de Informática da turma de 2012. Mestrando em Engenharia de Telecomunicações pelo IFCE no biênio 2019-2020. Especialista em Aplicações Complementares às Ciências Militares pela EsFCEx em 2012. Bacharel em Engenharia de Telecomunicações pelo IFCE em 2018. Tecnólogo em Análise e Desenvolvimento de Sistemas pela Unibratec de João Pessoa em 2009.

1 INTRODUÇÃO

A Informática evoluiu muito dos anos 60 até os dias atuais. Essa evolução permitiu que as instituições dos mais diversos ramos de atividade, substituíssem de maneira gradual, muitos dos serviços oferecidos somente de maneira presencial, com execução manual (KUROSE; ROSS, 2013).

A partir daquele momento, tais serviços passaram a ter sua execução automatizada por aplicações de computador e seus dados foram armazenados em discos magnéticos desses mesmos computadores.

A grande aceitação deste tipo de serviço pelas pessoas, devido às comodidades oferecidas (não ser necessário se deslocar da residência, ausência de filas, celeridade, diminuição do retrabalho), gerou uma imensa demanda de recursos computacionais, o que forçou por parte das instituições, o uso de máquinas de grande desempenho, denominadas servidores (TANEMBAUM, 2011).

Essas máquinas, chamadas de servidores, eram desenvolvidas especialmente para funcionamento de longo prazo, com muitos recursos e *hardware* de melhor qualidade, de modo que a demanda dos clientes pudesse ser atendida de maneira satisfatória.

Esses servidores, eram grandes consumidores de recursos (espaço, energia elétrica, pessoal especializado), motivo pelo qual, sua gerência se tornou muito dispendiosa (FERNANDES; NUNO, 2018) .

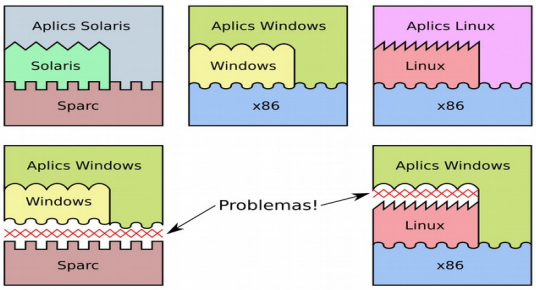
Em muitos casos, a gerência demandava acessar cada máquina, e aplicar configurações e fazer correções, não havia um controle centralizado hierarquizado. Também muitas vezes havia desperdício de recursos, pois cada serviço era hospedado em um único servidor, mas nem todo o serviço demanda a mesma quantidade de recursos (FERNANDES; NUNO, 2018).

Veras (2011), observa que somente 15% da capacidade dos servidores é usada nas empresas. Os 85% restantes ficam subutilizados.

Laureano e Maziero (2008) ressaltam que nos sistemas operacionais atuais, as interfaces de baixo nível são fixas, ou pouco flexíveis. Não é dada a possibilidade de criar novas instruções de processador ou novas chamadas de sistema. Mesmo se fosse possível, teria de haver certa cautela, para não comprometer o funcionamento de outras aplicações.

Essa fraca compatibilidade entre as interfaces dos sistemas operacionais trazem vários problemas na operação e gerenciamento dos diversos sistemas, tal situação é apresentada de uma maneira sintética, na Figura 1, abaixo.

Figura 1 - Problemas de compatibilidade entre interfaces



Fonte: Adaptada de Smith e Nair (2005).

De certo modo, era necessário algo que tornasse essa interoperabilidade mais eficiente, facilitando assim, a operação diária e que os recursos fossem utilizados de maneira otimizada.

Essas dificuldades levaram à investigação de outras formas de relacionamento entre os componentes de um sistema computacional (LAUREANO; MAZIERO, 2008).

Dados estes motivos, a indústria também, foi obrigada a se adaptar a essa nova arquitetura. Um exemplo dessa mudança, foi que fabricantes de *hardware* (processadores), tais como Intel e AMD para atender a essa nova demanda, passaram a implementar em seus produtos instruções que permitiram a operação de uma ferramenta de virtualização de uma maneira menos traumática (LAUREANO; MAZIERO, 2008) (LOTTI; PRADO, 2011).

O conceito de virtualização não é recente, de acordo com Lotti e Prado (2011), os primeiros sistemas virtualizados surgiram nos anos 60 e nos anos 70 foram estabelecidos os princípios que até hoje resguardam a virtualização (POPEK; GOLDBERG, 1974).

Veras (2011), afirma que, com o passar do tempo, a virtualização ganhou mais destaque no mundo corporativo e rapidamente as ferramentas de virtualização se tornaram um recurso fundamental nos *Data Centers*, devido à otimização do uso de recursos e a economia gerada a partir disso.

Somado a esse crescimento da virtualização, as boas práticas de segurança passaram também a ter grande destaque pois o hypervisor por ser uma camada de software a mais, demandava ser protegido tanto quanto qualquer outro software, de falhas e ataques.

Os aspectos de segurança sempre devem ser considerados ao implementar um serviço de virtualização. Em todos os serviços almejados, a segurança deve nortear não só o projeto de implantação do *hypervisor*, bem como a operação diária dos serviços virtualizados, a segurança abrange não só a proteção dos dados sensíveis, bem como a disponibilidade da informação no momento que ela for requisitada. (MACEDO; SANTOS, 2014)

De maneira semelhante ao mundo corporativo, o Exército Brasileiro (EB) também aderiu a proposta de virtualização de seu parque computacional, e têm

implementado tal prática em suas Organizações Militares (OM), bem como, também possui normas que regulamentam as boas práticas de segurança, de acordo com os vários tipos de serviço atualmente disponibilizados, seja na rede local ou *Internet* (EXERCITO BRASILEIRO, 2007).

O presente estudo pretende apresentar através de uma revisão bibliográfica, os benefícios da virtualização através da implantação de um hypervisor *VMWare*, elencando seus pontos fortes e características mais importantes, sem descuidar da segurança, apresentando a adequação às boas práticas de segurança preconizadas nas legislações vigentes no Exército Brasileiro.

2 REFERENCIAL TEÓRICO

A revisão de literatura foi realizada com o intuito de reunir e expor conceitos e abordar, de forma crítica e sucinta, aquilo que interessa ao presente trabalho, buscou-se ainda, o uso de boas práticas utilizadas no setor.

2.1 Conceitos e definições

A virtualização nada mais é que o particionamento de um sistema operacional em vários outros, ela tem por finalidade a otimização de uso dos recursos do *hardware*, executar simultaneamente vários sistemas operacionais diferentes, visa facilitar o gerenciamento de um parque computacional por meio da portabilidade e flexibilidade e até mesmo, colaborar com uma política de economia de energia (CARISSIMI, 2020).

As VM são idênticas a uma máquina real, podendo ser considerada uma duplicata (POPEK; GOLDBERG, 1974), mas na verdade funcionam dentro de um ambiente controlado e gerenciado por um programa especial, que pode ser instalado diretamente sobre o *hardware* ou sobre o S.O. da máquina física, chamada também de máquina hospedeira (SMITH; NAIR, 2005).

Carissimi (2020) afirma que cada máquina virtual pode ter seu próprio sistema operacional; bibliotecas; aplicativos e periféricos, tais como, interfaces de rede, disco rígido, memória e processador.

Arriel (2014) destaca em seu trabalho, que um ambiente de máquina virtual possui de três partes:

• O sistema real (chamado nativo ou hospedeiro), que contém os recursos reais de hardware e software do sistema;

• O sistema virtual (chamado de convidado), que executa sobre o sistema virtualizado em nível de usuário;

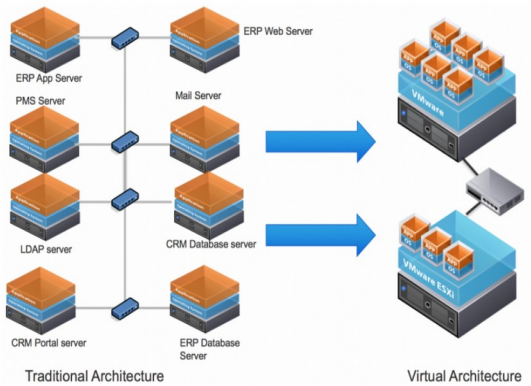
• A camada de virtualização (gerenciada por um programa especial, um

monitor), que constrói as *interfaces* virtuais a partir da *interface* real.

De acordo com Sahoo et al. (2010), dois principais benefícios oferecidos por qualquer tecnologia de virtualização são o compartilhamento de recursos, pois em ambiente virtualizado as máquinas virtuais compartilham os recursos físicos ao contrário do ambiente não virtualizado e o isolamento já um ponto importante na virtualização é fornecer isolamento entre as máquinas virtuais que estão sendo executados no mesmo *hardware* físico.

A Figura 2, abaixo, mostra um comparativo entre a arquitetura na qual há um servidor para cada serviço/aplicação em comparação com a arquitetura virtualizada (DECIPHERING CLOUDS, 2016).

Figura 2 - Arquitetura Tradicional *versus* Virtualização



Fonte: Adaptada de Deciphering Clouds (2016)

Os programas executados em determinada máquina virtual não podem ver os programas de outra máquina virtual. Isso evita que uma aplicação afete ou invada o espaço de memória da outra.

2.2 O *hypervisor*

O Monitor de máquina Virtual, também chamado de *hypervisor* é o programa especial citado anteriormente que tem a capacidade de emular o *hardware* para os sistemas virtualizados que serão hospedados na camada imediatamente acima de si (POPEK; GOLDBERG, 1974).

Nieh e Leonard (2000) afirmam que ele cria um ambiente de execução de hardware virtual chamada de máquina virtual.

Em outras palavras, o *hypervisor* realiza o controle dos recursos de *hardware* e não mais o sistema operacional, logo, é possível executar vários sistemas operacionais em paralelo no mesmo *hardware* (SAHOO et al., 2010).

Agora em *Linux* é possível executar uma aplicação escrita para *Windows*, pois as chamadas ao Sistema original (*System Calls*), emitidas pelo programa serão compreendidas pelo Sistema Operacional abaixo dele, no caso o *Linux* (ARRIEL, 2014).

O *hypervisor* oculta ao sistema convidado, os recursos físicos do sistema de computação, permitindo assim, o gerenciamento, criação, remoção e modificação de recursos de hardware de máquinas virtuais (LOTTI; PRADO, 2011; SAHOO et al, 2010).

Tudo agora pode ser feito em tempo

real, sem necessidade de formatações demoradas, sempre sob o controle *hypervisor*, observando sempre a ressalva de que a soma de recursos a disponibilizados às VM, não ultrapassasse o total de recursos da máquina hospedeira.

A utilização da técnica de virtualização oferece uma maior flexibilidade no uso de recursos, possibilitando que o hardware seja ajustado conforme a necessidade de uma determinada máquina virtual (VERAS, 2011).

Laureano e Maziero (2008) afirmam que o *hypervisor* deve prover um ambiente de execução aos programas idêntico ao da máquina real. São tolerados no máximo, leves degradações de desempenho.

Popek e Goldberg (1974) definem as seguintes propriedades a serem satisfeitas por um *hypervisor* ideal:

• Equivalência: Todo programa executando em uma máquina virtual, provida pelo *hypervisor*, deve se comportar da mesma forma que o faria em uma máquina real;

• Controle de recursos: o *hypervisor* deve possuir o controle completo dos recursos da máquina real: nenhum programa executando na máquina virtual deve possuir acesso a recursos que não tenham sido explicitamente alocados a ele pelo *hypervisor*, que pode resgatar estes recursos previamente alocados;

• Eficiência: grande parte das instruções do processador virtual (o processador provido pelo *hypervisor*) deve ser executada diretamente pelo processador da máquina real, sem intervenção do *hypervisor*. As instruções da máquina virtual que não puderem ser executadas pelo processador real devem ser interpretadas pelo *hypervisor* e traduzidas em ações equivalentes no processador real. Instruções simples, que não afetem outras máquinas virtuais ou aplicações, podem ser executadas diretamente no *hardware*.

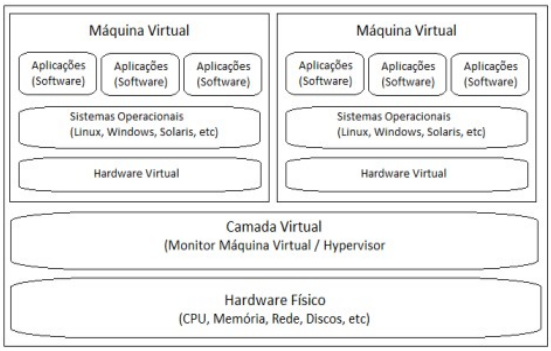
Segundo Seo (2009), o monitor de máquina virtual pode atuar de duas maneiras:

Máquinas virtuais clássicas (**Tipo I**) Figura 3: Também chamada de instalação *Bare Metal*, aqui o *hypervisor* funciona diretamente sobre o *hardware*, tendo logo acima os sistemas convidados e suas aplicações.

É a mais utilizada em ambientes de produção, pois apresenta um desempenho superior ao tipo *Hosted*, pois atua diretamente no *hardware* (MARSHALL; REYNOLDS; MCCRORY, 2006).

Usam esta abordagem os virtualizadores *VMWare ESXi* e *Xen Server*.

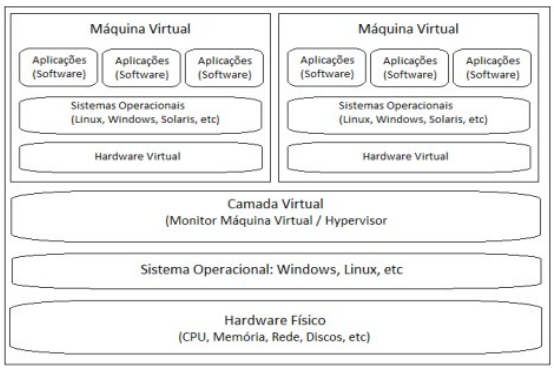
Figura 3 - Máquinas virtuais Tipo I - Hosted



Fonte: Adaptada de Marshall et al (2006)

Máquinas virtuais hospedadas (**Tipo II**) Figura 4: Também chamada de *Hosted*, aqui o monitor funciona sobre o sistema hospedeiro, de forma que os sistemas convidados ficam em uma terceira camada de *software*. Esta abordagem é utilizada pelos virtualizadores *VMWare Workstation, VirtualBox e QEMU*.

Figura 4 - Máquinas virtuais Tipo II - *Hosted*



Fonte: Adaptada de Marshall et al (2006)

2.3 Tipos de Virtualização

Conforme Buytaert et al (2007), existem muitas formas de virtualização. A mais comum é a virtualização de servidor, que é o que vem à cabeça quando a palavra “virtualização” é mencionada.

Mas, além da virtualização de servidores, existem outros tipos de virtualização. O mais comuns são a virtualização de armazenamento, de rede e de aplicativos.

Buytaert et al (2007), relaciona como virtualização de servidor, que é o escopo deste trabalho, as seguintes abordagens:

- Virtualização de hardware ou virtualização nativa: É quando o hardware da máquina hospedeira provê recursos para virtualização, ou seja, há instruções no processador e no controlador de memória que permitem que o hardware execute simultaneamente mais de um sistema operacional.

Exemplos de Virtualização de hardware são a *Intel Virtualization Technology (Intel-VT)* e a *AMD Virtualization (AMD-V)*.

- Paravirtualização: Técnica que provê uma virtualização parcial do hardware subjacente. Nem todos os recursos de *hardware* são simulados. O principal recurso é a virtualização do espaço de endereço, garantindo a cada máquina virtual seu próprio espaço de endereço exclusivo. Há a necessidade de que os sistemas operacionais convidados possuam modificações significativas para garantir seu funcionamento.

- Virtualização de S.O: Este conceito se baseia em uma única instância

de S.O. Roda em velocidade normal e suporta todas as funcionalidades do *hardware* nativo. Não suporta misturar famílias, tal como *Windows* com *Linux.*

• Virtualização completa: Tipo de virtualização que fornece simulação completa do hardware subjacente. Esta virtualização requer que cada característica do *hardware* seja devidamente refletida na máquina virtual, incluindo todo o conjunto de instruções de entrada e saída de operações, interrupções, acesso à memória e todos os demais elementos utilizados por um *software* que fosse executado em uma máquina real (LOTTI; PRADO, 2011).

2.4 Quando virtualizar

Buytaert et al. (2007), em seu trabalho, afirma que utiliza-se a virtualização para as seguintes atividades:

• Atualização de tecnologia: Permite que uma determinada atualização possa ser testada em uma cópia da máquina virtual, evitando assim, a interrupção do funcionamento dessa máquina virtual - *downtime*;

• Suporte a aplicações legadas: Permite que sistemas operacionais e aplicações que foram descontinuadas e sem suporte a hardwares novos, possam ser facilmente migrados para *hardware* mais recentes sem riscos de incompatibilidade;

• Suporte a sistemas operacionais múltiplos: Este é um dos principais atrativos da virtualização;

• Demostrar *softwares*: Realizar demonstrativos de softwares que podem ser executados de uma maneira eficiente e sem grandes esforços para sua implantação;

• Continuidade de negócios: Virtualização pode ajudar uma empresa a alcançar a alta disponibilidade, tolerância a desastres e uso de ferramentas de *backup* de um sistema inteiro.

2.5 Quando não virtualizar

Buytaert et al. (2007) também orienta para quando não se utiliza a virtualização:

• Jogos no computador: Os requisitos para execução de jogos de computador são extremamente rigorosos e ter a camada de virtualização entre o hardware e o jogo pode impactar no desempenho do mesmo;

• Hardware e periféricos especializados: Não há meios de poder colocar em ambientes virtualizados periféricos de hardware customizado.

• Testes de performance: A sobrecarga devido a camada de virtualização irá causar resultados errôneos na execução de testes de performance;

• Depurar *drivers* de hardware: Devido ao fato de todas as máquinas

virtuais terem o mesmo *hardware*, não há como testar ou depurar *drivers* de *hardware* nesta plataforma.

2.6 Riscos e práticas de segurança em ambientes virtualizados

Em um primeiro momento a virtualização oferece um aumento nos níveis de segurança. Seja por ofertar o isolamento entre as máquinas virtuais, a possibilidade de escalabilidade, tolerância a falhas em razão da alta disponibilidade, a possibilidade de rapidamente desativar ou migrar uma máquina virtual de um ambiente comprometido e ainda poder realizar *backups* de uma máquina durante o seu pleno funcionamento (BUYTAERT et al, 2007).

Essas funcionalidades ajudam a promover a correta Segurança da Informação, que é a preservação da confidencialidade, integridade e disponibilidade das informações (ISO/EIC, 2000).

Contudo isso não é suficiente para proteger um ambiente virtualizado. A inclusão de mais uma camada de software, centralizada, com plenos poderes sobre várias outras máquinas, o *hypervisor*, o torna o principal alvo de ataques e uma vez comprometido o monitor de máquinas virtuais, todas as VM por ele gerenciadas viram alvos fáceis (MACEDO; SANTOS, 2014).

Macedo e Santos (2014) relacionam em seu trabalho, alguns tipos de ataques a ambientes virtualizados:

• *VM Escape* (*escape to hypervisor*, fuga para o *hypervisor*): Trata-se de uma brecha de segurança em *hypervisors VMware ESXi*. Através dessa brecha um invasor consegue executar códigos maliciosos dentro de uma máquina virtual, podendo também executar comandos em outra VM ou até mesmo no *hypervisor;*

• Ataque de Negação de Serviço (DoS – *Denial of Service*): Ataques de negação de serviço são comuns a qualquer tipo de sistema ou aplicação. O DoS envia um grande número de pacotes (maliciosos ou não) endereçados a algum sistema ou aplicação, acarretando um alto processamento no alvo que está sendo acatado, causando falhas no sistema;

• Roubo de Máquina Virtual: Tendo em vista que as máquinas virtuais são apenas arquivos, um usuário/funcionário com acesso físico ao local de armazenamento (em geral *storages*) onde os dados das VMs estão guardados, pode extrair todos os arquivos das VMs para uma mídia local;

• Injeção de Código / Arquivo Malicioso: Pelo fato das máquinas virtuais serem, a grosso modo, apenas arquivos armazenados, qualquer alteração realizada

nesses arquivos pode trazer grandes riscos. Os ataques de injeção de código malicioso visam fazer com que esse código injetado seja executado;

• *Footprinting*: É uma técnica de invasão baseada em conseguir informações de um possível alvo sem parecer que aquilo é um ataque. Geralmente a obtenção dessas informações se dá a partir de comandos remotos direcionados a quem se quer atacar. O objetivo de quem está tentando invadir é traçar um perfil daquele alvo, identificando padrões anômalos de tráfego pela rede.

Além disso, há a necessidade de ponderar com extrema cautela, qualquer tipo de acesso (linha de comando ou *interface web*) ao *hypervisor*, restringindo-o somente ao pessoal estritamente necessário e a partir de locais pré-determinados (BUYTAERT, 2007).

De acordo com Macedo e Santos (2014), a implementação de um ambiente virtual não traz praticamente nenhuma ameaça à segurança ou um aumento ou diminuição das ameaças e vulnerabilidades.

As mesmas ameaças, vírus e vulnerabilidades continuam presentes. O que pode ocorrer é uma forma diferente de ataque e defesa devido a esse novo ambiente.

Apresentam ainda, algumas técnicas de segurança em Ambientes Virtualizados, que devem ser acrescentadas às já existentes para os ambientes não virtualizados:

• Criptografia de Máquina Virtual: Uma máquina virtual é essencialmente composta por arquivos, por conta disso um possível roubo de uma VM se torna ainda mais fácil. Sair de uma empresa com um *pendrive* é muito mais discreto do que sair com um servidor nas mãos. Existem diversas formas de se criptografar os arquivos de uma máquina virtual, independentemente de onde ela esteja, se em um *datacenter* ou na nuvem, por exemplo;

• Movimentação de Máquinas Virtuais: Outra funcionalidade bastante presente nas ferramentas de virtualização é a migração das máquinas virtuais presentes em um hospedeiro para outro, provendo alta disponibilidade ao ambiente virtual;

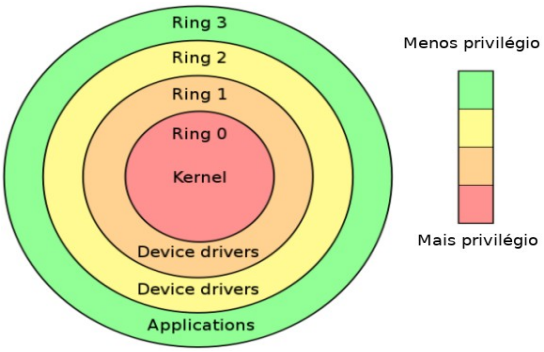
• Monitoramento da Máquina Virtual: O *hypervisor* possui recurso de auditoria, podendo monitorar cada sistema operacional convidado que executa sobre ele, sendo esta técnica conhecida como introspecção. A introspecção pode prover um monitoramento completo, que pode incluir tráfego de rede, memória, processos e diversos outras funcionalidades de um S.O., mesmo quando a segurança deste já foi comprometida;

• Isolamento da Máquina Virtual: O *hypervisor* é responsável por gerenciar o acesso ao hardware pelos sistemas

operacionais das VM. Assim, a máquina virtual enxerga o *hardware* como sendo apenas seu, mas na verdade o *hardware* está sendo compartilhado com diversas outras VM.

• Anéis de Proteção (*Protection Rings*) Os anéis de proteção, como mostra a Figura 5, são um mecanismo para proteger dados, prover tolerância a falhas e coibir comportamento malicioso. O anel 0 (*Kernel*) interage com o *hardware* e é utilizado pelo sistema operacional. Ele pode executar qualquer tipo de instrução ou endereçamento de memória. Falhas neste nível do anel são praticamente irreversíveis. Já o anel 3 é empregado para os processos do usuário (*Applications*). Caso um processo do usuário tente acessar alguma instrução privilegiada do anel 0, uma exceção é gerada, pois este nível não permite o acesso aos níveis mais privilegiados. Falhas no modo usuário são, na maioria dos casos, passíveis de recuperação.

Figura 5 – Níveis de privilégio de um Sistema



Fonte: adaptado de Macedo e Santos (2014).

Macedo e Santos (2014) afirmam que, prevenir e manter uma infraestrutura de virtualização, seguindo as recomendações de segurança, não se restringe apenas ao *hypervisor*, *hardware* ou sistema operacional. Há também as interfaces de armazenamento e de rede, ambas virtualizadas. Por isso, o acesso a elas também deve ser restrito aos sistemas que os utilizam.

Se um disco rígido de um dispositivo de armazenamento é compartilhado com duas máquinas virtuais, é preciso que haja um controle de acesso para que apenas essas duas venham a acessá-los.

No que tange aos componentes de rede, nem todos oferecem um gerenciamento ideal. Desse modo, deve-se adotar tecnologias de segurança adicionais para garantir o monitoramento, controle e inspeção da rede.

Macedo e Santos (2014) apresentam a Tabela 1, a qual confronta as ameaças e suas respectivas defesas:

Tabela 1: Confronto entre ameaças e ataques

Ameaças	Defesas
VM Escape	Anéis de Proteção
N. Serviço (DoS), VM Escape	Monitoramento de VM
Footprinting, Inserção de Código Malicioso	Criptografia de VM

Fonte: Adaptada de Macedo e Santos (2014).

2.7 As Legislações de Segurança da Informação no Exército Brasileiro

O Exército Brasileiro (EB) possui um grupo de unidades voltadas exclusivamente para proporcionar o apoio de TI às demais Organizações Militares (OM) (CITEx, 2020).

Essas unidades são os Centros de Telemática de Área (CTA) e Centros de Telemática (CT). São 12 unidades espalhadas pelo território nacional e coordenadas pelo CITEx (Centro Integrado de Telemática do Exército) formam o Sistema Integrado de Telemática do Exército – SISTEx.

Tais unidades tem como missão principal Gerenciar a infraestrutura física e lógica de tecnologia da informação do SISTEx, oferecendo e garantindo a alta disponibilidade da hospedagem de sistemas corporativos e do Sistema Estratégico de Comando e Controle do Exército (CITEx, 2020).

No desenrolar destas atividades, os CTA/CT, necessitam de estabelecer políticas de Segurança da Informação, a fim de proteger e garantir a segurança e idoneidade dos dados e serviços necessários as demais OM de vinculação sob sua responsabilidade.

Tais políticas são amparadas por meio de decretos e portarias publicadas pela Autoridade Competente, que estabelece diretrizes aos CTA/CT acerca de quais políticas de segurança devem ser implementadas.

Em 2008 por meio da Estratégia Nacional de Defesa (BRASIL, 2008) que estabeleceu dentre várias outras medidas, Três setores tecnológicos essenciais para Defesa Nacional: O nuclear, o cibernético e o espacial. A Mesma END designou o Exército Brasileiro como responsável pelo Setor Cibernético. Desde então, o EB tem se debruçado em capacitação e consequente domínio desse Setor em especial.

Além do viés da Defesa e da Guerra Cibernética, o Exército também tem seus próprios sistemas de informação, orgânicos de suas unidades. Como meio de resguardar informações e padronizar procedimentos, têm estabelecido diretrizes, buscando uma melhor organização da tecnologia da informação e procedimentos que reforcem a Segurança da Informação dentro da Força. Dentre estas normatizações pode-se citar:

- Portaria nº 006-DCT - Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército (NORTI) (EXERCITO BRASILEIRO, 2007). A mesma tem seu objetivo já estabelecido em seu artigo 2º:

> Controlar o conteúdo das informações ou dados armazenados ou veiculados em pastas, arquivos ou mensagens, utilizando dispositivos de TI de propriedade do Exército, de modo a coibir a inserção de assunto ou

matéria considerada ilícita, contrária à disciplina militar, à moral e bons costumes, bem como atentatória à ordem pública ou que viole qualquer direito de terceiros, e buscar a utilização mais adequada daqueles dispositivos (BRASIL, 2007).

- A Cartilha Emergencial de Segurança (EXERCITO BRASILEIRO, 2011), busca incentivar o uso de procedimentos de segurança básicos, de baixo custo e complexidade.
- A EB 10-IG-01.010 - Rede Mundial de Computadores. (EXERCITO BRASILEIRO, 2013), que têm por finalidade estabelecer as condições de acesso e utilização dos recursos da Rede Mundial de Computadores (Internet).

Tais legislações servem de guia às políticas de segurança implementadas dentro de um CTA/CT e paralelamente vão de encontro à busca de um ambiente mais seguro, diante dessa nova necessidade de mais uma camada de segurança, criada pelas política de implantação da virtualização.

2.8 O VMware

O *VMware*, é virtualizador que será utilizado no presente estudo. É uma dentre as várias ferramentas de virtualização existentes atualmente no Mercado.

Pertencente à empresa de mesmo nome, a qual foi criada em 1998, por *Diane Greene*, *Edouard Bugnion*, *Scott Devine*, *Mendel Rosenblum* e *Edward Wang*. Teve sua primeira versão, o *Workstation* 1.0 lançada em 1999 (VMWARE INC, 2020).

Atualmente a *VMware Inc.* pertence à *EMC Corporation* e tem a sua sede em Palo Alto, Califórnia. (VMWARE INC, 2020).

De acordo com Ferguson (2014), o *VMWare Server* usa o conceito de virtualização completa. Ele pode ser instalado tanto em sistemas *Linux* quanto em sistemas *Windows*.

O Vmware dentre seus vários produtos, tem 03 (três) linhas de virtualizadores:

- O *VMware Player* - Esta é a versão mais simples do produto e que também é disponibilizada gratuitamente para *download* no site do fabricante (*VMWare*, 2014). O *VMware Player* é indicado para aplicações leves e não cria máquinas virtuais, porém executa as máquinas virtuais criadas por outras versões mais completas;
- O *VMware Workstation* - Esta é a versão comercial do *VMware* que é utilizada em estações de trabalho (VMWare, 2014). Possui basicamente os mesmos recursos do *VMware Server* inclusive com a possibilidade de criar máquinas virtuais;
- O *VMware ESXi* - É um sistema operacional hospedeiro (MATTOS, 2008).

VMware ESXi é a versão comercial do produto VMware voltado para o uso corporativo em servidores de grande porte.

Ele é uma máquina virtual do Tipo I que possui um sistema operacional próprio e otimizado para gerenciar máquinas virtuais. No *VMware ESXi*, cada máquina virtual representa um sistema completo (VMWare, 2014).

Para este trabalho, o objeto de estudo será a versão *ESXi*, em razão da mesma atender a uma estrutura de Data Center semelhante à existente em um Centro de Telemática, Organização Militar de Tecnologia da Informação, existente no Exército Brasileiro.

3 METODOLOGIA

Foi realizada pesquisa acerca da implementação do *VMware*, sob a ótica dos preceitos de segurança e das legislações sobre o assunto, vigentes no Exército Brasileiro, buscando sempre um equilíbrio entre performance e segurança.

Em um projeto de implantação de uma infraestrutura de virtualização, uma parte sensível, que demanda bastante atenção, é o planejamento.

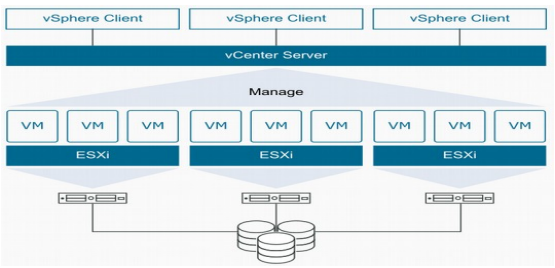
Um planejamento detalhado antes da implantação, configuração e instalação, pode evitar retrabalho e atrasos na fase de implementação. Muito dos problemas de segurança e desempenho ocorrem devido a erros de planejamento. É recomendado que aspectos de segurança devam ser os primeiros a serem levados em consideração no planejamento para melhorar ambientes virtuais e diminuir os custos (MACEDO; SANTOS, 2014).

Uma vez realizado o planejamento, parte-se para a instalação do virtualizador escolhido, o *VMware ESXi*, na configuração *bare metal*, isto é diretamente sobre o *hardware*.

É necessário atentar aos requisitos de hardware mínimos para a instalação. A verificação pode ser feita no endereço eletrônico https://docs.vmware.com/en/Vmware-vSphere/index.html.

Ao acessar a página, há uma explicação sobre a arquitetura *VMware* e demais funcionalidades existentes na ferramenta, conforme a Figura 6.

Figura 6 – *Arquitetura do VMware*



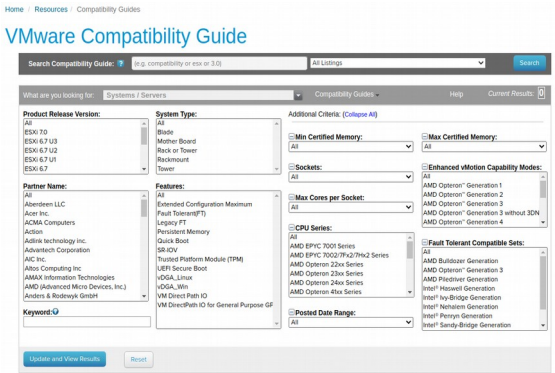
Fonte: Adaptada de VMware (2020).

Na página também é apresentado qual o papel da ferramenta *Vsphere*, já que no início pode parecer complicado saber qual o papel desempenhado por cada uma das soluções:

> O *vSphere* 7.0 oferece várias opções de instalação e configuração. Para garantir uma implantação bem-sucedida do *vSphere*, você deve compreender as opções de instalação e configuração e a sequência de tarefas.
>
> Os dois componentes principais do *vSphere* são *ESXi* e *vCenter Server*. *ESXi* é a plataforma de virtualização na qual você pode criar e executar máquinas virtuais e dispositivos virtuais.
>
> O *vCenter Server* é um serviço que atua como administrador central para *hosts ESXi* conectados em uma rede. O *vCenter Server* permite agrupar e gerenciar os recursos de vários *hosts*. (VMWARE, 2020, tradução nossa.)

A seguir, é recomendado verificar a lista de compatibilidade, figura 7, para que o hardware seja preparado para a instalação do virtualizador, tal lista se encontra no endereço eletrônico: https://www.vmware.com/resources/compatibility/search.php.

Figura 7 – Lista de compatibilidade de *hardware*

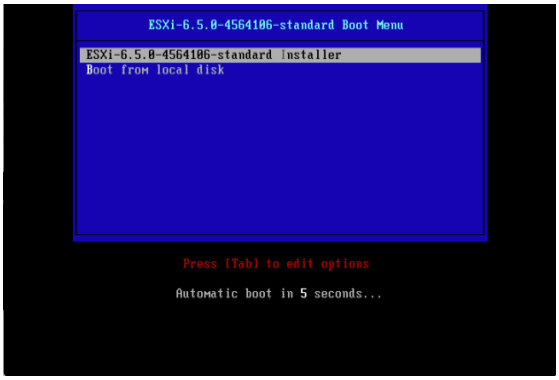


Fonte: Adaptada de VMware (2020).

Satisfeitos os requisitos e estando dentro da lista de compatibilidade, é hora de fazer o download da versão de avaliação do *VMWare*, gravar em um DVD e iniciar a instalação.

Inicia-se o Servidor pelo DVD e escolhe-se o *boot* pelo DVD do *ESXi*, conforme Figura 8, abaixo:

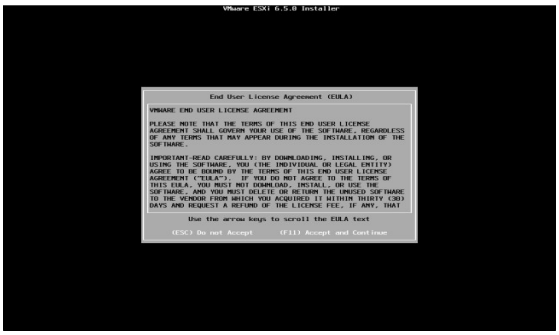
Figura 8 – Tela de *boot* do servidor escolhido para a ferramenta de virtualização



Fonte: Adaptada de Lira (2016).

Em seguida espere os drives carregarem e na tela seguinte, aceite a licença de uso teclando <F11>, conforme a Figura 9.

Figura 9 – Licença de uso

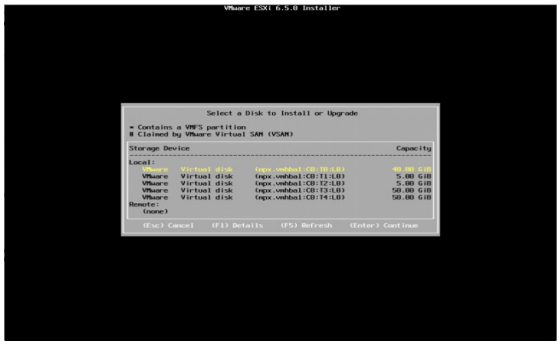


Fonte: Adaptada de Lira (2016).

A próxima tela, apresentada na Figura 10, apresenta os discos físicos

existentes e basta escolher onde o sistema será instalado e tecle <ENTER>

Figura 10 – Escolha do disco para instalação



Fonte: Adaptada de Lira (2016).

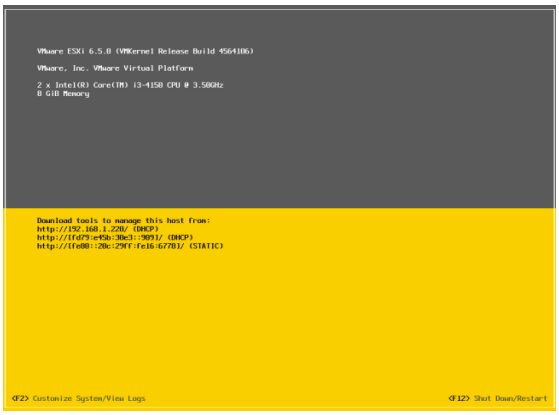
As telas seguintes são bastante intuitivas, basta clicar <ENTER>, e o assistente de instalação vai solicitando sua confirmação, após configurar o usuário e uma senha (muito forte) para o usuário administrador, aparece a tela da Figura 11 e finalmente é iniciada a instalação.

Figura 11 – Processo de instalação do ESXi

Fonte: Adaptada de Lira (2016).

Após a conclusão da instalação basta teclar <ENTER> para reiniciar. Após o sistema reiniciar, ele irá pegar um endereço IP dinamicamente, caso a sua rede possua um servidor DHCP – *Dynamic Host Control Protocol* ou protocolo de controle de host dinâmico, caso não tenha, é possível configurar um IP manualmente através da tela apresentada na Figura 12, abaixo, teclando <F2>.

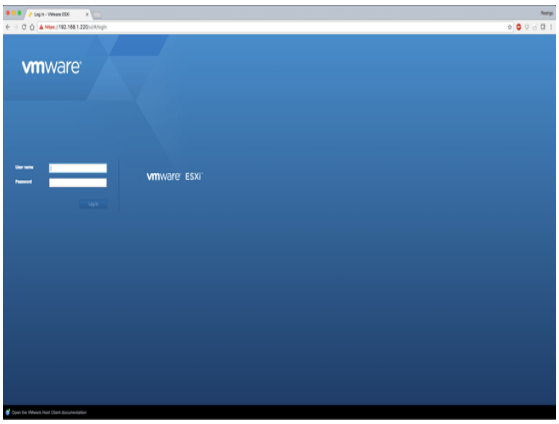
Figura 12 - Tela de configuração



Fonte: Adaptada de Lira (2016).

Também é possível o acesso via *interface web*, conforme Figura 12. Basta digitar o endereço IP configurado previamente, tal como http://<ip configurado>/ui e inserindo o usuário e a senha escolhidos na etapa de instalação:

Figura 12 – Acesso via *Interface Web*



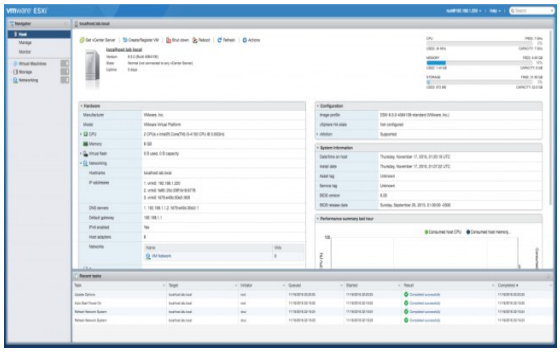
Fonte: Adaptada de Lira (2016).

Após a instalação, a próxima tela já dentro do ambiente *ESXi*, o qual

disponibiliza a possibilidade de criar, mover e apagar máquinas virtuais. Agora tem-se um ambiente virtualizado e pronto para a implantação de máquinas virtuais que irão realizar os mais diversos tipos de serviço, facilmente gerenciáveis por meio do painel de virtualização, conforme a figura 13. Convém lembrar que nem todos os recursos estão disponíveis na interface web por motivo de segurança.

O gerenciamento pleno se dá com o uso do *vCenter*, que deve ser instalado em uma outra máquina com acesso a este *hypervisor*.

Figura 13 – Ambiente *ESXi*



Fonte: Adaptada de Lira (2016).

4 RESULTADOS

Concluída a etapa de implantação da ferramenta, foi possível verificar os seguintes aspectos no que tange a performance do *hypervisor* VMware.

A implementação do *hypervisor* proporciona uma melhor gerência dos serviços hospedados. Uma vez que cada um destes serviços geralmente hospedados em uma VM, permite uma visão geral de todas as máquinas por meio do painel do virtualizador.

Atividades como *backups*, migrações e redimensionamento de configurações se tornam mais fáceis pois no ambiente virtualizado não há a necessidade de manipular dispositivos de hardware diretamente, o que torna tais atividades menos dispendiosas

À medida que, a gerencia e manipulação dos serviços ficaram mais facilitadas, há a necessidade de um cuidado maior na manipulação do *hypervisor* pois agora os serviços estão centralizados em um único ponto, por um lado, isso é bom, pois reduz os pontos de falhas, mas em compensação esse único ponto pode causar uma pane grave em caso de falha humana ou se tornar o objetivo principal de um ataque virtual.

Desse modo, apesar de observado várias melhorias de performance com o virtualizador, chega-se a conclusão que na mesma proporção, a segurança fica comprometida pela grade importância do mesmo no cenário da virtualizado, boa parte pela vulnerabilidade que ele traz por ser o elemento central de controle das máquinas virtuais.

É necessário proteger o virtualizador do acesso físico indiscriminado à sua localização e também protegê-lo do acesso total por meio de estranhos no ambiente

virtual, por meio da utilização ativos de proteção, tais como, Firewalls, Sistemas de Prevenção de Intrusão (*Intrusion Prevent System* – IPS) e Sistemas de Detecção de Intrusão (*Intrusion Detect Systems* – IDS), além de uma forte política de controle de acesso.

O acesso rotineiro ao virtualizador deve ser reduzido ao mínimo necessário e por um pequeno grupo de pessoas, de modo a promover um nível ainda maior de segurança, somados aos controles e ferramentas já citadas anteriormente.

A capacitação e contínuo aperfeiçoamento da equipe responsável pelo ambiente de virtualização deve ser uma prioridade dentro da Organização.

Constantemente é anunciado que um grupo A ou B tem encontrado brechas de segurança em recursos de hardware e em softwares de gerenciamento, geralmente considerados seguros e até mesmo respeitados na comunidade de tecnologia.

5 CONCLUSÃO

Os benefícios para Instituição com a implantação da virtualização são enormes, seja pela facilidade de manutenção do parque computacional em virtude da diminuição de ativos físicos, pela diminuição do tempo de resposta a incidentes em razão do controle centralizado.

Proporciona um gerenciamento mais cerrado devido à existência do *hypervisor*, provê ferramenta de *backups* de dados integrada, a flexibilidade ao configurar uma VM em caso de mudança de perfil (CARISSIMI, 2008).

A virtualização ainda ajuda a economizar energia, pois há poucas máquinas consumindo, com o diferencial de que ao invés de apenas uma, serão dezenas de máquinas hospedadas em um mesmo *hardware*, assim diminuindo a consumo por máquina.

A virtualização também colabora com a sustentabilidade pois em teoria, se produz menos *hardware*, porque agora, o mesmo ativo poderá realizar vários serviços diferentes, existem por parte de algumas empresas de energia, programas de bonificação ao haver diminuição de consumo de energia. Isso contribui para a Tecnologia da Informação - (TI) Verde (BUYTAERT, 2014).

A economia no processo de aquisição também é um diferencial relevante em razão de que há a possibilidade de diminuir a quantidade de máquinas de grande desempenho a serem adquiridas, em razão da multiplicidade de tarefas permitidas pela virtualização. Isso pode permitir a economia necessária para que desloque novos recursos para aquisição de licenças do *VMware* (SAHOO et al., 2010; FERNANDES; NUNO, 2018).

O *VMware* é uma ferramenta consolidada no mercado, por diversos aspectos dentre os quais a estabilidade e robustez. Se por um lado, o fato de ser uma aplicação de código fechado, pode soar como desvantagem, por outro lado, em razão deste mesmo aspecto, é disponibilizado pelo fabricante a seus clientes, uma grande estrutura de suporte, recuperação de falhas e treinamento, no que tange ao funcionamento da ferramenta (VMWARE, 2020).

Contudo apesar das vantagens proporcionadas pela virtualização, deve-se pesar o aspecto da segurança, em razão de que o virtualizador se torna um alvo de *malwares*, dado a sua importância no ambiente do *Data Center*.

Um ambiente mais seguro e à prova de ataques providos por hackers é um objetivo a ser alcançado, porém as vantagens proporcionadas pela virtualização tem seu lugar nesse comparativo segurança versus virtualização.

Logo, deve-se sempre buscar aquilo que virá a favorecer a produtividade da Organização, com o máximo de segurança possível.

REFERÊNCIAS

ARRIEL J. **Análise Comparativa Entre As Ferramentas De Virtualização Vmware E Xen.** 2014. Disponível em: <http://repositorio.ufla.br/bitstream/1/3069 6/1/TCC_An %C3%A1lise_comparativa_entre_as_ferra mentas_de_virtualiza %C3%A7%C3%A3o_vmware_e_xen.pdf>. Acesso em 23 ago. 2020.

BRASIL. EXÉRCITO BRASILEIRO. Portaria nº 006-DCT, de 05 de fevereiro de 2007. **Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército (NORTI)**. 2007

BRASIL. EXÉRCITO BRASILEIRO. Portaria 720 - Cmt Ex - **Aprova Cartilha Emergencial de Segurança**. 2011

BRASIL. EXÉRCITO BRASILEIRO. EB 10-IG-01.010 - Portaria 1.313, de 23 de Dezembro de 2013. **Rede Mundial de Computadores.** 2013

BUYTAERT, Kris, DITTNER, Rogier, GARCIA Juan R. et al. **The Best Damn Server Virtualization**. Book Period. Syngress Publishing Inc, 2007.

CARISSIMI, Alexandre. **Virtualização: Da Teoria A Soluções.** Disponível em: <http://hostel.ufabc.edu.br/~marcelo.nascim ento/BC1518Q3/arquivos/ virtualizacao_cap4-v2.pdf>. Acesso em: 07 jul 2020.

DECIPHERING CLOUDS. **vRealize Operations Manager - Monitoring vs Forensic**. 2016. Disponível em: <https://sajaldebnath.github.io/vrealize-operations-manager-monitoring-vs-forensic.html>. Acesso em 04 jul 2020.

EXÉRCITO BRASILEIRO. CENTRO INTEGRADO DE TELEMÁTICA DO EXÉRCITO – CITEX. **Missão, Visão e Valores.** 2020. Disponível em

<http://www.citex.eb.mil.br/index.php/editoria-b>. acessado em 01 Ago 2020.

FERGUSON, Bill. **VCP5-DCV Official Certification Guide: VMware Certified Professional 5 – Data Center Virtualization** – 2nd Edition. VMware Press Technology, 2014.

FERNANDES, Rafael Silva; NUNO, Claudinei Di. **Virtualização De Servidores**. 2018. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 03, Ed. 04, Vol. 05, pp. 34-44. ISSN:2448-0959. Disponível em: <https://www.nucleodoconhecimento.com.br/tecnologia/virtualizacao-de-servidores>. Acesso em: 02 jul 2020.

ISO/IEC 17799. **Tecnologia da Informação: Código de Prática para Gestão da Segurança de Informações**. 2000.

KUROSE, James F.; ROSS, Kevin. W. **Redes de computadores e a Internet: umaabordagem top-down.** 6th. ed. [S.l.]: Pearson Education do Brasil., 2013. ISBN9788543014432.

LAUREANO, Marcos Aurelio Pchek; MAZIERO, Carlos Alberto. **Virtualização: Conceitos E Aplicações Em Segurança.** 2008. Disponível em: <http://wiki.inf.ufpr.br/maziero/lib/exe/fetch.php?media=research:2008-sbseg-mc.pdf>. Acesso em: 28 jun 2020.

LIRA, Rodrigo. **Instalação do VMware ESXi 6.5.** 2016. Disponível em <https://rodrigolira.eti.br/instalacao-do-vmware-esxi-6-5/> Acesso em: 25 ago 2020.

LOTTI , Luciane Politi; PRADO, Alysson Bolognesi. **Sistemas Virtualizados – Uma Visão Geral.** 2011. Disponível em: <https://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G09_012096_931544-t2.pdf>. Acesso em: 08 jul 2020.

MACEDO, A. S.; SANTOS, C. C. G. **Hypervisor: Segurança em ambientes virtualizados**. 2014. Revista Infra Magazine Ed. 17.

MARSHALL, David, REYNOLDS, Wade A, MCCRORY, Dave. **Advanced server virtualization – Vmware and Microsoft Platforms in the Virtual Data Center.** Auerbach Publications, 2006.

MATTOS, D. M. F. **Virtualização: VMWare e Xen**. Universidade Federal do Rio de Janeiro. 2008.

NIEH J.; LEONARD O. **Examining VMWare.** Dr. Dobb's Journal, August 2000. Disponível em: <http://www.cs.columbia.edu/~nieh/pubs/drdobbs2000.pdf> Acesso em: 28 jul 2020.

POPEK, Gerald J.; GOLDBERG, Robert P. **Formal requirements for virtualizable third generation architectures. 1974.** Communications of ACM, July 1974, Volume 17, Number 7.

SAHOO J.; MOHAPATRA S.; LATH R. **Virtualization: A survey on concepts, taxonomy and associated security issues.** In: Second International Conference on Computer and Network Technology, p.222-226, April 23-25, 2010.

SEO C.E. VIRTUALIZAÇÃO – **Problemas e desafios.** IBM Linux Technology Center,

2009. Disponível em: <http://www.ic.unicamp.br/~ducatte/mo401/1s2009/T2/008278-t2.pdf>.

SILVA, Rodrigo Ferreira da. **Virtualização De Sistemas Operacionais**. 2007. Disponível em: <https://www.lncc.br/~borges/doc/Virtualizacao%20de%20Sistemas%20Operacionais.TCC.pdf>. Acesso em: 27 jun 2020.

SMITH, J. E.; NAIR, R. **The architecture of virtual machines.** 2005. IEEE Computer, pages 32–38. Disponível em: <https://web.stanford.edu/group/comparch/papers/Computer_SmithNair.pdf >. Acesso em: 09 jul 2020.

TANENBAUM, Andrew S.;WETHERALL, David. **Redes de Computadores**.5th. ed. [S.l.]: Pearson Education do Brasil. 2011.

VERAS, Manuel. **Virtualização: componente central do datacenter**. 2011. Rio de Janeiro. Ed: Brasport Livros e Multimídia Ltda.

VMWARE INC. **Gerenciamento da virtualização**. 2020. Disponível em: <https://www.vmware.com/br/solutions/virtualization/virtualization-management.html> Acesso em 12 jun 2020.

_____. **Linha do tempo da VMware**. 2020. Disponível em: <https://www.vmware.com/br/timeline.html > Acesso em 10 jun 2020.

_____. **Virtualization for Desktop & Server, Application, Public & Hybrid Clouds.** 2014.

_____. **Introduction to vSphere Installation and Setup**. 2020. Disponível em: <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.install.doc/GUID-A71D7F56-6F47-43AB-9C4E-BAA89310F295.html> Acesso em 25 ago. 2020.