FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Paulo Henrique Tadei

SEGURANÇA DA INFORMAÇÃO COM FOCO EM APLICAÇÕES VIRTUALIZADAS

Americana, SP

2016

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Paulo Henrique Tadei

SEGURANÇA DA INFORMAÇÃO COM FOCO EM APLICAÇÕES VIRTUALIZADAS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Segurança da Informação, sob a orientação do Professor Esp. Edson Roberto Gaseta

Americana, S. P.

2016

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

T128s	Tadei, Paulo Henrique Segurança da Informação com foco em aplicações virtualizadas. / Paulo Henrique Tadei. – Americana: 2016. 34f. Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza. Orientador: Prof. Edson Roberto Gaseta 1.Segurança em sistemas de informação I. Gaseta, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana. CDU: 681.518.5

Paulo Henrique Tadei

SEGURANÇA DA INFORMAÇÃO COM FOCO EM APLICAÇÕES VIRTUALIZADAS

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, 22 de junho de 2016.

Banca Examinadora:

Edson Roberto Gaseta
Especialista
CEETEPS – Faculdade de Tecnologia de Americana.

Antônio Alfredo Lacerda
Especialista
CEETEPS – Faculdade de Tecnologia de Americana

Kléber de Oliveira Andrade
Mestre
CEETEPS – Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus por me presentear com o dom da vida.

Gostaria de agradecer aos meus pais por incentivarem meus estudos e me darem o suporte sempre que necessário, me fortalecendo para enfrentar não só a graduação, mas também a vida.

A todos os funcionários da FATEC Americana que trabalham com o intuito de proporcionar o ambiente mais agradável possível para nós alunos.

Aos docentes da FATEC Americana que trabalham todos os dias semeando seus conhecimentos e se preocupando com seus alunos.

Ao querido Professor Especialista Edson Roberto Gaseta, pelo suporte prestado, pela orientação fornecida e por todos os conselhos que obtive no desenvolvimento deste projeto.

A querida Professora Mestre Maria Cristina Luz Fraga Moreira Aranha, pelas sugestões, dedicação e dicas prestadas neste trabalho, que sem dúvidas foram essenciais.

A minha irmã Ana Paula Tadei Pinto de Oliveira e o seu esposo William Cesar Pinto de Oliveira, pelo carinho e atenção dedicados a mim no decorrer da vida.

Aos meus amigos adquiridos no decorrer dos anos estudando na FATEC, amigos que pretendo levar para a vida toda e que me fizeram aprender o significado de amizade verdadeira, em especial, aos amigos da republica do Bigode.

RESUMO

A Segurança da Informação é um assunto que vem crescendo e ganhando espaço cada vez mais nas organizações do Brasil e do mundo, com o crescimento dos usuários da internet e os diversos tipos de ataques direcionados a essas organizações é inevitável que ocorra o aumento das preocupações com as informações que circulam nas redes das mesmas, ainda mais quando muitas destas informações são capazes de interferir até mesmo no preço das ações corporativas.
Este trabalho tem por finalidade apresentar os conceitos de Segurança da Informação aplicados a um ambiente virtualizado, mostrando diversas formas de virtualização e por final um estudo de caso que demonstra mais segurança na execução de sistemas que possuem informações privilegiadas, mostrando que as atividades desenvolvidas com mais segurança possuem diversas vantagens para o negócio quando utilizada de forma correta, diminuindo os riscos e contribuindo para a redução dos custos da organização. Será citado no decorrer do trabalho diversas situações onde serão utilizados os pilares da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade) como base para o replanejamento e melhoria do ambiente utilizado, tornando assim, o ambiente mais seguro, robusto e disponível.

Palavras Chave: Segurança da Informação; Virtualização de Aplicativos; Redução de Custos.

ABSTRACT

The Information Security is one subject that is increasing and getting more and more space in organizations of the Brazil and world, with the increase of the internet users and several kinds of attacks directed for it organizations is inevitable that happens the increase of the concerns with the information that keep rolling on the network of it organizations, especially when many of these information are able to interfere even in the price of corporate stocks. This study aims to present the Information Security concepts applied to a virtualized environment, showing several ways of virtualization and at the end, a case study showing more security on executing applications that have privileged information, showing that the applications developed with more security have many advantages for business when used correctly, reducing the risks and contributing to the reduction of the organization's costs. Will be cited in this study several situations where the pillars of the Information Security will be used (Confidentiality, Integrity and Availability) as the basis for the redesign and improvement of the environment used, making it the most secure, robust and available.

Keywords: *Information Security; Application Virtualization; Costs Reduction.*

SUMÁRIO

LISTA DE FIGURAS

1 INTRODUÇÃO

A Segurança da Informação tem como objetivo a proteção de um conjunto de informações, visando preservar o valor da mesma, independentemente se esse valor é significante para uma pessoa ou para uma organização. A Segurança da Informação possui algumas características, mais comumente chamadas de: Pilares da Segurança, entre eles estão: a confidencialidade, integridade e a disponibilidade. O conceito da Segurança da Informação não se aplica apenas aos meios eletrônicos, ele se estende também a qualquer tipo de segurança física, por exemplo, onde haja um objetivo comum, o da proteção dos dados e das informações.

O propósito deste projeto é relatar a melhoria realizada nos sistemas de uma empresa multinacional situada na região de Piracicaba, onde foi realizado uma alteração na maneira em que a aplicação era acessada, permitindo aumentar os padrões de segurança e integridade dos dados neles contidos, afinal as informações fazem parte dos principais bens da empresa.

A empresa com base em melhorar o desempenho das suas aplicações e baixar o custo de mantê-las nos servidores brasileiros, decidiu mudar a forma com que as aplicações eram acessadas, migrando os servidores para os Estados Unidos, com isso, apesar de atingir o objetivo de redução de custo, surgiram novos problemas graves em relação a segurança dos aplicativos.

Nessa perspectiva buscou-se respostas à seguinte questão de pesquisa: **Qual seria a melhor forma de impedir que usuários pudessem acessar a aplicação sem possuir qualquer tipo de cadastro na mesma?**

A segurança da informação é importante nas empresas, pois é a partir da informação, por exemplo, que surgem novos projetos e negócios os quais lhes trarão lucros, sendo que as informações não sendo protegidas poderão cair em mãos erradas, podendo causar muitos prejuízos.

Com base nos problemas relatados, surgiu então a ideia de replicar a validação padrão da empresa para o acesso da Intranet, onde apenas funcionários possuem acesso nas aplicações no novo local e também adaptar um cadastro na

própria aplicação onde apenas usuários que realmente precisam do acesso seriam cadastrados.

O objetivo geral deste trabalho é identificar qual seria uma boa forma de impedir que usuários pudessem acessar a aplicação sem possuir qualquer tipo de cadastro na mesma.

Como objetivo específico, relatar melhorias realizadas no acesso aos sistemas de informação, garantindo mais na segurança alcançada após a alteração do método em que a aplicações eram acessadas.

2. PROCEDIMENTOS METODOLÓGICOS

2.1 Tipo de Metodologia

Neste projeto será inserida uma forma metodológica de estudo de caso, pois segundo FACHIN (2006) “No método do estudo de caso, leva-se em consideração, principalmente, a compreensão, como um todo, do assunto investigado. ”, como participei ativamente de projetos envolvendo segurança da informação implantados na empresa, tive a oportunidade de avaliar diversas situações onde havia-se falhas de segurança e no que essas falhas causariam caso não fossem solucionadas.

3 SEGURANÇA DA INFORMAÇÃO

O mundo é movido pela informação e assim consegue-se saber como tudo está caminhando. Segundo Fontes (2006) “[...] se prestarmos atenção, podemos identificar que somos o que somos porque transformamos informação em vida! ”. O autor alega ainda que “Informação é muito mais que um conjunto de dados. Transformar esses dados em informação é transformar algo com pouco significado em um recurso de valor para a nossa vida pessoal ou profissional”.

Para proteger e gerenciar as informações de uma organização existem regulamentos como políticas, normas e regras a serem seguidas. Estes regulamentos têm como objetivo além de gerenciar as informações, fazer com que o negócio não seja prejudicado devido a um mau uso da informação, independentemente se foi causado por um erro ou acidentalmente. Sabendo da grande importância que a informação tem, importante garantir a sua segurança.

> “A segurança da Informação existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos de informação para o funcionamento da organização. Sem a informação ou com uma incorreta, o negócio pode ter perdas que comprometem o seu funcionamento e o retorno de investimentos dos acionistas” (FONTES, 2006).

Segurança é um assunto muito importante e discutido há décadas, levando em consideração a informação como um bem muito valioso, tendo então os seguintes pontos a serem garantidos e em qual a segurança é responsável, entre eles, segundo Lyra (2008, p. 03):

> “**Confidencialidade**: capacidade de um sistema de permitir que alguns usuários acessem determinadas informações ao mesmo tempo em que impede que outros, não autorizado, as vejam.
>
> **Integridade**: a informação deve estar correta, ser verdadeira e não estar corrompida.
>
> **Disponibilidade**: a informação deve estar disponível para todos que precisarem dela para a realização dos objetivos empresariais.
>
> Além destes três aspectos principais, temos:
>
> **Autenticação**: garantir que um usuário é de fato quem alega ser;

> **Não-repúdio**: capacidade do sistema de provar que um usuário executou uma determinada ação;
>
> **Legalidade**: garantir que o sistema esteja aderente à legislação pertinente;
>
> **Privacidade**: capacidade de um sistema manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações (por exemplo, o sistema de voto eletrônico);
>
> **Auditoria**: capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataques"

Qualquer evento, seja ele físico ou ambiental, que possa intervir em alguns dos aspectos relacionados à segurança da informação pode ser considerado um incidente de segurança, pois podem afetar a disponibilidade e a integridade da informação. Outros aspectos que podem influenciar na Segurança da Informação são os ataques ou operações incorretas.

Lyra (2008, p. 05) afirma que:

> "A informação é um bem de grande valor para processos de negócios da organização, mas também devemos considerar a tecnologia, o meio que a suporá, que a mantém e que permite que ela exista, as pessoas que a manipulam e o ambiente onde ela está inserida. Assim podemos descrever que ativo da informação é composto pela informação e tudo aquilo que suporta ou se utiliza dela"

Segundo Lyra (2008) "Um tipo de incidente de segurança é caracterizado pela existência de um agente que busca obter algum tipo de retorno, atingindo algum ativo de valor". O autor ainda alega que "Os ativos de informação possuem vulnerabilidade ou fraquezas que podem gerar, intencionalmente ou não, a indisponibilidade, a quebra de confidencialidade ou integridade. A vulnerabilidade de um ativo é o seu ponto fraco.

Essas vulnerabilidades poderão ser exploradas ou não, sendo possível, que um ativo da informação apresente um ponto fraco que nunca será efetivamente explorado".

Lyra (2008) entende por ameaça um potencial ataque a ativos da informação. É considerado como um agente externo que, aproveitando-se da vulnerabilidade, poderá quebrar um ou mais dos três pilares da segurança da informação.

Probabilidade para Lyra (2008) “É a chance de uma falha de segurança ocorrer levando-se em conta as vulnerabilidades do ativo e as ameaças que venham a explorar esta vulnerabilidade. ”

O autor ainda diz que podem-se ter um ativo com várias vulnerabilidades, mas sem ameaças de ataque, o que leva a uma probabilidade próxima de zero. O impacto de um incidente de segurança é medido pelas consequências que ele possa gerar aos processos do negócio suportados pelos ativos. Lyra (2008).

“Os ativos possuem valores diferentes, pois suportam informações com relevâncias diferentes para o negócio da organização. Quanto maior for o valor do ativo, maior será o impacto de um eventual incidente que possa ocorrer”. Lyra (2008).

É possível perceber que os ativos de informação possuem vulnerabilidades e estas vulnerabilidades podem ser exploradas por ameaças, quando isso acontece, origina-se então um incidente de segurança. As ameaças e as vulnerabilidades podem ser medidas para se ter uma noção da probabilidade e do impacto caso um incidente venha acontecer.

Como uma ameaça é um fator externo, não se tem o controle sobre ela, segundo Lyra (2008):

> “Por originar-se em um agente externo, não temos controle sobre as ameaças e, portanto, não podemos agir preventivamente sobre elas. Já as vulnerabilidades estão sob o contexto da nossa gestão, e é necessário concentrar esforços na diminuição das mesmas para mitigar o risco”.

A Segurança da Informação está diretamente ligada à proteção dos dados e recursos da empresa, pois esses dados são mais do que um conjunto de informações, entre elas, confidencias comerciais, projetos inovadores e informações pessoais de fornecedores e funcionários.

A Segurança da Informação nas empresas apesar de ser uma das coisas mais importantes, nem sempre é um assunto levado a sério. Sempre que a empresa necessita de algum investimento na área de TI (Tecnologia da Informação) surge um grande problema a ser discutido entre o técnico da área e o executivo, segundo Dawel (2005) “O técnico analisa a solução do problema, seleciona alguns produtos

e serviços, analisa-os técnica e economicamente e propõe o mais barato, desde que cumpridos os pré-requisitos técnicos", já o executivo "[...] tem outro ponto de vista e já está cansado de ouvir técnicos falando em custo-benefício e em retorno sobre o investimento", sendo assim surgem os primeiros problemas relacionados à área.

Contudo a segurança da informação não está somente ligada à tecnologia de ponta envolvendo equipamentos de última geração e profissionais altamente qualificados, tudo isso ajuda, porém não é o suficiente. As ameaças externas são perigosas, mas os técnicos também precisam ficar atentos às ameaças internas, como os próprios funcionários, segundo Dawel (2005, p. 59):

> "Em 1983, Richard Hollinger e John Clark pesquisaram 9.175 empregados em três diferentes segmentos da indústria. Mais de dois terços dos respondentes admitiram comportamentos contraproducentes de alguma forma, enquanto aproximadamente um terço admitiu que roubaram coisas que pertenciam à companhia, tais como suprimentos ou mercadorias no trabalho"

Com isso, consegue-se perceber que a confidencialidade é um assunto sério para as empresas e que ela necessita de uma atenção especial. Muitos processos requerem sigilo de informação, principalmente quando está relacionado à novas tecnologias, estratégias e mercadorias que estão em fase de desenvolvimento e que por um descuido pode acabar com o sucesso da empresa.

A tecnologia se desenvolveu de uma certa maneira que dificulta o monitoramento e a auditoria da segurança da informação, por exemplo, possuem-se mecanismos para evitar que o usuário tire *screen shots* de projetos, mas nada impede do usuário tirar o seu *smartphone* do bolso e fotografar a tela do computador, feito isso, em poucos segundos a imagem já pode estar rodando a quilômetros de distância. Nada adianta criar formas e mecanismos digitais de proteção à informação se o proprietário da informação não contribuir para o sigilo da mesma.

A confidencialidade é aquilo que se pretende atingir quando se trata de algo como uma informação que apenas pessoas autorizadas podem ter acesso. Este conceito é o mais importante dos três pilares pois está relacionado a segredo e curiosidade, o que mais desperta interesse no ser humano. Em um mundo corporativo este também é um conceito importante pois se trata de proteger propriedade intelectual e segredos de negócio que geram vantagens competitivas.

As empresas investem no conhecimento do funcionário quando o assunto é criação de novas tecnologias, o que demanda tempo e dinheiro, porem todo esse tempo gasto no futuro será recuperado caso as ideias se transformem em sucesso, porem o vazamento destas informações possibilita os concorrentes a obterem o sucesso do projeto, porém, sem o tempo e o dinheiro investido para a criação da ideia, ou seja, possibilitando que o sucesso do concorrente seja ainda mais vantajoso.

Segundo Fontes (2006) ”Quando o vazamento acontece, estabelece-se uma corrida injusta em que a empresa vai a pé e o concorrente de helicóptero, o que me faz pensar que é bem melhor e sai bem mais barato investir para preservar a confidencialidade do que entregar de bandeja para o concorrente todo o investimento feito na inteligência do negócio”.

4 VIRTUALIZAÇÃO

A primeira Virtualização produzida na história foi chamada de VM / 370 na década de 1970 produzida por uma equipe de programadores da IBM em Armonk.

Segundo Veras (2009), o marco inicial da virtualização surgiu em 1998 com a VMware, criada por Diana Greene e Mendel Rosenblun. Já existia uma empresa desde 1996 que era a CONNECTIX que foi fundada em 1988, mas essa tratava de virtualização para ambiente Mac.

Essa técnica de virtualização sempre atendeu a demanda de TI por se tratar de maximizar o uso de um servidor físico. A virtualização faz com que o dia-a-dia dos serviços de TI fiquem mais seguros e disponíveis, pois se um sistema operacional de um servidor físico que suporta diversas aplicações precisar ser atualizado, todos os serviços desse servidor, vão ficar indisponíveis durante o processo, o que não precisa ser feito, por exemplo, quando se utiliza a virtualização. Esse é apenas um dos diversos benefícios que citarei no decorrer do estudo.

Desde o momento da criação da virtualização até o presente, essa tecnologia vem se desenvolvimento muito. O que para o caso dos servidores com arquitetura x86 foi muito importante pois “[...] ajudaram a justificar o uso e permitiram melhorar o *TCO*[1] e o nível de serviços fornecidos pelos componentes do datacenter virtualizado. ” (Veras, 2009, p. 198)

Uma outra parte da história que contribuiu para o desenvolvimento, crescimento e utilização da virtualização nas empresas, foi o fato de que ela também traria redução de custo, devido a menor necessidade de utilização de muitos hardwares. “O fato de otimizar o uso de recursos promove a economia de energia e refrigeração, pois sabe-se que um servidor à plena carga e um servidor sem carga consomem energia de maneira muito próxima. ” (Veras, 2009, p. 198)

---

[1] Análise de custo do ciclo de vida.

4.1 INTRODUÇÃO A VIRTUALIZAÇÃO

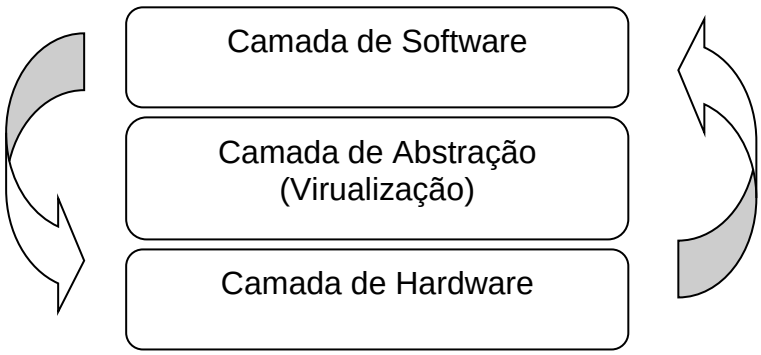
Existem diversas formas de se aplicar a virtualização, “[...] A virtualização pode ser aplicada a computadores, sistemas operacionais, dispositivos de armazenamento, aplicativos ou redes. No entanto, a virtualização de servidor é a principal. ” (VMware, 2016)

Ainda de acordo com o autor, as empresas em geral, que possuem uma área de TI, possuem o desafio de trabalhar com os servidores atuais, que são projetados para utilizar um sistema operacional e executar um aplicativo de cada vez. Com isso, até mesmo para manter um data center com serviços básicos são necessários diversos servidores, o grande problema é que, muitas vezes, eles não rodam nem com 30% de sua capacidade.

Para contribuir com economias de escala e uma maior eficiência no serviço, o autor VMware (2016) diz que a virtualização usa software para simular a existência de hardware e criar um sistema de computadores virtual. Com isso, as empresas podem executar mais de um sistema virtual, e vários sistemas operacionais e aplicativos, em um único servidor.

Uma maneira mais fácil de se entender a virtualização é entende-la como uma camada entre o hardware e o software, “A virtualização permite que a camada de software (aplicações e sistema operacional) seja isolada da camada de hardware[...]. ” Conforme a Figura 1.

Figura 1 – Camadas de Virtualização



Fonte: Autoria Própria.

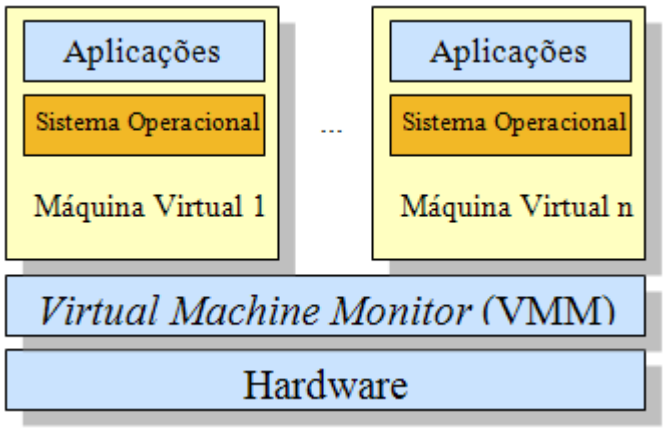
4.2 CONCEITO

O conceito de virtualização é muito interessante, pois ele veio para resolver o problema de falta de recurso nas empresas, o que gera custo. Diversos processos precisam ser executados para que um datacenter agregue valor dentro da empresa, mas para isso, são necessários recursos físicos e com a virtualização essa necessidade diminui.

Segundo Veras (2012) a virtualização simplifica o gerenciamento, torna flexível e amplia o poder de processamento. O autor ainda conclui que “Funcionalidades contidas nos softwares de virtualização também permitem melhorar a disponibilidade e a recuperação de desastres de ambientes de TI de uma maneira mais simples e com menor custo quando comparado a formas tradicionais. ” (Veras, 2012, p.128)

A virtualização é implementada por um software gerenciável, este software faz com que a camada das aplicações, onde encontra-se os serviços e o sistema operacional, fique separada da camada de hardware, podendo assim, fazer com que seja possível ter diversos sistemas operacionais rodando diversos aplicativos simultaneamente sendo processados ao mesmo tempo e pelo mesmo hardware, acabando com o problema da necessidade de se ter diversos servidores físicos para realizar pequenas tarefas. A Figura 2 ilustra como funciona esse conceito de virtualização.

Figura 2 – Conceito de Virtualização



Fonte: http://www.itsbrasilonline.com.br/virtualizacao.htm (acessado em 25/04/2016)

“A camada de virtualização entrega para o sistema operacional convidado um conjunto de instruções de maquinas equivalentes ao processador físico. A camada de virtualização de servidores mais conhecida é o hypervisor [...]. ” (Veras, Manuel – 2012, p.129)

4.3 PRINCÍPIOS DE VIRTUALIZAÇÃO

Os princípios a seguir foram retirados do livro “The Book of Xen” dos Autores Chris Takemura e Luke S. Crawford.

Em primeiro lugar, podem-se mencionar que os computadores, mesmo os mais novos e rápidos com sistemas operacionais multitarefa modernos, realizam apenas uma instrução por tempo, "Mas, meu computador está executando muitas tarefas ao mesmo tempo, mesmo agora, eu posso ver um relógio correr, ouvir música tocando, baixar arquivos, e conversar com amigos, tudo ao mesmo tempo." E isso é verdade. No entanto, o que está realmente acontecendo é que o computador está fazendo a comutação entre estas diferentes tarefas tão rapidamente que os atrasos se tornam imperceptíveis. Assim como um filme é uma sucessão de imagens que dão a ilusão de movimento, um computador executa tarefas que são tão perfeitamente entrelaçadas que chegam a aparecer simultâneas.

Virtualização apenas estende essa metáfora um pouco. Esta multiplexação realiza-se sob a direção do sistema operacional, que atua para supervisionar tarefas e certificar-se de que cada um recebe parte do seu processo a tempo na CPU. Como o sistema operacional deve, portanto, agendar tarefas para serem executadas na CPU, este aspecto do sistema operacional é chamado de agendamento.

Há diversas maneiras e finalidades de se utilizar a virtualização, segundo (Veras, Manoel, 2012, p.200), alguns dos principais usos são:

> “Consolidar servidores com a execução de diversos aplicativos em um único servidor físico; Proteger a continuidade dos negócios a um custo adequado, utilizando recursos já incorporados ao produto de virtualização como a alta disponibilidade (HA); Simplificar os testes e o desenvolvimento de software com a utilização de um único servidor de teste e desenvolvimento para as diversas aplicações e sistemas operacionais; Proteger e gerenciar os desktops da empresa hospedando-os em máquinas virtuais acessadas por um *thin clientes* ou *desktops;* Re-hospedar as aplicações legadas transferindo

> sistemas operacionais antigos como o Windows NT para maquinas virtuais executadas em servidores novos. ”

4.4 VITUALIZAÇÃO ESTÁTICO

Os softwares de virtualização vêm em três partes. Em um extremo, você tem plena virtualização ou emulação, em que a máquina virtual é uma simulação de software, hardware de real ou ficcional, contanto que há um motorista, que não importa muito. Produtos nesta categoria incluem VMware[1] e QEMU[2] por exemplo.

Com a virtualização completa, um sistema operacional não modifica *hosts*, um programa de espaço do usuário que emula uma máquina na qual o sistema operacional "convidado" é executado. Esta é uma abordagem popular, porque ele não necessita que o sistema operacional convidado seja alterado de forma alguma. Tem também a vantagem de que a arquitetura pode ser completamente virtualizada.

No entanto, este nível de independência de hardware tem como custo uma enorme perda de velocidade, que será abordado futuramente.

VMware continua sendo o fornecedor mais conhecido de produtos full-virtualização, com um conjunto robusto de ferramentas, um amplo apoio, e uma marca forte. As versões recentes do VMware resolvem o problema de velocidade, executando instruções no lugar onde possível e dinamicamente traduzindo código quando necessário. Embora esta abordagem é elegante e não requer modificação do OS, não é tão rápido como Xen, tornando-o menos desejável para configurações de produção ou para um full-time ambiente de trabalho.

Segundo o autor (Veras, Manoel, 2012) os principais fornecedores de software de virtualização para servidores das empresas são a VMware, a Microsoft e a Citrix.

---

[1] Ferramenta de virtualização desenvolvida pela VmWare

[2] Ferramenta de virtualização desenvolvida por Fabrice Bellard

Para melhor entendimento, a ferramenta utilizada no estudo de caso será citada a seguir e o que será abordado foi retirado do artigo "*Citrix XenServer Industry-leading open source platform for cost-effective cloud, server and desktop virtualization.*" do site *https://www.citrix.com.br*.

- **CITRIX XEN**

Enquanto o mercado de virtualização de servidores tem amadurecido, a virtualização está sendo vista como uma continua inovação e impulso para o mercado, onde empresas e provedoras de serviços estão construindo *clouds* públicas e privadas

Citrix XenServer e Linux Foundation Xen Project™ alimentam muitas das maiores *clouds* do mundo e está se tornando de fato o padrão para infraestruturas *cloud.* Para atender a essas novas demandas, XenServer passou por uma modernização plataforma para escalabilidade horizontal máxima e aumentou desempenho, densidade, flexibilidade e disponibilidade de armazenamento.

4.5 VIRTUALIZAÇÃO DE SISTEMA OPERACIONAL

No outro extremo vem a virtualização de nível Sistema Operacional (SO), onde o que está sendo virtualizado é o ambiente de operação, em vez de toda a máquina.

Virtualização de SO assume a posição de que o sistema operacional já fornece, ou, pelo menos, pode ser feito para fornecer, isolamento suficiente para fazer tudo que um usuário normal da Máquina Virtual espera, instalar todo o sistema de software, atualizar as bibliotecas do sistema sem afetar o funcionamento do mesmo, e assim por diante.

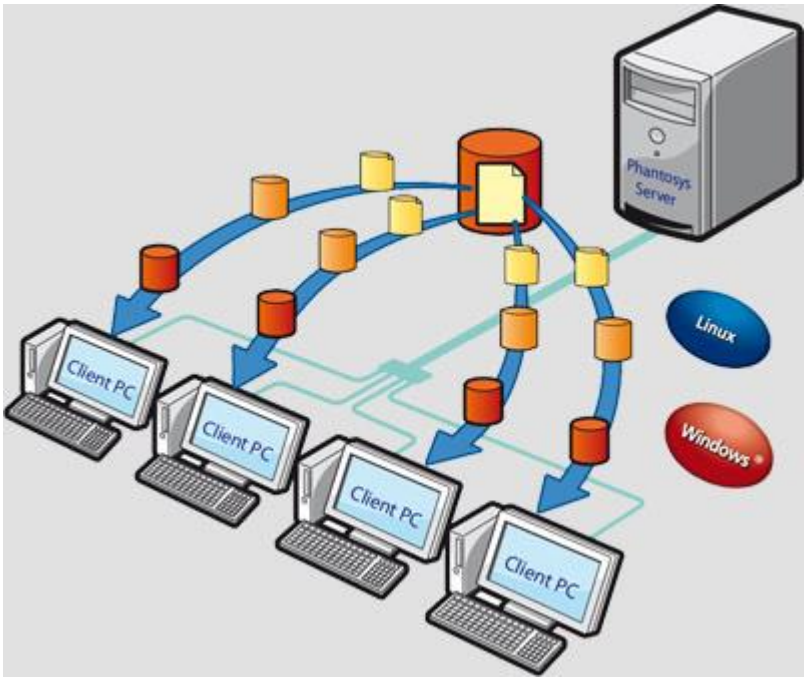
Assim, ao invés de emular hardware físico, virtualização de SO emula um espaço completo do usuário do SO usando recursos do sistema operacional. Jail FreeBSD e Solaris Containers são duas implementações populares de virtualização de nível SO. Ambos derivam do chroot clássico Unix Jail. A ideia é que o processo Jail só pode acessar partes do sistema de arquivos que residem em um diretório. Se instalar um sistema operacional em um diretório, ele pode ser considerado um ambiente virtual completo. Jail e Zones expandem no conceito de também restringir certas chamadas de sistema, fornecendo uma interface virtual de rede para melhorar

o isolamento entre as máquinas virtuais. Isso é útil, não é tão versátil como de um direito de máquina virtual seria. Uma vez que as Jails compartilham um núcleo, por exemplo, um kernel panic derrubaria todas as maquinas virtuais no hardware.

4.6 VIRTUALIZAÇÃO DE APLICATIVOS

A técnica de virtualização de aplicativos nada mais é do que deixar de instalar uma aplicação no desktop, adapta-la e instala-la em um servidor. Ao executar esta aplicação de um desktop, é gerada uma interface de comunicação com o servidor (geração de um aplicativo virtual) que compila e baixa informações especificas para o funcionamento da mesma, porém sem consumir tantos recursos de hardware do desktop pois afinal, a grande parte do processamento das atividades está sendo feita pelo servidor. A figura 3, ilustra uma virtualização onde 4 tipos de sistemas operacionais acessam aplicações ao mesmo tempo:

Figura 3 – Esquema de virtualização



Fonte: http://www.k-bit.de/schulloesungen/phantosys.php (acessado em 25/04/2016)

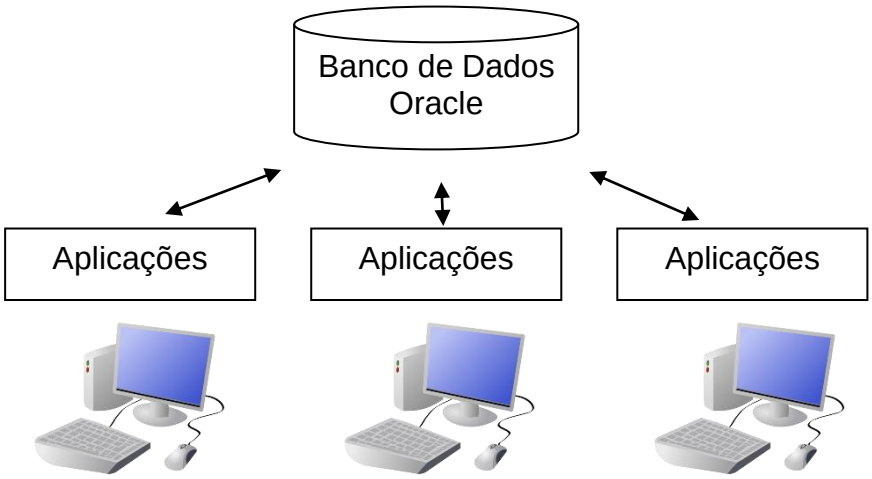
5 ESTUDO DE CASO

A empresa utilizada neste estudo de caso possuía sua matriz em Peória, uma cidade situada no estado americano de Illinois, no Condado de Peória, e possui uma filial em Piracicaba/SP, onde foram realizados os estudos.

A filial situada em Piracicaba/SP utilizava alguns servidores para suportar os sistemas que eram utilizados para desenvolver as atividades dos funcionários apenas do Brasil, esses servidores eram suportados pela equipe de Tecnologia da Informação (TI) local e ficava localizado dentro de uma área que possuía controle de acesso físico, refrigerada e monitorada por alguns responsáveis. Todo o suporte necessário para o funcionamento dos servidores era de responsabilidade da equipe de TI local: backups, atualizações de segurança, manutenções preventivas entre outros serviços necessários para o bom funcionamento dos equipamentos, o que envolvia um grande investimento para manter o funcionamento deste datacenter ativo.

Esse ambiente funcionava de maneira em que as aplicações eram instaladas nas maquinas dos usuários através de solicitações via Help-Desk e essas aplicações se conectavam com o banco de dados que ficava hospedado nos servidores da empresa (Cliente/Servidor), como na figura 4 para facilitar o entendimento:

Figura 4 – Esquema de Aplicação Cliente/Servidor



Fonte: Autoria Própria.

5.1 EQUIPAMENTOS

Para que existisse o funcionamento completo dos serviços era extremamente necessário que os Servidores que hospedavam os bancos de dados das diversas aplicações estivesse conectado e disponível e o usuário precisava de um terminal de conexão com a aplicação desejada instalada localmente, podendo esse terminal ser um Desktop ou mesmo um Notebook.

Esses desktops e Notebooks também eram suportados pelas equipes de Help-Desk nível 2 local, trabalhando com chamados e atendendo sempre que necessário, seja reparos físicos de hardware ou até mesmo de configurações. Também era solicitado para o Help-Desk os chamados de instalações dos aplicativos, que após passarem por uma avaliação de necessidade feita pelo superior imediato do funcionário e em seguida, aprovado, era encaminhado e dado continuidade no processo para os funcionários responsáveis.

5.2 AUTENTICAÇÃO DE ACESSO

Todos os sistemas do setor analisado utilizavam a mesma tecnologia de hospedagem de banco de dados e possuíam o mesmo padrão de acesso para os usuários.

Para se conectar aos sistemas era necessário o usuário solicitar uma aprovação do superior imediato, identificando a real necessidade do acesso e caso aprovado, era encaminhado a solicitação para o departamento de Help-Desk nível 2, que realizava a instalação do aplicativo na máquina local do usuário solicitante e em seguida, era encaminhado o chamado para a equipe de TI responsável pelo suporte do aplicativo que cadastravam o logon de rede do usuário na aplicação necessária.

Com isso, o usuário teria acesso livremente a aplicação desejada sem sequer nenhum acesso de usuário e senha, bastava apenas estar credenciado, conectado à rede (ativo) e autenticado pelos funcionários analistas responsáveis pela aplicação.

5.3 VULNERABILIDADES

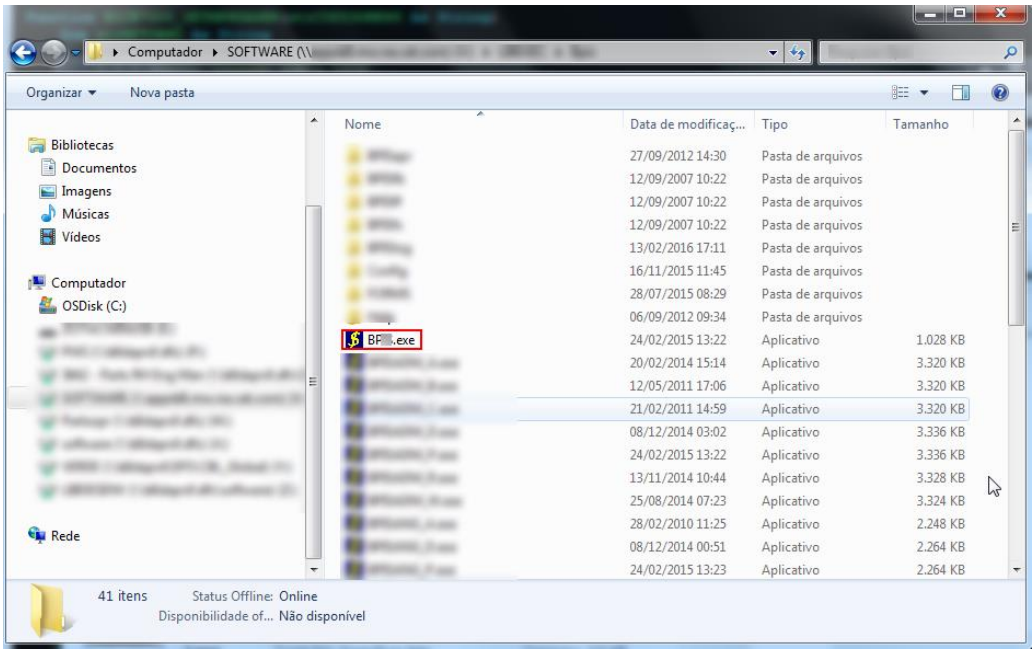
Neste cenário existiam muitas vulnerabilidades devido à falta de validação de usuário para utilizar a aplicação gerando uma perda de confidencialidade, um item

fundamental citado como um dos pilares da segurança da informação. A maioria dos sistemas possuíam informações fundamentais para a empresa como sistema de faturamento, sistema de entrada de pedidos e sistema de importação/exportação, ambos com informações diretamente relevantes para investidores e se utilizado por pessoas não autorizadas poderiam dar sequência à uma outra falha grave, a falta de integridade, pois a partir do momento em que o usuário mal intencionado tivesse acesso à aquelas informações, podendo altera-las e manipula-las, a integridade da mesma seria seriamente danificada, atingindo facilmente mais um pilar da segurança da informação.

Previamente o departamento de TI através da solicitação aprovada pelo superior imediato do usuário, cadastrava o logon de rede utilizado pelo usuário do sistema, porem nada impedia do usuário deixar o computador desbloqueado enquanto fosse ao banheiro fazendo com que facialmente qualquer outra pessoa poderia acessar as aplicações se passando pelo usuário autenticado.

Além disso, conforme vê-se na figura 5 a seguir, os módulos dos sistemas eram separados por arquivos executáveis, onde quem possuía acesso ao driver de rede onde eram hospedados esses arquivos, podiam acessa-los livremente e sem validação nenhuma, limitando acessos à algumas informações, porém ainda podendo visualizar outras informações relevantes para o negócio. Isso poderia acontecer por exemplo, com um funcionário que trabalhou em alguma área na qual possuía a necessidade de utilizar esses sistemas, porém foi transferido ou promovido e passou a não precisar mais do acesso. Este tipo de exemplo foi identificado diversas vezes durante o estudo onde nenhuma ação de bloqueio de atividade era documentada e exigida no processo, tornando o usuário que uma vez permitido, teria sempre permissão.

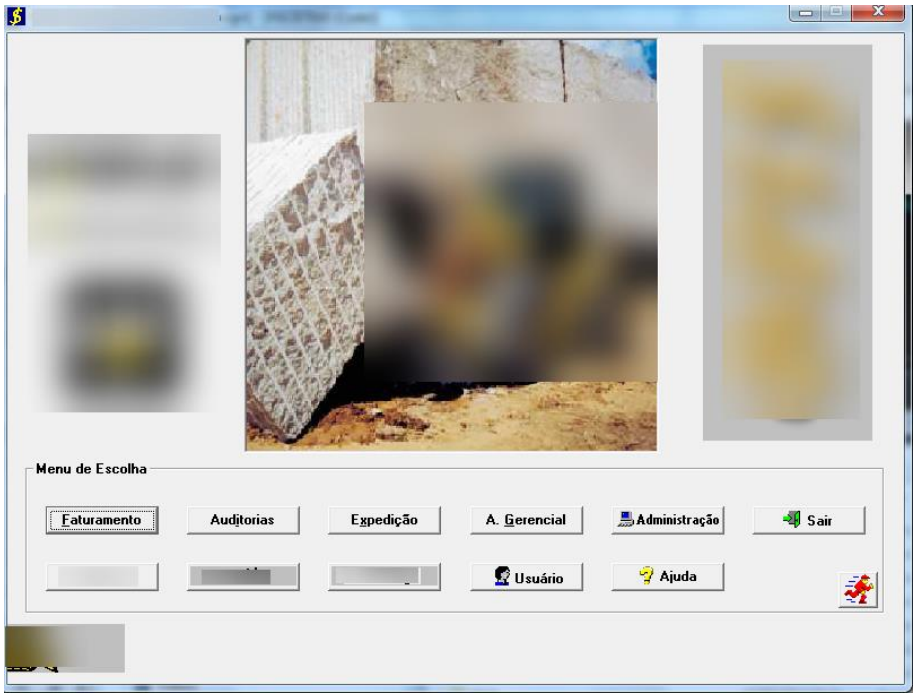
Figura 5 – Acessando o executável pela rede.



Fonte: Autoria própria.

E como pode-se ver na figura 6, bastava o usuário executar o aplicativo utilizando o clique duplo do mouse que o sistema abriria normalmente, com diversas informações relevantes para a empresa.

Figura 6 – Acesso à tela principal.



Fonte: Autoria própria.

5.4 MELHORIA IMPLEMENTADA

Com base em diminuir os custos financeiros da empresa e melhorar a segurança e o controle dos aplicativos, surgiu então o projeto de migrar os servidores brasileiros, os quais suportavam as aplicações utilizadas pelos próprios funcionários do Brasil, para a sede em Peória. Com isso algumas mudanças na maneira em que as aplicações funcionavam teriam que ser realizadas, entre elas, a mudança do ambiente de execução, que deixaria de ser realizado através da máquina local e passaria a ser utilizado através de um ambiente virtualizado, não por necessidade, mas sim por identificarmos uma oportunidade de melhoria de performance e segurança que já era seguida por outras filiais e que possuíam um histórico de sucesso.

Essas melhorias tiveram grande relevância para o negócio da empresa e seriam muito impactantes caso o *backout plan* não funcionasse como foi planejado, e então, ela foi dividida em duas etapas que serão abordadas a seguir.

5.5 PRIMEIRA ETAPA

A primeira etapa foi a mudança completa do ambiente de execução dos aplicativos, que foi deixado de ser instalado no desktop do usuário e passado a ser acessado através de um ambiente de virtualização de aplicativos, no caso, foi escolhido o ambiente CITRIX, o qual foi previamente citado no tópico sobre virtualização deste trabalho e que é uma ferramenta utilizada corporativamente pela empresa, que já possuía licença da mesma.

A mudança se constituía em desligar os servidores situados no Brasil, e migrar todos os serviços e processos vinculados às aplicações para a sede em Peória, onde ficavam localizados os servidores configurados para o ambiente de virtualização.

Esta mudança já havia sido realizada em ambiente de teste, onde nenhum usuário seria impactado, visando também servir de estudo para minimizar o risco de falhas em um ambiente de produção, no qual seria extremamente impactante e prejudicial para o negócio, nela, conseguimos identificar e mitigar futuros problemas que poderiam ocorrer na migração do ambiente de produção como algumas DLLs necessárias que não estivessem registradas no ambiente virtualizado e também

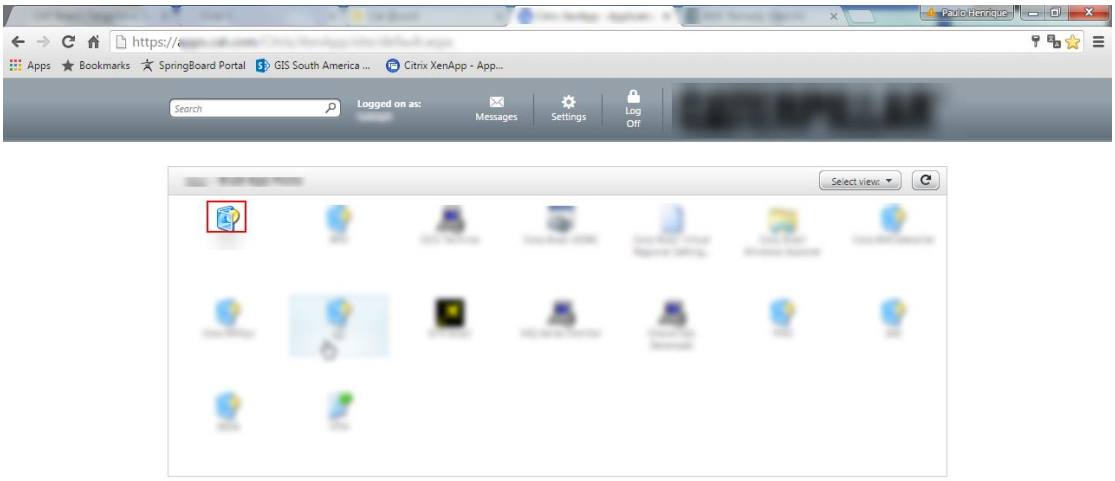
algumas consultas a banco de dados que precisariam ser melhoradas, visando aumentar a velocidade do acesso a informação. Este estudo juntamente com as melhorias durou aproximadamente 12 meses.

A mudança em ambiente de produção foi realizada durante um fim de semana devido à baixa utilização das ferramentas pelos funcionários nos quais foram previamente atualizados pelos seus gestores e através de e-mails que notificavam a indisponibilidade de todos os processos relacionados ao TI no período desta mudança, e não se tiveram muitas surpresas, devido ao estudo previamente realizado.

Após a migração ser realizada os usuários deixaram de acessar as aplicações que estavam instaladas nos seus desktops, pois as mesmas ficaram indisponíveis devido ao servidor não se encontrar mais no mesmo endereço e passaram a utilizar o ambiente virtualizado através do login e senha de rede utilizando um link divulgado previamente através do e-mail e o navegador padrão de internet como meio para acessar o link.

Pode-se ver na figura 7, o ambiente virtualizado é similar a um “Windows Explorer” no qual o usuário já estava acostumado a utilizar e não precisou de treinamento para passar a acessar os mesmos aplicativos, que não precisaram sofrer nenhuma grande mudança de funcionamento, através do novo ambiente CITRIX.

Figura 7 – Acesso ao sistema através do CITRIX.



Fonte: Autoria própria.

5.6 ACESSO AOS APLICATIVOS

Para não ser necessário solicitar acesso em todas as aplicações novamente, foi realizado uma seleção de todos os usuários ativos, setor por setor, e previamente criado grupos de administração no *Active Directory* e cada aplicação virtualizada passou a possuir como padrão de acesso apenas os usuários atribuídos a um grupo especifico para cada aplicação. Com isso, um usuário novo, para ter acesso necessitava ser incluído no novo grupo para poder visualizar a aplicação no seu portal do CITRIX, além de necessitar realizar a solicitação para a liberação de seu login para o acesso ao aplicativo desejado.

5.7 SEGUNDA ETAPA

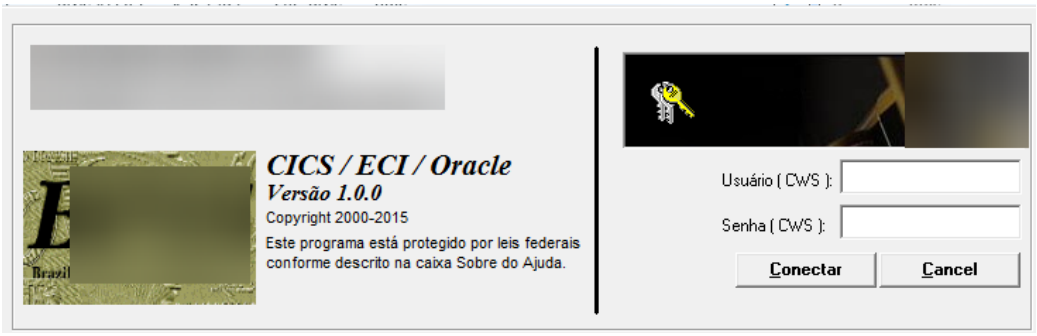
Após a implementação do novo ambiente e da migração dos nossos sistemas de informação, em uma de nossas reuniões semanais, foi detectado uma oportunidade de melhoria na segurança da informação dos aplicativos. Com o intuito de ter a segurança em primeiro lugar notou-se que a forma de validação em que o usuário utilizava, não estava nenhum pouco segura, com isso, chegou-se à conclusão de que o sistema precisava de uma atualização.

A empresa possui um meio de autenticação padrão utilizado para acessar os sistemas da Intranet como: dados cadastrais, consultas e relatórios de RH, atualização de currículos, agendamento de consultas e entre outras funcionalidades. Com o intuito de padronizar a autenticação, foi utilizado o mesmo padrão de validação da intranet, onde foi identificado mais aplicações que já utilizavam deste padrão, como o padrão para todas as aplicações virtualizadas.

Esse mecanismo de autenticação chama-se Global Directory, uma ferramenta padrão de validação de senhas, que com apenas algumas linhas de comando, passou-se a fazer parte também das aplicações virtualizadas, garantindo maior segurança no acesso dos funcionários nas mesmas.

Foi desenvolvido novos formulários de validação no sistema, utilizando a ferramenta Visual Basic 6, conforme figura 8, visando bloquear qualquer tipo de acesso de pessoas não autorizadas, lembrando que o padrão utilização do sistema continua sendo através do cadastro feito pelos administradores do sistema em si, onde não basta ter usuário e senha cadastrado no padrão da intranet, tem também que ser cadastrado previamente no menu da aplicação.

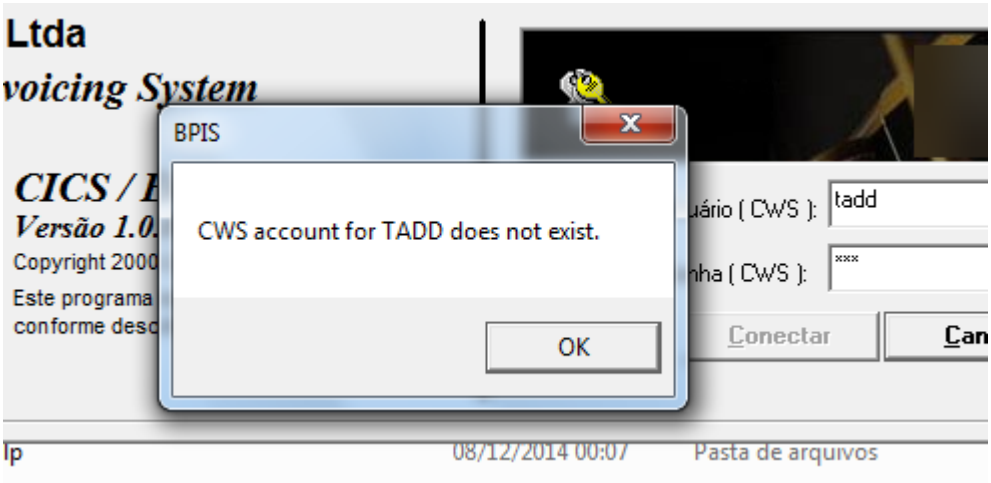
Figura 8 – Tela de Validação



Fonte: Autoria própria.

E se o usuário tentar se conectar sem possuir este padrão de login e senha, receberá a mensagem conforme figura 9.

Figura 9 Validação de usuário.

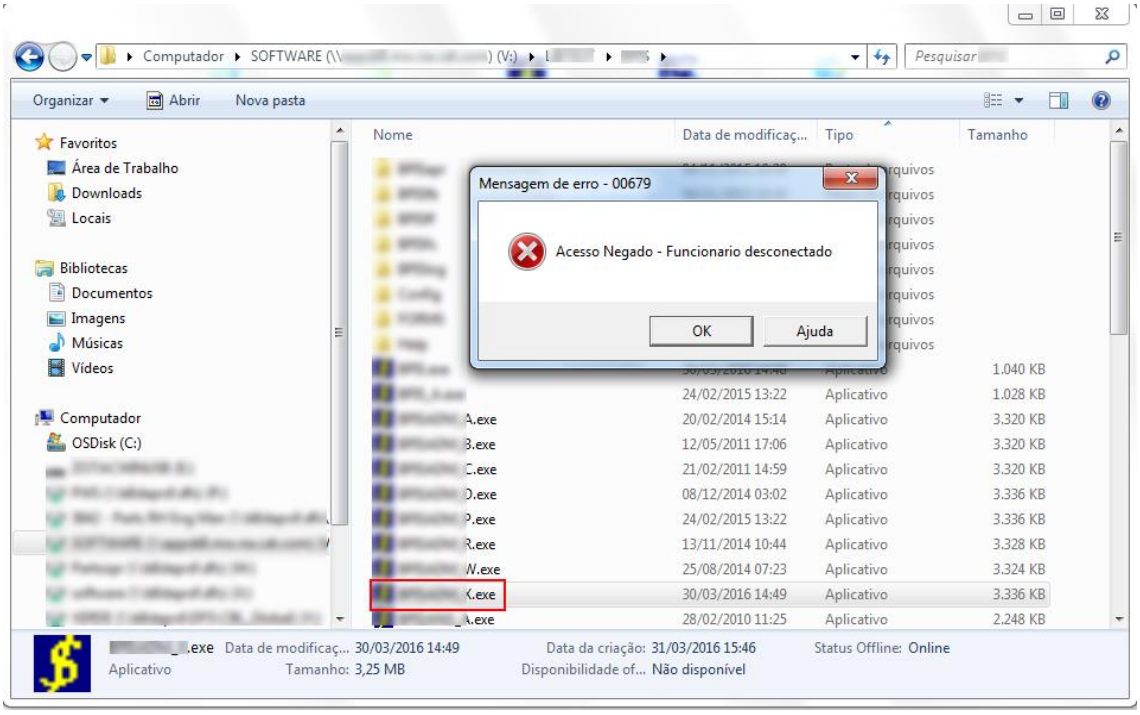


Fonte: Autoria própria.

Como os aplicativos são divididos em módulos e possuem uma segurança de maturidade baixa, visando atingir os objetivos de integridade e confidencialidade dos mesmos, manteve-se o padrão de separa-los por módulos, porem foi incrementado uma validação simples, porém eficaz onde em termos de programação, se o usuário não estiver solicitando o modulo desejado, através da tela principal, o programa

simplesmente não abre e além disso informa ao usuário uma mensagem, ilustrada na figura 10.

Figura 10 – Acesso fora da tela principal.



Fonte: Autoria própria.

6 CONSIDERAÇÕES FINAIS

Devido ao cenário econômico e político atual não estar tão favorável no Brasil, torna-se cada vez mais desafiador para as organizações encontrar novas formas de se destacar no mercado, maximizar os seus lucros e aumentar a qualidade nos seus produtos e serviços. E para o setor de Tecnologia da Informação, falar em mudanças e investimentos em um pleno período de austeridade está cada vez mais difícil, porém, pequenos investimentos, quando bem planejados, podem trazer inúmeras vantagens competitivas para uma organização, podendo até eliminar custos desnecessários sem que os usuários percebam grandes mudanças.

O estudo de caso mostra que é possível realizar grandes mudanças gerando pequenos impactos para os usuários finais e além disso, facilitar o acesso aos serviços que antes eram apenas utilizados em maquinas onde os sistemas estavam instalados, gerando sempre um desconforto caso fosse necessário realizar a troca do computador do usuário, tendo então que realizar todas as solicitações para a instalação dos sistemas novamente.

Consegue-se perceber que existiam muitas falhas de segurança da informação na estrutura antiga do nosso estudo de caso, porém com passos simples como o acréscimo de um formulário de validação de usuário e senha utilizando o *Global Directory* (ferramenta padrão já utilizada em outros aplicativos *Visual Basic 6* da empresa) obtêm-se um ganho significativo com relação integridade das informações, garantindo mais segurança e confiança nos dados exibidos para os usuários. Além disso, adicionando o procedimento via código nos executáveis dos sistemas, validando se o mesmo foi logado por um usuário através do menu principal ou não, garante uma segurança extra caso um invasor tente executar o aplicativo através da raiz do servidor e não possuir um usuário e senha valido.

Com base em todas as mudanças relatadas no ambiente, conclui-se que as qualidades dos serviços em termos de disponibilidade tiveram grande evolução devido a robustez que a ferramenta de virtualização nos proporciona e também pelo fato de que o grau de importância do servidor onde estão hospedados todos os serviços é muito maior do que antes, tendo em vista que não é mais só suportado os serviços do Brasil e sim de diversas outras localidades. Com isso, a política aplicada sobre este serviço é muito melhor avaliada e seguida, devido ao alto índice de criticidade. Portanto garante mais ainda ao usuário uma disponibilidade e

flexibilidade, podendo até, visando atender à necessidade do negócio, trabalhar remotamente numa eventual indisponibilidade causada por falta de energia por exemplo.

Pode-se analisar também que a integridade dos dados contidos nos sistemas teve um elevado padrão de segurança, onde foram acrescentadas diversas validações tornando ao mesmo tempo que seguro, prático para a utilização dos sistemas e para o administrador trabalhar com os usuários.

Vale ressaltar que a confidencialidade dos aplicativos cresceu juntamente com as novas formas de validação, pois, um sistema que garante maior segurança e dificulta a utilização de pessoas não autorizadas, automaticamente garante também maior confidencialidade, deixando o acesso às informações disponíveis apenas para quem realmente precisa delas.

7 REFERÊNCIAS BIBLIOGRÁFICAS

CITRIX. Dica de leitura. Disponível em: **<https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-xenserver-industry-leading-open-source-platform-for-cost-effective-cloud-server-and-desktop-virtualization.pdf>.** Acesso em: 10 de abr. 2016.

Dawel, George. **SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS**. Editora: Ciência Moderna Ltda. Rio de Janeiro. 2005.

Fachin, Odília. **FUNDAMENTOS DE METODOLOGIA**. 5 Ed., São Paulo, Editora: Saraiva 2006.

Fontes, Edison. **SEGURANÇA DA INFORMAÇÃO**. Editora: Saraiva, São Paulo. 2006.

Lyra, Maurício. **SEGURANÇA E AUDITORIA EM SISTEMAS DE INFORMAÇÃO**. Editora: Ciência Moderna Ltda. 2008.

Marconi, Marisa de Andrade. **TÉCNICAS DE PESQUISA**: Planejamento e Execução de Pesquisa, Amostragem e Técnicas de Pesquisa, Elaboração e Analise e Interpretação de Dados. Ed.: 2, Reimpr, São Paulo: Atlas, 2009.

Takemura , Chris and Crawford, Luke S. **THE BOOK OF XEN.** Editora: No Starch Press, Inc. 2010.

Veras, Manoel. **DATACENTER: COMPONENTE CENTRAL DA INFRAESTRUTURA DE TI**. Editora: Brasport. 2009.

Vmware. Dica de leitura. Disponível em: **< http://www.vmware.com/br/virtualization/how-it-works >**. Acesso em: 11 de abr. 2016.