



**FACULDADE DE TECNOLOGIA DE AMERICANA
SEGURANÇA DA INFORMAÇÃO**

JOÃO FLAVIO DINIZ

**SEGURANÇA EM SISTEMAS VIRTUALIZADOS PARA
EMPRESAS DE PEQUENO PORTE**

Americana, S. P.

2016



**FACULDADE DE TECNOLOGIA DE AMERICANA
SEGURANÇA DA INFORMAÇÃO**

JOÃO FLAVIO DINIZ

**SEGURANÇA EM SISTEMAS VIRTUALIZADOS PARA
EMPRESAS DE PEQUENO PORTE**

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior em Segurança da informação, sob a orientação da Prof.^o Esp. Ricardo Kiyoshi Batori
Área de concentração: Segurança da Informação

Americana, S. P.

2016

**FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte**

D611s	<p>DINIZ, João Flavio Segurança em sistemas virtualizados para empresas de pequeno porte. / João Flavio Diniz. – Americana: 2016. 44f.</p> <p>Monografia (Curso de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza. Orientador: Prof. Esp. Ricardo Kiyoshi Batori</p> <p>1. Segurança em sistemas de informação I. BATORI, Ricardo Kiyoshi II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.</p> <p>CDU: 681.518.5</p>
-------	---

JOÃO FLÁVIO DINIZ

**SEGURANÇA EM SISTEMAS VIRTUALIZADOS PARA
EMPRESAS DE PEQUENO PORTE**

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Segurança da Informação

Americana, 07 de Dezembro de 2016.

Banca Examinadora:



RICARDO KIYOSHI BATORI

Especialista


Faculdade de Tecnologia de Americana – FATEC/Americana



JOSÉ LUIZ ZEM

Doutor

Faculdade de Tecnologia de Americana – FATEC/Americana



VALDECI OTACILIO DOS SANTOS

Mestre

Faculdade de Tecnologia de Americana – FATEC/Americana

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus por me dar forças para continuar a jornada na conclusão deste curso.

Agradeço ao meu orientador professor Esp. Ricardo Kiyoshi Batori pelo apoio e dedicação com que me ajudou a concluir este trabalho, a nossa coordenadora Dra. Maria Cristina Aranda pela ajuda e esclarecimentos de nossas dúvidas e a todos os meus professores pela paciência, dedicação, amizade, e pelo empenho com que nos guiaram na conclusão desta etapa.

Gostaria de agradecer também a meu amigo e parceiro de estudos Alcindo Facioli que me acompanhou durante este percurso me apoiando durante as muitas horas de estudos dedicados para a conclusão desta jornada.

DEDICATÓRIA

A minha família pelo apoio que me motivou a continuar, compreensão nos momentos em que estive ausente e pela paciência durante toda a minha jornada.

RESUMO

A virtualização é uma realidade cada vez mais presente no ambiente empresarial, pois, esta técnica permite a utilização de vários sistemas operacionais a partir de uma única máquina física e traz muitos benefícios a quem a utiliza. Novos serviços podem ser oferecidos aos usuários, mas junto com tantas vantagens surge também vários perigos e vulnerabilidades. As redes formadas por essas máquinas virtuais estão sujeitas aos mesmos riscos e vulnerabilidades que as redes físicas, e devem ser protegidas com ferramentas desenvolvidas para esses ambientes. O desafio é proteger a informação a um custo acessível e garantir pelo menos os três pilares básicos da segurança da informação: confidencialidade, integridade e disponibilidade. Diante de todas as ameaças, os fabricantes de antivírus travam verdadeiras batalhas para criar ferramentas de combate aos novos códigos maliciosos desenvolvidos especificamente para atacar os ambientes virtuais. Atualmente existem diversas soluções oferecidas para as organizações com o intuito de proteger os ativos de informação, mas o preço não é um fator muito amigável e as pequenas empresas geralmente não podem arcar com estes altos custos. Mas nem tudo está perdido, existem soluções muito eficientes que proporcionam muitos recursos de segurança com políticas personalizadas e eficientes, além de serem fáceis de implantar no ambiente da empresa, que no geral, já está funcionando. A proposta apresentada neste trabalho, além de apresentar custo acessível, não demanda a alteração de nenhuma máquina ou serviço, somente precisa instalar um *appliance* virtual de um servidor de segurança centralizada SVA na rede e um *Endpoint* nas máquinas virtuais que se deseja proteger, configurar a política de segurança desejada em um console de gerenciamento online e os serviços já são incorporados ao ambiente da empresa.

Palavras Chave: Virtualização; segurança em redes virtuais; hipervisor; máquina virtual

ABSTRACT

Virtualization is a reality increasingly present in the business environment because, this technique allows the use of several operational systems from of a single physical machine and brings many benefits whom the uses. New services can be offered customers, but along with so many advantages arises also several dangers and vulnerabilities The networks formed for these virtual machines are subject to the same risks and vulnerabilities the physical networks, and must be protected with tools developed for these environments. The challenge is to protect the information at a cost accessible and ensure at least the three basic pillars of information security confidentiality, integrity and availability. Before all these threats manufacturers of antivírus true lock battles for create tools to combat the new malicious codes developed specifically to attack the virtual environments. Currently there are several solutions offered to organizations with the aim of protect the assets of information, but the price is not a fator very user friendly and small company generally can't afford with these high costs. But not everything is lost, there are solutions very eficiente that provide many features with security custom policies and efficient, In addition to being easy to deploy in the company's environment, that in general, is already running. The proposal presented in this work, in addition to presente affordable, don't demand change of any machine or service, only need to install a virtual appliance from a server of security centered SVA on the network and an Endpoint on the virtual machines that if you want to protect, Configure the security policy you want in a console of management online and the services are already incorporated into the company's environment.

Keywords: *virtualization; security of virtual environments; hypervisor; virtual machine.*

LISTA DE FIGURAS

Figura 1: Virtualização de servidores.....	7
Figura 2: Virtualização de desktops.....	8
Figura 3: Virtualização de aplicativos.....	9
Figura 4: Virtualização total.....	10
Figura 5: Paravirtualização	11
Figura 6: Máquina virtual de processo.....	12
Figura 7: Hipervisores do tipo I e II.....	13
Figura 8: Componentes do Xen hipervisor e domínios.....	18
Figura 9: Plataforma GravityZone SVE.....	28
Figura 10: Diagrama esquemático da rede virtual.....	29
Figura 11: Plataforma de virtualização VMware ESXi.....	31
Figura 12: Console de gerenciamento vSphere Client.....	32
Figura 13: Console de gerenciamento online Bitdefender GravityZone.....	32
Figura 14: Configurações da rede do SVA.....	33
Figura 15: Endereço web da console Bitdefender GravityZone.....	33
Figura 16: Pacotes de Endpoint.....	34
Figura 17: Máquinas virtuais no console de gerenciamento.....	35
Figura 18: Monitoramento dos Endpoints da rede virtual.....	35
Figura 19: Relatório de atividades Malware.....	36
Figura 20: Política de bloqueio da Internet.....	37
Figura 21: Política de liberação da Internet.....	37
Figura 22: Relatório de escaneamento inicial da VM com Windows 8 PRO.....	38
Figura 23: Aproveitamento do cache da VM Windows 8 PRO.....	38
Figura 24: Escaneamento da VM Windows 8 PRO sem o servidor SVA.....	39
Figura 25: Monitoramento do SVA.....	39
Figura 26: Monitoramento dos Endpoints.....	40
Figura 27: Monitoramento do status da rede.....	40

LISTA DE TABELAS

Tabela 1: Descrição das configurações das máquinas virtuais.....	30
---	----

LISTA DE SIGLAS

ABI: Application Binary Interface

API: Application Programming Interface

DLL: Dynamic Link Library

ES: Entrada e saída

GPL: General Public License

ISA: Industry Standard Architecture

JVM: Java Virtual Machine

SVA: Security Virtual Appliance

SVE: Security for Virtualized Environments

TCP: Transmission Control Protocol

TI: Tecnologia da Informação

VM: Virtual Machine

VME: Virtual Machine Escape

VMM: Virtual Machine Monitor

SUMÁRIO

1 INTRODUÇÃO	1
2 VIRTUALIZAÇÃO	3
2.1 HISTÓRICO	3
2.2 CARACTERÍSTICAS DOS SISTEMAS OPERACIONAIS.....	3
2.3 O SISTEMA OPERACIONAL COMO MÁQUINA VIRTUAL	4
2.4 VANTAGENS E DESVANTAGENS DA VIRTUALIZAÇÃO	5
2.5 TIPOS DE VIRTUALIZAÇÃO	6
2.5.1 Virtualização de servidores	6
2.5.2 Virtualização de desktops	7
2.5.3 Virtualização de aplicativos.....	8
2.6 TÉCNICAS DE VIRTUALIZAÇÃO.....	9
2.6.1 Virtualização total.....	9
2.6.2 Paravirtualização.....	10
3 MÁQUINAS VIRTUAIS	11
3.1 MÁQUINA VIRTUAL DE PROCESSO	11
3.3 HIPERVISOR	14
3.4 FERRAMENTAS DE VIRTUALIZAÇÃO.....	14
3.4.1 VMware.....	14
3.4.2 Microsoft Hyper-V	16
3.4.3 XenServer	17
4 SEGURANÇA EM REDES DE COMPUTADORES	19
4.1 SEGURANÇA DA INFORMAÇÃO	19
4.2 POLÍTICAS DE SEGURANÇA.....	20
4.3 NECESSIDADE DE SEGURANÇA.....	21
4.4 AMEAÇAS ÀS REDE DE COMPUTADORES.....	21
4.4.1 Vulnerabilidades.....	21
4.4.2 Tipos de ataques.....	22
4.4.3 Ameaças a ambientes virtualizados.....	22
4.4.5 Vírus.....	24

4.4.6 Worm	24
4.5 FERRAMENTAS DE PROTEÇÃO	25
4.5.1 Antivírus	25
4.5.2 Firewall.....	25
4.5.3 Proxy	25
4.5.4 Sistema de Detecção de Intrusão	26
4.5.5 VMware vShield Endpoint	26
4.6 FERRAMENTA PARA PROTEÇÃO DE REDES VIRTUALIZADAS.....	26
5 ESTUDO DE CASO	29
5.1 IMPLANTAÇÃO.....	31
5.2 TESTES E ANÁLISE DOS RESULTADOS	36
6 CONSIDERAÇÕES FINAIS	41

1 INTRODUÇÃO

Um sistema operacional tradicional é baseado há algum tempo no modelo *hardware*, sistema operacional e aplicações, assim sendo, neste modelo uma aplicação só executa sobre o sistema operacional para a qual foi projetada. Desta forma o usuário é obrigado a utilizar um sistema operacional sobre determinado *hardware* para usar as aplicações que deseja (SILVA, 2007).

A virtualização surge como uma provável solução, apesar de já existir desde a época do *mainframe* da IBM na década de 70. Esta técnica vem ganhando força com o crescente aumento da capacidade computacional por apresentar inúmeras vantagens principalmente financeiras.

A medida que a tecnologia evolui aparecem novos serviços para ser disponibilizados aos usuários, mas, com esses serviços surgem também novas ameaças e vulnerabilidades, nesse cenário a segurança da informação é de primordial importância para a proteção dos dados das empresas e seus clientes (NAKAMURA; GEUS, 2010).

A segurança tem o papel de prevenir que alguma coisa errada venha a acontecer na infraestrutura tecnológica da organização. Na verdade, ninguém percebe a existência da segurança, mas percebe a sua falta, quando acontece algum incidente e resulta em prejuízos financeiros para a organização. O ideal é que a segurança seja um processo transparente para a organização e também deve ser avaliado não somente se existe segurança, mas em que nível essa segurança se encontra (NAKAMURA; GEUS, 2010).

Existem códigos maliciosos desenvolvidos especificamente para ambientes virtualizados que conseguem sobreviver até mesmo a uma formatação do ambiente virtual. Um ambiente virtual deve ser protegido por soluções de segurança desenvolvidas especialmente para sistemas virtuais (ASSOLINI, 2012).

O objetivo geral deste trabalho é propor a implantação de uma ferramenta de baixo custo como uma alternativa à segurança da informação para empresas de pequeno porte que se utilizam de sistemas virtualizados, e que não dispõem de muitos recursos de *hardware* ou financeiros para implantar um sistema de segurança capaz de proteger adequadamente os ambientes virtuais. A proposta visa

mostrar uma das soluções existentes, que estão disponíveis no mercado atualmente e que ainda não estão bem difundidas.

O objetivo específico deste trabalho é implantar uma plataforma de virtualização para criar uma rede de máquinas virtuais, simulando um ambiente corporativo, a fim de implementar uma solução de segurança através de um servidor de segurança centralizada (SVA), que se utiliza de um console em nuvem para criar e gerenciar políticas de segurança, e desta forma, realizar alguns testes com esta ferramenta e analisar os resultados obtidos.

O método científico utilizado foi a pesquisa em livros, teses de mestrado e doutorado, artigos científicos e pesquisas na Internet em *sites* especializados, além dos *sites* dos fabricantes das principais plataformas de virtualização e fabricantes de antivírus atuais.

Este trabalho foi estruturado da seguinte forma, no capítulo 2 é apresentado um breve resumo do histórico da virtualização, os aspectos dos sistemas operacionais, além das vantagens e desvantagens da utilização da virtualização. O capítulo 3 conceitua os tipos de virtualização assim como suas principais técnicas, e também apresenta os tipos de máquinas virtuais, apresenta o hipervisor e as principais ferramentas de virtualização usadas atualmente. O capítulo 4 conceitua as redes de computadores, *firewall*, *proxy*, *vírus*, *worms*, sistema de detecção de intrusão, mostra as ameaças aos sistemas virtualizados e apresenta uma ferramenta para proteção de ambientes virtuais. O capítulo 5 mostra a implantação e a análise de resultados dos testes realizados na solução de segurança sugerida, a qual oferece diversos recursos de gerenciamento centralizado com um baixo custo. Finalmente no capítulo 6 são apresentadas as considerações finais e a conclusão do trabalho.

2 VIRTUALIZAÇÃO

A virtualização permite que em uma mesma máquina sejam executadas simultaneamente dois ou mais sistemas operacionais distintos e isolados.

2.1 HISTÓRICO

A ideia de máquina virtual já é antiga, nos anos 70 era muito comum que cada computador (*mainframe*), mesmo que fosse de um único fabricante, possuísse um sistema operacional próprio, isso, causava problemas de portabilidade e de sistemas legados (CARISSIMI, 2008).

Na década de 60 a IBM deu os primeiros passos na construção de máquinas virtuais, desenvolvendo o sistema operacional experimental M44/44X. A partir deste, a IBM desenvolveu vários sistemas comerciais com suporte à virtualização, entre os quais o famoso OS/370 (GOLDBERG, 1973) e Goldberg e Mager (1979) *apud* Laureano e Maziero (2014).

A virtualização de plataforma ou sistema, tornou-se popular na década de 60 através da IBM. Neste tipo de virtualização, a plataforma de *hardware* é virtualizada para compartilhar os recursos com outros sistemas operacionais e usuários distintos. Na década de 80 com o surgimento das plataformas de *hardware* baratas como o PC, a virtualização perdeu importância, pois, era mais barato, fácil e prático fornecer um computador completo para cada usuário do que investir em sistemas de grande porte complicados e complexos. Com a grande procura por serviços e performance da atualidade, as máquinas virtuais estão de volta novamente dentro do ambiente corporativo dos departamentos de tecnologia da informação das pequenas e médias empresas, devido as grandes vantagens oferecidas pela virtualização (LAUREANO; MAZIERO, 2014).

2.2 CARACTERÍSTICAS DOS SISTEMAS OPERACIONAIS

Qualquer usuário que utiliza um computador, de alguma forma sabe da existência de um sistema operacional que controla os diversos dispositivos de

hardware que o compõem. A definição mais comum para sistema operacional, encontrada em alguns livros, é a de uma camada de *software* entre o *hardware* e os programas que executam as tarefas dos usuários e cuja função é facilitar o uso do computador (SILBERSCHATZ, 2001) *apud* Carissimi (2008).

Segundo Carissimi (2008) o conceito fundamental de sistemas operacionais é o de processo, o qual é uma abstração que representa um aplicativo em execução. O sistema operacional é organizado em camadas hierárquicas, com diferentes níveis e interfaces, que simula o funcionamento do *hardware* e torna mais agradável o uso do sistema operacional.

Os sistemas operacionais e aplicativos podem ser executados em máquinas virtuais, da mesma forma como são executados em uma máquina física. Possuem *hardwares* próprios como placa de rede, memória e outros dispositivos, porém, são arquivos comuns, de tamanho reduzido e portáteis, facilitando a cópia para outros locais (VMWARE, [200?]) *apud* Bosing e Kaufmann (2010).

2.3 O SISTEMA OPERACIONAL COMO MÁQUINA VIRTUAL

O sistema operacional é simplesmente um *software* que funciona sobre um determinado *hardware* para gerar um ambiente computacional, assim definido por (CARISSIMI; OLIVEIRA & TOSCANI, 2010).

Um sistema operacional nada mais é que um *software* que executa sobre um determinado *hardware* com o objetivo de controlar seus recursos e oferecer um ambiente de execução para os programas aplicativos. Esse ambiente, definido no momento da criação do processo, é composto por um espaço de endereçamento, contendo as instruções do programa de usuário a serem executadas, e por uma versão lógica (virtual) dos registradores do processador real. Quando um processo é posto em execução pelo escalonador do sistema operacional, os valores dos registradores lógicos são atribuídos aos registradores reais e assim o programa é executado. Isso equivale a imaginar que cada vez que um processo é criado, o sistema operacional atribui a ele um processador virtual.

Ainda de acordo com Carissimi (2008) além de virtualizar o processador, o sistema operacional oferece para os processos de usuário uma abstração dos recursos de *hardware* através do subsistema E/S e do sistema de arquivos. Em um

sistema Unix, por exemplo, o subsistema de E/S classifica os dispositivos em orientados a bloco, orientados a caractere e rede.

2.4 VANTAGENS E DESVANTAGENS DA VIRTUALIZAÇÃO

O uso da virtualização traz vários benefícios como: a redução de custos com dispositivos de rede, energia elétrica e refrigeração, otimização de processos com alta confiabilidade, consolidação, performance, escalabilidade e a simplificação do ambiente, além de contribuir com a tecnologia da informação (TI) verde, com a redução do consumo de energia, reduz também a emissão de gás carbônico na atmosfera (COELHO, 2009).

A Disponibilização de novos servidores é feita em alguns minutos sendo possível migrar um servidor para um novo *hardware* de forma simplificada ou recuperar um servidor em caso de desastre reduzindo o tempo de *downtime* (tempo de paralisação dos serviços), pois com a facilidade de migrar os ambientes, não é necessário a reinstalação e reconfiguração dos sistemas (DEVEL, 200?).

Através da virtualização é possível usar máquinas virtuais para definir a plataforma mais adequada à execução de um determinado serviço ou sistema operacional, pois, uma falha em um *software* não afeta os demais, já que as máquinas virtuais são isoladas entre si (MATTOS, 2008). Ainda de acordo com o autor utilizar um servidor mais robusto para virtualizar vários pequenos servidores, reduz bastante os custos, além disso, como as máquinas virtuais são isoladas é fácil trocá-las de plataforma para balancear a rede e aumentar a performance.

Quando uma empresa resolve atualizar seu hardware e trocar o sistema operacional para uma versão mais nova, alguns *softwares* mais antigos podem não funcionar mais. A virtualização é útil nesses casos, pois, permite rodar as aplicações que executavam em *hardwares* antigos sujeitos a falhas, em máquinas virtuais executando sobre um *hardware* mais novo e de maior confiabilidade (MATTOS, 2008).

As máquinas virtuais podem ser independentes e ficar isoladas entre si, inclusive da máquina hospedeira. Com menos dispositivos físicos para gerenciar, melhora o aproveitamento dos espaços em *hacks*, além da redução em custos com pessoal, energia elétrica e refrigeração. A virtualização permite aproveitar melhor a

máquina hospedeira, compartilhando seus recursos com as máquinas virtuais e reduzindo dessa forma a ociosidade do equipamento (DEVEL, 200?).

Toda tecnologia por melhor que seja, está sujeita a apresentar algumas desvantagens, a virtualização não é diferente e possui algumas desvantagens. Segundo Prado (2010) *apud* Bosing e Kaufmann (2010), verifica-se: a dificuldade para acessar o *hardware*; consumo elevado de memória RAM em decorrência do uso da mesma pelas máquinas virtuais; uma vez que um mesmo equipamento físico executará diversas máquinas virtuais, a segurança precisa ser aumentada.

De acordo com Mattos (2008), a virtualização apresenta algumas desvantagens com relação a segurança, pois, caso o sistema operacional hospedeiro possuir alguma vulnerabilidade, todas as máquinas virtuais hospedadas estarão vulneráveis. Os ambientes virtuais necessitam ser instanciados, monitorados, configurados e salvos, devido a grande facilidade e rapidez que são criados. Com a introdução de uma camada extra de *software* entre o sistema operacional e o *hardware*, o hipervisor, usa mais processamento do que sem a virtualização.

2.5 TIPOS DE VIRTUALIZAÇÃO

Existem basicamente três tipos de soluções em virtualização que são: virtualização de servidores, *desktops* e aplicativos.

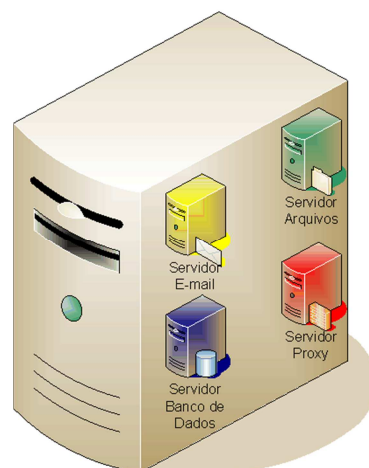
2.5.1 Virtualização de servidores

A virtualização de servidores é motivada pelos seguintes benefícios: o aumento da taxa de uso do *hardware* dos servidores, redução de custos operacionais com *data centers*, melhoria dos procedimentos na recuperação de desastres e de *backup* (CARISSIMI, 2008). O autor afirma ainda que este tipo de virtualização aproveita melhor os recursos, em vez de possuir vários servidores com um baixo percentual de uso dos recursos, é possível ter somente um equipamento com vários servidores virtuais instalados, rodando quantos serviços sua capacidade total de processamento possa suportar.

Este tipo de virtualização apresenta como propriedade, o isolamento de falhas e segurança de *hardware* e os controles de recursos avançados que preservam o desempenho, assim, se uma empresa possuir um servidor rodando três servidores virtuais, no caso de uma dessas máquinas virtuais falhar, não vai afetar as outras máquinas virtuais dentro desse servidor. Existe também o isolamento, que possibilita salvar todo o estado da máquina virtual em arquivos. Como a máquina virtual é controlada e encapsulada em arquivos, então, é possível mover uma máquina virtual de um local para outro fazendo um *backup* ou uma migração (FAGUNDES; VICENTE & PRATES, 2015).

A Figura 1 ilustra o aproveitamento de recursos através da virtualização de um servidor físico em quatro servidores virtuais sendo um servidor de e-mail, servidor de arquivos, servidor de banco de dados e servidor *proxy*.

Figura 1 Virtualização de Servidores.



Fonte: Universidade Federal do Rio de Janeiro

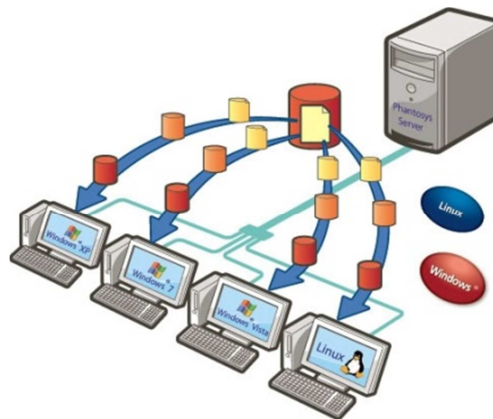
2.5.2 Virtualização de desktops

Esta técnica apresenta as mesmas vantagens da virtualização de servidores, pois, esta última também pode ser usada em *desktops*. Este tipo de virtualização oferece uma maneira segura de testar novas configurações e programas que foram desenvolvidos para executar sobre outras plataformas diferentes da nativa na máquina física. Assim, o desenvolvedor pode usar este recurso para executar seu *software* em versões diferentes de sistemas operacionais. Outra aplicação interessante é o uso em instituições de ensino, que com o uso deste tipo de

virtualização, a instituição pode oferecer um ambiente diversificado de sistemas operacionais e serviços sem comprometer suas máquinas com ameaças originadas por vírus, cavalo de troia e todo tipo de *malware* (CARISSIMI; OLIVEIRA & TOSCANI, 2010).

A Figura 2 ilustra uma virtualização de *desktops* com diferentes sistemas operacionais rodando no mesmo servidor físico.

Figura 2 Virtualização de *Desktops*



Fonte: Pulse Ti.

2.5.3 Virtualização de aplicativos

A virtualização de aplicativos tem como característica copiar todas as aplicações dos recursos compartilhados, fazendo com que não haja necessidade de instalar vários programas para executar os aplicativos em conflitos.

A técnica consiste em ter uma única cópia de determinado aplicativo, instalada em um servidor virtual; usuários que desejarem ter acesso a tal aplicativo podem fazê-lo diretamente, sem a necessidade de que ele também esteja instalado na máquina física.

Assim transformando um programa em um arquivo em que possa ser executado sem a necessidade de usar vários arquivos de DLLs. A virtualização de aplicativos usa um sistema não físico, mas sim virtual para resolver e corrigir falhas de certos programas em conflito, dando assim uma solução virtual. A grande vantagem deste tipo de virtualização é de ordem econômica devido ao uso de apenas uma licença do *software*, além de evitar a incompatibilidades dos aplicativos (FAGUNDES; VICENTE & PRATES, 2015).

A Figura 3 mostra a virtualização de aplicativos.

Figura 3 Virtualização de aplicativos



Fonte: SlideShare

2.6 TÉCNICAS DE VIRTUALIZAÇÃO

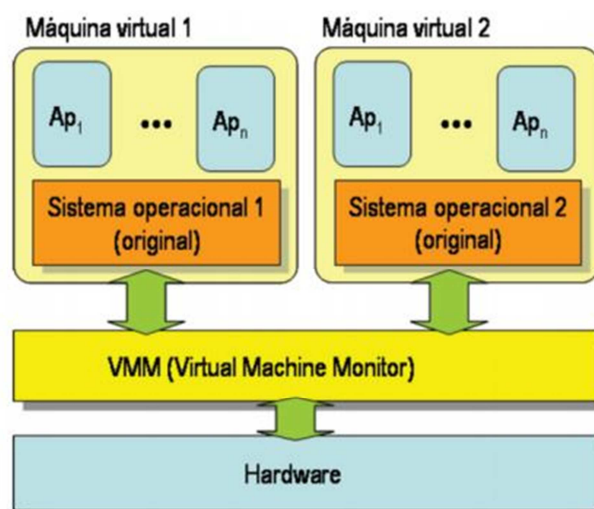
Os monitores de máquinas virtuais (VMM) podem ser implementados basicamente através das técnicas de virtualização total e paravirtualização.

2.6.1 Virtualização total

Na virtualização total, todos os *softwares* podem ser executados sem nenhuma alteração, pois, o *hardware* é simulado por completo, sendo assim, todos os sistemas operacionais podem ser executados sem nenhum problema. A virtualização total faz uma simulação para reproduzir as instruções do processador, a memória principal, ou o acesso aos outros dispositivos existentes (MACAGNANI, 2009).

A virtualização total oferece ao sistema operacional visitante uma réplica do *hardware* subjacente, em contrapartida, o sistema virtualizado funciona lentamente e o monitor das máquinas virtuais tem que implementar alternativas para que as operações privilegiadas sejam executadas em processadores sem suporte à virtualização nativa.

Figura 4 Virtualização total.



Fonte: Carissimi (2009)

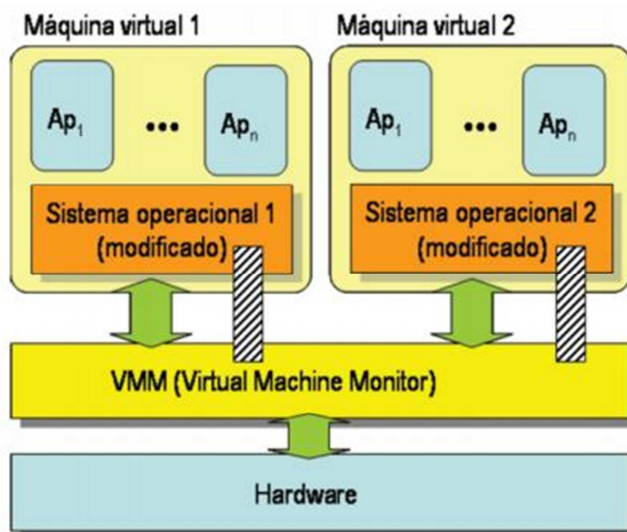
2.6.2 Paravirtualização

Na paravirtualização, o sistema convidado, deve ser modificado para interagir com o monitor de máquinas virtuais. Apesar de esta modificação reduzir a portabilidade do sistema, a paravirtualização permite que máquinas virtuais se comuniquem diretamente com o *hardware* (SILVA, 2007). O autor alega ainda que ao invés de todas as máquinas virtuais se comunicarem com o sistema anfitrião, é a máquina privilegiada que gerência a interação e recebe as chamadas passadas pelos outros sistemas virtuais.

Na paravirtualização, os dispositivos de *hardware* são utilizados em sua capacidade total, pois são acessados por *drivers* da própria máquina virtual, o que dispensa utilização de *drivers* genéricos para o seu funcionamento. O ganho de desempenho é o principal fator para que se opte por utilizar a paravirtualização (LAUREANO, 2006).

A paravirtualização explora de maneira apropriada os recursos disponíveis pelo *hardware* real da máquina, além de apresentar um melhor desempenho comparado com a virtualização total. Esse ganho de desempenho significativo frente à virtualização total tem sido superado devido à presença de instruções de virtualização nos processadores Intel e AMD, os quais favorece a virtualização total (MATTOS, 2008).

Figura 5 Paravirtualização.



Fonte: Carissimi (2009)

3 MÁQUINAS VIRTUAIS

De acordo com (CARISSIMI; OLIVEIRA & TOSCANI, 2010), uma máquina virtual é um ambiente completo que prove suporte para execução de diversas aplicações conhecidos como processos. O processo ou sistema operacional que executa sobre uma máquina virtual é denominado de hóspede ou convidado, enquanto que a plataforma subjacente na qual a máquina virtual executa, é denominada de hospedeiro ou sistema nativo. A camada de virtualização que implementa a máquina virtual é genericamente denominada de *runtime* (ou executivo) para as máquinas virtuais de processo, e de monitor de máquina virtual (VMM) ou Hipervisor (*hypervisor*), para as máquinas virtuais de sistema.

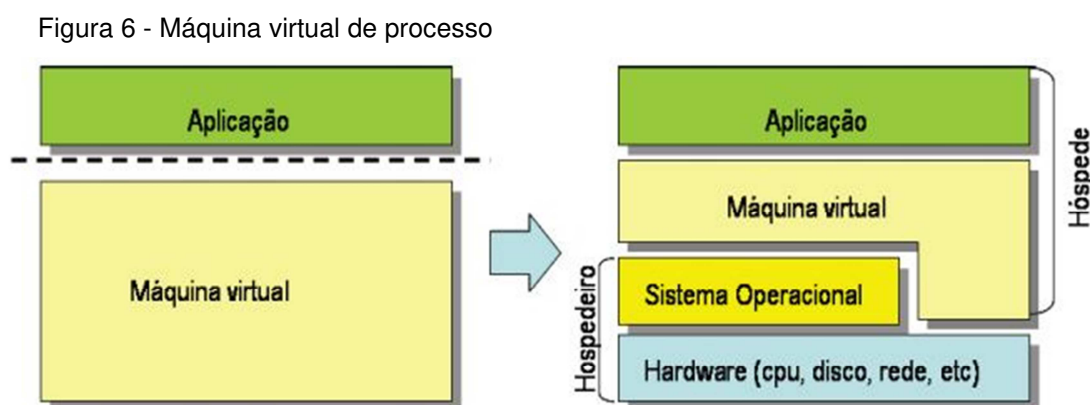
3.1 MÁQUINA VIRTUAL DE PROCESSO

“Uma máquina virtual de processo é aquela que fornece um ambiente de execução para uma única aplicação de usuário através de uma ABI virtual (chamadas de sistema e user ISA)” (CARISSIMI; OLIVEIRA & TOSCANI, 2010).

Um processo é uma entidade temporária existindo apenas enquanto o programa está em execução. Sendo assim, uma máquina virtual de processo é

criada sob demanda e deixa de existir quanto o processo for finalizado. A máquina virtual utiliza as funcionalidades providas pelo sistema operacional como chamadas de sistema e funções de biblioteca e pelo próprio processador através de instruções não privilegiadas. A aplicação emprega apenas a interface (ABI) provida pelo ambiente (máquina) virtual (CARISSIMI; OLIVEIRA & TOSCANI, 2010).

Na Figura 6, uma aplicação executa sobre um programa que implementa a máquina virtual de processo (*runtime* ou executivo).



Fonte: Carissimi (2009)

Um desafio importante na concepção de máquinas virtuais de processo é quando a aplicação hóspede possui um código binário incompatível com o processador do hospedeiro. A maneira mais direta de resolver isso é através de um programa interpretador que realiza um ciclo de busca de instrução, decodificação e emulação dessa instrução para o sistema hospedeiro (CARISSIMI; OLIVEIRA & TOSCANI, 2010).

Um exemplo típico dessa abordagem é a linguagem de programação *Java* e de sua máquina virtual (Java Virtual Machine - JVM). A JVM é uma máquina virtual de processo que possui um código binário específico, os *bytecodes*, para os quais uma aplicação *Java* é compilada. A máquina virtual *Java* interpreta, *bytecode* a *bytecode*, transformando-os em ações e instruções equivalentes da máquina real subjacente (hospedeiro), a vantagem desse método é a portabilidade, mas o processo de interpretação apresenta baixo desempenho (CARISSIMI; OLIVEIRA & TOSCANI, 2010).

3.2 Máquina virtual de sistema

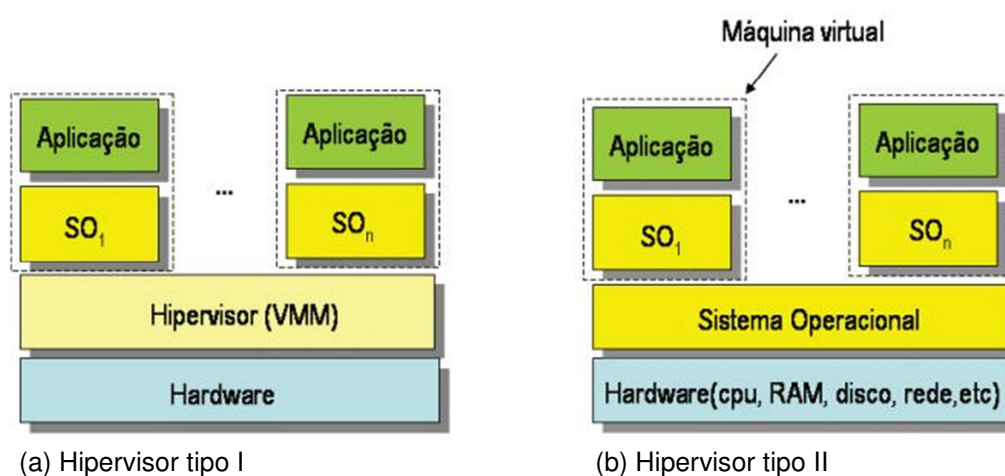
Uma máquina virtual de sistema oferece um ambiente de execução completo no qual podem coexistir um sistema operacional e vários processos, possivelmente de diferentes usuários. Dessa forma, uma única plataforma de *hardware* pode executar múltiplos sistemas operacionais hóspedes, um em cada máquina virtual, simultaneamente. É esse tipo de abordagem que permite a consolidação de servidores (CARISSIMI; OLIVEIRA & TOSCANI, 2010).

Existem duas formas básicas de implementação de máquinas virtuais de sistema ou hipervisores (GOLDBERG, 1973) *apud* Carissimi (2010). Os hipervisores tipo I, ou nativos, executam diretamente sobre o *hardware* de uma máquina real e as máquinas virtuais são colocadas sobre ele.

O hipervisor tipo I ou nativo, que compartilha os recursos de *hardware* (processador, memória, meios de armazenamento e dispositivos de E/S) entre as diferentes máquinas virtuais de forma que cada uma delas tenha a ilusão de que esses recursos são privativos a ela (CARISSIMI; OLIVEIRA & TOSCANI, 2010).

Os hipervisores tipo II, ou hóspedes, são caracterizados por executar sobre um sistema operacional nativo como se fossem um processo deste, a Figura 7 (a) apresenta a estrutura de um hipervisor do tipo I e a Figura 7 (b) apresenta a estrutura de um hipervisor do tipo II.

Figura 7 Hipervisores do tipo I e II



(a) Hipervisor tipo I

(b) Hipervisor tipo II

Fonte: Carissimi; Oliveira & Toscani (2010)

3.3 HIPERVISOR

O hipervisor também chamado de Monitor de Máquina Virtual (VMM), nada mais é do que uma camada de *software* localizada entre o *hardware* e o sistema operacional, a qual fornece ao sistema operacional visitante uma abstração da máquina virtual. É função do hipervisor controlar o acesso dos sistemas operacionais visitantes aos dispositivos de *hardware*, o mesmo não pode ser executado em modo usuário, pois, deve simular a execução das instruções privilegiadas requisitadas pelo sistema operacional visitante (MATTOS, 2008).

O hipervisor retoma o controle do processador apenas quando a máquina virtual tentar executar operações que possam prejudicar o funcionamento do sistema, o conjunto de operações de outras máquinas virtuais ou do próprio *hardware*. O hipervisor precisa simular com segurança a operação solicitada e devolver o controle à máquina virtual (LAUREANO; MAZIERO, 2014).

3.4 FERRAMENTAS DE VIRTUALIZAÇÃO

A virtualização tornou-se uma revolução na área de TI ultimamente, basta observar o enorme volume de investimentos nessa área e o crescimento das empresas de soluções para virtualização. Para a elaboração deste trabalho optou-se por apresentar as principais ferramentas de virtualização que dominam o mercado da virtualização atualmente como VMware, Hyper-V e XenServer.

3.4.1 VMware

O VMware é um dos aplicativos de virtualização para plataforma x86 uma das mais populares atualmente. Ele surgiu em 1999 e foi a primeira solução de virtualização desenvolvida para a arquitetura x86 a fornecer uma implementação completa para o sistema convidado. A VMware Inc., desenvolvedora do *software*, disponibiliza vários produtos destinados a virtualização e também possui algumas versões de seus produtos isenta de custos com licenciamento, mas estas versões, geralmente, possuem alguma limitação (VMWARE, 2010).

O VMware fornece soluções para virtualização que vai desde ambientes *desktops* à ambientes de *datacenters*, organizados em três categorias: gestão e automatização, infraestrutura virtual e virtualização de plataformas (CARISSIMI, 2008).

O sistema operacional hospedeiro fornece suporte para os diversos dispositivos de *hardware*. Para acessar os dispositivos, o VMware instala um *driver* de dispositivo, chamada de VMDriver. Este *driver* tem a função de colocar a placa de rede em modo promíscuo, o que faz com que a mesma receba todos os quadros *ethernet*, além disso, cria uma ponte (*bridge*), que encaminha esses quadros para o sistema operacional hóspede ou para a máquina virtual especificada (MATTOS, 2008).

As principais versões do VMware são: VMware ESX, VMware ESXi e VMware Player:

VMware ESX: é um sistema operacional hospedeiro e conta com um console de serviço rodando em sistema operacional Linux, o qual desempenha algumas funções de gerenciamento, execução de *scripts* e a instalação de agentes de terceiros para monitoramento de *hardware*, *backup* ou gerenciamento de sistemas. Esta versão é destinada ao uso comercial, voltada para o uso corporativo em servidores de grande porte (VMWARE, 2014).

VMware ESX i: a diferença básica com o VMware ESX está na arquitetura e no gerenciamento operacional do VMware ESXi. O console de serviço foi removido, o que reduziu a ocupação de espaço. Com a remoção do console de serviço da interface local, ocorre a migração para ferramentas de gerenciamento remotas. A tecnologia VMware VMsafe presente, fornece um conjunto de APIs de segurança que permite aos parceiros da VMware desenvolver soluções de segurança com a capacidade de identificar e eliminar *malwares* como vírus, cavalo de Tróia e *keyloggers* durante a operação de uma máquina virtual, com a mesma visibilidade do VMware ESXi e do ESX. O VMware ESXi é distribuído e licenciado gratuitamente (VMWARE, 2014).

VMware Player: é a versão mais simples do produto indicada para aplicações leves, pois, a mesma não possui a capacidade de criar máquinas virtuais (SILVA, 2007).

3.4.2 Microsoft Hyper-V

O Hyper-V fornece ferramentas de gerenciamento básico e infraestrutura de *software* que possibilita criar e gerenciar um ambiente de computação de servidor virtualizado. A tecnologia Hyper-V foi apresentada no lançamento do Windows Server 2008, que teve seu *kernel* reescrito para que esta versão do sistema operacional provesse melhorias em relação à tecnologia de virtualização. O Hyper-V facilitou o processo de adição de virtualização no ambiente corporativo, bastando abrir a ferramenta de gerenciamento do servidor e adicionar esta opção (MORIMOTO; GUILLET, 2009).

O Hyper-V é uma plataforma de virtualização do tipo I que atua como sistema operacional hospedeiro. Com a adoção desta tecnologia os sistemas operacionais das VMs comunicam-se diretamente com o *hardware* sem a necessidade passar pelo sistema operacional *host*. Isto garante maior independência, escalabilidade, melhor performance e maior confiabilidade (MORIMOTO; GUILLET, 2009).

O hipervisor é executado na plataforma Windows, o que a torna familiar à maioria dos administradores de redes, sendo assim, facilita o aprendizado desta ferramenta, uma vez que não precisa aprender um novo sistema operacional ou ferramenta de gerenciamento especializada. A ferramenta de gerenciamento é simples o que torna a criação de máquinas virtuais, o monitoramento destas e o seu gerenciamento um processo familiar para os administradores de TI (MORIMOTO; GUILLET, 2009).

Para garantir a disponibilidade dos serviços em um ambiente virtualizado, são necessários mecanismos de prevenção a falhas e recuperação de desastres. De acordo com Morimoto e Guillet (2009) o Hyper-V possui quatro formas de se garantir a disponibilidade dos serviços para que não haja interrupção:

- **Recursos nativos:** algumas aplicações possuem recursos nativos que garante a alta disponibilidade como os controladores de domínios do Windows que replicam as informações entre si e no caso de um controlador de domínio falhar outro assume a sua função automaticamente;
- **Clusterização da máquina virtual:** existe a opção de clusterizar aplicações como servidores de correio Exchange, SQL Server. Estas aplicações ficam instaladas em máquinas virtuais diferentes e caso algum *host* pare de

funcionar, a aplicação clusterizada passa a funcionar automaticamente em outro *host*, garantindo alta disponibilidade;

- **Clusterização do host:** Através da criação de *cluster* Hyper-V é possível garantir que todas as máquinas virtuais de um *host* que apresente falhas, sejam reiniciadas em outro *host* automaticamente. Isto é possível através do uso de um *storage* compartilhado;
- **Aplicativos de terceiros:** para garantir a alta disponibilidade e recuperação de desastres, pode se usar uma ferramenta especializada quando há uma necessidade de disponibilidade mais alta do que as soluções apresentadas anteriormente e é necessária a aquisição de ferramentas especializadas para este caso.

3.4.3 XenServer

O XenServer é um hipervisor do tipo I, licenciado nos termos da GNU *General Public Licence* (GPL). O XenServer permite a execução de diversos sistemas operacionais hóspedes em uma mesma máquina hospedeira. O XenServer surgiu a partir de um projeto da universidade de *Cambridge*, no qual surgiu uma empresa de nome *XenSource inc*, que foi adquirida pela *Citrix System* em outubro 2007 (CARISSIMI, 2008).

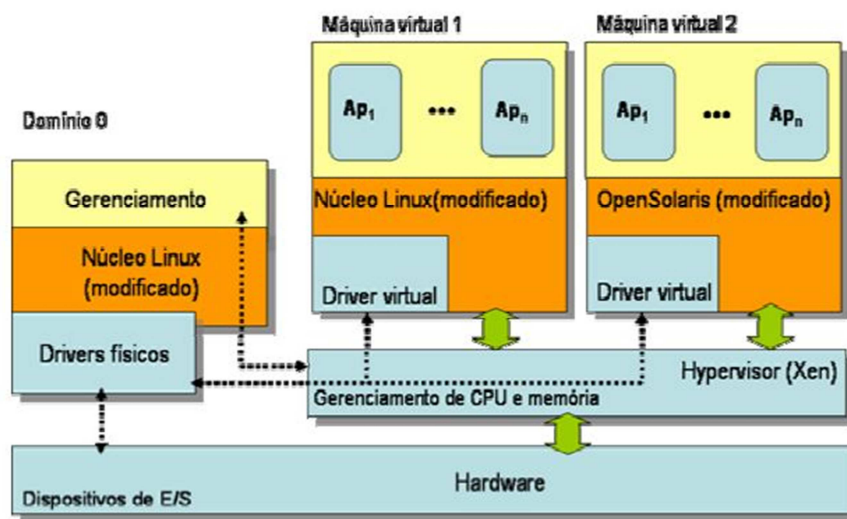
Os principais conceitos do Xen são os domínios e hipervisor. Os domínios são as máquinas virtuais do Xen e podem ser de dois tipos: privilegiada (domínio 0) ou não privilegiada (domínio U). O hipervisor possui a função de controlar os recursos de comunicação de memória e de processamento das máquinas virtuais, e não possui drivers de dispositivos. O hipervisor Xen, não é capaz de suportar nenhum tipo de interação com sistemas operacionais hóspedes. Sendo assim, é necessário que exista um sistema inicial para ser invocado pelo hipervisor, esse sistema é denominado de domínio 0. As outras máquinas virtuais U podem ser executadas depois que ele for iniciado. As máquinas virtuais de domínio U são criadas, iniciadas e terminadas por meio do domínio 0 (CARISSIMI, 2008).

De acordo com Carissimi (2008), existe apenas um domínio 0, que é uma máquina virtual executando sobre um núcleo Linux modificado com privilégios especiais de acesso aos recursos físicos de entrada e saída, esta consegue interagir

com as outras máquinas virtuais presentes no domínios U. O fato do domínio 0 ser um sistema operacional modificado, faz com que o mesmo possua os drivers de dispositivos da máquina física e mais dois *drivers* especiais para processar as requisições de acesso a rede e ao disco efetuados pelas máquinas virtuais dos domínios U.

A Figura 8 mostra o relacionamento entre o hipervisor, o domínio 0 e as demais máquinas virtuais.

Figura 8 Componentes do Xen: Hipervisor e domínios



Fonte: Carissimi (2008)

4 SEGURANÇA EM REDES DE COMPUTADORES

Quando surgiram, as redes de computadores eram usadas por pesquisadores universitários para enviar mensagens de correio eletrônico e por funcionários de empresas para compartilhamento de impressoras. Na época, essas condições não precisavam de muita segurança. Porém, atualmente, milhares de pessoas estão usando as redes para executar operações bancárias, fazer compras e arquivar sua devolução de impostos. Sob este contexto, a segurança das redes aparece como um problema em potencial. A segurança engloba inúmeros tipos de problemas e em sua forma mais simples se preocupa em garantir que pessoas não intencionadas não tenham acesso, modifiquem secretamente mensagens enviadas a outros destinatários ou obtenham acesso a serviços remotos aos quais elas não estão autorizadas a usar. A maior parte dos problemas de segurança é causada intencionalmente por pessoas maliciosas que tentam obter algum benefício, chamar a atenção ou prejudicar alguém (TANENBAUM, 2003).

4.1 SEGURANÇA DA INFORMAÇÃO

Segurança da informação é o conjunto de orientações, normas, procedimentos, políticas, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada. A segurança da informação existe para mitigar os riscos do negócio em relação à dependência do uso dos recursos de informação para o funcionamento da organização, pois, sem a informação ou com a alteração desta por pessoas não autorizadas, uma organização pode ter prejuízos de ordem financeiras ou perder a confiança de seus clientes ou acionistas (FONTES, 2010).

Conforme a norma ABNT NBR ISO/IEC 27002:2005 (ABNT, 2005):

A segurança da informação consiste na preservação da confidencialidade, integridade, e disponibilidade da informação; adicionalmente outras propriedades tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem estar envolvidas.

De acordo com Fontes (2010) proteger a informação significa garantir ao menos os três pilares básicos da segurança da informação C.I.D.:

- ✓ Confidencialidade: a informação deve ser acessada e utilizada somente por quem necessita dela para realizar suas funções profissionais dentro da organização e possua autorização para usá-la.
- ✓ Integridade: a informação deve estar correta, livre de alterações e ser verdadeira.
- ✓ Disponibilidade: a informação deve estar acessível para o uso da organização sempre que for necessário, para o alcance dos objetivos e missão.

4.2 POLÍTICAS DE SEGURANÇA

Segundo a cartilha de segurança do **CERT.br** (2012) (Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores), a política de segurança existe para definir os direitos e as responsabilidades de cada usuário com relação à segurança dos recursos computacionais que este utiliza e das penalidades às quais está sujeito, caso não as cumpra. É considerada um importante mecanismo de segurança não só para a empresa, mas como para o funcionário também, pois, com ela é possível deixar claro o comportamento esperado de cada um.

A política da segurança pode conter outras políticas específicas como:

- ✓ Política de senhas: define as regras sobre o uso das senhas, como tamanho mínimo e máximo, regras de formação e período de troca;
- ✓ Política de *backup*: define as regras sobre a realização de cópias de segurança, como que tipo de mídia usar, e frequência de execução;
- ✓ Política de privacidade: define como tratar as informações dos clientes, funcionários ou usuários;
- ✓ Política de confidencialidade: define como são tratadas as informações institucionais, se elas devem ou não ser repassadas a terceiros;
- ✓ Política de uso aceitável: define as regras dos termos de uso dos recursos computacionais, os direitos e as responsabilidades de seus usuários bem como as situações que são consideradas abusivas.

4.3 NECESSIDADE DE SEGURANÇA

Conforme a tecnologia evolui surgem novos serviços para disponibilizar aos usuários, porém, para cada novo serviço aumenta o número de riscos que uma empresa oferece aos seus clientes. Nesse cenário, a segurança da informação acaba sendo primordial para que os dados das empresas e dos clientes estejam seguros e disponíveis. Devido à grande quantidade de vulnerabilidades existentes nos diversos tipos de serviços oferecidos, os profissionais da segurança da informação devem se certificar de cada vulnerabilidade e tomar as medidas necessárias para impedir que essas vulnerabilidades sejam a porta de entrada para um possível ataque. Para que um atacante obtenha sucesso em um ataque é preciso existir uma brecha no sistema, por isso, o gestor de segurança da informação deve possuir sólidos conhecimentos para conhecer e fechar todas as brechas, para que o sistema de informação esteja em um nível aceitável de segurança (NAKAMURA; GEUS, 2010).

4.4 AMEAÇAS ÀS REDE DE COMPUTADORES

Os servidores virtuais estão sujeitos aos mesmos ataques que atingem os servidores físicos, da mesma forma que novas ameaças estão sendo desenvolvidas para explorar as falhas do hipervisor. As funcionalidades que permitem tanta flexibilidade computacional, faz como que os gerentes de rede e segurança reflitam se uma ameaça no ambiente virtual, pode se espalhar para toda a rede, segundo a Network World (2007).

4.4.1 Vulnerabilidades

De acordo com a Norma ABNT ISO/IEC 27002:2005 (ABNT, 2005) vulnerabilidade é a “fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças”.

Um grande problema segundo (LAUDON; LAUDON, 2006) é a presença de vulnerabilidades (*bugs*) ou defeitos ocultos no código do programa devido a

complexidade do código de tomada de decisões, mesmo um programa pequeno com poucas linhas pode conter centenas ou milhares de caminhos diferentes. Estudos mostram que é praticamente impossível eliminar todos os *bugs* nos programas de grande porte.

4.4.2 Tipos de ataques

Com a globalização, a infraestrutura de rede de comunicação se tornou um item indispensável para o funcionamento dos serviços de tecnologia da informação. Os ataques buscam as falhas existentes em qualquer um dos níveis de proteção da informação. A proteção deve estar presente em todos os níveis como: sistema operacional, serviços e protocolos, rede e telecomunicações, aplicação, usuários, organização e físico.

Os *hackers*, são pessoas que utilizam conhecimentos técnicos para invadir sistemas, as vezes sem a intenção de causar danos às vítimas, apenas como um desafio às suas habilidades. São várias as razões que podem motivar um ataque, que varia de acordo com o tipo de *hacker*, desde de uma simples curiosidade até o roubo de informações confidenciais por exemplo (NAKAMURA; GEUS 2010).

O *hacker* é um indivíduo que obtém acesso não autorizado a uma rede de computadores com a intenção de obter lucro, intervir criminosamente ou apenas para satisfazer o seu ego (LAUDON; LAUDON, 2006).

À medida que cresce a utilização da Internet por empresas e indivíduos, aumenta a quantidade de violações de segurança na rede. A preocupação maior é por conta de intrusos indesejáveis ou *hackers* que fazem uso das mais novas e variadas tecnologias juntamente com suas habilidades técnicas para invadir ou desativar computadores supostamente seguros.

4.4.3 Ameaças a ambientes virtualizados

A virtualização de *desktops* e servidores é uma realidade e tornou-se uma prática comum no meio corporativo, a qual traz muitos benefícios à empresa que a utiliza, especialmente de ordem financeira, uma vez que possibilita a redução de custos, velocidade de manutenção, estabilidade e administração centralizada.

Os fabricantes de antivírus travam verdadeiras batalhas diárias contra *trojans*, *backdoors*, *rootkits*, *file infectors*, *malware* em geral, que estão prontos para atacar e infectar os diversos ambientes computadorizados existentes pelo mundo. Sabe-se que um simples código malicioso pode infectar um sistema virtualizado da mesma forma que o faz com uma máquina física. Existem códigos maliciosos especializados em penetrar e infectar a infraestrutura de rede de uma empresa, mesmo que os ambientes estejam virtualizados (ASSOLINI, 2012).

De acordo com o “*Guide to Security for Full Virtualization Technologies*” do *National Institute for Standards & Technology (NIST)*, quando “[...] uma única máquina virtual é comprometida, isso impacta uma infraestrutura virtualizada por completo”. (NIST *apud* ASSOLINI (2012)).

Quando uma máquina virtual é infectada ela pode comprometer os dados armazenados e os arquivos de sistema, que serão compartilhados por outras máquinas virtuais, espalhando a infecção em toda a infraestrutura virtualizada. Essa máquina virtual infectada poderá ser usada como vetor de distribuição de ataques ou como ‘espiã’ na rede, executando o tráfego entre outras máquinas virtuais (ASSOLINI, 2012).

Alguns códigos maliciosos possuem uma função chamada “antivirtualização”, que impede a sua execução ou instalação em sistemas virtualizados, para dificultar o trabalho das companhias antivírus. Percebe-se que os criadores de *malware* atuais preparam ataques que infectam tanto máquinas reais como virtuais (ASSOLINI, 2012). Ainda de acordo com o autor existem códigos maliciosos como o vírus “Crisis” criados para infectar máquinas virtuais, que após infectar o *host* real, procura por arquivos de máquinas virtuais da VMware, e caso encontre-os, remonta a máquina virtual usando a ferramenta VMware Player, recompilando uma imagem infectada da máquina virtual. Outros vírus conseguem sobreviver a uma “formatação” do ambiente virtual, sendo capazes de retornar após a restauração da máquina virtual, basta para isso infectar a máquina física que está hospedando o sistema virtualizado. Chama-se isso de VME (Virtual Machine Escape).

4.4.4 Virtual Machine Escape

Segundo Assolini (2012) “é o processo onde ocorre a ‘quebra’ do isolamento entre o sistema virtualizado e seu *host* físico, possibilitando, por exemplo, que uma infecção presente na máquina virtual possa ‘escapar’ e chegar até o *host* físico”.

O virtual machine escape (VME) pode ocorrer em dois cenários distintos:

- **Explorando falhas de segurança do *software* ou *hardware* usado na virtualização**, este cenário é menos comum porque os fabricantes de soluções virtualizadas agem de forma rápida para consertar as falhas que possibilitam esse tipo de ataque.
- **Uso indiscriminado de unidades compartilhadas e permissões de escrita**, possibilitando uma infecção se auto copiar para fora do ambiente virtual e assim se disseminar na rede. Este cenário é mais comum e acontece pela configuração incorreta do ambiente virtual, ou por abuso dos compartilhamentos, permitindo que unidades compartilhadas na rede sejam usadas como vetor de distribuição de códigos maliciosos.

4.4.5 Vírus

Um vírus é um programa de computador com a capacidade de unir-se aos discos ou arquivos e reproduzir-se repetidamente sem o conhecimento ou a permissão do usuário. Geralmente um vírus é acionado quando o arquivo infectado é executado e pode causar os mais variados problemas que vai desde uma simples brincadeira até prejuízos financeiros para a organização (STAIR; REYNOLDS, 2011).

4.4.6 Worm

Um *worm* é um programa parasita que diferentemente do vírus não infecta os outros arquivos ou programas, mas possui a capacidade de reproduzir-se e enviar suas cópias para outros computadores da rede infectando todo um ambiente de uma organização (STAIR; REYNOLDS, 2011).

4.5 FERRAMENTAS DE PROTEÇÃO

4.5.1 Antivírus

Um antivírus é um *software* utilizado para proteger os computadores de códigos maliciosos como vírus, *worms*, cavalo de Tróia, *malwares*, etc. que funciona na retaguarda escaneando os dispositivos a procura de atividades maliciosas com o intuito de eliminar e impedir que os vírus se espalhem pela organização (STAIR; REYNOLDS, 2011).

Observa-se que alguns antivírus executam suas funções de forma automática como escaneamento do sistema e atualização das definições, sendo, que muitas vezes essas operações não são percebidas pelos usuários.

4.5.2 Firewall

O *firewall* é um ponto entre duas ou mais redes que pode ser um componente ou conjuntos de componentes pelo qual passa todo o tráfego da rede, permitindo o controle, autenticação e o registro de todo o tráfego. O *firewall* geralmente é utilizado para proteger uma rede confiável de uma rede pública não confiável, através de um conjunto de regras pré-estabelecidas por uma política de segurança adotada por uma determinada organização (NAKAMURA; GEUS, 2010).

4.5.3 Proxy

De acordo com Nakamura e Geus (2010) é um tipo de *firewall*, porém mais complexo que filtra o conteúdo dos pacotes. A comunicação direta entre a rede e a Internet não é permitida no *proxy*. Tudo deve passar pelo *firewall* que atua como uma espécie de intermediador da conexão interna com a conexão externa por meio da avaliação do número da sessão dos pacotes TCP.

Uma das grandes vantagens de se usar um *proxy* é a possibilidade de registrar todo o tráfego da rede interna ou externa, podendo ativar um sistema de alarme quando algo fora da política de segurança acontece, alertando o administrador da rede.

4.5.4 Sistema de Detecção de Intrusão

Os fornecedores de segurança comercial oferecem além do *firewall*, ferramentas e serviços de detecção de intrusos que protegem o tráfego suspeito na rede e tentativas de acessos a arquivos do banco de dados.

Os sistemas de detecção de intrusão são ferramentas que monitoram de forma contínua os pontos mais vulneráveis da rede corporativa, a fim de inibir e detectar o invasor. Um *software* procura por padrões indicativos de métodos de ataques, como senhas erradas, verifica alterações em arquivos importantes e envia alertas de vandalismo e erros de administração dos sistemas, desta forma, esta ferramenta consegue detectar ataques a segurança em tempo real e pode até ser customizada para isolar uma parte sensível da rede, caso receba tráfego não autorizado (STAIR; REYNOLDS, 2011).

4.5.5 VMware vShield Endpoint

É um recurso que revoluciona o modo de proteção das máquinas virtuais *guest* contra vírus e *malwares*, uma solução que otimiza a segurança nos ambientes virtuais, entretanto, não faz a varredura por vírus nem verifica a presença de *malware*. O *vShield* Endpoint é uma tecnologia da VMware implantada como um *appliance* virtual em cada um dos *hosts* ESXi que se deseja proteger. Esse *appliance* virtual é incorporado a uma das soluções integradas fornecidas por um dos parceiros de sistema de rede e segurança da VMware, que fornecem o dispositivo de segurança centralizada virtual (SVA) com a função de se conectar ao *appliance* virtual, o qual, é o mecanismo por trás de toda a varredura (ROSE, 2013).

4.6 FERRAMENTA PARA PROTEÇÃO DE REDES VIRTUALIZADAS

O Bitdefender GravityZone é uma solução empresarial de segurança da Bitdefender para empresas, que protege discretamente uma grande quantidade de dispositivos, oferecendo suporte para os sistemas operacionais Windows, Linux e Mac OS X. Os sistemas Windows beneficiam-se de uma segurança ainda mais avançada com um firewall bidirecional, detecção de intrusão, controle de acesso à web e filtragem, proteção de dados sensíveis, controle de aplicativos e dispositivos.

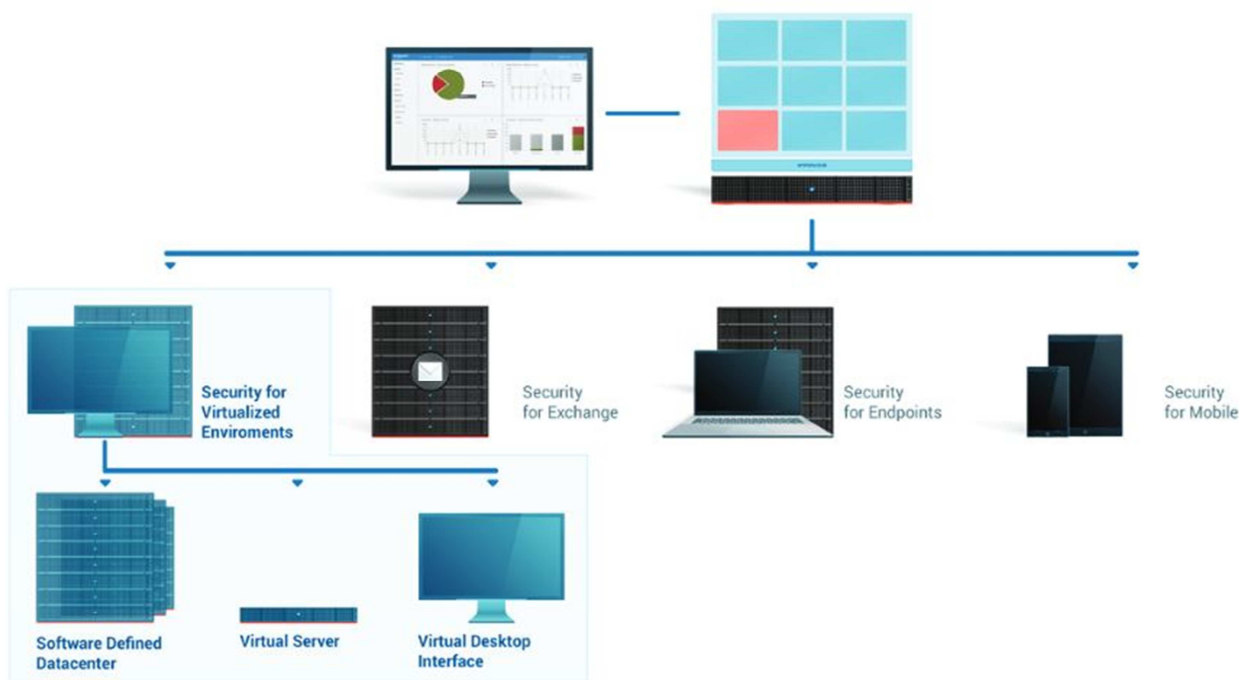
Não é apenas um antivírus, mas um conjunto de ferramentas que ajuda as organizações a atingirem seus objetivos de projetos de virtualização e proteger os dados, preservando o desempenho dos sistemas e a produtividade de seus usuários (BITDEFENDER, 201?).

O GravityZone SVE (*security virtual environments*) proporciona proteção *antimalware* utilizando dispositivos virtuais de segurança SVA (servidores de segurança) funcionando como ponto centralizado de inteligência *antimalware* e usa um mecanismo de multicamadas que mantem o *cache* dentro de cada máquina virtual, assim, os objetos são verificados uma única vez. O *cache* compartilhado é mantido dentro do servidor de segurança SVA para que os objetos verificados em uma máquina virtual não sejam verificados novamente em outra máquina (BITDEFENDER, 201?).

Quando vShield Endpoint é iniciado, ele fornece acesso ao sistema de arquivos para o servidor de segurança através da camada do hipervisor, este processo também é conhecido como proteção sem agente. Na versão vShield integrada da Bitdefender do SVE, essa proteção limitada pode ser ampliada para incluir a memória, registro e processos em execução, através da cooperação entre o VMware Tools e o gerenciamento do Endpoint Security (BITDEFENDER, 201?).

O GravityZone SVE é implementado como uma solução em nuvem privada que funciona em camadas e permite as organizações protegerem seus ativos de TI, e é gerenciado online através da console *web* (*Control Center*) fornecida pela Bitdefender, reduzindo custos com infraestrutura de TI para a empresa (BITDEFENDER, 201?).

Figura 9 Plataforma GravityZone SVE



Fonte: Bitdefender

O console de gerenciamento da Bitdefender permite criar pacotes com as soluções que o cliente deseja instalar nas máquinas virtuais, nas versões 32 e 64 *bits* dos sistemas operacionais Windows e Linux. Depois de escolhido o pacote de instalação é necessário realizar o *download* e fazer a instalação dos Endpoints manualmente ou pode optar por fazer a instalação remota das máquinas virtuais.

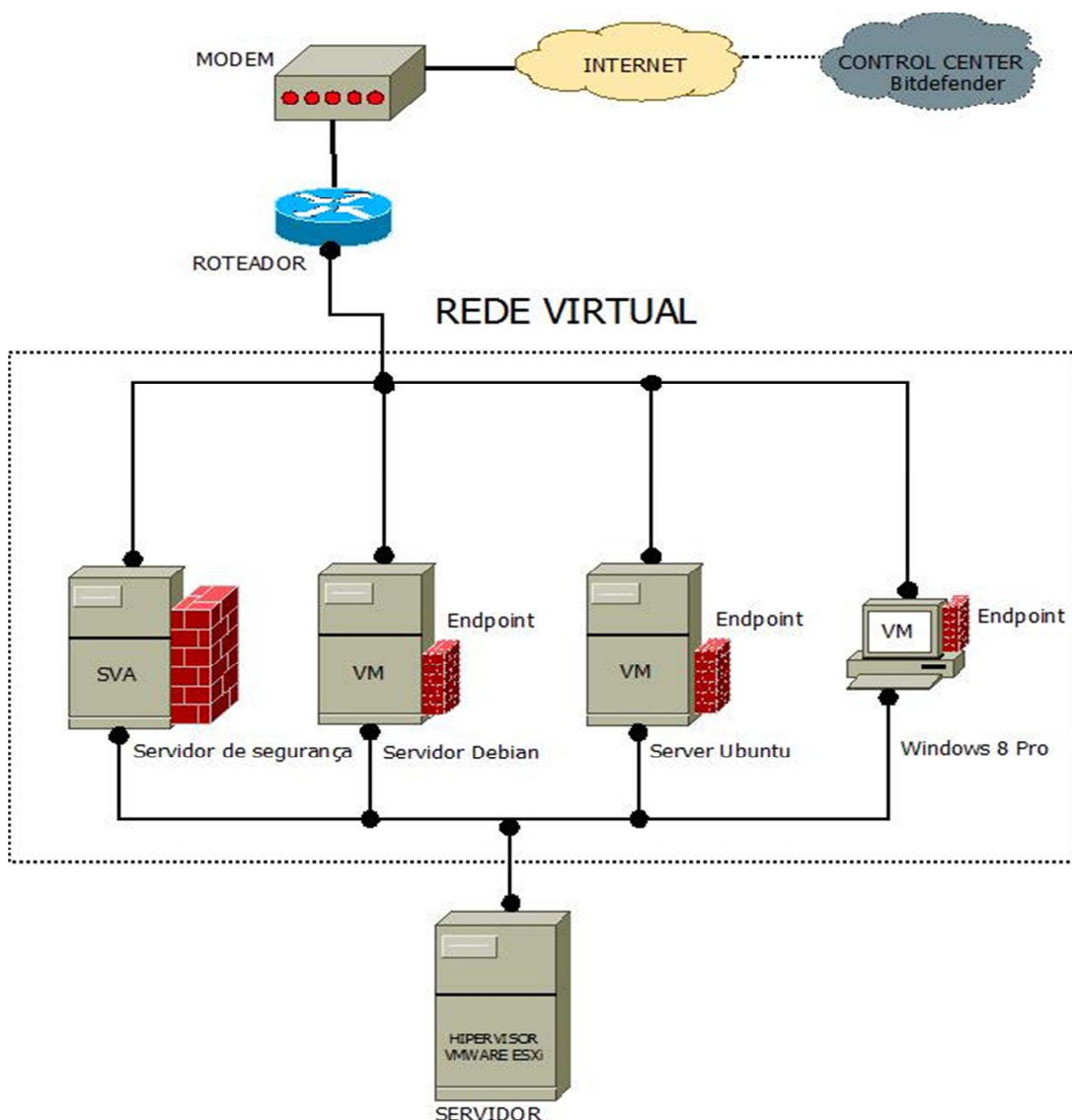
Um Endpoint é basicamente um *software* capaz de se conectar a uma rede de computadores com a função de monitorar a segurança das informações de ameaças e de intrusão. Uma proteção Endpoint normalmente trabalha no modelo cliente e servidor. Um programa é instalado para cada dispositivo cliente da rede, mas a proteção é gerenciada centralmente por um servidor. Um exemplo típico de Endpoint são os *firewalls* e *softwares* antivírus (COMPUTER, 201?).

5 ESTUDO DE CASO

Para o desenvolvimento deste trabalho foi montado um cenário em um computador I5 2.2 GHZ 6GB RAM 1 TB.

Foram usadas as seguintes máquinas virtuais: um servidor Ubuntu server, servidor Debian, Windows 8 PRO e um servidor de segurança SVA. O diagrama da rede virtual é apresentado na Figura 10.

Figura 10 Diagrama esquemático da rede virtual



Fonte: Próprio autor

A solução utilizada para a implementação da segurança foi o *security sever virtual appliance* (SVA) da plataforma GravityZone SVE (*security for virtualized environments*) do fabricante de *antimalware* Bitdefender e a plataforma de

virtualização usada foi o hipervisor de tipo I da VMware o vSphere ESXi 6.0, que pode ser adquirido gratuitamente no site da VMware.

Tentou-se ao máximo reproduzir um ambiente de rede comum usado nas pequenas empresas, lembrando que este tipo de ambiente varia de acordo com a empresa, a Tabela 1 exibe as configurações das máquinas virtuais utilizadas.

Tabela 1 Descrição das configurações das máquinas virtuais

MÁQUINA VIRTUAL	MEMÓRIA RAM	HARD DISK	SISTEMA OPERACIONAL
Ubuntu Server	512 MB	40 GB	Ubuntu server 14.04.5 64 bits
Servidor Debian	1024 MB	40 GB	Debian Jessie 8
SVA	1024 MB	30 GB	Ubuntu 12.04.5 LTS
Windows 8 PRO	1024 MB	40 GB	Windows 8.1 professional
VMware ESXi	4096 MB	200 GB	vSphere ESXi 6.0

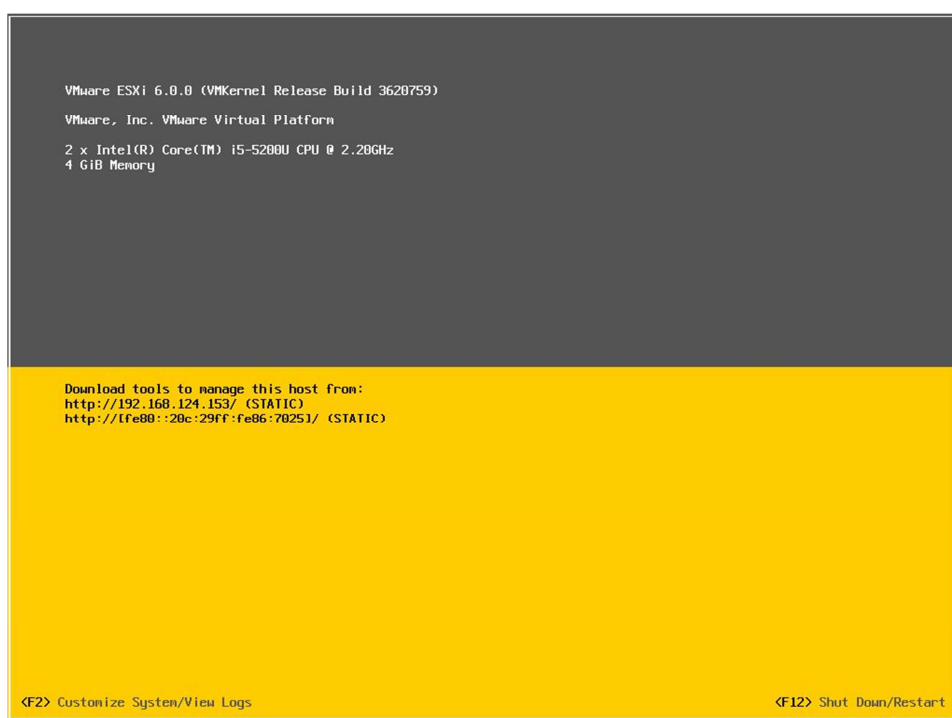
Fonte: Próprio autor

O GravityZone SVE precisa de conexão com a Internet para funcionar, pois, a mesma é uma plataforma online baseada em um console de gerenciamento único para plataformas como VMware, Hyper-v e Citrix. O acesso é feito via *browser* na *web Control Center* da Bitdefender desenvolvido para fazer o gerenciamento remoto das políticas de segurança das máquinas virtuais da rede que se deseja proteger.

5.1 IMPLANTAÇÃO

Para a realização dos testes inicialmente foi instalada a plataforma de virtualização da VMware ESXi, o vSphere 6.0 que é gratuito e fácil de instalar, lembrando que se pode utilizar a estrutura (em uso) da rede virtual da empresa. A Figura 11 mostra a interface do Hipervisor ESXi.

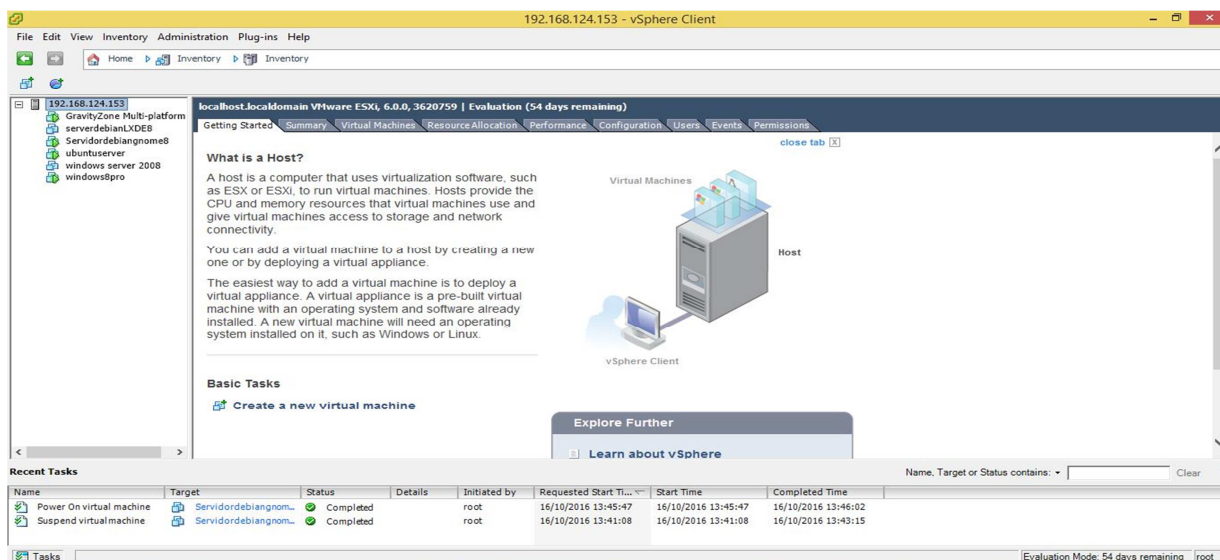
Figura 11 Plataforma de virtualização VMware ESXi.



Fonte: Próprio autor

Para acessar e gerenciar o hipervisor ESXi é necessária a instalação de um cliente, pois, o VMware ESXi não possui o console de serviço e o gerenciamento será feito através do VMware vSphere Client, o qual pode ser obtido através de uma interface web de mesmo endereço de IP que o hipervisor (conforme mostra a Figura 11), então, após digitar o endereço, que neste caso é <http://192.168.124.153>, foi só fazer o *download* do instalador do vSphere Client, e instalar o cliente para acessar o console de gerenciamento das VMs, no qual é possível configurar, excluir, apagar, criar e modificar as VMs da rede virtual como mostra a Figura 12.

Figura 12 Console de gerenciamento vSphere Client.

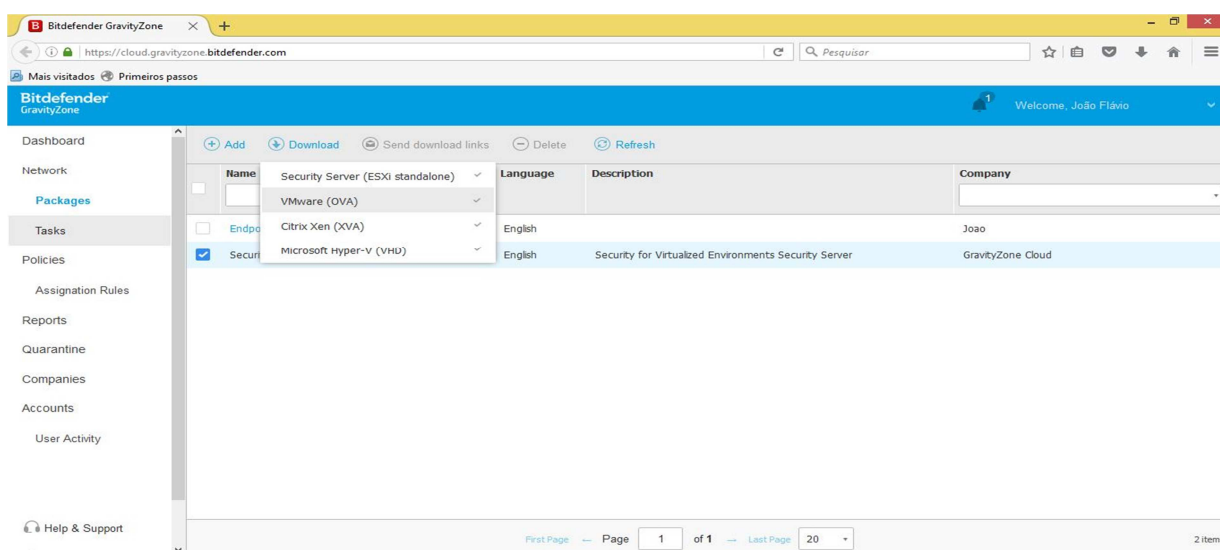


Fonte: Próprio autor

Depois de criada a rede virtual para a implantação da ferramenta de segurança GravityZone, foi preciso fazer o *download* do *appliance* virtual do SVA no console *web control center*, que pode ser acessado de qualquer lugar, através de um navegador no endereço <https://cloud.gravityzone.bitdefender.com/>.

Na guia *packages* selecionar o *appliance* do SVA de acordo com a plataforma de virtualização utilizada, no caso VMware (OVA) conforme figura 13.

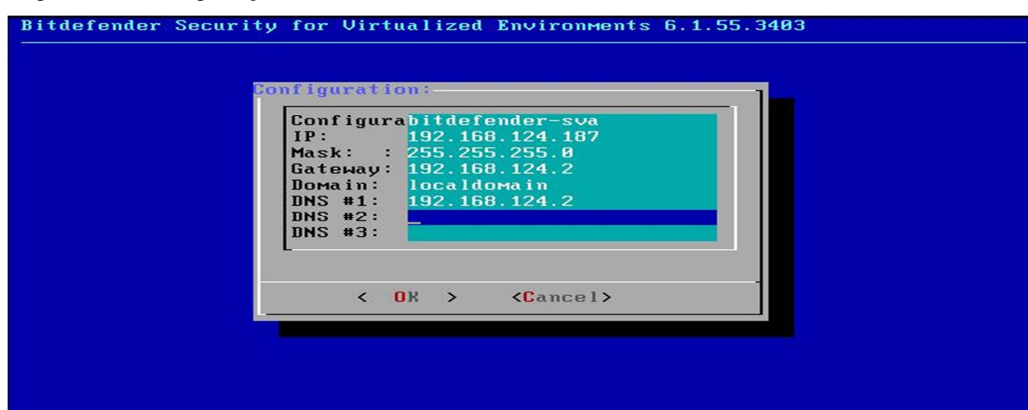
Figura 13 Console de gerenciamento online Bitdefender GravityZone.



Fonte: Próprio autor

Depois de fazer o *download*, o SVA deve ser instalado no ambiente virtual que se deseja proteger. O SVA é uma máquina virtual dedicada que possui acesso as máquinas virtuais através do vShield Endpoint da VMware e já vem com todos os serviços configurados, necessitando apenas receber um endereço de IP da rede. Para configurar o *appliance* do SVE é só entrar no *setup* de configuração, digitando o comando *#sva-setup* e em *Network configuration*, atribuir um endereço de IP da rede que será protegida como no exemplo da Figura 14.

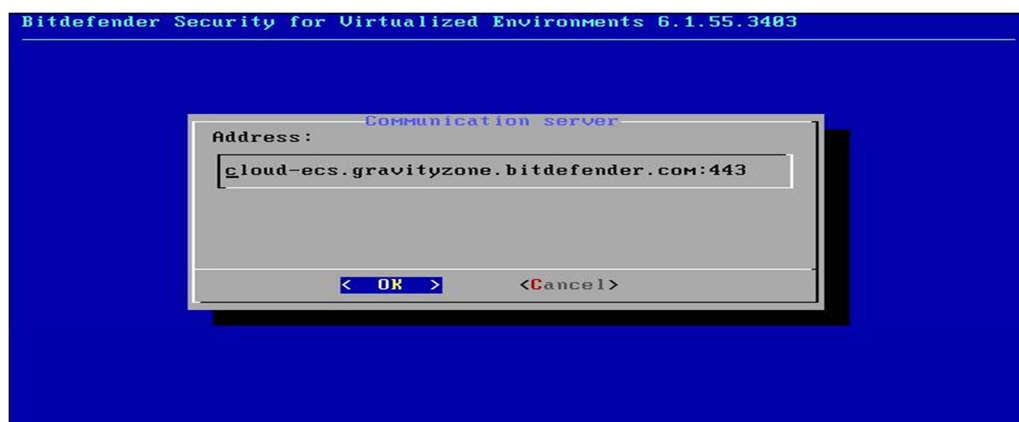
Figura 14 Configurações da rede do SVA.



Fonte: Próprio autor

Na guia *Communication server configuration* escolher a opção *cloud* e digitar o endereço do console da Bitdefender <https://cloud-ecs.gravityzone.bitdefender.com:443> como mostra a Figura 15.

Figura 15 Endereço web da console Bitdefender GravityZone.

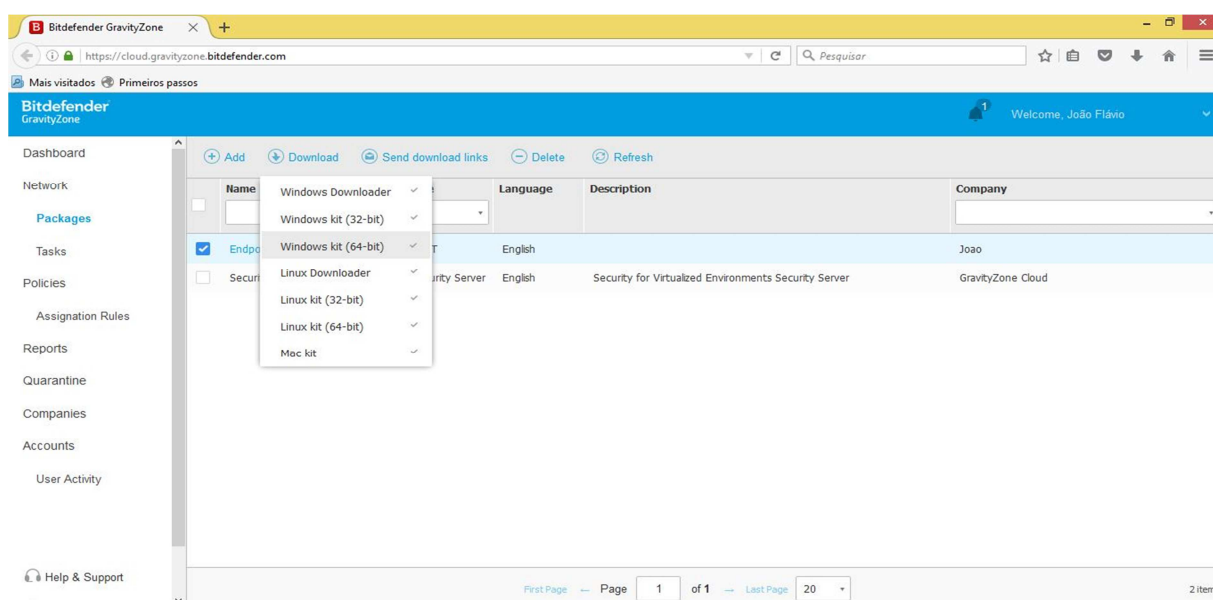


Fonte: Próprio autor

Após esta etapa aparece um novo item, o *Configure the client ID* que deve ser preenchido com o ID do cliente, disponível no console *control center* em *my company*, feito isso o SVA estabelece conexão com o console de gerenciamento online.

A próxima etapa é a instalação dos Endpoints nas máquinas virtuais da rede. Para fazer o apontamento, basta criar os pacotes com as configurações desejadas como controle de acesso, *antimalware*, *firewall*, política de senhas, etc. A console disponibiliza várias opções de pacotes para os Sistemas Operacionais Windows, Linux e MAC nas versões de 32 e 64 *bits* conforme mostra a Figura 16.

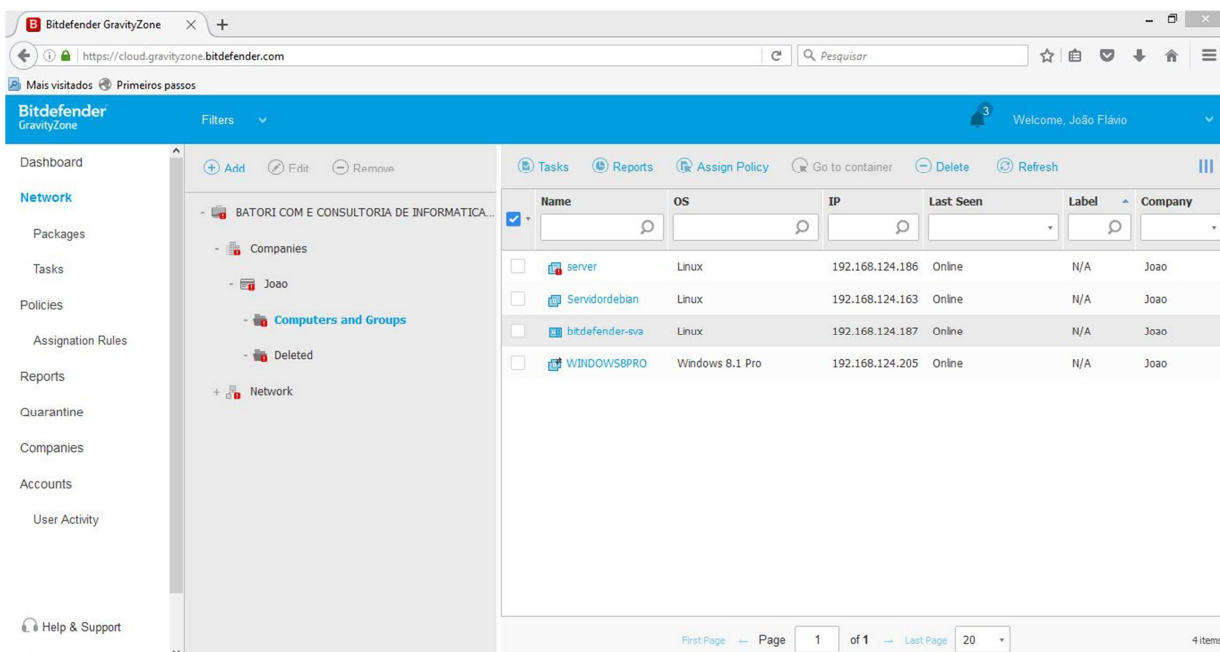
Figura 16 Pacotes de Endpoint



Fonte: Próprio autor

Para instalar os Endpoints optou-se por baixar os pacotes e instalar manualmente nas máquinas virtuais. Após a instalação dos pacotes, as máquinas virtuais estabelecem a conexão com a console no *cloud* da Bitdefender e já é possível estabelecer as políticas de segurança para cada dispositivo individualmente ou usar políticas diferenciadas de acordo com a necessidade da empresa, conforme exibe a Figura 17 a seguir.

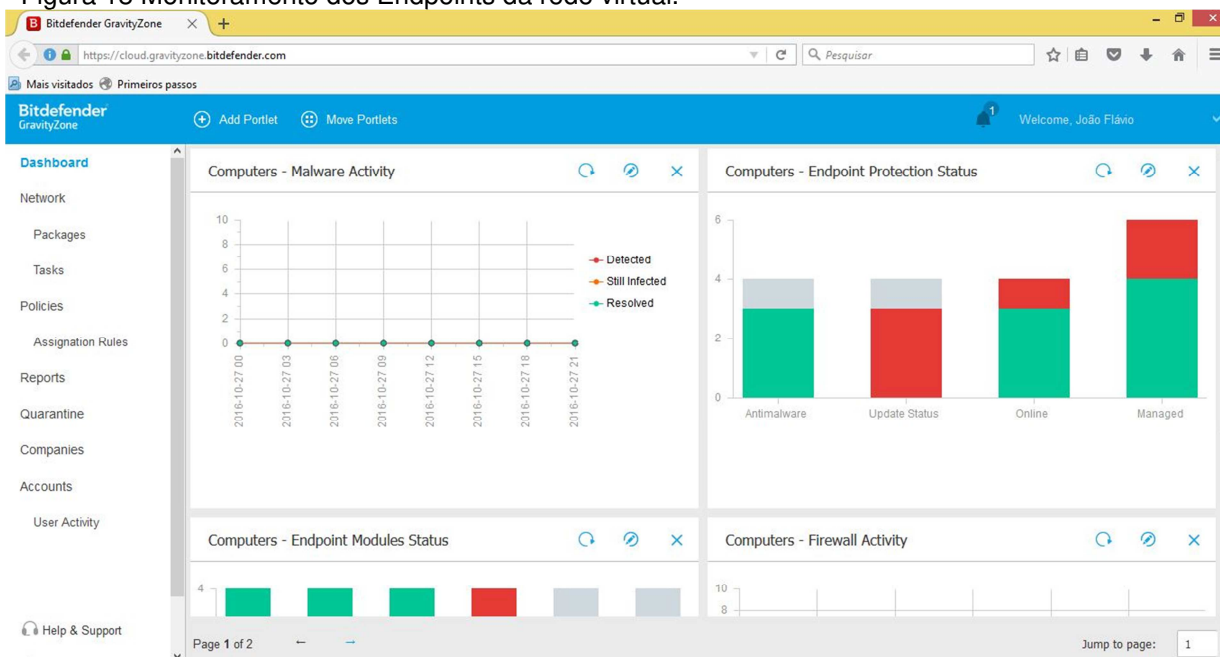
Figura 17 Máquinas virtuais no console de gerenciamento.



Fonte: Próprio autor

Na tela inicial é possível selecionar o tipo de serviço que se deseja exibir, podendo alterar, acrescentar, excluir e visualizar as informações detalhadas dos relatórios, conforme ilustra a Figura 18.

Figura 18 Monitoramento dos Endpoints da rede virtual.

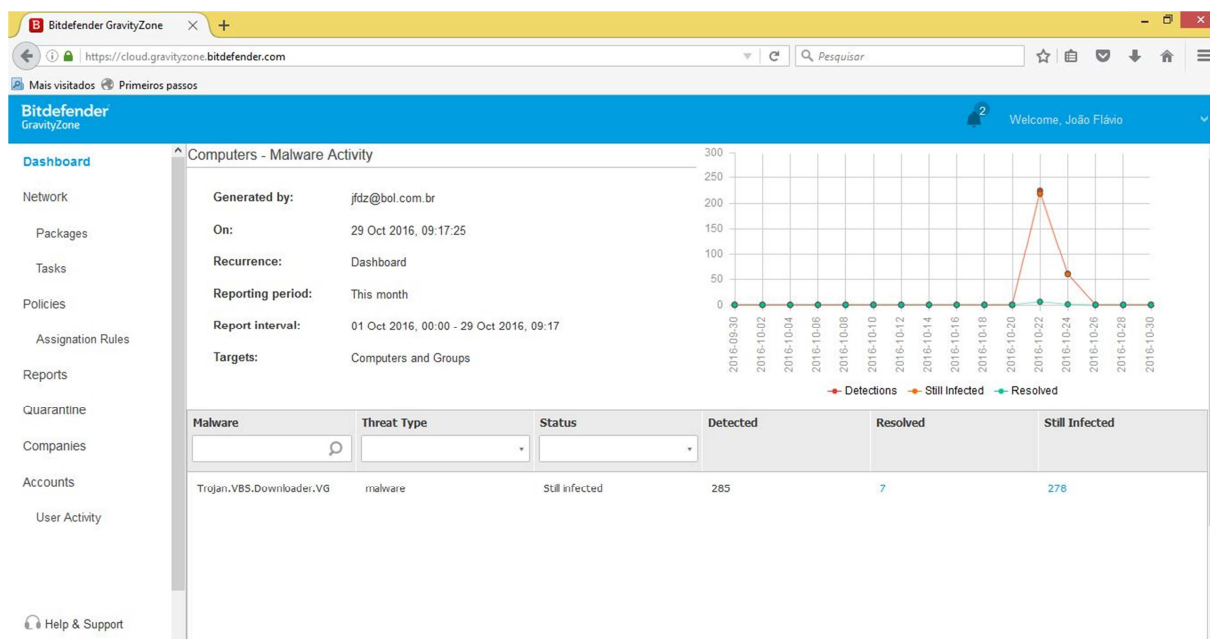


Fonte: Próprio autor

5.2 TESTES E ANÁLISE DOS RESULTADOS

O primeiro teste realizado foi a detecção de *malware* nas máquinas virtuais, para tanto, tentou-se introduzir um vírus no ambiente virtual, executando o sistema operacional cliente Windows 8 PRO, simulando a cópia de um arquivo infectado com um vírus. Ao tentar copiar o arquivo infectado, o Endpoint local detectou a ameaça e imediatamente iniciou os procedimentos apontados na política de segurança para realizar a desinfecção do arquivo. O arquivo foi movido para a quarentena e isso gera um relatório de atividades *malware*, o qual pode ser visualizado no console *control center* conforme mostra a Figura 19.

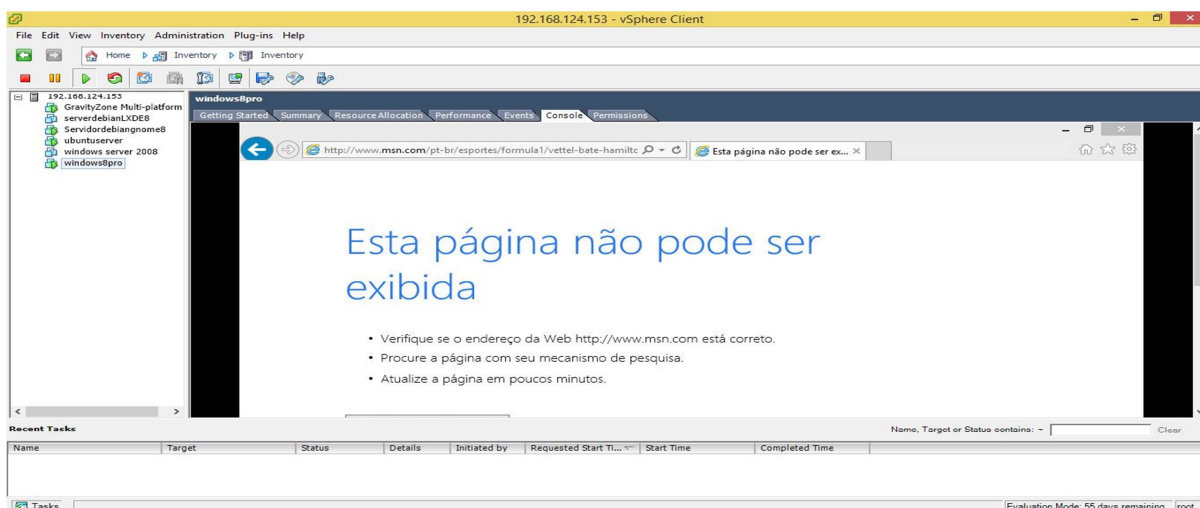
Figura 19 Relatório de atividades *malware*.



Fonte: Próprio autor

O segundo teste foi alterar a política e proibir a conexão com a internet (*proxy*), logo após a política ser alterada as novas configurações são enviadas para as máquinas virtuais e as novas regras entram em vigor imediatamente, bloqueando a conexão de internet de todas as VMs que utilizam a política em questão. O bloqueio pode ser verificado através do vSphere Client como, mostra a Figura 20.

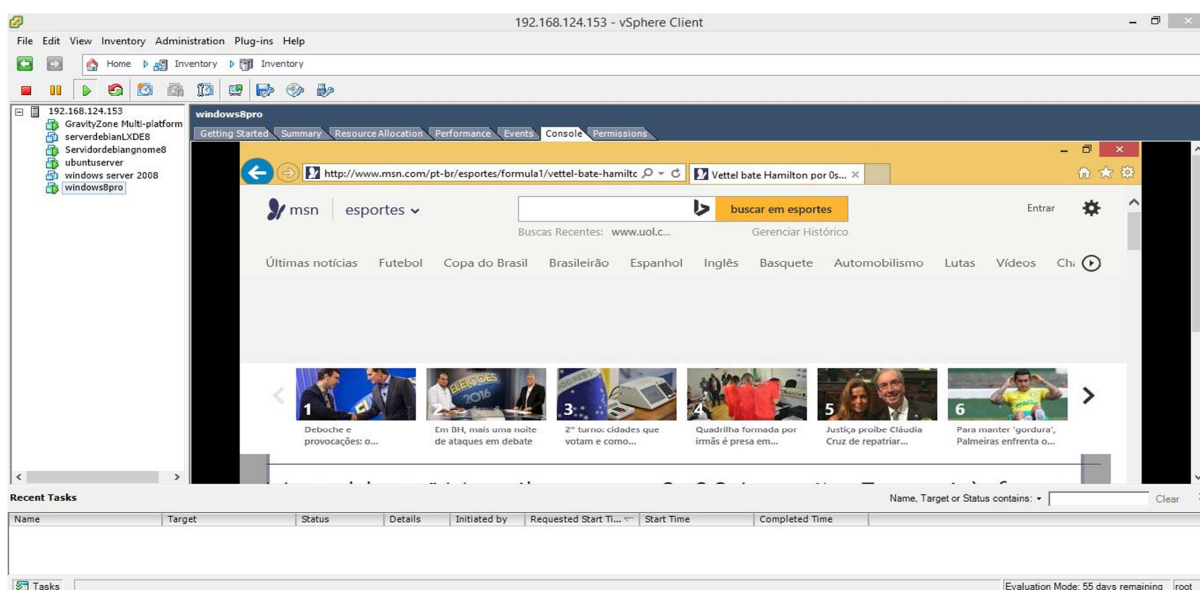
Figura 20 Política de bloqueio da Internet.



Fonte: Próprio autor

A figura 21 mostra a conexão com a internet restabelecida simplesmente com a alteração da política, sem a necessidade de configurar a VM.

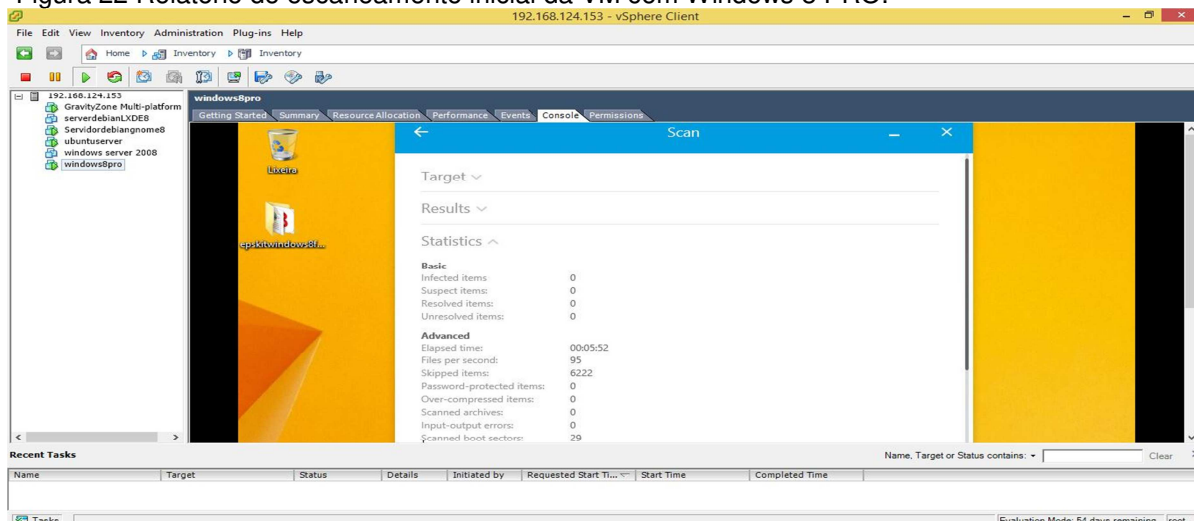
Figura 21 Política de liberação da Internet.



Fonte: Próprio autor

O terceiro teste foi avaliar o desempenho do escaneamento das VMs da rede, o escaneamento foi feito aplicando uma política de segurança com o servidor de segurança (SVA) em uma VM executando o sistema operacional Windows 8 Pro com uma instalação “limpa” (instalação padrão) como mostra a figura 22.

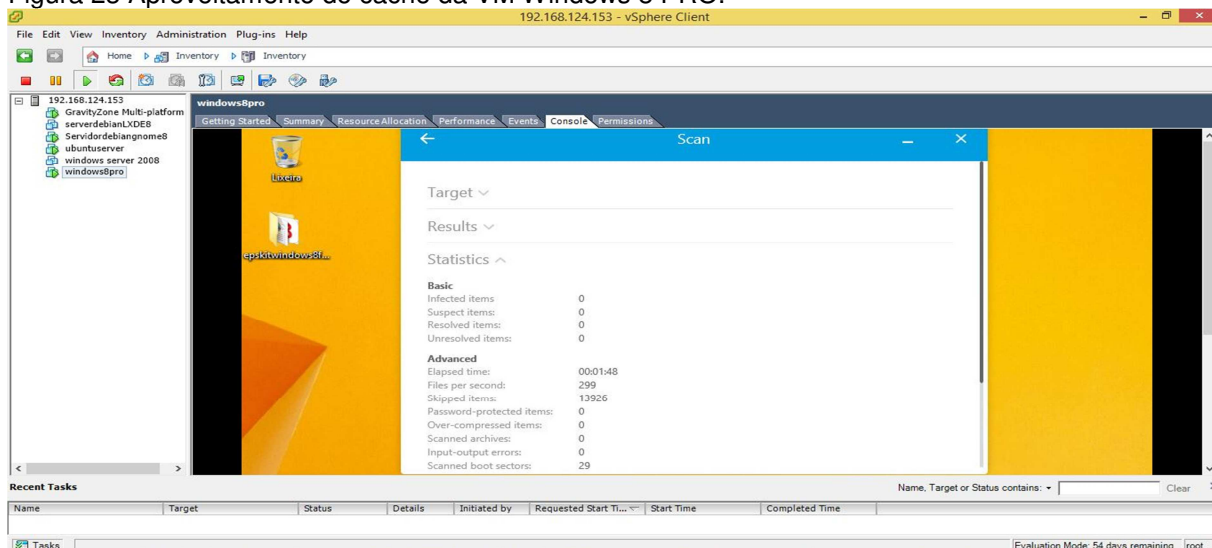
Figura 22 Relatório de escaneamento inicial da VM com Windows 8 PRO.



Fonte: Próprio autor

Após o terminar o escaneamento, o processo foi repetido, mantendo a mesma política para verificar o aproveitamento do *cache* que fica armazenado no SVA, conforme mostra a figura 23.

Figura 23 Aproveitamento do cache da VM Windows 8 PRO.

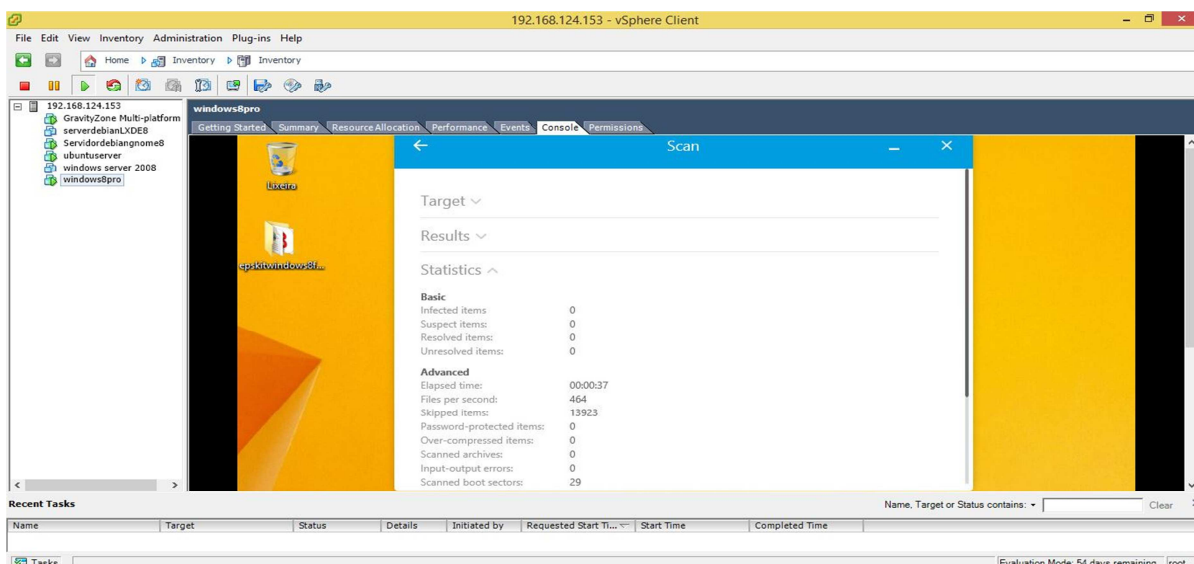


Fonte: Próprio autor

De acordo com o observado na figura 24 acima, o resultado do escaneamento foi bem mais rápido, o que comprova o aproveitamento do *cache* prometido pela solução proposta. Logo em seguida foi realizado outro

escaneamento, porém desta vez, sem o uso do servidor de segurança SVA. Percebe-se uma performance um pouco melhor, mas que não compromete muito o desempenho da VM, como mostra a figura 24.

Figura 24 Escaneamento da VM Windows 8 PRO sem o servidor SVA.



Fonte: Próprio autor

O console de gerenciamento *control center* oferece uma série de recursos de segurança ao administrador, como informar se o servidor de segurança apresentar qualquer problema, conforme mostra a figura 25.

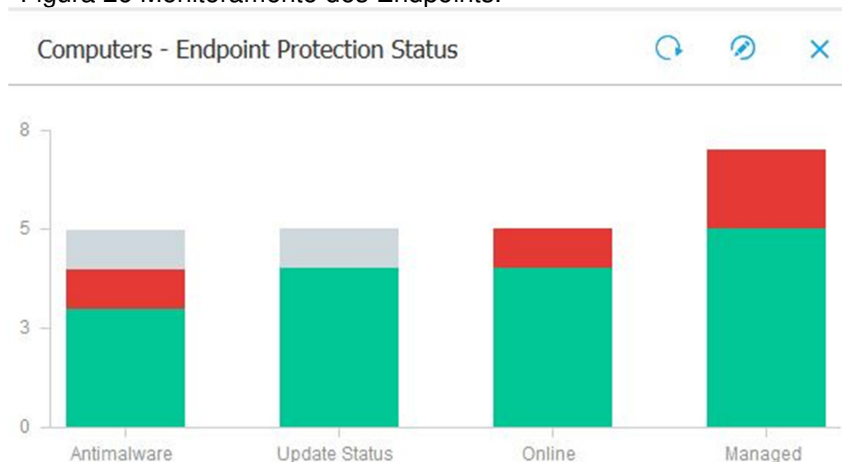
Figura 25 Monitoramento do SVA.



Fonte: Próprio autor

O console *control center* fornece informações sobre o status das VMs da rede como atividades *malware*, VM indisponível ou precisando de *upgrade*, informa também caso alguma VM esteja fora do gerenciamento conforme mostra a figura 26.

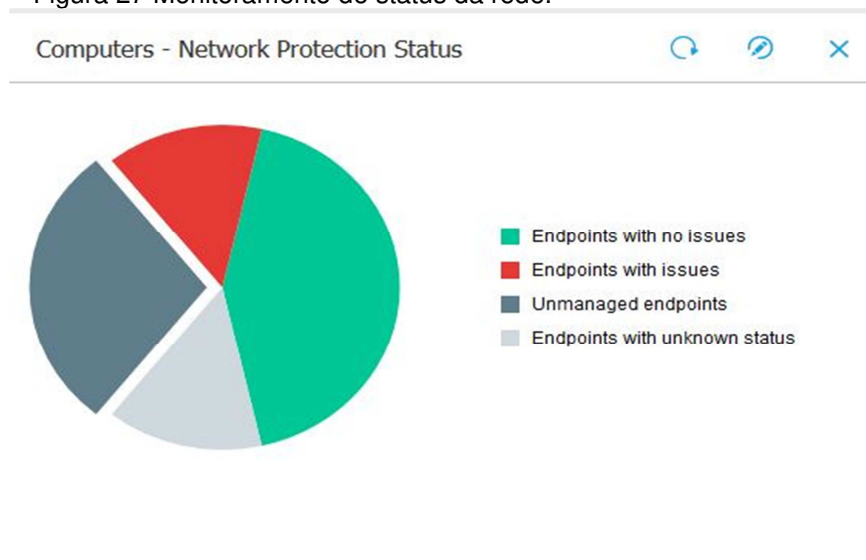
Figura 26 Monitoramento dos Endpoints.



Fonte: Próprio autor

No *control center* também é possível verificar o *status* da rede e ainda pode ser verificado um relatório no qual mostra os Endpoints que apresentam problemas, então, pode-se clicar sobre o gráfico para ver mais detalhes sobre a situação da VM e assim identificar e solucionar o incidente de segurança, conforme mostra a figura 27.

Figura 27 Monitoramento do status da rede.



Fonte: Próprio autor

A ferramenta proporciona uma série de serviços à rede sem a necessidade de executar nenhuma alteração das máquinas virtuais já em funcionamento no ambiente virtualizado da empresa, desta forma, a implementação pode ser feita em poucos minutos, não sendo necessário interromper as atividades da empresa.

6 CONSIDERAÇÕES FINAIS

Através desse trabalho observa-se que virtualização proporciona inúmeros benefícios a quem a utiliza e está se tornando uma tendência que aumenta cada vez mais dentro do ambiente corporativo.

Uma grande parte das empresas de pequeno porte apresentam dificuldades em lidar com novas tecnologias, pois, carece de grandes investimentos e de mão de obra altamente qualificada e, portanto, não consegue implantar esses recursos tecnológicos, estes ficam restritos às grandes empresas.

A plataforma de virtualização VMware ESXi por ser gratuita e apresentar um bom desempenho, uma vez que se trata de uma virtualização de pequeno porte, mostrou-se uma boa opção para a implantação da solução proposta, apresentando um excelente desempenho em ambientes com poucas máquinas virtualizadas e com sistemas operacionais heterogêneos. A plataforma VMware ESXi, mostrou-se mais simples de ser configurada do que o Microsoft hyper-v e do XenServer.

Os benefícios proporcionados pela solução apresentada neste trabalho são de grande valia na proteção de ambientes virtualizados e oferecem recursos de alto nível operacional sem a necessidade de possuir uma grande infraestrutura de TI, além do que, os serviços podem ser ampliados conforme a necessidade da empresa através da aquisição de novos módulos de proteção.

Observa-se que o console de gerenciamento demora alguns minutos para perceber uma VM off-line e que o primeiro escaneamento é mais demorado, porém, os próximos escaneamentos, devido ao compartilhamento do cache, são bem mais rápidos e não chega a afetar muito o desempenho da rede.

Através de uma análise da solução proposta por este trabalho conclui-se que os resultados apresentados são interessantes e atende as necessidades básicas de segurança da informação de uma boa parte das pequenas empresas, além do que, o custo da licença por Endpoint diminui conforme o número de máquinas aumenta.

Vale lembrar que não é necessário a implantação de nenhum serviço ou configurações nas máquinas virtuais em uso na rede para a obtenção destes recursos, uma vez que seria preciso instalar vários serviços de segurança, o que poderia acarretar em uma perda de desempenho ou até mesmo uma configuração inadequada do ambiente.

REFERÊNCIAS

ABNT. **NBR ISO/ IEC 27002 Tecnologia da informação – Técnicas de segurança – código de prática para a gestão da segurança da informação**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

ASSOLINI, Fabio. **Ameaças a ambiente virtualizados**. 31 Out. 2012. Disponível em: <<http://brazil.kaspersky.com/sobre-a-kaspersky/centro-de-imprensa/blog-da-kaspersky/2012/ameacas-virtualizadas>>. Acesso em: 18 Out. 2016.

BITDEFENDER. **FAQ do bitdefender gravityzone**. 201?. Disponível em :<<http://www.bitdefender.com.br/business/virtualization-security.html>>. Acesso em: 04 Out. 2016.

BITDEFENDER. **O Security for virtualized environments**. 201?. Disponível em: <<http://www.bitdefender.com.br/business/virtualization-security.html#n>>. Acesso em: 27 Out 2016.

BOSING, Angela; KAUFMANN, Evelacio Roque. **Virtualização de servidores e desktops**. Joaçaba, SC: Editora Unoesc, 2012. Disponível em <:<http://editora.unoesc.edu.br/index.php/acet/article/view/1483/pdf>>. Acesso em: 20 maio 2016.

CARISSIMI, Alexandre S.; OLIVEIRA, Rômulo S.; TOSCANI, Simão S. **Sistemas operacionais**. 4ª Edição. São Paulo: Editora Bookman, 2010.

CARISSIMI, Alexandre. Virtualização: da teoria a soluções. In: **SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUIDOS**, 26. 2008, Rio de Janeiro. Anais. Rio de Janeiro, 2008. Capítulo 4. Disponível em: <<http://www.gta.ufrj.br/ensino/CPE758/artigos-basicos/cap4-v2.pdf>>. Acesso em: 10 Abr. 2016.

CERT.BR. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Cartilha de segurança 2012. Disponível em: <<http://www.cgi.br/media/docs/publicacoes/1/cartilha-seguranca-internet.pdf>> Acesso em 3 Out. 2016.

COELHO, Paulo. **A virtualização e suas vantagens**. Oficina da Net, 13 maio, 2009. Disponível:<http://www.oficinadanet.com.br/artigo/1674/a_virtualizacao_e_suas_vantagens.com>. Acesso em: 1 Abr. 2016.

Computer. **O que é o Endpoint Protection**. (CARISSIMI, OLIVEIRA, & TOSCANI, 2010) Disponível em: <<http://ptcomputador.com/Software/antivirus-software/100945.html#.WBiRWcmaXVI>>. Acesso em: 01 Nov. 2016.

DEVEL. **Virtualização de servidores: vantagens e desvantagens**. 201?. Disponível em: <<http://www.develsistemas.com.br/virtualizacao-de-servidores-vantagens-e-desvantagens/>>. Acesso em 03 Mai. 2016.

FAGUNDES, Antoniel N.C; VICENTE, Jonatas R; PRATES Lorryanne M.

Virtualização de hardware. 2015. Disponível

em:<http://www.sr.ifes.edu.br/~eduardomax/arquivos/artigos_2015/Virtualizacao_de_Hardware_IN1.pdf>. Acesso em 1 mai. 2016.

FONTES; Edison Luiz Gonçalves. **Praticando a segurança da informação.** Rio de Janeiro: Editora Brasport, 2008.

LAUREANO, Marcos. **Máquinas virtuais e emuladores: conceitos, técnicas e aplicações.** São Paulo: Editora Novatec, 2006. Disponível em:<http://www.mlaureano.org/aulas_material/so/livro_vm_laureano.pdf> Acesso em 01/04/2016.

LAUREANO, Marcos Aurelio Pchek; MAZIERO, Carlos Alberto. Cap. 4, 13 Jul. 2014. Artigo. Disponível em: <https://www.researchgate.net/publication/237681120_Virtualizacao_Conceitos_e_Aplicacoes_em_Seguranca>. Acesso em: 20 Abr. 2016.

LAUDON, C. Kenneth; LAUDON, P. Jane. **Sistemas de informação gerenciais.** 5ª Edição. São Paulo, Editora Pearson, 2006.

MACAGNANI, Bruno. **Ferramentas de virtualização.** 13 Mai. 2009. Disponível em: <<http://www.guiadohardware.net/artigos/ferramentas-virtualizacao/>>. Acesso em: 21 Mai. 2016.

MATTOS, Diogo Menezes Ferrazani. **Virtualização total e para-virtualização.** 05 jun. 2008. Disponível em:<http://www.gta.ufrj.br/grad/08_1/virtual/Virtualizaototalepara-virtualizacao.html>. Acesso em: 1 Mai. 2016.

MORIMOTO, Rand, GUILLET, Jeff. **Windows Server 2008 Hyper-V Unleashed.** Sams Publishing, 2009. Centrix Disponível em : <www.cnpms.embrapa.br/downloads/xen/Tutorial_XenServer6.docx>. Acesso em Mai. 2016.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. **Segurança de redes:** em ambientes cooperativos. 2. ed. São Paulo: Futura, 2003.

Network World. **Virtualização:** segurança é o calcanhar-de-aquiles. Revista publicado em: 29 Nov. 2007. Disponível em: <<http://computerworld.com.br/seguranca/2007/11/29/idgnoticia.2007-11-28.9921851123>>. Acesso em 30 Out. 2016.

PAULO, Vilela. **Virtualização de aplicações.** 5ª Edição. Disponível em :<<http://pt.slideshare.net/adorepump/virtualizacao-de-aplicacoes-presentation>>. Acesso em 13 Abr. 2016.

Pulse, Ti. **Virtualização.** 201? Disponível em :<<http://www.pulseti.com.br/virtualizacao.html>>. Acesso em 13 Abr. 2016

ROSE, Mike. **vShield Endpoint**: revolucione o modo como protege seu ambiente virtual. VMware INC, 24 Abr. 2013. Disponível em: <<https://blogs.vmware.com/brasil/2013/04/vshield-endpoint-revolucione-seu-ambiente-virtual.html>>. Acesso em: 10 Set 2016.

STAIR, Ralph; REYNOLDS, George. Princípios de sistemas de informação. 9ª Edição. São Paulo: Editora Cengage Learning, 2011.

SILVA R.F. **Virtualização de sistemas operacionais**. Monografia (Graduação em tecnologia da Informação e Comunicação), Instituto Superior de Tecnologia em Ciências da Computação, Petrópolis, 2007. Disponível em:<http://thiagocavalcante.googlepages.com/Artigo_Virtualizacao.pdf>. Acesso em 10 Mai. 2016.

TANENBAUM, Andrew S. **Redes de Computadores**. 7ª Edição. Tradução: Vanderberg D. Souza. Rio de Janeiro, Elsevier, 2003.

Universidade Federal do Rio de Janeiro. Disponível em: <http://www.gta.ufrj.br/grad/09_1/versao-final/virtualizacao/virtualizacao%20em%20ambientes%20de%20redes.html>. Acesso em: 03 Abr. 2016.

VMWARE. **Virtualization for desktop & server, application, public & hybrid clouds**, 2014. Disponível em:< <http://www.vmware.com/>>. Acesso em 29 Mai. 2016.

VMWARE, INC. Folheto. **VMware ESX e VMware ESXi**. 2009 Disponível em: <https://www.vmware.com/files/br/pdf/products/VMW_09Q1_BRO_ESX_ESXi_BR_A4_P6_R2.pdf>. Acesso em 03 Mai. 2016.

VMWARE, INC.; **VMware documentation**. 201?. Disponível em:<<http://www.vmware.com/support/pubs/>>. Acesso em: 20 Abr. 2016.